

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم
الإستقرار المالي في البنوك الإلكترونية
(دراسة ميدانية)

دكتور محمد حارس محمد طه أبو الخير

مدرس المحاسبة والمراجعة

المعهد العالي للحاسبات والمعلومات وتكنولوجيا الإدارة بطنطا

2022

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

الملخص :

يهدف البحث إلى دراسة وإختبار أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية، ولتحقيق هدف البحث تم إجراء دراسة ميدانية على عينة من مسؤولي المراجعة الداخلية ، مسؤولي إدارة الإئتمان ، مسؤولي ادارة خدمة العملاء ، مسؤولي تكنولوجيا المعلومات ، مسؤولي إدارة المخاطر في البنوك الإلكترونية المقيدة بسوق المال المصري ، وقد توصلت الدراسة إلى مجموعة من النتائج النظرية والعملية لعل أهمها : التطور الحادث في المخاطر السيبرانية يحفز المنظمات المالية وخاصة البنوك الإلكترونية على البحث المستمر والمكثف نحو إتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك البنوك ، الأمر الذي يؤدي إلى دعم الإستقرار المالي في تلك البنوك .

وفي النهاية أوصت الدراسة بالعديد من التوصيات كان أهمها : العمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين بقطاع البنوك بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني .

الكلمات المفتاحية : جودة المراجعة الداخلية – الحد من مخاطر الأمن السيبراني – دعم الإستقرار المالي .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

Abstract :

The research aims to study and test the impact of internal audit quality in reducing cyber risks in order to support financial stability in electronic banks. The study found a set of theoretical and practical results, perhaps the most important of which are: The development in cyber risks motivates financial institutions, especially electronic banks, to continuously and intensively search towards taking preventive measures against these risks through regulations that make these procedures clearer before the boards of directors. The managements of those banks, which leads to support the financial stability of those banks.

In the end, the study recommended several recommendations, the most important of which were: Working to intensify awareness of customers through audio-visual programs and educational seminars to raise the level of cybersecurity culture among customers in the banking sector in order to understand the controls and instructions related to the security of information systems and cyberspace.

Keywords: Internal Audit Quality - Reducing Cyber Security Risks - Support Financial Stability.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

المحور الأول : الإطار العام للبحث .

1/1 مقدمة :

أدت زيادة الأنشطة الافتراضية للإدارة والنمو السريع للإنترنت وضوابط البيانات الكبيرة ، إلى إحتياج أعضاء مجلس الإدارة في بعض المنظمات إلى فهم واضح لتعرض المنظمة للمخاطر السيبرانية التي حدثت ، ولكن في بعض الأحيان تكون الصورة غير واضحة في هذا الشأن ، لذلك تدعو المجالس ولجان المراجعة إلى الإحتكام لإدارة المراجعة الداخلية لتوفير الضمانات فيما يتعلق بإدارة المنظمة للمخاطر السيبرانية ، كما يحدد المراجع الداخلي أوجه القصور التنظيمية التي يمكن أن تعرض المنظمة للخطر ، وكذلك الضوابط الداخلية اللازمة للتخفيف منها أكثر من أي وقت مضى (Kahyaoglu & Caliyurt, 2018, P.368) لذلك زادت الحاجة إلى الإعتماد على المراجع الداخلي لأن الجهود الذي يقدمها كبير مسؤولي المعلومات وكبير مسؤولي التكنولوجيا وكبير مسؤولي أمن المعلومات قد لا تفي بإحتياجات مجالس الإدارة .

وفي هذا الإطار فإن التطور المستمر في وظيفة المراجعة الداخلية ودعم جودتها أصبح آلية فاعلة نحو المساهمات البناءة والداعمة لمعظم القضايا الإستراتيجية داخل المنظمة وخاصة فيما يتعلق بقضايا الأمن السيبراني ، ومما لا شك فيه أن المراجعة الداخلية بصفقتها أحد آليات الحوكمة وأحد دعائم القيمة المضافة للمنظمات ، الأمر الذي يترتب عليه أن تصبح تلك الوظيفة أحد العوامل القوية داخل المنظمات في دعم الإستقرار المالي والتشغيلي لها وخاصة المنظمات المالية وعلى رأسها البنوك (شحاتة ، 2020 ، ص ص 109 – 115 ، PWC, 2018) .

ومن ثم فإن هذا البحث يستهدف إستكشاف دور جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على دعم الإستقرار المالي في البنوك الإلكترونية المصرية ، وتحقيقاً لهدف البحث سوف يعتمد الباحث على المنهج التحليلي لأهم الإصدارات المهنية والدراسات ذات الصلة بموضوع البحث ، وإختبار فروض البحث من خلال دراسة ميدانية سوف يتم إجرائها من خلال إستمارة إستبيان موزعة على مجموعة من الفئات المستهدفة ، مع إستخدام الأساليب الإحصائية المناسبة .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

2/1 مشكلة البحث :

أدى التطور في بيئة الأعمال بشكل سريع إلى إتجاه العديد من المنظمات نحو مواكبة إستخدامات التكنولوجيا الحديثة ، حيث تطبق تقنيات وأدوات تكنولوجية متطورة في مباشرة أعمالها لجعلها أكثر كفاءة ، هذا علاوة على قيام معظم المنظمات الكبرى بتخزين بياناتها الهامة عبر الشبكات الإلكترونية ، وفي ذات الوقت تجبر بيئة الأعمال العالمية المنظمات على الحفاظ على بنية تحتية رقمية آمنة لإجراء معاملاتها التجارية وتسمى هذه البنية التحتية الرقمية العالمية المترابطة بالفضاء السيبراني ، والذي يشتمل على الإنترنت وأنظمة الكمبيوتر والأجهزة والبرامج والمعلومات الرقمية (Kahyaoglu & Caliyurt, 2018, Pp.367-369) .

وفي هذا السياق تُعد تهديدات الأمن السيبراني من أهم التهديدات التي تواجه البنوك الإلكترونية ومستقبلها ، حيث أكدت دراسة كل من (IIA , 2016 ; ISACA , 2019) على أن الهجمات السيبرانية تتطور بشكل أسرع من تطور الحلول الأمنية ، الأمر الذي يترتب عليه أن تصبح تلك الانتهاكات الأمنية تمثل جانباً سلبياً على البنوك الإلكترونية وعملائها ، وتعتبر برامج الأمان المعمول بها مثل برامج مكافحة الفيروسات والبرامج الضارة والجدران النارية غير كافية حتى الآن للحماية من مخاطر تكنولوجيا المعلومات وتوفير ضمانات بشأن الأمن السيبراني ، والجدير بالذكر أن قطاع الخدمات المالية يشهد هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 70% وفق تقديرات البنك الدولي وقد تصل تكلفة الهجمات السيبرانية في قطاع الخدمات المالية إلى ما يقدر بنحو 300 إلى 380 مليار دولار سنوياً حال إتساع نطاق إنتشارها وفقاً لتقديرات صندوق النقد الدولي الأمر الذي دفع البنوك المركزية العربية إلى تشديد التعليمات الرقابية والتي تلزم البنوك بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية ومن أهمها تثبيت برامج الحماية ضد الإختراق (صندوق النقد العربي ، 2019 ؛ البغدادي ، 2021 ، ص 1520) .

ومع إستمرار تقنيات المعلومات والاتصالات في الابتكار في إيجاد وتقديم طرق جديدة للوصول إلى العملاء فإن البنوك الإلكترونية تتعرض في الوقت نفسه لمخاطر جديدة ، حيث أن الاستخدام الضار لتقنية المعلومات والاتصالات يمكن أن يؤدي إلى تعطيل الخدمات المالية الضرورية للأنظمة المالية الوطنية والدولية وتقويض الأمن والثقة وتعرض الاستقرار المالي للخطر .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

هذا وقد أكدت دراسة كل من (البنك الدولي ، 2021 ؛ steinbart et al., 2018, Pp. 15-) على أن نسبة العملاء الذين عانوا من الهجمات السيبرانية خلال عام 2020 على المستوى العالمي نحو 72% بزيادة قدرها حوالي 31% مقارنة بعام 2019 وذلك وفقاً للتقرير الصادر عن البنك الدولي في هذا الشأن نتيجة لذلك وإعترافاً بالتهديدات الناجمة عن المخاطر السيبرانية ومدى أهمية تعزيز قدرة الأجهزة البنكية على تحمل هذه المخاطر والتحوط منها فقد اتخذت السلطات الرقابية على مستوى العالم خطوات تنظيمية وإشرافية تهدف إلى تجنب أثر تلك المخاطر السيبرانية على البنوك ، في هذا الصدد قامت البنوك المركزية العربية بإصدار التعليمات البنكية التي تحث فيها البنوك على تعزيز قدراتها لمواجهة تلك الهجمات الإلكترونية .

ومما لاشك فيه أن اتساع نطاق المراجعة الداخلية ليشمل كافة الإجراءات اللازمة لإدارة المخاطر ، أصبح يوفر للمراجع الداخلي رؤية واضحة تمكنه من تقديم توصيات بتبني إجراءات رقابية جديدة ، الأمر الذي يترتب عليه أن تكون المراجعة الداخلية في حالة ديناميكية مستمرة حتى تستطيع أن تتماشى مع التغيير الحادث في تلك المخاطر ، ولذلك يمكن أن تلعب وظيفة المراجعة الداخلية دوراً مهماً في إدارة التهديدات السيبرانية ، من خلال تقديم منظور موضوعي إلى لجنة المراجعة وأعضاء مجلس الإدارة ، ثم استخدام هذه النتائج لتطوير خطة مراجعة داخلية واسعة تتناول مجالات المخاطر السيبرانية ، وبالتالي إجراء تقييم مشاكل للمخاطر السيبرانية للمنظمة .

وفي سياق متصل يقترح (ضيف ، 2016 ، ص ص 496 – 554) أن يتحمل قسم المراجعة الداخلية مهمة الفحص الدوري لبيئة المعلومات الرقمية للمنظمات وتقييم مستوى مخاطر التلاعب المحيطة بها ، ومن ثم فإن تحمل قسم المراجعة الداخلية مسؤولية توفير التقارير المهنية والمستقلة عن نتيجة الفحص الدوري لبيئة المعلومات الرقمية لا يمثل فقط أحد متطلبات مجالس إدارات المنظمات ولكنه يمثل أيضاً أحد متطلبات معايير المراجعة الداخلية ، فقد أكدت معايير المراجعة الداخلية الصادرة عن معهد المراجعين الداخليين IIA ضرورة إمتلاك المراجع الداخلي المعرفة الكافية بالمخاطر والأدوات الرقابية على تقنية المعلومات بالإضافة إلى ضرورة إلمامهم بأساليب المراجعة المعتمدة على تقنية المعلومات (IIA , 2013).

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

هذا وقد أكدت دراسة كل من (Islam et al., 2018, Pp.388-400 ; صالح، 2022، -15

4) علي أن مراجعة الأمن السيبراني يتطلب معرفة متطورة بتكنولوجيا المعلومات (IT) ويجب أن يكون لدى المراجعين الداخليين معرفة كافية بمخاطر تكنولوجيا المعلومات الرئيسية وأن يتحكموا في تقنيات وأساليب المراجعة القائمة على التكنولوجيا والمتاحة لأداء عملهم (IIA ، 2017) وأن يكون لديهم معرفة حول تقنيات مراجعة نظم المعلومات ومعايير أمن المعلومات ، وأن المراجع الداخلي يحتاج إلى مراجعة مستمرة لتقييم ومراجعة الأمن السيبراني وأن مراجعة الأمن السيبراني تعد بعداً جديداً لممارسة الأمان يهدف إلى دعم حماية أصول المعلومات الهامة للمنظمة زيادة قيمتها والتأثير المباشر على دعم الإستقرار المالي من خلال المساعدة في تحديد المخاطر وإقتراح أنشطة الرقابة ومراقبة عملية إدارة المخاطر .

وبمراجعة الأداب المحاسبي في هذا الشأن وجد الباحث أن هناك إهتماماً بالغاً من عدة أطراف حول موضوع مخاطر الأمن السيبراني حيث لاحظ الباحث إرتباطه بالعديد من القضايا المحاسبية الهامة ، كذلك رصد الباحث أن هناك إتجاه حديث لدراسة القضايا المتعلقة بأثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية ، وهذا ما دفع الباحث نحو مساهمة الإتجاه العالمي في هذا الشأن .

وإنطلاقاً مما سبق يمكن تحديد المشكلة البحثية لهذا البحث من خلال عرض التساؤلات البحثية

التالية :

- 1- ما المقصود بمفهوم ومخاطر الأمن السيبراني ؟
- 2- ما هي محددات جودة المراجعة الداخلية للأمن السيبراني ؟
- 3- ما هية البنوك الإلكترونية ؟
- 4- ما المقصود بالإستقرار المالي وما هي أدوات قياسه في البنوك الإلكترونية؟
- 5- ما هي طبيعة مخاطر وتهديدات الأمن السيبراني في البنوك الإلكترونية ؟

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

6 - إلى أي مدى يمكن أن تساهم جودة المراجعة الداخلية المستخدمة في الحد من مخاطر الأمن السيبراني في دعم الإستقرار المالي في البنوك الإلكترونية؟

7- هل يمكن الحصول على دليل ميداني عن أهمية الدور الذي يمكن أن تلعبه جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني في البنوك الإلكترونية وتأثير ذلك على دعم الإستقرار المالي؟

3/1 أهمية ودوافع البحث :

تتبع أهمية البحث الأكاديمية من أهمية الموضوع قيد الدراسة والذي يعتبر من الموضوعات الحديثة في أدبيات الفكر المحاسبي وهو دور جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني في البنوك الإلكترونية وإنعكاساته على دعم الإستقرار المالي ، علاوة على ندرة الدراسات الأكاديمية وخاصة باللغة العربية – في حدود علم الباحث – التي تناولت هذه العلاقة.

كما تتمثل أهمية البحث العملية في أهمية الأمن السيبراني والذي يعد أحد المواضيع التي لاقت إهتماماً واسعاً على الصعيد المحلي والعالمي خلال الفترة الأخيرة ، لا سيما مع التحول الرقمي في مجال أنشطة الأعمال ، مما يترتب عليه زيادة التهديدات الإلكترونية حيث يتوقع كل يوم إمكانية حدوث إختراق للبيانات مما يستدعي قيام اللجان المتخصصة بالضغط على المنظمات لإظهار كيفية تخفيف المخاطر الإلكترونية بوضوح ويعتبر ذلك محفز قوي لدخول المراجعين الداخليين إلى عالم الأمن السيبراني ، علماً بأن مراعاة تفعيل إدارة الأمن السيبراني والحد من مخاطره بشكل صحيح في المنظمات يساعد كثيراً في مواجهة أي كوارث تقنية وسيبرانية من خلال إقفال الثغرات ومعالجة القصور في الأنظمة وتعزيز سياسات أمن المعلومات ودعم الإستقرار المالي .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

4/1 أهداف البحث :

في ضوء مشكلة البحث يمكن توضيح أهدافه في الآتي :

- 1- عرض مفهوم ومخاطر الأمن السيبراني .
- 2- توضيح محددات جودة المراجعة الداخلية للأمن السيبراني .
- 3- توضيح المقصود بالبنوك الإلكترونية وآلية عملها .
- 4- توضيح المقصود بالإستقرار المالي وعرض أدوات قياسه في البنوك الإلكترونية .
- 5- عرض لطبيعة مخاطر وتهديدات الأمن السيبراني في البنوك الإلكترونية .
- 6 – إستعراض المدى الذي يمكن أن تساهم به جودة المراجعة الداخلية المستخدمة في الحد من مخاطر الأمن السيبراني في دعم الإستقرار المالي في البنوك الإلكترونية .
- 7- القيام بدراسة ميدانية حول أهمية الدور الذي يمكن أن تلعبه جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني في البنوك الإلكترونية وتأثير ذلك على دعم الإستقرار المالي؟

5/1 منهج وأسلوب البحث :

سوف يستخدم الباحث المنهج العلمي بشقيه الإستنباطي والإستقرائي ، حيث تستخدم المنهج الإستنباطي من خلال المسح المرجعي للدراسات والبحوث بغية بناء الإطار النظري للبحث وإشتقاق فروض البحث ، كما تستخدم المنهج الإستقرائي في الدراسة الميدانية عن طريق جمع البيانات اللازمة لإختبار فروض البحث .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

6/1 خطة البحث :

لتحقيق هدف البحث وفي ضوء مشكلته سوف يتم تنظيم البحث على النحو التالي :

المحور الأول : الإطار العام للبحث .

المحور الثاني : الأمن السيبراني (المفهوم - المخاطر) .

المحور الثالث : محددات جودة المراجعة الداخلية للأمن السيبراني .

المحور الرابع : البنوك الإلكترونية وآلية عملها .

المحور الخامس : الإستقرار المالي في البنوك الإلكترونية (المفهوم – أدوات القياس) .

المحور السادس : طبيعة مخاطر وتهديدات الأمن السيبراني في البنوك الإلكترونية .

المحور السابع : دور المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على دعم الإستقرار المالي في البنوك الإلكترونية .

المحور الثامن : دراسة ميدانية .

النتائج والتوصيات والتوجهات المستقبلية للبحث .

قائمة المراجع .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
المحور الثاني : الأمن السيبراني (المفهوم - المخاطر) .

1/2 مفهوم الأمن السيبراني :

يمثل الأمن السيبراني وفقاً لما ورد في التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الإتصالات للعام ٢٠١٨ – ٢٠١٩ مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات جيدة وتقنيات يمكن إستخدامها لحماية البيئة السيبرانية وموجودات المنظمات والمستخدمين (Eling & wirfs, 2016, Pp. 23-57)

ويمكن تعريف الأمن السيبراني وفقاً لما جاء بدراسة (Alina et al., 2017, Pp. 510-513) وإستناداً لأهدافه بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ، ويضمن إمكانية الحد من الخسائر والإضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الأضرار إلى خسائر دائمة .

٢/٢ مخاطر الأمن السيبراني :

أكدت دراسة (Hartmann& Carmenate, 2021, Pp.9-23) على أن المخاطر السيبرانية يقصد بها المخاطر التشغيلية على أصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية وسلامة ونظم المعلومات ومقارنة بفئات المخاطر التي يغطيها التأمين فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسئولية مع مخاطر كل من الممتلكات والخصوم وكذلك المخاطر الكارثية والتشغيلية ، ومما لاشك فيه أن تكنولوجيا المعلومات والإتصالات تتيح إمكانات هائلة وغير مسبوقه لإنتاجية أفضل في جميع القطاعات وللتواصل عبر القارات إلا أن البنية التحتية لهذه التقنيات تمثل إرتباطاً بين مصالح متعددة وخدمات مختلفة ودول عديدة الأمر الذي يجعل من الأخطار في المجال السيبراني أخطاراً عالمية فلا يمكن لأي جهة أن تضمن بقاءها في منأى عن الأخطار ما دامت سلامة الآخرين معرضة للخطر .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

هذا وقد أكدت دراسة (Shahimi & Mahzan,2018, Pp. 1257 – 1283) على أن

الهجمات السيبرانية تضم ثلاث أنواع يمكن سردها في الآتي :

أ- مخاطر سيبرانية تتعلق بالسرية : حيث تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل المنظمة إلى أطراف ثالثة كما في حالة حدوث إختراق البيانات .

ب- مخاطر سيبرانية تتعلق بالنزاهة : والتي تتعلق بإساءة استخدام الأنظمة كما هو الحال بالنسبة للاحتيال .

ج- مخاطر سيبرانية تتعلق باستمرارية الأداء : والتي تتلخص في تعطل أو التوقف عن ممارسة الأعمال .

والجدير بالذكر أن هناك مجموعة من الأسئلة يجب على الرئيس التنفيذي للمراجعة مراعاتها عن

تقييم حوكمة المنظمات المتعلقة بالأمن السيبراني تتمثل في : (IIA, 2016)

١- هل الإدارة العليا وحوكمة لجنة المراجعة – مجلس الإدارة على دراية بالمخاطر الرئيسية

المتعلقة بالأمن السيبراني هل تتلقى مبادرات الأمن السيبراني الدعم والأولوية المناسبين ؟

٢- هل أجرت الإدارة تقييماً للمخاطر لتحديد الأصول المعرضة للتهديدات السيبرانية أو

الإنتهاكات الأمنية وهل تم تقييم التأثير المحتمل (المالي وغير المالي) ؟

٣- هل سياسات وإجراءات الأمن السيبراني مطبقة وهل يتلقى الموظفون تدريباً دورياً للتوعية

بالأمن السيبراني ؟

٤- هل تم تصميم عمليات تكنولوجيا المعلومات وتشغيلها لإكتشاف التهديدات السيبرانية ؟ هل

لدى الإدارة ضوابط مراقبة كافية مطبقة ؟

المحور الثالث : محددات جودة المراجعة الداخلية للأمن السيبراني .

نالت جودة المراجعة الداخلية إهتمام كثير من الباحثين في الأونة الأخيرة، حيث تعد المراجعة

الداخلية أحد عناصر الرقابة الداخلية الفعالة، نظراً لطبيعة عملها داخل المنظمات وإمام المراجعين

الداخليين بظروف وأحوال تلك المنظمات بدرجة أكبر من مراقب الحسابات الخارجي، ومع الاهتمام

المتزايد برفع كفاءة نظم الرقابة من داخل وخارج المنظمات تطور مفهوم المراجعة الداخلية بحيث

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

خرج نطاق عملها من مجرد التركيز على النواحي المالية إلى ما هو أبعد من ذلك، وهذا واضح من تعريف معهد المراجعين الداخليين للمراجعة الداخلية حيث تناول مفهوم المراجعة الداخلية بأنها "نشاط مستقل وموضوعي، يقدم تأكيدات وخدمات استشارية بغرض إضافة قيمة وتحسين عمليات المنظمة، ويساعد المنظمة على تحقيق أهدافها، من خلال إتباع أسلوب منهجي منظم لتقييم وتحسين فعالية عمليات الحوكمة وإدارة المخاطر والرقابة" (Yang et al., 2020, Pp. 167-183)

وقد ترتب على هذا التعريف توسيع نطاق عمل المراجعة الداخلية ليشمل تقديم التأكيدات والاستشارات والتوصيات للإدارة، وإدارة المخاطر بهدف تحسين الرقابة والحوكمة، بل أن المراجعة الداخلية أصبحت تمثل أهم مكون في الإدارة وآليات الحوكمة في كل القطاعين العام والخاص (Betti et al., 2021, Pp. 872 – 888).

وفي سياق متصل أوصت لجنة مبادئ الإدارة السليمة للمخاطر الصادرة عن (COSO,2019) و (IIA, 2020) بأن إدارة مخاطر الأمن السيبراني يمكن أن تدار من خلال ثلاث خطوات دفاعية، حيث يتمثل الخط الدفاعي الأول في مديرو وحدات الأعمال جنباً إلى جنب مع وظيفة تكنولوجيا المعلومات IT حيث أنهم بحاجة إلى اعتبار مخاطر الأمن السيبراني جزءاً لا يتجزأ من عملهم وإنشاء الهياكل والضوابط المناسبة لإدارة العمليات والمخاطر، كما يتمثل الخط الدفاعي الثاني في إدارة مخاطر أمن المعلومات حيث توفر الخبرة لتنفيذ ومتابعة فعالية ضوابط الأمن السيبراني CS، بينما يتمثل الخط الدفاعي الثالث في وظيفة المراجعة الداخلية حيث تزود مجلس الإدارة ولجنة المراجعة التابعة لها بتوكيد مستقل عن فعالية إستراتيجية وسياسات وإجراءات وضوابط إدارة مخاطر الأمن السيبراني وهذا ينطوي على مراجعة مدى كفاية العمل الذي قامت به أدوار الخطين الأول والثاني (Vuko et al., 2021, Pp. 37-40).

وفي هذا الصدد يمكن القول أن جودة وظيفة المراجعة الداخلية فيما يتعلق بإدارة مخاطر الأمن السيبراني والحد من تلك المخاطر يركز على قيام مدير إدارة المراجعة الداخلية بتقديم النصح والإرشاد لمجلس الإدارة بصدد تحديد وتوصيف وقياس مخاطر الأمن السيبراني المحيطة ببيئة أعمال المنظمة التكنولوجية وكيفية مواجهتها والحد من أثارها بما يدعم تحقيق أهداف المنظمة (Florakis et al.,2020, P.46 ; Li & Wang .,2018, Pp. 53-55).

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
والجدير بالذكر أن هناك العديد من العوامل التي تحدد فعالية المراجعة الداخلية بشأن الأمن
السيبراني ولعل أهمها ما جاء بدراسة كل من (Islam et al., 2018, Pp. 394-398 ; IIA,
2017; Deloitte, 2017) :

1/3 التاهيل العلمي والعملي لفريق المراجعة الداخلية بالمنظمة : أشارت منظمة المراجعة الداخلية
(IAF, 2021) إلى ضرورة أن يتفهم المراجعون الداخليون ومعاهد ومنظمات المراجعة الداخلية
أهمية الإستفادة من التكنولوجيا ، حيث تتطلب مراجعة الأمن السيبراني بجودة عالية تأهيل فريق
المراجعة الداخلية بالمنظمة بمعرفة متطورة بتكنولوجيا المعلومات (IT) ومخاطرها ، وأن يكون لديهم
القدرة على التحكم في تقنيات المراجعة القائمة على التكنولوجيا الحديثة والمتاحة لأداء أنشطة المراجعة
الداخلية بجودة عالية ، الأمر الذي يترتب عليه القدرة على تطوير علاقات أعمق مع وظائف أمن نظم
المعلومات ومن ثم المساهمة في بناء برنامج إدارة أمن سيبراني أكثر فعالية وجودة وبالتالي من المتوقع
أن تؤدي المراجعة الداخلية التي تضم رؤساء مراجعة داخلية حاصلين على شهادات الأمن المناسبة
مثل (الشهادات الأمنية CISM و CSP) وكذلك شهادات مراجعة أمن أنظمة المعلومات مثل : (شهادة
CISA و QICA) إلى زيادة جودة مراجعة الأمن السيبراني .

2/3 مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية Enterprise Risk Management
(ERM) Management : نظراً لتطور دور المراجعة الداخلية حيث أصبح تركيزها الطبيعي على
الحوكمة وإدارة المخاطر والالتزام ، فأصبحت ذات أهمية بالغة في الإشراف على جميع مكونات أطر
عمل إدارة المخاطر المؤسسية ومن ثم فإن إدارة المخاطر المؤسسية لها تأثير كبير على أنشطة
المراجعة الداخلية ، الأمر الذي يترتب عليه تمتع المراجعة الداخلية بفعالية عالية في أداء أنشطتها ،
علاوة على قدرة الرؤساء التنفيذيين للمراجعة على تشغيل أقسامهم بشكل أكثر كفاءة من خلال الإستفادة
من موارد إدارة المخاطر للمنظمة ، هذا بالإضافة إلى أنه عند مشاركة المراجعة الداخلية في إدارة
المخاطر ينهج المراجعون نهج التفكير الإبتكاري الإستراتيجي مثل المديرين والتركيز على أهداف
العمل بدلاً من أهداف المراجعة فقط وبالتالي يمكن للمراجعة الداخلية من خلال إجراء تقييم شامل
للمخاطر السيبرانية تقديم وجهات نظر ونتائج موضوعية إلى لجنة المراجعة وأعضاء مجلس الإدارة

¹ تتمثل الشهادات المناسبة في الشهادات الأمنية مثل CISM – CISSP – CSP – CDP – CISRCP مثل CISA – CRISC – QICA شهادة مراجعة أنظمة المعلومات مثل

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

واستخدام هذه النتائج لتطوير خطة المراجعة الداخلية بشكل موسع تضم مجالات المخاطر السيبرانية التي تواجهها المنظمة خلال فترة مراجعة واحدة أو فترة مراجعة متعددة السنوات .

3/3 جودة وظيفة المراجعة الداخلية : أكدت دراسة كل من صالح ، 2022 ، ص 9 ; Islam et al., 2018, Pp. 385- 390 ; Christ et al., 2015, Pp. 37 – 59 ;Ege, 2015, Pp. 495

(497) – على أن وظيفة المراجعة الداخلية المصحوبة بالجودة العالية يترتب عليها مجموعة من المنافع للمنظمات لعل أهمها : تحسين حوكمة المنظمات ، جودة التقارير المالية ، فعالية هيكل الرقابة الداخلية ، القدرة على تقديم تقييمات أفضل للمخاطر ، الحد من سوء السلوك الإداري وزيادة كفاءة المراجعة الخارجية ، وفيما يتعلق بالأمن السيبراني يمكن أن تلعب المراجعة الداخلية دوراً هاماً وبارزاً في إدارة المخاطر السيبرانية من خلال إجراء تقييم شامل للمخاطر الإلكترونية ويمثل برنامج توكيد الجودة والتحسين (The Quality Assurance and Improvement Program) (QAIP) الخاص بالمراجعة الداخلية معياراً لتقييم جودة المراجعة الداخلية وبالتالي من المتوقع أن ترتبط المراجعة الداخلية عالية الجودة بشكل كبير وإيجابي بمراجعة الأمن السيبراني والحد من مخاطره .

4/3 حجم قسم المراجعة الداخلية ومشاركته في تطوير بيئة الأعمال : من المهم أن تدرك منظمات الأعمال أن الإستثمار التكنولوجي في المراجعة الداخلية له عائد ومردود إيجابي وبالتالي يكون لإدارة المراجعة الداخلية حجم يتناسب مع مكانتها وأهميتها لكل منظمة ، ويزيد من فعالية إدارة المراجعة الداخلية تواصلها الدائم مع كافة الإدارات وخاصة مع إدارة المخاطر ولجنة المراجعة ، فمن المعروف أن لجنة المراجعة تتمتع بتأثير هائل على المراجعة الداخلية حيث يقوم المديرون التنفيذيون للمراجعة بتقديم تقرير إلى لجنة المراجعة كما تخضع مجالات عمل المراجع الداخلي لمسؤوليات اللجنة ولذلك يجب أن يلعب المراجع الداخلي دوراً مركزياً في مساعدة لجنة المراجعة على الإشراف على الأمن السيبراني ، والجدير بالذكر أن اجتماعات المراجعين الداخليين المتكررة مع لجنة المراجعة يقلل من إحصائية حدوث مشاكل تتعلق بمراجعة الأمن السيبراني ، نظراً لتقارب المسافات بين لجنة المراجعة وإدارة المراجعة الداخلية ورفع التقارير إلى الإدارة العليا ، هذا علاوة على دعم مشاركة المراجعين الداخليين في طرح وتطوير الرؤى حول مخاطر الأمن السيبراني .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

ويرى الباحث أن المراجع الداخلي في البنوك الإلكترونية مطالب بتوفير تأكيدات معقولة عن مدى توافر متطلبات أمن الأنظمة والمعلومات وتأكيد كفاءتها وفعاليتها ، لتحقيق متطلبات الأمن السيبراني ، ومما لاشك فيه أن قيامه بهذا العمل يتطلب منه تطوير ذاته ليمتلك المهارات اللازمة لتقييم إدارة مخاطر الأمن السيبراني بشكل فعال ، وفهم وتقييم إجراءات التعامل مع المخاطر المتوقعة نظراً لأن فرق المراجعة الداخلية التي تمتلك مهارات رقمية ولديها إدراك بأهمية الإمكانيات الرقمية ، وكيفية الإستفادة منها سوف تمثل قيمة مضافة للمنظمة مما ينعكس بشكل قوي على دعم الإستقرار المالي في البنوك الإلكترونية .

المحور الرابع : البنوك الإلكترونية وآلية عملها .

ارتبطت ظاهرة العولمة المالية بالتحريك المالي الذي ترتب عليه إندماج الأنظمة المالية والنقدية للدول على المستوى العالمي بهدف تيسير الأعمال المالية والبنكية للعملاء ، ومحاولة إزالة القيود التي تحول دون تدفق رؤوس الأموال ، ودعم حرية المنظمات المالية والبنكية في إنجاز جميع المهام المنوطة بها .

1/4 طبيعة العمليات البنكية الإلكترونية

يستخدم اصطلاح البنوك الإلكترونية Electronic - Banking كتعبير متطور وشامل للمفاهيم التي تبلورت مع بداية التسعينات مثل مفهوم الخدمات البنكية عن بعد ، البنوك الإلكترونية عن بعد ، البنك المنزلي Banking Home ، الخدمات البنكية الذاتية Self-Service-Banking وجميعها تتعلق بقيام العميل بإدارة حساباته وإنجاز أعماله المتصلة بالبنك عن طريق المنزل أو المكتب أو أي مكان آخر وفي الوقت الذي يريده (العزي ، 2017 ، ص ص 6-7) .

ويرى الباحث أن العمليات البنكية الإلكترونية يقصد بها الخدمات المتطورة التي تقدمها البنوك من خلال قنوات إتصال إلكترونية وهي بذلك تحقق للبنك فوائد عديدة لاسيما تخفيض تكاليف الاستغلال ورفع كفاءة الأداء المالي والتشغيلي ومستويات الجودة للبنك .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
وتتمثل أهم صور العمليات البنكية الإلكترونية في الوقت الحالي في الآتي : (Emanuel et al., 2017)

1/1/4 النقود الإلكترونية Electronic money : حيث يصدر البنك وسائل الدفع في شكل وسائط تحتوي على شرائح ممغنطة تسمى ببطاقات القيمة المخزنة ، يقابلها مقدار من الوحدات النقدية بحيث يزود العميل بها للتعامل مع جهاز البنك الآلي من أجل السحب النقدي أو لطلب كشف الحساب ودفتر الشيكات وكذلك تحويل أموال أو دفع فواتير مستحقة ويفترض الاستفادة من هذه الخدمة على مدار 24 ساعة يوميا .

2/1/4 البنك المنزلي Home Banking : حيث يتم تحميل الحاسب الشخصي ببرنامج خاص يوفره البنك مجاناً أو لقاء رسوم للعملاء لأغراض الإطلاع على الحساب والسحب أو الإيداع في أرصدة الحسابات البنكية حيث يتمكن العميل من الدخول وإجراء المعاملات عبر الإتصال بالإنترنت في ظل ضوابط تتحكم في حركة هذه الأنشطة وتضمن حقوق العميل والبنك معاً علي حد سواء .

3/1/4 الخدمات البنكية التليفونية Telebanking : والتي تتمثل في مجموعة من الأنظمة تساهم في خدمة العملاء عبر جهاز التليفون ، خاصة التليفونات المحمولة على مدار اليوم ، وضمن سياق منظم يحدد العميل نوع الخدمة البنكية التي يريدتها من خلال البرنامج الصوتي الذي يضعه البنك في متناول عملائه .

2/4 أهداف العمليات البنكية الإلكترونية : (حسين ومعراج ، 2019 ، ص15)

تقدم البنوك الإلكترونية خدمات تقتصر على المشاركين فيها وفقاً لشروط العضوية التي تحددها البنوك وذلك من خلال أحد المنافذ على الشبكة كوسيلة لاتصال العملاء بها لتحقيق عدة أهداف من أهمها :

- إتاحة معلومات عن الخدمات التي يؤديها البنك .
- حصول العملاء على خدمات متعددة كالتعرف على معاملاتهم وأرصدة حساباتهم وتحديث بياناتهم وطلب الحصول على قروض .
- طلب العملاء تنفيذ عمليات وخدمات بنكية مثل تحويل الأموال .
- توفير المزيد من فرص العمل ودعم آليات الاستثمار .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

- تعزيز رأس المال الفكري والمساهمة في تطوير تكنولوجيا المعلومات .

ويرى الباحث في ضوء ما سبق أن العمليات البنكية الإلكترونية تمكن البنوك من الوصول إلى قاعدة عريضة من العملاء المودعين والمقترضين وطالبي الخدمات البنكية ، هذا علاوة على زيادة كفاءة أداء البنوك ، بالإضافة إلى خفض تكاليف تشغيل وإنجاز العمليات بالبنوك ، والمساهمة في تقديم خدمات بنكية جديدة .

وإستكمالاً لما سبق يؤكد الباحث على أن هناك مجموعة من المخاطر والتهديدات تتعلق بالأمن السيبراني في البنوك الإلكترونية لا بد من قيام تلك البنوك بإدارة تلك المخاطر ، وحيث أن البنك المركزي المصري هو الجهة المنوط بها قانوناً إصدار أوراق النقد للاستخدام كوسيلة دفع لها قوة إبراء توازي عملية إصدار وسائل دفع لنقود إلكترونية لذلك لا بد أن تتم تلك العمليات تحت إشراف البنك المركزي المصري ، وسوف يقوم الباحث بإستعراض الإستقرار المالي من حيث المفهوم وأدوات القياس في البنوك الإلكترونية في المحور القادم من البحث .

المحور الخامس : الإستقرار المالي في البنوك الإلكترونية (المفهوم – أدوات القياس) .

يعد القطاع المالي وخاصة البنوك قطاعاً مهماً لاستقرار النظم المالية ، وفي هذا الشأن فقد أشارت دراسة (Jan & Marimuthu, 2015, P.122) أن لاستقرار المالي في القطاع المصرفي دوراً حاسماً في تحقيق التنمية المستدامة في الدول مما يساهم في رفع قدرة النظام المصرفي على تأدية وظائفه كتوفير السيولة وتقديم الائتمان المالي وغيرها من المهام التي تجعل النظام المالي للدولة قادراً على إستيعاب ومواجهة الصدمات الداخلية والخارجية .

وفي هذا الشأن فقد هدفت دراسة (Marei & Eralp , 2017, Pp. 121-126) إلى قياس ومقارنة الاستقرار المالي للمصارف الإسلامية والتقليدية العامل في تركيا للفترة من 2006 – 2015 وقد تكونت العينة من 29 مصرفاً ، وقد ركزت الدراسة على ثلاثة أنواع من المتغيرات والمواصفات المصرفية والقطاع المصرفي والاقتصاد الكلي وقد أظهرت النتائج الرئيسية أن وجود أزمة مالية له تأثير سلبي كبير على الاستقرار المالي للقطاع المصرفي في تركيا كما تشير المؤشرات أيضاً إلى أن المتغيرات المتعلقة بحجم البنك ونسبة القروض إلى الأصول ونسبة التكلفة إلى الدخل وتنوع الدخل ومؤشر هرفندا هرشمان لها تأثير سلبي كبير على الاستقرار المالي للبنوك العامة في تركيا .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

وفي هذا السياق فقد هدفت دراسة (Vighneswara ,2014, P.4-11) إلى تحليل العوامل المؤثرة على الاستقرار المالي المصرفي في أعقاب الأزمة المالية بالإضافة إلى تسليط الضوء على أهمية الاستقرار المالي المصرفي في الاقتصادات الناشئة حيث تم بناء نماذج قياسية باستخدام نماذج البائل الساكنة والمتحركة وقد توصلت الدراسة إلى أن القروض غير العاملة والربحية وكفاية رأس المال تغطية السيولة لها دلالة إحصائية وبالتالي تعتبر أهم محددات الاستقرار المالي المصرفي .

1/5 مفهوم الإستقرار المالي في البنوك :

نال موضوع الاستقرار المالي في البنوك إهتمام الكثير من الباحثين منذ بداية القرن العشرين وحتى الآن وذلك نظراً للأهمية الكبيرة التي يحتلها القطاع المالي في إقتصاديات الدول بالإضافة إلى أن أي إنهيارات في وظائف النظام المالي سيقود إلى ضعف تلك الإقتصاديات ، وفي هذا الشأن فقد أكدت دراسة (عبد اللطيف ، 2017 ، ص 5) على أن الإستقرار المالي يمثل الحالة المعاكسة لعدم الاستقرار وبعبارة أخرى فإن النظام المصرفي يعد مستقراً طالما لا يعاني من عدم استقرار ، وقد فسرت الدراسة تعريف الإستقرار المصرفي بأنه الحالة التي يصل إليها البنك عندما يمر بكثير من الاضطرابات المالية الخطيرة والتي تجعله قريب جداً من مراحل أو مستويات التعثر المالي التي يمكن التدرج بها إلى مستوى إشهار إفلاسه سواء كانت هذه الاضطرابات تعني عدم قدرته على سداد التزاماته تجاه الغير أو تحقيق خسائر متتالية سنة بعد أخرى مما يجعله مضطراً إلى إيقاف نشاطه من حين إلى آخر وغالباً ما يحدث التعثر المالي كنتيجة لوجود المشكلتين معاً وبالتالي نكون أمام حالة عسر مالي حقيقي .

كما أكدت دراسة (خلف ، 2018 ، ص 254) على أن النظام البنكي المستقر يمثل النظام الذي تكون فيه معظم البنوك قادرة على الوفاء بالتزاماتها ومن المحتمل أن تبقى كذلك وذلك من خلال اعتماد عدة نواحي كقدرة البنك على تحقيق الأرباح وكفاءة الإدارة وكفاية رأس المال بالبنوك ، بحيث يتطلب تحقيق مبدأ السلامة المصرفية ضرر تمتع كل وحدة من وحدات الجهاز المصرفي بموقف مالي سليم بالإضافة إلى قدرتها على القيام بدورها في الوساطة بكفاءة .

ويرى الباحث أن الإستقرار المالي يمثل الحالة التي يكون عليها البنك المصحوبة بمستوى أرباح مستقرة بحيث يكون البنك قادراً على تخصيص موارده وبكفاءة بين الأنشطة وإدارة وتحديد المخاطر المالية ، هذا بالإضافة إلى قدرة البنك على مواجهة المخاطر والأزمات وإمتصاص الصدمات .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
2/5 مظاهر عدم الاستقرار المالي البنكي :

أكدت دراسة (JI & All, 2018, P. 23) على أن هناك مجموعة من المظاهر تعتبر مؤشراً لعدم الإستقرار المالي في البنوك يمكن عرضها في الآتي :

1/2/5 ارتفاع الديون غير العاملة المتعثرة : حيث يعتبر مؤشر الديون المتعثرة دليلاً هاماً في رصد الأزمات البنكية ، وطبقاً لمؤشر Bankometer يجب أن تكون نسبة الديون المتعثرة أقل من 15% من إجمالي الديون في البنك .

2/2/5 الذعر البنكي : وتتم هذه الحالة عندما يعرف الجمهور أن أحد البنوك أو بعضها في أزمة الأمر الذي يترتب عليه قيام الجمهور بسحب الودائع من البنوك التي تمر بحالة من عدم الإستقرار المالي وأيضاً من البنوك الأخرى ، فتقل إحتياطيات البنوك مما يتسبب في أزمة سيولة.

3/2/5 الاعسار البنكي : وهي الحالة التي تكون فيها البنوك غير قادرة على سداد الالتزامات المترتبة عليها مع أن إجمالي الموجودات لديها يفوق إجمالي التزاماتها ، حيث تمتاز هذه الحالة بضعف في ربحية البنك وضعف في التدفقات النقدية التشغيلية الداخلة فهو لا يشكل خطراً حقيقياً ولكن تكراره يؤدي إلى فقدان البنوك لسمعتها الائتمانية ، وقد يستطيع البنك تجاوز حالة نقص السيولة لديه دون وقوعه في الفشل المالي الكلي وذلك ببيع بعض موجوداته لتغطية التزاماته المستحقة والعاجلة ، وهذا ما أكدت عليه دراسة (Hassanpour & Nazemi, 2017, P. 219)

4/2/5 الفشل البنكي : وهي المرحلة التي تلي العسر البنكي والتي يكون فيها البنك قريباً من الإفلاس وعاجز عن سداد التزاماته إضافة إلى كونه يعاني تراكماً للخسائر بشكل كبير فتتجاوز القيمة السوقية لالتزاماته القيمة السوقية لمجموع أصوله أي أنه حتى لو قام ببيع أصوله بأكملها لن يكون قادراً على تغطية كامل ديونه وتكون قيمة رأس المال في البنك سالبة .

5/2/5 الإفلاس البنكي : هو عبارة عن إعلان قانوني بأن البنك في محنة مالية لا يستطيع مقابلة حقوق الغير لديه أو توقف أنشطته تمهيداً لتصفية أصوله وسداد الالتزامات المستحقة عليه وتعتبر المحصلة النهائية لحالة الفشل المالي للبنك (Onakoya & Ayooluwa, 2017 P. 706)

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية) 3/5 نماذج قياس الاستقرار المالي في البنوك :

تواجه عملية قياس الاستقرار البنكي بعض التحديات بسبب تعقيدات عملية التقييم ، وتوفر أدبيات الاستقرار المالي عدداً من المقاييس الكمية من أجل تقييم الاستقرار المالي يمكن إيجازها في الآتي :
(Hassanpour & Nazemi, 2017 P. 215)

1/3/5 نموذج اختبارات الضغط : والذي يعد من أحدث الطرق المستخدمة في قياس هشاشة حافظة القروض البنكية أو النظام المالي بالبنك بأكمله مقابل سيناريوهات افتراضية مختلفة ، ويعتمد اختبار الضغط على عبارة - ماذا لو- بمعنى أنه نموذج لتقدير ما يجب أن يحدث لرأس المال أو الربح أو التدفق النقدي للبنك أو النظام المالي بأكمله في ظل وجود بعض التهديدات والمخاطر ، وهذا النموذج يمثل نموذج محاكاة إدارة الموجودات (المطلوبات) لجعل تقييم إستراتيجيات الميزانية العمومية المختلفة ممكناً تحت سيناريوهات مختلفة ، ويمكن اعتبار اختبارات الضغط كاختبار تطبيقات السيناريو الأسوأ فإذا نظرنا إلى اختبار الضغط من جهة عوامل الخطر التي يختبرها فإننا نجد أنه يتضمن نوعين رئيسيين من النماذج الفرعية يتمثلان في الآتي : (عثمان وصالح ، 2021 ، ص ص ١٠-١٥)

1/1/3/5 تحليل السيناريو : وهو يستند أساساً إلى أن السيناريوهات يمكن أن تكون إما أحداث تاريخية أو أحداث افتراضية وهي تتحكم بالتأثير على الأحداث ذات الصلة من خلال عدد من عوامل الخطر ، بينما تمثل الخسارة الناتجة عن الظروف الضاغطة والتي يمكن إخضاعها للإختبار تأثير مركباً من التحركات المتزامنة التي تتم في نفس الوقت للعديد من عوامل الخطر .

2/1/3/5 تحليل الحساسية : إن تحليل الحساسية يفصل تأثير المحفظة الاستثمارية خسائر وأرباح بالديناميكية في معلمات الخطر المالي .

2/3/5 نموذج القيمة المعرضة للخطر Value At Risk VAR : تعتمد طريقة قياس القيمة المعرضة للخطر VAR على تحليل مخاطر السوق باستخدام نماذج إحصائية من خلال حساب أقصى قيمة للخسائر التي يتوقع أن يتحملها البنك للمحافظ التي بحوزته في ظل الظروف الطبيعية خلال فترة زمنية معينة بسبب التعرض لمخاطر أسعار العائد ، حيث يقوم هذا النموذج بطرح السؤال التالي ما مقدار المال الذي قد يخسره البنك خلال الفترة الزمنية المقبلة ؟ وذلك في ظل درجة ثقة معينة (95%)

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

- 97% - 99%) تطبق هذه الطريقة بصفة أساسية على الأصول المحتفظ بها لغرض المتاجرة حيث تكون النية لدى البنك هو المتاجرة في المراكز لديه على أساس يومي ويمكن حساب القيمة المعرضة للمخاطر VAR باستخدام أحد الطرق الثلاث التالية طريقة التباين والتغاير وطريقة المحاكاة التاريخية وطريقة محاكاة مونت كارلو .

3/3/5 نموذج تكساس (TXR) Texas ratio : يركز هذا النموذج بشكل كبير على مخاطر الائتمان التي تواجه البنوك ، وهو يقوم على تحليل الوضعية المالية وقياس الاستقرار المالي للبنوك التجارية ، ويقوم هذا النموذج على العلاقة الرياضية التالية :

$$TXR = \frac{NPL + Fixt Assets}{Equity + NPL pro}$$

حيث NPL : تمثل القروض غير العاملة (المتعثرة) .

Fixt Assets : تمثل الأصول الثابتة الملموسة .

Equity : تمثل حقوق الملكية .

NPL pro : تمثل مخصصات تغطية خسائر القروض المتعثرة .

ووفقاً للعلاقة الرياضية السابقة تكون البنوك متسقرة مالياً في حالة عدم تجاوز هذه النسبة الواحد الصحيح ، أما إذا تجاوزت هذه النسبة الواحد الصحيح يكون هناك عدم إستقرار مالي لدى البنك .

4/3/5 نموذج الحيطه والحذر CAMELS : يقوم هذا النموذج على مجموعة من المؤشرات التي يتم من خلالها تحليل الوضعية المالية للبنك ومعرفة درجة تصنيفه ، وقد عملت السلطات الرقابية في الولايات المتحدة على الأخذ بنتائج معايير CAMELS والاعتماد عليها في إتخاذ القرارات وذلك من خلال مؤشرات تتمثل اساساً في العناصر التالية : حيث (C) تمثل كفاية رأس المال ، بينما (A) يمثل جودة الأصول ، بينما (M) تمثل جودة الإدارة ، و (E) تمثل إدارة الربحية ، و (L) تمثل درجة السيولة ، و (S) تمثل مخاطر السوق ، وفي دراسة قدمها أدرج نموذج معدل يتكون من النسب التالية نسبة كفاية رأس المال (CAR) القروض المتعثرة NPL صافي هامش الربح NPM معدل العائد على

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)
الأصول ROA ، وقد أظهرت نتائج تكوين النموذج في الجدول التالي, (Abdul Karim & All, 2018, p. 172)

جدول رقم (1-5) التعثر والاستقرار المالي وفق نموذج CAMELS

المتغيرات	الفئة	النتيجة
CAR	100-81	البنك مستقر ماليا بعيد عن التعثر
NPL	80-66	البنك مستقر ماليا
NPM	65-51	البنك أقل استقرار ماليا (إحتمال التعثر)
ROA	51-0	البنك غير مستقر ماليا

Source (Permata & Purwanto, 2018, P.1315)

ويرى الباحث أن تلك النماذج تساهم بشكل كبير في قياس الإستقرار المالي في البنوك ، ولكن يجب أن يؤخذ في الحسبان العوامل الخارجية مثل الظروف الإقتصادية والإجتماعية والسياسية التي تمر بها الدول في الحسبان نظراً لتأثيراتها الكبيرة على الإستقرار المالي للبنوك ، هذا بالإضافة إلى أن المخاطر السيبرانية ومدى قوة البنك في التعامل معها والحد منها يمكن أن تؤثر في الإستقرار المالي للبنك من عدمه ، وسوف يقوم الباحث في المبحث التالي بتناول طبيعة مخاطر وتهديدات الأمن السيبراني في البنوك الإلكترونية .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية) المحور السادس : طبيعة مخاطر وتهديدات الأمن السيبراني في البنوك الإلكترونية.

يصاحب تقديم العمليات البنكية الإلكترونية مخاطر متعددة وقد أشارت لجنة بازل للرقابة البنكية في هذا الشأن إلى أنه ينبغي قيام البنوك بوضع السياسات والإجراءات الكافية التي تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها (العباسي والهاشمي ، 2018 ، ص ص 1-22)
1/6 أسباب تعرض البنوك الإلكترونية للمخاطر السيبرانية :

أكدت دراسة كل من (Antoine, 2018, Pp.6-14) ; البغدادي ، 2021 ، ص ص 1438 – 1440 على أن البنوك الإلكترونية تتعرض لمجموعة من المخاطر والتهديدات ذات الصلة بالأمن السيبراني يمكن عرضها في الآتي:

1/1/6 إستهداف البنية التحتية للبنك الإلكتروني أو تعطيل عمله : تشمل البنية التحتية في أي قطاع مالي أنظمة الدفع والتسوية ومنصات التداول وودائع الأوراق المالية المركزية والأطراف المقابلة المركزية ، وتعتبر البنية التحتية للقطاعات المالية في الدول خاصة النامية منها نقطة الضعف الرئيسة في فشل الأمن السيبراني لهذه القطاعات ، والذي قد يتحقق نتيجة لتهاك أو تعطل عمل البنية التحتية للقطاع ذاته ، أو لمجموعة من المنظمات المالية الرئيسة في القطاع نتيجة لتركز المخاطر أو عدم وجود بدائل ، الأمر الذي يترتب عليه إضطرابات كبيرة في سير العمل بالقطاع المالي والحد من ثقة العملاء في البنوك فعلى سبيل المثال في 27 يونيو 2014 شهد أكبر بنك محلي في بلغاريا FIB أزمة مالية حيث وجد أن هناك رسائل بريد إلكتروني مخادعة تشير إلى أن FIB يعاني من نقص في السيولة ، الأمر الذي ترتب عليه بلوغ التدفقات النقدية الخارجة في ذلك اليوم 10% من إجمالي الودائع لدى البنك مما أثر بشكل كبير على الموقف المالي للبنك .

2/1/6 إستغلال الثغرات : ويسمى أيضاً بالهجوم دون إنتظار Zero Day Attack وهو عبارة عن إستغلال نقاط الضعف في البرمجيات وثغراتها الأمنية خاصة غير المعروفة وغالبا ما يتم إستغلال هذه الثغرات من قبل المهاجمين قبل أن تكتشف الجهات المطورة برامج تصحيحية تعمل على مواجهتها.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

3/1/6 إختراق البيانات : حيث تتعرض المنظمات المالية بشكل خاص لإنتهاكات البيانات نظراً لإعتمادها على بيانات العميل في إدارة الأعمال ، فقد مر القطاع المالي في العديد من الدول النامية والكبرى أيضاً بحوادث إختراق البيانات أو فقدانها في السنوات الأخيرة ، فقد تم سرقة المعلومات الشخصية لأكثر من 147 مليون عميل في بنوك الولايات المتحدة خلال الفترة من عام 2018 وحتى عام 2020 ، والجدير بالذكر أنه يصعب تقييم الأثر الاقتصادي لانتهاكات البيانات نظراً لأن التأثيرات غير المباشرة (فقدان العملاء ، مخاطر السمعة) من المحتمل أن تكون أكثر أهمية من التأثيرات المباشرة (تكاليف الاسترداد والتقاضى) ، فقد تم إختراق أكثر من 260 مليون سجل في الولايات المتحدة وحدها بسبب الهجمات السيبرانية على القطاع المالي في تلك الفترة ، وقد قدرت الخسائر الناجمة عن خرق البيانات خلال هذه الفترة بحوالي 41 مليار دولار للشركات المالية الأمريكية وحدها (Kamiya et al., 2021, P. 732)

4/1/6 إستهداف الهواتف الذكية : والتي أصبحت وسيلة الاتصال السيبراني ودخول الكثير من العملاء على حساباتهم البنكية من خلالها أو إجراء عمليات البيع والشراء من خلال تلك الهواتف ويحاول المهاجمون تركيز إهتمامهم على إختراق هذه الأجهزة والتي ينشأ تهديدها نتيجة للأسباب التالية :

- أ- إن غالبية مستخدمي الهواتف الذكية ليس لديهم المعرفة الكافية بالثغرات الأمنية لهذه الهواتف .
- ب- إن المهاجمين دائماً ما يلجأون إلى التحايل على مالكي الهواتف الذكية لتوجيههم على تحميل تطبيقات تحت سيطرتهم .
- ج- يكمن خطر الهواتف الذكية في تطبيقاتها الخاصة بدخول العملاء من خلالها لحساباتهم البنكية الأمر الذي يتيح للمهاجمين فرصة الحصول على المعلومات البنكية أو إصابة النظام الإلكتروني للبنك بالفيروسات التي تعطل عمل النظام أو بعض أجزائه .

2/6 ضوابط وإستراتيجية البنوك في مواجهة مخاطر وتهديدات الأمن السيبراني :

أشارت دراسة كل من (الطاهر وورنيقي ، 2019 ، ص ص 275-282 ؛ Al-Moshaigh et al., 2019, P.38) إلى أن أهم الضوابط الأساسية في إدارة عمليات المخاطر السيبرانية البنكية الإلكترونية سواء لكل من البنك والعميل يمكن أن تكون على النحو التالي :

**أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
1/2/6 بالنسبة للبنك عند تقديم خدماته عبر شبكات الإتصال الإلكترونية :**

1/1/2/6 موافقة مجلس إدارة البنك على إستراتيجية تتضمن قيام البنك بتقديم خدماته عبر الشبكات على أن يحاط المجلس بكافة المخاطر السيبرانية الناشئة عن ذلك .

2/1/2/6 موافقة مجلس إدارة البنك على سياسة الإدارة التنفيذية للبنك فيما يتعلق بأسلوب إدارة المخاطر وتدعيم نظم الرقابة الداخلية بشأن تلك المخاطر .

3/1/2/6 تصميم نماذج عقود لتأدية مختلف الخدمات البنكية التي تؤدي عبر شبكات الاتصال الإلكترونية وأن يتأكد البنك من توافر القوى البشرية المؤهلة للتعامل مع عملاء البنك عبر الشبكات مع تحديد ساعات تقديم هذه الخدمات .

4/1/2/6 في حالة وجود طرف آخر تقدم من خلاله الخدمة فيتعين على مجلس إدارة البنك إقرار إتفاقية التشغيل التي تنظم العلاقة بين البنك مع هذا الطرف وتحديد مسؤوليته في الحفاظ على سرية التعليمات والمعاملات التي تتم عبر الشبكات وأية معلومات تتاح له .

5/1/2/6 الإفصاح على صفحة الـ Web الخاصة بالبنك بما يفيد حصوله على ترخيص بتقديم خدماته عبر الشبكات من البنك المركزي المصري ورقم وتاريخ الحصول على الترخيص والخدمات التي يجوز للبنك تقديمها عبر الشبكات مع ربط هذا الموقع بصفحة البنك المركزي المعلن فيها عن أسماء البنوك المرخص لها بذلك من خلال Hypertext links حتى يتحقق العملاء من صحة التصريح .

6/1/2/6 إفصاح البنك عن أن القوانين المصرية هي التي تحكم الخدمات التي يقوم بتأديتها للعملاء عبر الشبكات .

7/1/2/6 ضرورة أن يتحقق البنك من شخصية طالب / متلقي الخدمة بأساليب قانونية ثابتة تضمن الحقوق المتبادلة .

2/2/6 بالنسبة للعميل عند تلقي خدماته عبر شبكات الاتصال الإلكترونية :

1/2/2/6 يتحمل العميل مسؤولية صحة المعلومات التي يقوم بإدخالها عبر الشبكات بإعتباره مستخدماً للخدمات ، ويقر العميل بأن التعليمات والمعاملات التي يدخلها يتم التعامل عليها بدون أية مراجعة إضافية من البنك أو إشعارات خطية أو التأكد منها بطرق أخرى .

2/2/2/6 لا يلتزم البنك بقبول أية تعديلات أو إلغاء تعليمات أو معاملات سبق أن أرسلها العميل عبر الشبكات .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

3/2/2/6 يتحمل العميل مسؤولية إعداد البيانات الخاصة بالمستفيد أو الإضافة أو التعديل عليها .

4/2/2/6 يلتزم العميل بمراعاة إجراءات الحماية في التعامل عبر الشبكات مع البنك .

5/2/2/6 يتحمل العميل مسؤولية سوء استخدام الخدمة الناتج عن عدم الإلتزام بإجراءات الحماية والشروط والأحكام الواردة في العقد الذي يتم إبرامه مع البنك بشأن العمليات البنكية الإلكترونية أو الناتج عن قيامه بالكشف عن إجراءات الحماية أو مخالفتها لدى الاستخدام .

6/2/2/6 عدم تحمل البنك مسؤولية تعطل الخدمة لظروف خارجة عن إرادته .

7/2/2/6 تعتبر سجلات البنك حجة قاطعة ملزمة قانوناً على صحة المعاملات والتعليمات .

8/2/2/6 يلتزم العميل في حالة فقد أو سرقة جهاز الشفرة بإخطار البنك لكي يقوم بإبطال هذا الجهاز .

9/2/2/6 تعتبر أدوات الحماية وسيلة للتعرف والتحقق من شخصية العميل وبمجرد إتمام إدخالها بنجاح يعتبر العميل هو مصدر جميع التعليمات والمعاملات .

والجدير بالذكر أن إجراءات وضوابط المراجعة الداخلية كأحد الآليات الداخلية للحوكمة تلعب دوراً هاماً في الحد من المخاطر السيبرانية مما ينعكس بشكل كبير على دور المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على دعم الإستقرار المالي في البنوك الإلكترونية وهذا ما سوف يتناوله الباحث في المحور القادم .

المحور السابع : دور المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على دعم الإستقرار المالي في البنوك الإلكترونية .

نال موضوع إدارة مخاطر الأمن السيبراني والحوادث المتعلقة به إهتماماً بالغاً من جانب الباحثين والجهات المهنية والأكاديمية ، نظراً لتأثيره الكبير على قرارات بعض أصحاب المصالح مثل المحللين الماليين وكذلك على الأداء المالي للمنظمات وسمعتها ، وتعتبر مخاطر الأمن السيبراني من أكبر المخاطر التي تواجهها البنوك الإلكترونية ، حيث على غرار المخاطر المالية ومخاطر السمعة التي تتعرض لها المنظمات يمكن لمخاطر الأمن السيبراني أن تؤدي إلى إرتفاع التكاليف والتأثير السلبي على الإستقرار المالي ، وهذا ما أكدت عليه دراسة كل من (Kelton&Pennington, 2020, Pp. 152-155; Tuson, 2021,Pp.9-15 ;Frank et) al.,2019, Pp.183-200; Kamiya et al., 2021, Pp. 735-738 ص 32-17) .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

وفي سياق متصل فقد أكدت دراسة (AL- Moshaigeh et al., 2019, Pp. 37-39; Badawy, 2021,P.6) على أن الهجمات الإلكترونية تعتبر مكلفة وقد يكون لها تأثير شديد على الوضع المالي للمنظمة ، وقد تتسبب في تحريف جوهرى في سجلات المنظمة والحد من قدرة المنظمة على الإستمرار ، ولهذا السبب تعتبر مخاطر الأمن السيبراني ذات أهمية كبيرة في دعم الإستقرار المالي .

هذا وقد أكدت بعض الدراسات (Hilary el al., 2016, Pp. 1-59; Heroux & Anne, 2020, Pp. 73-100; Kelton & Pennington, 2020, Pp.147-153) يمكنها استخدام نظرية الإشارة Theory Signaling للحد من عدم تماثل المعلومات بين الإدارة وأصحاب المصالح من خلال إفصاح المنظمات عن تقرير إدارة مخاطر الأمن السيبراني ، وذلك لإرسال إشارات إيجابية لأصحاب المصالح حول الجهود المبذولة من المنظمة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية حيث أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني يمكن أصحاب المصالح من تقييم مدى قدرة المنظمة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل مما يدعم الإستقرار المالي لها .

والجدير بالذكر أن عملاء البنوك يهتمون بمخاوف مخاطر وجرائم الأمن السيبراني ، حيث يسعى مسؤولي البنوك إلى تخصيص المزيد من الموارد لمواجهة المخاطر السيبرانية وذلك نظراً لأن بعض العملاء يهتمون بالأبعاد والرؤى المستقبلية التي تتعلق بمخاطر الأمن السيبراني (Kelton & Pennington, 2020, Pp.138-150) .

وفي سياق متصل تتمثل متابعة المخاطر السيبرانية في البنوك الإلكترونية في إختبارات النظم التي تقوم بها إدارة المراجعة الداخلية في البنوك والتي تتمثل في : إجراء إختبار إمكان الاختراق penetration testing الذي يهدف إلى تحديد وعزل وتعزيز تدفق البيانات من خلال النظم ، وإتباع إجراءات لحماية النظم من المحاولات غير العادية للإختراق ، علاوة على إجراء مراجعة دورية من خلال النظم للتأكد من فاعلية إجراءات التأمين والوقوف على مدى إتساقها مع سياسات وإجراءات التأمين المقررة من قبل إدارة البنك ، هذا بالإضافة إلى مساهمة المراجعة الداخلية في تتبع الثغرات

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

وحالات عدم الكفاءة وتخفيض حجم المخاطر بهدف التحقق من توافر سياسات وإجراءات مطورة والتأكد من التزام البنك بها .

وبناء على ما سبق وفي ظل مشكلة البحث وأهميته وتحقيقاً لأهدافه يمكن صياغة فروض البحث على النحو التالي :

فروض البحث :

الفرض الأول الرئيسي : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين محددات جودة المراجعة الداخلية والحد من مخاطر الأمن السيبراني .

وينبثق من هذا الفرض الفروض الفرعية التالية :

الفرض الفرعي الأول : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين المقدرة المهنية لفريق المراجعة الداخلية والحد من مخاطر الأمن السيبراني .

الفرض الفرعي الثاني : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية والحد من مخاطر الأمن السيبراني .

الفرض الفرعي الثالث : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين جودة تنفيذ المهام والحد من مخاطر الأمن السيبراني .

الفرض الفرعي الرابع : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين حجم قسم المراجعة الداخلية ودعم الإدارة والحد من مخاطر الأمن السيبراني .

الفرض الثاني : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين الحد من مخاطر الأمن السيبراني والإستقرار المالي .

وبعد أن قام الباحث بإستعراض فروض البحث فسوف يقوم الباحث في الجزء التالي بإعداد الدراسة الميدانية وإختبار الفروض السابقة .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية) المحور الثامن : دراسة ميدانية .

تستهدف الدراسة الميدانية معالجة مشكلة الدراسة واختبار الأهداف والتساؤلات احصائياً من خلال تفسير العلاقة بين المتغيرات المستقلة المتمثلة في: المقدرة المهنية لفريق المراجعة الداخلية، ومشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية، وجودة تنفيذ المهام، حجم قسم المراجعة الداخلية ودعم الإدارة وبين المتغير التابع المتمثل في: الحد من مخاطر الأمن السيبراني ، بالإضافة إلي تحليل العلاقة بين مخاطر الأمن السيبراني ودعم الاستقرار المالي وذلك بالتطبيق على البنوك الإلكترونية.

1/8 مجتمع وعينة الدراسة الميدانية:

يتمثل مجتمع الدراسة في كافة العاملين بالادارات المختلفة للبنوك التجارية العاملة في جمهورية مصر العربية على مستوى الجمهورية ، والجدير بالذكر أن مفردات المجتمع في هذه الدراسة يتجاوز 10000 فرد، فضلاً عن صعوبة الوصول اليهم على مستوى فروع البنوك المختلفة بالجمهورية ، ومن ثم يمكن للباحث الاعتماد على أسلوب المعاينة الإحصائية واختيار عينة عشوائية بشرط ألا تقل عن 384 مشاهدة ، وذلك بناء على ما جاء بقانون حجم العينة - (Weijters et al., 2021,Pp85-103) .

وبالتالي، قام الباحث بصياغة وتصميم قائمة الاستبيان موجهة إلي كافة العاملين بالادارات المختلفة بتلك البنوك الإلكترونية، واعتمد الباحث على توزيع قائمة الاستبيان على المستقضي منهم إلكترونياً من خلال تصميم Google Form، وذلك اعتماداً على العينة العشوائية المنتظمة (كل خمسة أفراد تم التواصل مع واحد منهم). وفي هذا الصدد، تم توزيع الاستبيان على مجموعة من المستقضي منهم بمجتمع الدراسة وقد بلغ عددهم 485 فرد، فقط 448 منهم من قبل الاجابة على الاستبيان، وباستبعاد 55 استبيان مفقود البيانات (اجابات منقوصة) وقد تبين أن العينة النهائية صالحة التحليل تبلغ 393 مشاهدة. وبالتالي يمكن للباحث بيان اجراءات اختيار وتوزيع العينة من خلال الجدول التالي:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
جدول رقم (1-8): اجراءات تحديد عينة الدراسة

الادارة	الاستبيانات الموزعة	الاستبيانات المستلمة	نسبة المستلمة إلي الموزعة	الاستبيانات غير المستلمة	نسبة غير المستلمة إلي الموزعة	استبيانات بدون استجابة	استبيانات غير مكتملة	العينة النهائية	نسبة العينة النهائية إلي الموزعة
ادارة المراجعة الداخلية	١١٢	١٠٥	%٩٣,٧٥	٧	%٦,٢٥	٩	٩	٨٧	%٧٧,٦٨
ادارة الائتمان	١٣٥	١٢٧	%٩٤,٠٧	٨	%٥,٩٣	٥	٧	١١٥	%٨٥,١٩
ادارة المخاطر	١٠٧	٩٧	%٩٠,٦٥	١٠	%٩,٣٥	٨	٤	٨٥	%٧٩,٤٤
ادارة خدمة العملاء	٨٧	٨١	%٩٣,١٠	٦	%٦,٩٠	٦	٠	٧٥	%٨٦,٢١
ادارة تكنولوجيا المعلومات	٤٤	٣٨	%٨٦,٣٦	٦	%١٣,٦٤	٤	٣	٣١	%٧٠,٤٥
الاجمالي	٤٨٥	٤٤٨	%٩٢,٣٧	٣٧	%٧,٦٣	٣٢	٢٣	٣٩٣	%٨١,٠٣

وتأسيساً على العرض السابق لعينة الدراسة يتبين للباحث أن العينة النهائية للدراسة هي (٣٩٣) مفردة صالحة للتليل.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
2/8 مقاييس متغيرات الدراسة:

تحتوي هذه الدراسة على ستة متغيرات رئيسية تتمثل في:

- المتغير الأول: المقدرة المهنية لفريق المراجعة الداخلية: ويتم قياسه من خلال تصميم مقياس اعتماداً على المقاييس الأكثر استخداماً في الدراسات السابقة والتي ثبت صدقها وثباتها ويتضمن هذا المقياس ٥ عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي. ويمكن للباحث عرض المتغير وكيفية قياسه من خلال الجدول رقم (8-2) التالي :

جدول رقم (8-2): مقياس المقدرة المهنية لفريق المراجعة الداخلية

المتغير	العبرة
المتغير الأول: المقدرة المهنية لفريق المراجعة الداخلية	توافر المؤهلات العلمية اللازمة لإنجاز المهام.
	توافر الشهادات المهنية المناسبة لإنجاز المهام.
	توافر الخبرة والمعرفة اللازمة لعمليات المنظمة .
	توافر المعرفة التكنولوجية لإنجاز المهام.
	توافر عدد ساعات تدريب وتعليم مستمر لإنجاز المهام.

المصدر: اعداد الباحث

- المتغير الثاني: مشاركة المراجعة الداخلية في ادارة المخاطر المؤسسية: ويتم قياسه من خلال تصميم مقياس اعتماداً على المقاييس الأكثر استخداماً في الدراسات السابقة والتي ثبت صدقها وثباتها ويتضمن هذا المقياس ٥ عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي. ويمكن للباحث عرض المتغير وكيفية قياسه من خلال الجدول رقم (8-3) التالي:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
جدول رقم (3-8): مقياس مشاركة المراجعة الداخلية في ادارة المخاطر المؤسسية

المتغير	العبرة
المتغير الثاني: مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	القيام بالتحديث والمتابعة الدورية لمختلف أطر المخاطر التي تتعرض لها المنظمة .
	المساهمة في تقديم توصيات ومقترحات للإدارة بشأن الحد المقبول من المخاطر .
	تقديم المشورة لإدارة المنظمة بشأن تحديد أفضل الطرق لتحقيق الأهداف في ظل المخاطر التي تمر بها المنظمة.
	تطوير وتنمية الإستراتيجيات المتبعة لإدارة المخاطر.
	تقديم التقارير المتعلقة بمدى صدق إدارة المخاطر بالمنظمة في إعداد تقاريرها.

المصدر: اعداد الباحث

- المتغير الثالث: جودة تنفيذ المهام: ويتم قياسه من خلال تصميم مقياس اعتماداً على المقاييس الأكثر استخداماً في الدراسات السابقة والتي ثبت صدقها وثباتها ويتضمن هذا المقياس ٥ عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي. ويمكن للباحث عرض المتغير وكيفية قياسه من خلال الجدول رقم (٤-٨) التالي:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
جدول رقم (4-8): مقياس جودة تنفيذ المهام

المتغير	العبرة
المتغير الثالث: جودة تنفيذ المهام	وجود نظام لرقابة جودة الأداء .
	بذل العناية المهنية الواجبة تجاه أداء المهام.
	تحديد الإجراءات التي يجب إتباعها في عمليات التخطيط والتوثيق والمشورة .
	الإلتزام بالمعايير المهنية المتعارف عليها .
	السعي نحو المحافظة على الجودة وإستمرارية تحسينها.

المصدر: اعداد الباحث

- المتغير الرابع: حجم قسم المراجعة الداخلية ودعم الإدارة: ويتم قياسه من خلال تصميم مقياس اعتماداً على المقاييس الأكثر استخداماً في الدراسات السابقة والتي ثبت صدقها وثباتها ويتضمن هذا المقياس ٦ عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي. ويمكن للباحث عرض المتغير وكيفية قياسه من خلال الجدول رقم (٥-8) التالي:

جدول رقم (5-8): مقياس حجم قسم المراجعة الداخلية ودعم الإدارة

المتغير	العبرة
المتغير الرابع: حجم قسم المراجعة الداخلية ودعم الإدارة	عدد مرات الإجتماعات مع لجان المراجعة .
	المساهمة في تفعيل عمليات الحوكمة وتحقيق أهدافها .
	العمل على إدارة وإكتشاف المخاطر .
	تقديم تأكيد موضوعي إلي مجلس الإدارة عن مدى فعالية أنشطة الإدارة الشاملة للمخاطر .
	التأكد من أن نظام الرقابة يعمل بفعالية.
	توافر الدعم والتمويل والتعاون الكافي من الإدارة العليا .

المصدر: اعداد الباحث

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

- المتغير الخامس: مخاطر الأمن السيبراني: ويتم قياسه من خلال تصميم مقياس اعتماداً على المقاييس الأكثر استخداماً في الدراسات السابقة والتي ثبت صدقها وثباتها ويتضمن هذا المقياس ١٢ عبارة تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي. ويمكن للباحث عرض المتغير وكيفية قياسه من خلال الجدول رقم (8-6) :

جدول رقم (8-6): مقياس مخاطر الأمن السيبراني

المتغير	العبارة
المتغير الخامس: مخاطر الأمن السيبراني	تعدّ البرامج الضارة أكثر أشكال مخاطر الأمن السيبراني انتشاراً، ويقصد بها البرامج الضارة أو الفيروسات التي تعمل على تثبيت نفسها تلقائياً على نظام مستهدف
	قد تتعرض الحسابات الإلكترونية للاختراق من قبل شخص مجهول، وذلك من خلال قيامه بسرقة كلمة المرور، إما عن طريق تخمينها، أو استخدام برامج اختراق.
	يُعرف قطع واعتراض الازدحام بالتنصت أيضاً، ويقصد به قيام طرف ثالث غير مرغوب به بالتنصت على المعلومات التي يشاركها شخص ما مع آخر مضيف، فيؤدي ذلك إلى سرقة المعلومات، وكلمات المرور الخاصة به
	تعدّ هجمات التصيد من الطرق القديمة التي تهدد الأمن السيبراني، وذلك عن طريق قيام طرف مجهول بإرسال رسالة، أو بريد إلكتروني إلى الشخص المستهدف، ويطلب فيها معلومات خاصة، مثل: كلمة المرور، أو النقر فوق رابط مرفق يؤدي لسرقة معلومات مهمة.
	يقصد برفض الخدمة الموزعة استهداف الخوادم وتحميلها بشكل زائد، مما يجعلها غير قادرة على معالجة الطلبات التي تصل إليها، وخاصة كلمات مرور المستخدمين، فيؤدي ذلك إما لإغلاق الموقع الإلكتروني المستخدم، أو تباطؤ عمله، مما يجعله غير قابل للاستخدام

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

تشفير قواعد البيانات، مما يؤدي إلي تعطيل الخدمات التي يستخدمها الشخص، أو سرقة معلوماته، ويرمز لمثل هذه الهجمات بالرمز (XXS)
هجمات تستهدف نظام، أو شبكة، أو برنامج بعد اكتشاف ثغرة أمنية فيها تمّ التغاضي عنها، وذلك بإحداث سلوك غير مرغوب به في العنصر المستهدف، أو إتلاف البيانات المستهدفة، أو سرقة المعلومات.
وصول طرف خارجي غير مرغوب به إلي معلومات مهمّة لا يُقصد بأن تكون متاحة للآخرين.
إرسال طلبات صداقة من أشخاص مجهولين، أو إرسال رسائل، أو بريد إلكتروني، ويستخدم الطرف المهاجم معلومات خاصّة بالمستخدم المستهدف يحصل عليها من وسائطه الاجتماعية
برامج الفدية والتي نوع من أنواع البرامج الضارة التي تعمل على تثبيت نفسها على نظام أو شبكة مستخدم مستهدف، وتتسبب بمنع وصول المستخدم للوظائف على جهازه، إمّا بصورة كليّة أو جزئيّة، وعندها يطلب الطرف المهاجم فدية لإزالة هذه البرامج الضارة المثبتة على النظام
تثبيت برامج ضارة على جهاز المستخدم المستهدف، ممّا يجعل النظام يخرج العملات المشفرة بشكل تلقائي، وعادةً ما يستهدف هذا النوع من البرامج الأنظمة غير المحميّة، كما أنّ عمليّة الحصول على الرموز المشفرة تتطلب العديد من الأجهزة
استهداف المواقع الإلكترونية التي تستخدم بشكل متكرر من قبل المؤسسات أو المنظمات، إذ يُحمّل الهجوم فيروسات وبرامج ضارة على المواقع المستهدفة

المصدر: من اعداد الباحث

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

- المتغير السادس: دعم الاستقرار المالي: ويتم قياسه من خلال تصميم مقياس اعتماداً على المقاييس الأكثر استخداماً في الدراسات السابقة والتي ثبت صدقها وثباتها ويتضمن هذا المقياس ٨ عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي. ويمكن للباحث عرض المتغير وكيفية قياسه من خلال الجدول رقم (٧-٨) التالي:

جدول رقم (٧-٨): مقياس دعم الاستقرار المالي

المتغير	العبرة
المتغير السادس: دعم الاستقرار المالي	يعتبر مؤشر الديون المتعثرة دليلاً هاماً في رصد الأزمات البنكية فوفقاً لمؤشر (Bankometer) يجب أن تكون النسبة أقل من ١٥٪ من إجمالي الديون.
	عندما يعرف الجمهور أن أحد البنوك أو بعضها في أزمة يسارع إلي سحب ودائعه من البنوك السليمة أو المصابة مما يؤدي إلي التسبب في أزمة.
	اختبار الضغط من أحدث الطرق المستخدمة في قياس هشاشة حافظة القروض البنكية أو النظام المالي بأكمله مقابل سيناريوهات افتراضية مختلفة.
	تحليل السيناريو يستند أساساً إلي أن السيناريوهات يمكن أن تكون إما أحداث تاريخية أو أحداث افتراضية. وهي تتحكم بالتأثير على الأحداث ذات الصلة من خلال عدد من عوامل الخطر.
	تعتمد طريقة قياس القيمة المعرضة للمخاطر VAR على تحليل مخاطر السوق باستخدام نماذج إحصائية من خلال حساب أقصى قيمة للخسائر التي يتوقع أن يتحملها البنك للمحافظ التي بحوزته في ظل الظروف الطبيعية خلال فترة زمنية معينة.
	العسر المالي هي المرحلة التي تكون فيها المؤسسة البنكية غير قادرة على سداد الالتزامات المترتبة عليها مع أن إجمالي الأصول لديها يفوق إجمالي التزاماتها.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

الفشل البنكي أحد مظاهر عدم الاستقرار المالي هي المرحلة التي تلي العسر المالي، والتي يكون فيها البنك قريباً من الإفلاس وعاجز عن سداد التزاماته، إضافة إلى كونه يعاني تراكمًا للخسائر بشكل كبير.
الإفلاس المالي هو عبارة عن إعلان قانوني بأن البنك في أزمة مالية لا يستطيع مقابلة حقوق الغير لديه، أو توقف أنشطته تمهيداً لتصفية أصوله وسداد الإلتزامات المستحقة عليه.

المصدر: من اعداد الباحث وفقاً للدراسات السابقة

٣/8 اختبارات الصدق والثبات:

يمكن للباحث اجراء اختبارات الصدق والثبات على النحو التالي:

أ. اختبارات الثبات:

قبل الدخول في التحليل نتأكد من جودة المقياس المستخدم وأن بنود كل محور لا يمكن حذفه أو الاستغناء عنه. ويقصد باختبار ثبات المقياس درجة الاتساق بين مقاييس الشيء المراد قياسه، والثبات يعني الاستقرار بمعنى لو كررت عمليات القياس للفرد الواحد لأظهرت النتائج شيئاً من الاستقرار، ويظهر الجدول التالي الثبات لبنود متغيرات المقياس:

جدول رقم (8-8): اختبار كرونباخ ألفا لقياس ثبات وصدق أداة الإستبيان

المتغيرات	ترتيب العبارات	عدد العبارات	قيمة معامل ألفا للثبات	قيمة معامل الصدق
المقدرة المهنية لفريق المراجعة الداخلية	من ١ : ٥	٥	٠,٨٩٧	٠,٩٤٧
مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	من ٦ : ١٠	٥	٠,٩٠٣	٠,٩٥٠
جودة تنفيذ المهام	من ١١ : ١٥	٥	٠,٨٨٥	٠,٩٤١
حجم قسم المراجعة الداخلية ودعم الإدارة	من ١٦ : ٢١	٦	٠,٩١٣	٠,٩٥٦
مخاطر الأمن السيبراني	من ٢٢ : ٣٣	١٢	٠,٨٠٩	٠,٨٩٩
دعم الاستقرار المالي	من ٣٤ : ٤١	٨	٠,٩٥٤	٠,٩٧٧
اجمالي قائمة الاستقصاء		٤١	٠,٩٨٥	٠,٩٩٢

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

يتبين للباحث من خلال الجدول السابق أن معامل الثبات كرونباخ ألفا وصدق أداة الإستبيان لكل أسئلة متغيرات أداة الإستبيان لأداة القياس تتمتع بدرجة عالية من الثبات والصدق لأنها أكبر من ٦٠٪ (بالنسبة إلي معامل كرونباخ ألفا) وأكبر من ٨٠٪ (بالنسبة إلي معامل الصدق) وبالتالي يعني هنالك إتساق داخلي لإجابات عبارات متغيرات أداة الإستبيان وجميع عبارات أداة الإستبيان بشكل عام.

ب. قياس مستوى الاتساق الداخلي بين العبارات والمحاور:

جدول رقم (8-9): بيرسون لقياس الاتساق الداخلي

الاجمالي المصحح	معامل الارتباط	معامل الثبات لو حذفت العبارة	رقم العبارة	المتغير
٠,٦٥٣	٠,٧١٢	٠,٧١٢	Q1	المتغير الأول: المقدرة المهنية لفريق المراجعة الداخلية
٠,٣٤٩	٠,٧٦٤	٠,٧٦٤	Q2	
٠,٣٩٣	٠,٨١٢	٠,٨١٢	Q3	
٠,٣٩٢	٠,٧٥٠	٠,٧٥٠	Q4	
٠,٤١٦	٠,٨١١	٠,٨١١	Q5	
٠,٦٥١	٠,٧٤٤	٠,٧٤٤	Q6	المتغير الثاني: مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية
٠,٦٥٢	٠,٧١٥	٠,٧١٥	Q7	
٠,٤٧٥	٠,٧٤٦	٠,٧٤٦	Q8	
٠,٦٤٨	٠,٧٧٧	٠,٧٧٧	Q9	
٠,٤٦٩	٠,٦٤٠	٠,٦٤٠	Q10	
٠,٤٤٤	٠,٨٠١	٠,٨٠١	Q11	المتغير الثالث: جودة تنفيذ المهام
٠,٣٤٠	٠,٦٤٥	٠,٦٤٥	Q12	
٠,٦٤٦	٠,٧٧٧	٠,٧٧٧	Q13	
٠,٦٧٥	٠,٨٠٥	٠,٨٠٥	Q14	
٠,٣٧٠	٠,٧٣٥	٠,٧٣٥	Q15	
٠,٣٥٩	٠,٦٦٠	٠,٦٦٠	Q16	

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

٠,٦٢٧	٠,٧٤٥	Q17	المتغير الرابع: حجم قسم المراجعة الداخلية ودعم الإدارة	
٠,٥٧٠	٠,٧١١	Q18		
٠,٤٢٢	٠,٦٤٤	Q19		
٠,٤٦٧	٠,٧٤١	Q20		
٠,٣٣٢	٠,٧٨٢	Q21		
٠,٤٥٦	٠,٦٧٥	Q22	المتغير الخامس: مخاطر الأمن السيبراني	
٠,٥٥٣	٠,٦٦٨	Q23		
٠,٥١٦	٠,٦٤١	Q24		
٠,٦٤٣	٠,٦٣٩	Q25		
٠,٣٢٠	٠,٧٤٣	Q26		
٠,٤٣٢	٠,٧٨٨	Q27		
٠,٤٥٠	٠,٧٨٥	Q28		
٠,٣٤١	٠,٧٩٨	Q29		
٠,٣٦٣	٠,٦٦١	Q30		
٠,٣٥١	٠,٦٨٦	Q31		
٠,٤٩٦	٠,٦٤٨	Q32		
٠,٦٣٤	٠,٧٧٦	Q33		
٠,٣٧٧	٠,٦٨٣	Q34		المتغير السادس: دعم الإستقرار المالي
٠,٤٣٣	٠,٧٩٨	Q35		
٠,٦٢٠	٠,٦٦٦	Q36		
٠,٣٧٦	٠,٧٩٢	Q37		
٠,٦٧٩	٠,٧٢٦	Q38		
٠,٤٢٨	٠,٨١٣	Q39		
٠,٤٣٩	٠,٦٨٢	Q40		
٠,٥٤٢	٠,٨٠٣	Q41		

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

يتضح لدى الباحث من خلال العرض السابق لنتائج ارتباط بيرسون بين كل عبارة من عبارات المحور والمتوسط العام للمحور ارتفاع مستوى الاتساق الداخلي لهذه العبارات داخل كل مقياس وذلك لأن كافة معاملات الارتباط أكبر من ٠,٣ .

٤/8 الإحصاء الوصفي:

قام الباحث بإجراء التحليل الوصفي للبيانات باستخدام برنامج الحزم الإحصائية SPSS لمتغيرات الدراسة، وذلك بهدف الوقوف على شكل وطبيعة البيانات والتعرف على قيمة المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة، ويمكن توضيح ذلك من خلال الجدول التالي:

جدول رقم (8-10): الإحصاءات الوصفية الإجمالية لمتغيرات الدراسة

الأبعاد والمتغيرات	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	معامل الالتواء	معامل التفرطح
المقدرة المهنية لفريق المراجعة الداخلية	3.67	0.93	25.25%	-0.407	-0.598
مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	3.81	0.91	23.83%	-0.458	-0.387
جودة تنفيذ المهام	3.62	0.90	24.97%	-0.258	-0.573
حجم قسم المراجعة الداخلية ودعم الإدارة	3.47	1.05	30.22%	-0.182	-0.896
مخاطر الأمن السيبراني	3.54	0.88	24.72%	-0.354	0.308
دعم الاستقرار المالي	3.20	1.00	31.16%	0.089	-0.818

يتبين للباحث من خلال النتائج سالفه العرض بالجدول السابق مجموعة من الملاحظات التي يمكن توضيحها فيما يلي:

- وجود ادراك من جانب عينة الدراسة حول متغيرات الدراسة، حيث جاءت قيمة الوسط الحسابي العام للمتغيرات جميعاً أكبر من الوسط الحسابي للمقياس والمعبر عنها ب (٣).
- جاء المتغير الثاني المتعلق بمشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية في المركز الأول بوسط حسابي قدره (٣,٨١). كما جاء المتغير الأول المتعلق بالمقدرة المهنية لفريق

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

المراجعة الداخلية في المركز الثاني بوسط حسابي قدره (٣, ٦٧). ويليهما في المركز الثالث المتغير الثالث المتعلق بجودة تنفيذ المهام بوسط حسابي قدره (٣, ٦٢). ثم في المركز الرابع المتغير الخامس الخاص بمخاطر الأمن السيبراني بوسط حسابي قدره (٣, ٥٤)، ويليه في المركز الخامس المتغير الرابع المتعلق بحجم قسم المراجعة الداخلية ودعم الإدارة وذلك بوسط حسابي قدره (٣, ٤٧) وأخيراً المتغير السادس المتعلق بدعم الاستمرار المالي وذلك بوسط حسابي قدره (٣, ٢٠).

٣. كما يتبين من نتائج معاملات الالتواء أنها تتراوح بين ± ٣ ، وأن معاملات التفرطح تتراوح بين ± ١٠ ، وهو ما يشير إلي اعتدالية البيانات واتباعها للتوزيع الطبيعي. وعلى مستوى العبارات داخل كل متغير من متغيرات قائمة الاستبيان فقد أسفرت نتائج التحليل الإحصائي عن الجدول التالي:

جدول رقم (8-11): الاحصاءات الوصفية التفصيلية للعبارات داخل متغيرات الدراسة

المتغير	رقم العبارة	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	معامل الالتواء	معامل التفرطح
المتغير الأول: المقدرة المهنية لفريق المراجعة الداخلية	Q1	4.25	0.77	18.12%	-0.826	-0.452
	Q2	4.32	0.55	12.73%	-0.101	-0.871
	Q3	4.42	0.83	18.78%	-0.381	-0.702
	Q4	4.43	0.91	20.54%	-0.575	-0.269
	Q5	3.9	0.67	17.18%	-0.168	-1.103
المتغير الثاني: مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	Q6	3.98	0.69	17.34%	-0.617	-0.522
	Q7	4.21	0.65	15.44%	-0.474	-0.981
	Q8	4.38	0.86	19.63%	-0.907	0.111
	Q9	4.23	0.48	11.35%	-0.656	-0.3
	Q10	3.89	0.83	21.34%	-0.711	-0.443
	Q11	4.29	0.84	19.58%	-0.636	-0.594

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

-1.232	-0.083	22.09%	0.91	4.12	Q12	المتغير الثالث: جودة تنفيذ المهام
-0.624	-0.449	16.89%	0.64	3.79	Q13	
-0.754	-0.426	16.83%	0.68	4.04	Q14	
-0.872	-0.269	17.48%	0.68	3.89	Q15	
-1.058	-0.214	11.36%	0.46	4.05	Q16	المتغير الرابع: حجم قسم المراجعة الداخلية ودعم الإدارة
-1.017	-0.064	21.21%	0.95	4.48	Q17	
-0.771	-0.249	17.93%	0.71	3.96	Q18	
-0.574	-0.045	12.20%	0.46	3.77	Q19	
-0.147	-0.634	11.39%	0.45	3.95	Q20	
-0.296	-0.662	22.17%	0.94	4.24	Q21	
-0.821	-0.312	22.12%	0.94	4.25	Q22	المتغير الخامس: مخاطر الأمن السيبراني
-0.413	-0.514	12.15%	0.52	4.28	Q23	
-0.481	-0.458	8.56%	0.38	4.44	Q24	
-0.91	-0.301	22.48%	0.87	3.87	Q25	
-1.176	0.159	19.41%	0.86	4.43	Q26	
-1.277	0.214	12.91%	0.51	3.95	Q27	
-1.002	0.275	16.09%	0.7	4.35	Q28	
-0.952	0.339	24.47%	0.93	3.8	Q29	
-1	0.118	24.48%	0.95	3.88	Q30	
-1.202	0.171	12.82%	0.55	4.29	Q31	
-0.83	-0.383	21.46%	0.91	4.24	Q32	المتغير السادس: دعم الإستقرار المالي
-0.494	-0.67	22.09%	0.93	4.21	Q33	
-0.448	-0.231	15.38%	0.66	4.29	Q34	
-0.788	-0.429	24.36%	0.95	3.9	Q35	
-0.972	0.122	15.90%	0.69	4.34	Q36	

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

-1.066	-0.228	16.74%	0.73	4.36	Q37
-0.639	-0.036	13.84%	0.62	4.48	Q38
-1.044	-0.29	9.81%	0.41	4.18	Q39
-1.061	-0.448	13.51%	0.55	4.07	Q40
-1.174	-0.129	9.16%	0.38	4.15	Q41

١- بالنسبة للمتغير الأول (المستقل) الخاص بالمقدرة المهنية لفريق المراجعة الداخلية يتضح

ارتفاع متوسط اراء عينة الدراسة حول العنصر (توافر المعرفة التكنولوجية لإنجاز المهام) وذلك بمتوسط (٤,٤٣) وانحراف معيارى (٠,٩١) وبمعامل اختلاف (٢٠,٥٤٪) أى ان معظم الاراء تتراوح ما بين موافق وموافق جداً وتميل إلى أن تكون موافق.

٢- بالنسبة للمتغير الثانى (المستقل) الخاص بمشاركة المراجعة الداخلية فى ادارة المخاطر

المؤسسية يتضح ارتفاع متوسط اراء عينة الدراسة حول العنصر (تطوير وتنمية الإستراتيجيات المتبعة لإدارة المخاطر) وذلك بمتوسط (٤,٣٨) وانحراف معيارى (٠,٨٦) وبمعامل اختلاف (١٩,٦٣٪) أى ان معظم الاراء تتراوح ما بين موافق وموافق جداً وتميل إلى أن تكون موافق.

٣- بالنسبة للمتغير الثالث (المستقل) الخاص بجودة تنفيذ المهام يتضح ارتفاع متوسط اراء عينة

الدراسة حول العنصر (وجود نظام لرقابة جودة الأداء) وذلك بمتوسط (٤,٢٩) وانحراف معيارى (٠,٨٤) وبمعامل اختلاف (١٩,٥٨٪) أى ان معظم الاراء تتراوح ما بين موافق وموافق جداً وتميل إلى أن تكون موافق.

٤- بالنسبة للمتغير الرابع (المستقل) الخاص بحجم قسم المراجعة الداخلية ودعم الادارة يتضح

ارتفاع متوسط اراء عينة الدراسة حول العنصر (المساهمة في تفعيل عمليات الحوكمة وتحقيق أهدافها) وذلك بمتوسط (٤,٤٨) وانحراف معيارى (٠,٩٥) وبمعامل اختلاف (٢١,٢١٪) أى ان معظم الاراء تتراوح ما بين موافق وموافق جداً وتميل إلى أن تكون موافق.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

٥- بالنسبة للمتغير الخامس (التابع) الخاص بمخاطر الأمن السيبراني يتضح ارتفاع متوسط آراء عينة الدراسة حول العنصر (يُعرف قطع واعتراض الازدحام بالتنتصت أيضاً، ويقصد به قيام طرف ثالث غير مرغوب به بالتنتصت على المعلومات التي يشاركها شخص ما مع آخر مضيف، فيؤدي ذلك إلي سرقة المعلومات، وكلمات المرور الخاصة به) وذلك بمتوسط (٤,٤٤) وانحراف معياري (٠,٣٨) وبمعامل اختلاف (٨,٥٦٪) أي ان معظم الآراء تتراوح ما بين موافق وموافق جداً وتميل إلي أن تكون موافق.

٦- بالنسبة للمتغير السادس الخاص بدعم الإستقرار المالي يتضح ارتفاع متوسط آراء عينة الدراسة حول العنصر (تعتمد طريقة قياس القيمة المعرضة للمخاطر VAR على تحليل مخاطر السوق باستخدام نماذج إحصائية من خلال حساب أقصى قيمة للخسائر التي يتوقع أن يتحملها البنك للمحافظ التي بحوزته في ظل الظروف الطبيعية خلال فترة زمنية معينة) وذلك بمتوسط (٤,٤٨) وانحراف معياري (٠,٦٢) وبمعامل اختلاف (١٣,٨٤٪) أي ان معظم الآراء تتراوح ما بين موافق وموافق جداً وتميل إلي أن تكون موافق.

بالإضافة إلي ذلك، يتبين انخفاض قيمة الانحراف المعياري مما يدل على انخفاض التباين في الآراء حول عناصر هذا المتغير من وجهة نظر عينة الدراسة، ويؤكد ذلك انخفاض قيمة معامل الاختلاف، فضلاً عن انخفاض معاملات الالتواء والتفرطح، وهو ما يشير إلي اتباع العينة للتوزيع الطبيعي.

٥/8 اختبار الفروض الإحصائية

يمكن للباحث اختبار فروض الدراسة في ضوء الأساليب الإحصائية التي تتناسب مع طبيعة الفرض، حيث أن الفروض الإحصائية للدراسة تعتمد على اجراء الاختبارات الإحصائية المتعلقة باستخدام تحليل الانحدار وتحليل المسار، ومن ثم سيقوم الباحث باجراء التحليل العملي أولاً للاستبيان، ثم اختبار الفروض الإحصائية للدراسة وذلك على النحو التالي:

- التحليل العملي الاستكشافي والتوكيدي:

باستخدام التحليل العملي الاستكشافي ببرنامج SPSS V.26 لعينة قوامها (٣٩٣ مفردة، ٤١ عبارة) موزعة إلي ٥ عبارة للمتغير الأول الخاص بالمقدرة المهنية لفريق المراجعة الداخلية، وه

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

عبارات للمتغير الثاني مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية، و ٥ عبارات للمتغير الثالث جودة تنفيذ المهام، و ٦ عبارات للمتغير الرابع حجم قسم المراجعة الداخلية ودعم الإدارة، و ١٢ عبارة للمتغير الخامس الخاصص بمخاطر الأمن السيبراني، وأخيراً ٨ عبارات لقياس دعم الاستقرار المالي. وكانت نتائج التحليل العملي على النحو التالي:

جدول رقم (8-12): نتائج مقياس KMO & Bartlett's Test لمتغيرات الدراسة

Bartlett's Test		معامل KMO	المتغيرات
مستوى المعنوية	مربع كاي		
٠,٠٠٠	١٣٣١,٨٩٧	٠,٧٥٦	المقدرة المهنية لفريق المراجعة الداخلية
٠,٠٠٠	١٣٠٠,١٣٧	٠,٧٠٨	مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية
٠,٠٠٠	١٣١٠,١٧٧	٠,٦٦٥	جودة تنفيذ المهام
٠,٠٠٠	١٣١٩,٣٩٦	٠,٧٤٥	حجم قسم المراجعة الداخلية ودعم الإدارة
٠,٠٠٠	١٣٦١,٦٠٦	٠,٧١٤	مخاطر الأمن السيبراني
٠,٠٠٠	١٣٢٥,٥٣١	٠,٦٣٧	دعم الاستقرار المالي

يوضح الجدول السابق أن مقياس KMO لكافة المتغيرات المدرجة بالدراسة أكبر من ٠,٥ بالإضافة إلي أن نتائج اختبار Bartlett's Test لكافة أبعاد ومتغيرات الدراسة معنوية، وبالتالي فإن البيانات ذات جودة عالية وصالحة لاجراء اختبار التحليل العملي الاستكشافي.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
ويوضح الجدول التالي رقم (8-13) نتائج التحليل الاحصائي فيما يخص صلاحية متغيرات
الدراسة للنموذج أحادي المستوى:

جدول رقم (8-13): صلاحية متغيرات الدراسة للنموذج أحادي المستوى

الصدق التقاربي		معامل التحميل	العبارات	المتغير
الثبات المركب CR	التباين المستخلص AVE			
0.776	0.745	0.731	Q1	المتغير الأول: المقدرة المهنية لفريق المراجعة الداخلية
		0.794	Q2	
		0.745	Q3	
		0.705	Q4	
		0.749	Q5	
0.767	0.739	0.698	Q6	المتغير الثاني: مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية
		0.724	Q7	
		0.763	Q8	
		0.735	Q9	
		0.775	Q10	
0.759	0.734	0.755	Q11	المتغير الثالث: جودة تنفيذ المهام
		0.723	Q12	
		0.754	Q13	
		0.753	Q14	
		0.683	Q15	
0.792	0.734	0.760	Q16	المتغير الرابع: حجم قسم المراجعة الداخلية ودعم الإدارة
		0.728	Q17	

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

		0.677	Q18	
		0.684	Q19	
		0.760	Q20	
		0.793	Q21	
0.886	0.737	0.698	Q22	المتغير الخامس: مخاطر الأمن السيبراني
		0.731	Q23	
		0.725	Q24	
		0.768	Q25	
		0.746	Q26	
		0.734	Q27	
		0.769	Q28	
		0.790	Q29	
		0.757	Q30	
		0.697	Q31	
		0.726	Q32	
		0.697	Q33	
0.858	0.755	0.738	Q34	المتغير السادس: دعم الإستقرار المالي
		0.758	Q35	
		0.746	Q36	
		0.773	Q37	
		0.784	Q38	
		0.728	Q39	
		0.751	Q40	
		0.761	Q41	

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
ويتضح لدى الباحث من النتائج المعروضة بالجدول السابق مجموعة الملاحظات التي يمكن
توضيحها فيما يلي:

- جميع المعاملات المعيارية مقبولة حيث يرى (Hair et al., 2014, Pp.106-121) أن قيم المعاملات المعيارية المقبولة لا بد وأن تكون مساوية أو أكبر من ٠,٥، ومن ثم لن يتم حذف أي عبارة من عبارات قائمة الاستقصاء.
 - أن قيم الصدق التقاربي المعبر عنه بمتوسط التباين المستخلص (AVE) والثبات المركب (CR) ذات قيم كبيرة، حيث كانت قيم الثبات المركب أكبر من ٠,٦، ومن ثم قبول الصدق التقاربي للنموذج وذلك لارتفاع متوسط التباين عن ٠,٥ حيث أن قيم AVE المقبولة لا بد وأن تكون مساوية أو أكبر من ٠,٥.
- وبناء على ما سبق تم اختبار الصدق التمايزي عن طريق الجذر التربيعي لمتوسط التباين المستخرج، وأظهرت نتائج التحليل الاحصائي والتي يوضحها الجدول رقم (٤-٥) أن جميع قيم (Square root of AVE) مقبولة حيث أن جميع قيم معاملات ارتباط كل بعد أو متغير بنفسه أكبر من ارتباطه بباقي متغيرات الدراسة الأخرى (Hair et al., 2010, Pp.514-527) مما يؤكد وجود صدق تمايزي واتساق عالي للمقاييس المستخدم في الدراسة.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
جدول رقم (8-14): مصفوفة الارتباط بين المتغيرات باستخدام الجذر التربيعي لـ (AVE)

المتغيرات	المقدرة	مشاركة	جودة تنفيذ	حجم قسم	مخاطر	دعم
	المهنية لفريق	المراجعة	المهام	المراجعة	الأمن	الاستقرار
	المراجعة	الداخلية في		الداخلية	السيبراني	المالي
	الداخلية	إدارة		ودعم		
		المخاطر		الإدارة		
		المؤسسية				
المقدرة المهنية لفريق	0.863					
المراجعة الداخلية						
مشاركة المراجعة	0.839	0.86				
الداخلية في إدارة						
المخاطر المؤسسية						
جودة تنفيذ المهام	0.794	0.833	0.857			
حجم قسم المراجعة	0.802	0.828	0.789	0.857		
الداخلية ودعم الإدارة						
مخاطر الأمن	0.801	0.817	0.785	0.813	0.858	
السيبراني						
دعم الاستقرار المالي	0.796	0.826	0.804	0.842	0.827	0.869

وللتأكيد على النتائج السابقة العرض تم تحليل السمة المغايره – السمة الاحادية في برنامج اموس لصدق التمايز The Heterotrait-Monotrait (HTMT) Analysis In AMOS، وتستخدم هذه الطريقة التحليلية لقياس صدق التمايز، وقد تم اشتقاقها من Multitrait-Multimethod Matrix، وتسمى مصفوفه السمات المتعدده أو الطرائق المتعدده لكامل وريبسك عام ١٩٥٩، وقد أسفرت نتائج التحليل الاحصائي عن المصفوفة التالية:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
جدول رقم (8-15): مصفوفة صدق التمايز باستخدام طريقة (HTMT)

المتغيرات	المقدرة المهنية لفريق المراجعة الداخلية	مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	جودة تنفيذ المهام	حجم قسم المراجعة الداخلية ودعم الإدارة	مخاطر الأمن السيبراني	دعم الاستقرار المالي
المقدرة المهنية لفريق المراجعة الداخلية						
مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	0.602					
جودة تنفيذ المهام	0.688	0.629				
حجم قسم المراجعة الداخلية ودعم الإدارة	0.724	0.714	0.690			
مخاطر الأمن السيبراني	0.736	0.623	0.712	0.696		
دعم الاستقرار المالي	0.722	0.628	0.729	0.717	0.593	

ويتضح من القيم المدرجة بالجدول السابق أنها جميعاً أقل من ٠,٨ لجميع المتغيرات وأكبر من ٠,٥ مما يشير إلى ارتفاع مستوى صدق التمايز بين متغيرات الدراسة.

• مؤشرات تطابق النموذج للقياس أحادي المستوى:

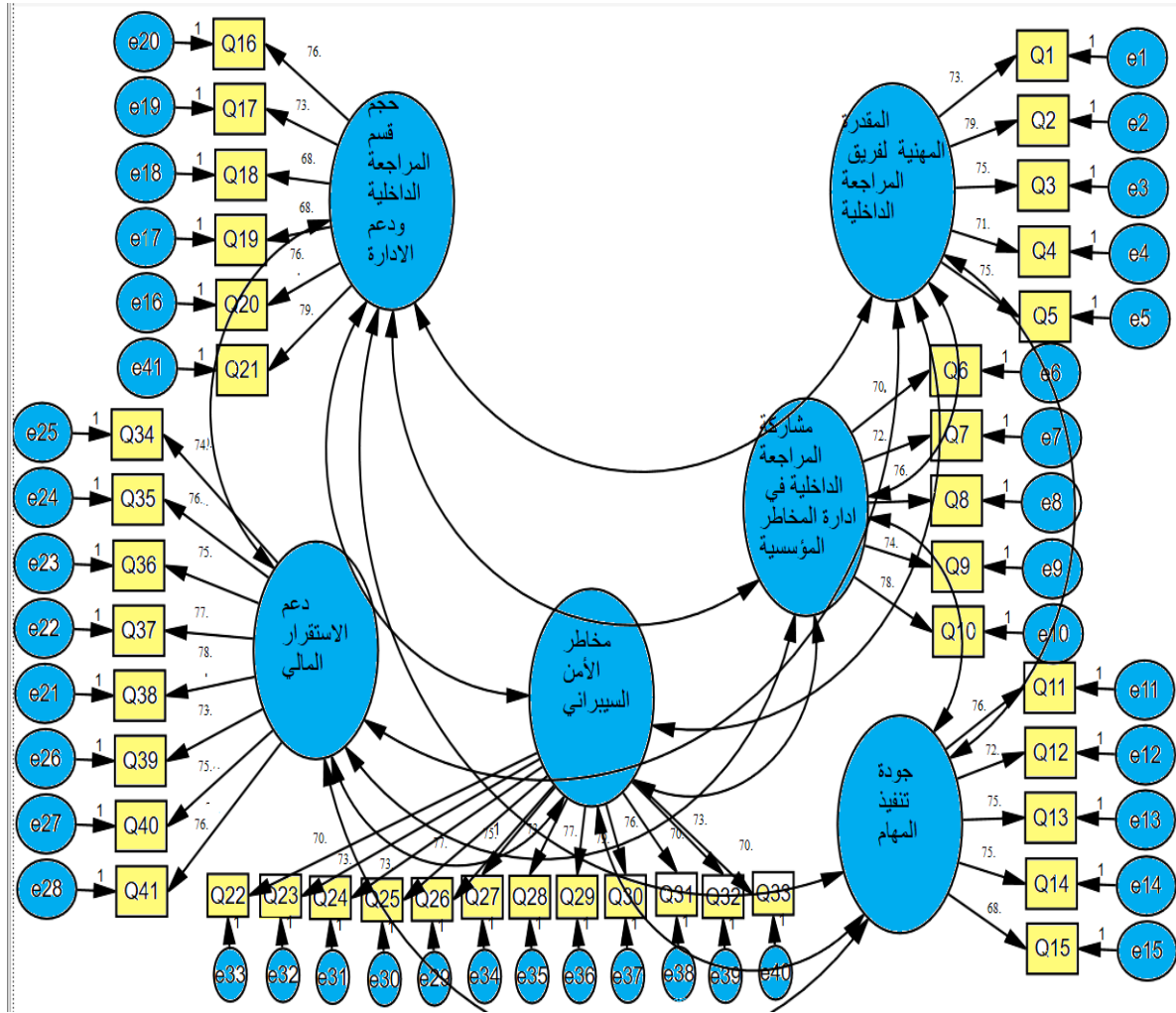
تعتبر عملية تطابق النموذج من العوامل الهامة في بناء وتقييم النموذج الهيكلي وذلك لأنه من خلالها يمكن التعرف على مدى تطابق النموذج النظري للدراسة مع النتائج الميدانية. ويمكن للتأكد من صحة نموذج القياس أحادي المستوى من خلال مؤشرات الجودة كما هو موضح في الجدول رقم (8-16) والشكل رقم (8-1) على النحو التالي:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
جدول رقم (8-16): مؤشرات جودة النموذج أحادي المستوى

مؤشر	الرمز الإحصائي	القيمة	مدى القبول	معيار القبول
جودة المطابقة	GFI	٠,٩٧ ٥	مقبول	كلما اقترب من الواحد الصحيح
جذر متوسط مربعات البواقي	RMR	٠,٠٤ ١	مقبول	كلما اقترب من الصفر
المطابقة المقارنة	CFI	٠,٩٧ ٣	مقبول	كلما اقترب من الواحد الصحيح
تاكر لويس	TLI	٠,٩٦ ٨	مقبول	كلما اقترب من الواحد الصحيح
الجذر التربيعي لمتوسط مربع الخطأ التقاربي	RMSEA	٠,٣٧ ٠	مقبول	أقل من ٠,٨

ويمكن توضيح المعاملات المعيارية للتحليل العاملي من خلال الرسم للنموذج أحادي المستوى
على النحو التالي:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

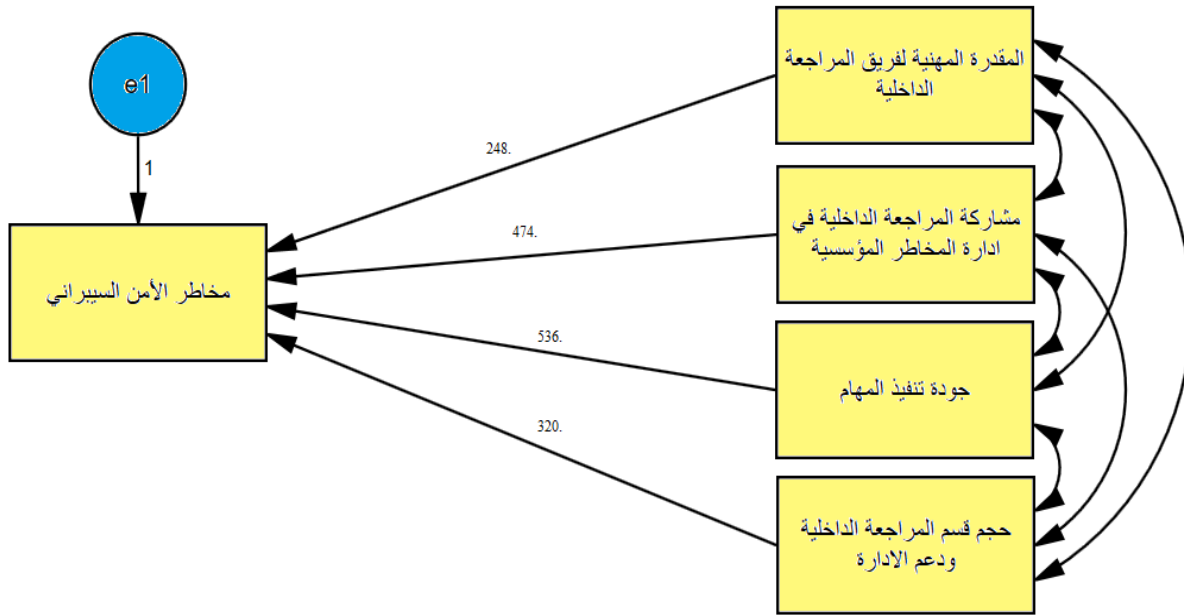


شكل رقم (1-8): نماذج القياس أحادي المستوى

١. النموذج الهيكلي للدراسة (نتيجة اختبار الفرض الاحصائي الأول للدراسة):

يمكن للباحث بناء النموذج الهيكلي للدراسة في ضوء النموذج الأحادي والذي من خلاله يمكن اختبار فروض الدراسة، ويستند بناء النموذج الهيكلي على المتغيرات والأبعاد التي أسفر عنها النموذج الأحادي القياس، وفي ضوء ما تم التوصل إليه من نتائج باستخدام AMOS V.26 يمكن توضيح النموذج الهيكلي الكلي من خلال الشكل التالي:

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)



شكل رقم (8-2): النموذج الهيكلي للدراسة

ومن خلال المؤشرات الإحصائية الموضحة بالجدول رقم (8-17) يمكن توضيح مؤشرات جودة النموذج الهيكلي على النحو التالي:

جدول رقم (8-17): مؤشرات جودة النموذج الهيكلي للدراسة

المؤشر	الرمز الاحصائي	القيمة	مدى القبول	معيار القبول
جودة المطابقة	GFI	0.968	مقبول	كلما اقترب من الواحد الصحيح
جذر متوسط مربعات البواقي	RMR	0.042	مقبول	كلما اقترب من الصفر
المطابقة المقارنة	CFI	0.974	مقبول	كلما اقترب من الواحد الصحيح
تاكر لويس	TLI	0.965	مقبول	كلما اقترب من الواحد الصحيح
الجذر التربيعي لمتوسط مربع الخطأ التقاربي	RMSEA	0.237	مقبول	أقل من ٠,٨

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

وفيما يتعلق باختبارات فروض الدراسة وفقاً للنتائج الإحصائية وذلك في ضوء النموذج

الهيكلية، ويمكن توضيحها في الجدول رقم (8-18) للتأثيرات المباشرة وذلك على النحو التالي:

جدول رقم (8-18): نتائج اختبارات التأثيرات المباشرة بين المتغيرات

النموذج الهيكلي			اتجاه الفرض		الفرض الفرعي	الفرض الرئيسي
النتيجة	قيمة المعنوية	معامل المسار				
قبول الفرض البديل	0.032	0.248	الحد من مخاطر الأمن السيبراني	المقدرة المهنية لفريق المراجعة الداخلية	ف ١ (أ)	الأول
قبول الفرض البديل	0.012	0.474	الحد من مخاطر الأمن السيبراني	مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	ف ١ (ب)	
قبول الفرض البديل	0.021	0.536	الحد من مخاطر الأمن السيبراني	جودة تنفيذ المهام	ف ١ (ج)	
قبول الفرض البديل	0.016	0.320	الحد من مخاطر الأمن السيبراني	حجم قسم المراجعة الداخلية ودعم الإدارة	ف ١ (د)	

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
وبناء على النتائج السابقة يمكن للباحث توضيح نتائج اختبارات الفروض المباشرة من
خلال العرض التالي:

أ- نتائج اختبار الفرض الأول:

ينص الفرض الأول على أنه "توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين محددات
جودة المراجعة الداخلية والحد من مخاطر الأمن السيبراني"، وينقسم هذا الفرض إلي الفروض
الفرعية التالية:

ف ١ (أ): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين المقدرة المهنية لفريق المراجعة الداخلية
والحد من مخاطر الأمن السيبراني.

ف ١ (ب): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين مشاركة المراجعة الداخلية في إدارة
المخاطر المؤسسية والحد من مخاطر الأمن السيبراني.

ف ١ (ج): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين جودة تنفيذ المهام والحد من مخاطر
الأمن السيبراني.

ف ١ (د): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين حجم قسم المراجعة الداخلية ودعم الإدارة
والحد من مخاطر الأمن السيبراني.

وفيما يلي عرض لنتائج اختبارات الفروض الفرعية:

• ف ١ (أ): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين المقدرة المهنية لفريق المراجعة
الداخلية والحد من مخاطر الأمن السيبراني.

وفقاً لنتائج التحليل الإحصائي يوجد تأثير معنوي إيجابي للمقدرة المهنية لفريق المراجعة
الداخلية على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٢٤٨، وهو دال
إحصائياً عند مستوى معنوية ٠,٠٣٢. وعليه يتضح للباحث قبول الفرض الفرعي الأول بوجود تأثير
معنوي إيجابي للمقدرة المهنية لفريق المراجعة الداخلية على الحد من مخاطر الأمن السيبراني، أي أن
زيادة المقدرة المهنية لفريق المراجعة الداخلية تؤدي إلي زيادة القدرة على الحد من مخاطر الأمن
السيبراني.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

- ف ١ (ب): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية والحد من مخاطر الأمن السيبراني.

وفقاً لنتائج التحليل الإحصائي يوجد تأثير معنوي إيجابي لمشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٤٧٤، وهو دال احصائياً عند مستوى معنوية ٠,٠١٢. وعليه يتضح للباحث قبول الفرض الفرعي الثاني بوجود تأثير معنوي إيجابي لمشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية على الحد من مخاطر الأمن السيبراني، أي أن زيادة لمشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية تؤدي إلي زيادة القدرة على الحد من مخاطر الأمن السيبراني.

- ف ١ (ج): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين جودة تنفيذ المهام والحد من مخاطر الأمن السيبراني.

وفقاً لنتائج التحليل الإحصائي يوجد تأثير معنوي إيجابي لجودة تنفيذ المهام على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٥٣٦، وهو دال احصائياً عند مستوى معنوية ٠,٠٢١. وعليه يتضح للباحث قبول الفرض الفرعي الثالث بوجود تأثير معنوي إيجابي لجودة تنفيذ المهام على الحد من مخاطر الأمن السيبراني، أي أن زيادة جودة تنفيذ المهام تؤدي إلي زيادة القدرة على الحد من مخاطر الأمن السيبراني.

- ف ١ (د): توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين حجم قسم المراجعة الداخلية ودعم الإدارة وبين الحد من مخاطر الأمن السيبراني.

وفقاً لنتائج التحليل الإحصائي يوجد تأثير معنوي إيجابي لحجم قسم المراجعة الداخلية ودعم الإدارة على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٣٢٠، وهو دال احصائياً عند مستوى معنوية ٠,٠١٦. وعليه يتضح للباحث قبول الفرض الفرعي الرابع بوجود تأثير معنوي إيجابي لحجم قسم المراجعة الداخلية ودعم الإدارة على الحد من مخاطر الأمن السيبراني، أي أن زيادة حجم قسم المراجعة الداخلية ودعم الإدارة تؤدي إلي زيادة القدرة على الحد من مخاطر الأمن السيبراني.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)
وتأسيساً على العرض السابق لنتائج اختبارات الفروض الفرعية، يمكن للباحث قبول الفرض الأول كلياً على الشكل البديل التالي:

الفرض الأول: توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين محددات جودة المراجعة الداخلية والحد من مخاطر الأمن السيبراني

ب- نتائج اختبار الفرض الثاني:

ينص الفرض الثاني على أنه " توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين الحد من مخاطر الأمن السيبراني ودعم الإستقرار المالي"، ويمكن للباحث استخدام أسلوب الانحدار البسيط للتعرف على مدى وجود تأثير للحد من مخاطر الأمن السيبراني على دعم الاستقرار المالي، وقد أسفرت نتائج التحليل الإحصائي عن التالي:

جدول رقم (8-19): تأثير الحد من مخاطر الأمن السيبراني على دعم الاستقرار المالي

النموذج	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	المعنوية	معامل التفسير	معامل الارتباط
الانحدار	٢٦٢,٧٢٨	١	٢٦٢,٧٢٨	٤٤١,٨١٥	٠,٠٠٠	٠,٥٨٢	٠,٧٦٣
البواقي	١٨٨,٥٠٦	٣٩٢	٠,٥٩٥				
الاجمالي	٤٥١,٢٣٤	٣٩٣					

$$ن = ٣٩٣$$

المصدر: نتائج التحليل الإحصائي

يتضح من الجدول السابق ما يلي:

- ثبوت معنوية نموذج الانحدار، حيث بلغت قيمة (ف = ٤٤١,٨٢) وذلك عند مستوى معنوية $\alpha = ٥\%$.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

- بلغ معامل التفسير (R^2) ٠,٥٨٢، وهذا يعني أن الحد من مخاطر الأمن السيبراني يفسر ٥٨,٢٪ من التغيير الذي يحدث في دعم الاستقرار المالي، والباقي ٤١,٨٪ يرجع لعوامل لم تدخل في النموذج.
- وجود تأثير معنوي ايجابي بين الحد من مخاطر الأمن السيبراني ودعم الاستقرار المالي، حيث بلغت قيمة المعنوية (٠,٠٠٠) وهي أقل من مستوى المعنوية ٥٪، ويرجع الباحث ذلك إلى وجود علاقة ارتباط طردية معنوية بينهما قدرها (٠,٧٦٣).
- في ضوء ذلك يتضح رفض الفرض العدم وقبول الفرض البديل الذي ينص على " توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين الحد من مخاطر الأمن السيبراني ودعم الإستقرار المالي"، ويمكن صياغة معادلة نموذج الانحدار بين المتغيرين كما يلي:

$$Y = a + \beta X + \varepsilon$$

$$Y = 0.102 + 0.958 X + 0.77$$

حيث إن Y هي دعم الإستقرار المالي، X هي الحد من مخاطر الأمن السيبراني، a ثابت الانحدار، ε هي الخطأ العشوائي لمعادلة الانحدار.

جدول رقم (8-20): ملخص نتائج تحليل الاضافي لاختبارات الفروض الأساسية

الفرض الرئيسي	الفرض	النتيجة	اتجاه العلاقة
الأول	الفرض الفرعي الأول: توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين المقدرة المهنية لفريق المراجعة الداخلية والحد من مخاطر الأمن السيبراني	قبول الفرض البديل	العلاقة طردية
	الفرض الفرعي الثاني: توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية والحد من مخاطر الأمن السيبراني.	قبول الفرض البديل	العلاقة طردية

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

العلاقة طردية	قبول الفرض البديل	الفرض الفرعي الثالث: توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين جودة تنفيذ المهام والحد من مخاطر الأمن السيبراني.	
العلاقة طردية	قبول الفرض البديل	الفرض الفرعي الرابع: توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين حجم قسم المراجعة الداخلية ودعم الإدارة وبين الحد من مخاطر الأمن السيبراني.	
العلاقة طردية	قبول الفرض البديل	توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين الحد من مخاطر الأمن السيبراني ودعم الإستقرار المالي	الثاني

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)
النتائج والتوصيات والتوجهات المستقبلية للبحث :

أولاً - النتائج :

في ضوء مشكلة البحث وأهميته وأهدافه وإعداد الدراسة الميدانية يمكن عرض النتائج التالية:

أ- النتائج النظرية :

- 1- تعد الطبيعة المتطورة للمخاطر السيبرانية غير قابلة للتنظيم بشكل محدد ، كما أن القضايا الخاصة بها يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات .
- 2- التطور الحادث في المخاطر السيبرانية يحفز المنظمات المالية وخاصة البنوك الإلكترونية على البحث المستمر والمكثف نحو إتخاذ إجراءات وقائية ضد تلك المخاطر ، من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك البنوك ، الأمر الذي يؤدي إلى دعم الإستقرار المالي في تلك البنوك .
- 3- تحتاج المراجعة الداخلية في معظم البنوك الإلكترونية الي توسيع قاعدة مهاراتها و اجتذاب مهارات فنية مؤهلة بكافة وسائل التعامل مع تقنيات التكنولوجيا .

ب- النتائج العملية :

- 1- أثبتت نتائج التحليل الإحصائي وجود تأثير معنوي إيجابي للمقدرة المهنية لفريق المراجعة الداخلية على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٢٤٨، وهو دال احصائياً عند مستوى معنوية ٠,٠٣٢ .
- 2- أثبتت نتائج التحليل الإحصائي وجود تأثير معنوي إيجابي لمشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٤٧٤، وهو دال احصائياً عند مستوى معنوية ٠,٠١٢ .
- 3- أثبتت نتائج التحليل الإحصائي وجود تأثير معنوي إيجابي لجودة تنفيذ المهام على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٥٣٦، وهو دال احصائياً عند مستوى معنوية ٠,٠٢١ .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

٤- أثبتت نتائج التحليل الإحصائي وجود تأثير معنوي إيجابي لحجم قسم المراجعة الداخلية ودعم الإدارة على الحد من مخاطر الأمن السيبراني، حيث بلغت قيمة معامل المسار ٠,٣٢٠، وهو دال إحصائياً عند مستوى معنوية ٠,٠١٦ .

٥- أثبتت نتائج التحليل الإحصائي ثبوت معنوية نموذج الانحدار، حيث بلغت قيمة (ف ٤٤١,٨٢) وذلك عند مستوى معنوية ٥٪.

٦- أثبتت نتائج التحليل الإحصائي أن معامل التفسير بلغ (R²) ٠,٥٨٢ وهذا يعني أن الحد من مخاطر الأمن السيبراني يفسر ٥٨,٢٪ من التغير الذي يحدث في دعم الاستقرار المالي، والباقي ٤١,٨٪ يرجع لعوامل لم تدخل في النموذج.

٧- أثبتت نتائج التحليل الإحصائي وجود تأثير معنوي إيجابي بين الحد من مخاطر الأمن السيبراني ودعم الاستقرار المالي، حيث بلغت قيمة المعنوية (٠,٠٠٠) وهي أقل من مستوى المعنوية ٥٪، ويرجع الباحث ذلك إلى وجود علاقة ارتباطية معنوية بينهما قدرها (٠,٧٦٣).

ثانياً – التوصيات :

- ١- وضع أسس لمراجعة وإدارة المخاطر السيبرانية ، والتحديد الدقيق لمسئوليات مختلف الجهات ذات العلاقة بها ، وما يستلزم ذلك من الحصول على ترخيص من البنك وموافاته بالبيانات اللازمة.
- ٢- ضرورة قيام الأجهزة الرقابية والمنظمات بتوفير الدورات التدريبية عالية المستوى وتنظيم الندوات وورش العمل والمؤتمرات بمشاركة جميع البنوك المتطورة في مجال تقنيات المعلومات، وذلك بهدف خلق كوادر فنية عالية قادرة على التصدي للتحديات الجديدة المرتبطة بهذه التقنيات وكيفية التغلب عليها .
- ٣- قيام الأجهزة الرقابية العربية بوضع آليات رقابية واضحة على البنوك والمنظمات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني .
- ٤- العمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين بقطاع البنوك بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

- ٥- ضرورة الإطلاع على التجارب الرائدة في مجال عمليات البنوك الإلكترونية وإدارة مخاطرها ومحاولة إستخراج نقاط القوة ومعرفة الإستفادة منها .
- ٦- تحتاج الدولة العربية للمزيد من الإستثمار في مجال الأمن السيبراني من خلال توطين التكنولوجيا والبنية التحتية السيبرانية وتطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة على بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها .
- ٧- ضرورة قيام ادارة المراجعة الداخلية بتقديم تقارير مستقلة الي مجلس الادارة ولجنة المراجعة تركز علي مجموعة واسعة من المخاطر و القضايا الرئيسية للمنظمة وخاصة فيما يتعلق بمخاطر الامن السيبراني ، الأمر الذي يترتب عليه دعم الإستقرار المالي .
- ٨- دعم وتعزيز المهارات الرقمية للموارد البشرية العاملة بالمنظمات بشكل خاص وللمراجعين الداخليين بصفة خاصة ، لضمان كفاءة وفعالية التعامل مع المخاطر السيبرانية والحد منها ، من خلال توفير دورات تدريبية ومنح دراسية وورش العمل بما يدعم الإستقرار المالي لتلك المنظمات .

ثالثاً – التوجهات المستقبلية للبحث :

- ١- التكامل بين المراجعة الداخلية والخارجية لتحقيق التميز المؤسسي بالوحدات الحكومية .
- ٢- التكامل بين المراجعة الداخلية والخارجية لدعم إدارة المخاطر الرقمية في البنوك الإلكترونية.
- ٣- أثر جودة المراجعة الداخلية للأمن السيبراني على جودة إعداد التقارير المالية في البنوك الإلكترونية .
- ٤- أثر فعالية المراجعة الداخلية للأمن السيبراني على الحد من الجرائم المالية .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

قائمة المراجع :

أولاً- قائمة المراجع العربية :

- ١- البغدادي ، مروة فتحى السيد ، (2021) ، اقتصاديات الأمن السيبراني في القطاع المصرفي ، مجلة البحوث القانونية والاقتصادية كلية الحقوق - جامعة المنصورة ، ع76 ، ص ص 1513 – 1446.
- ٢- البنك الدولي ، (2021) ، تعليمات ومؤشرات البنك الدولي بشأن المخاطر السيبرانية المصرفية .
- ٣- حسين ، رحيم ، ومعراج ، هوارى ، (2019) ، الصيرفة الإلكترونية كمدخل لعصرنة المصارف الجزائرية ، ملتقى المنظومة المصرفية الجزائرية والتحولات الاقتصادية واقع وتحديات ، ص ص 18-1 .
- ٤- خلف ، عمار حمد ، (2018) ، نحو قياس مؤشر تجميحي للاستقرار المصرفي في العراق للمدة 2010 – 2016 مجلة العلوم الاقتصادية والإدارية ، 24 (106) ، ص ص 250 – 270 .
- ٥- شحاتة ، السيد شحاتة ، (2020) ، إطار مقترح لإسناد وظيفة المراجعة الداخلية بدوريتها الاستشاري والتوكيد في مجال إدارة المخاطر في الوحدات الصغيرة ومتوسطة الحجم ،المجلة العلمية التجارة والتمويل ، كلية التجارة - جامعة طنطا ، 40 ، ص ص 109 – 128 .
- ٦- صالح ، نرمين محمد شاكر إبراهيم ، (2022) ، محددات فعالية المراجع الداخلي للأمن السيبراني ، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين ، كلية التجارة – جامعة الإسكندرية ، ص ص 1-24 .
- ٧- صندوق النقد العربي ، (2019) ، سلسلة موجز سياسات حول أمن الفضاء السيبراني في القطاع المصرفي ، العدد الرابع .
- ٨- ضيف ، علاء الدين توفيق إبراهيم ، (2016) ، دور المراجعة القضائية في الحد من التلاعب في بيئة المعلومات الرقمية للشركات دراسة ميدانية في بيئة الأعمال السعودية ، مجلة البحوث المحاسبية قسم المحاسبة – كلية التجارة – جامعة طنطا المجلد الثالث العدد الأول ، ص ص 496 – 554 .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية (دراسة ميدانية)

- ٩- الطاهر ، زدريك ، وورنيقي ، محمد ، (2019) ، إستراتيجية مكافحة الإرهاب الإلكتروني في المجال الاقتصادي ، المركز العربي الديمقراطي ، مجلة الدراسات الأفريقية وحوض النيل ، المجلد الثاني ، العدد الخامس ، ص ص 275-282 .
- ١٠- العباسي ، حسن صبحي ، والهاشمي ، ليلي عبدالكريم ، (2018) ، اتفاقية بازل مدخل للاستدامة المالية ، مجلة جامعة الموصل ، كلية الإدارة والإقتصاد – جامعة الموصل ، ص ص 1-22 .
- ١١- عبد اللطيف ، أسار فخري ، (2017) ، التعثر المالي المصرفي الأسباب وأساليب المعالجة العراق البنك المركزي العراقي ، ص ص 1 – 22 .
- ١٢- عثمان ، ياسمين مجدي رجب ، وصالح ، محمد أحمد محمد ، (٢٠٢١) ، تأثير تطبيق سياسات الشمول المالي على الإستقرار المالي للبنوك التجارية المتداولة بالبورصة المصرية ، مجلة الإسكندرية للبحوث المحاسبية قسم المحاسبة والمراجعة ، كلية التجارة – جامعة الإسكندرية ، العدد الأول ، المجلد الخامس ، ص ص ١-٢٨ .
- ١٣- العزي ، خالد ممدوح ، (2017) ، الجرائم المالية الإلكترونية الجرائم المصرفية أنموذجا بحث مقدم في المؤتمر الدولي الرابع عشر الجرائم الإلكترونية طرابلس لبنان ، ص ص 6-7 .
- ١٤- على ، محمود أحمد أحمد ، وعلي ، صالح علي صالح ، (2022) ، أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية (دراسة تجريبية) ، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين ، كلية التجارة – جامعة الإسكندرية ، ص ص 17-32 .

ثانياً – قائمة المراجع الأجنبية :

- 1- Abdul Karim N., and All, (2018) ,Measuring bank stability A comparative analysis between Islamic and conventional banks in Malaysia Proceedings of the 2 nd Advances in Business Research International conference springer Singapore, Pp. 169 – 177

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

- 2- Alina , C. M., Cerasela S.E., and Gabriela G, (2017) ,Internal audit role in cybersecurity ovidius university Annals Economic Sciences Series 17 (2) Pp. 510 – 513 .
- 3- Al-Moshaigeh, A., Dickins, D. and Higgs, J. (2019) , Cybersecurity Risks and Con-trols: Is the AICPA's SOC for Cybersecurity a Solution?, The CPA Journal, Vol. 89, Issue 6, Pp. 36-41.
- 4- Antoine, Bouveret , (2018) ,Cyber Risk for the financial sector : A Framework for Quantitative assessment working paper IMF , Pp.6-14.
- 5- Badawy, H., (2021) , The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study, Alexandria Journal of Accounting Research, 3 (5) Pp. 1-56.
- 6- Betti N., Sarens G., and Poncin, (2021) ,Effects of digitalisation of organisations on internal audit activities and practices Managerial auditing Journal Vol 36, No 6, Pp. 872 – 888
- 7- Christ M., Masli N., Sharip N., and Wood D., (2015) ,Rotational internal audit programs and financial reporting quality Do compensating controls help ? accounting Organizations and society Vol., 44 , Pp. 37 – 59.
- 8- Committee of sponsoring organizations of the treadway commission (COSO), (2019) ,Enterprise wide management (ERM) for Cybersecurity available at <http://www.coso.org/documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf>
- 9- Deloitte, Development LLC, (2017), Cyber security and role of internal audit an urgent call to action, available at www2.deloitte.com .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

- 10- Ege M., (2015) ,Does internal audit function quality deter management misconduct ? the accounting review Vol., 90 No., 2, Pp. 495 – 497.
- 11- Eling M. and J.H. wirfs , (2016), Cyber Risk : too big to insure ? Risk transfer options for a mercurial risk class institute of Insurance Economics Univesity of St. Gallen , Pp. 23-57 .
- 12- Emanuel, kopp, Lincoln, kaffenberger and christopher Wilson, (2017) ,cyber Risk market failures and financial stability working paper No. 17/185 IMF .
- 13- Florakis C.C. Louca, R. Michaely and M Weber, (2020) ,Cybersecurity Risk, Pp. 1-73, Available at <http://ssrn.com>
- 14- Frank, M., Grenier, J. and Pyzoha, J., (2019) , How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance, Journal of Information Systems, 33 (3) , Pp. 183-200 .
- 15- Hair, J.F., Sarstedt, M., Hopkins, L. and Kuppelwieser, V.G, (2014) ,Partial Least Squares Structural Equation Modeling (PLS-SEM): An Emerging Tool in Business Research. European Business Review, 26, Pp.106-121, <https://doi.org/10.1108/EBR-10-2013-0128>
- 16- Hair, Joseph , Black, William, Babin, Barry and Anderson, Rolph, (2010). Multivariate Data Analysis: A Global Perspective. London, Upper Saddle River, NJ: Pearson Education, Pp.1-761.
- 17- Hartmann C.C. and J. Carmenate, (2021) ,Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches Implications for Practice Policy and Research, American Accounting Association, 15 (2) Pp. 9 - 23 .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

- 18- Hassanpour s., Nazemi ardakani, (2017) ,The effect of pre-bankruptcy financial distress on earnings management tools International review of management and marketing 7 (3), Pp. 213 – 219 .
- 19- Heroux, S. and Anne, F., (2020) , Cybersecurity Disclosure by the Companies on the S&PTX 60 Index, Accounting Perspectives/Perspectives Compatibles, 19 (2), Pp. 73-100 .
- 20- Hilary, G., Segal, B., and Zhang, M., (2016) , Cyber-risk disclosure: Who cares? Research paper, Pp. 1-59, <https://papers.ssrn.com>.
- 21- Institute of internal auditors (IIA), (2013) ,international standards for the professional practice of internal auditing .
- 22- Institute of internal auditors (IIA), (2016) ,assessing cybersecurity Risk Roles of the three lines of Defense available at : guidance@theiia.org
- 23- Institute of internal auditors (IIA), (2017) ,international standards for the professional practice of internal auditing institute of internal auditors (IIA) report available at : guidance@theiia.org
- 24- Institute of internal auditors (IIA), (2020) ,North american pulse of internal audit available at <http://theiia.mkt5790.com/2020-pulse-of-internal-audit> .
- 25- International Accreditation Forum (IAF), (2021) , Available at: <https://iaf.nu/en/home/> .
- 26- ISACA, (2019) ,auditors have a role in cyber resilience ISACA Journal vol. 6 available at www.isaca.org
- 27- Islam M.S, Nusrat, Farah, Thomas F. and Stafford., (2018) ,Factors associated with security / cyber security audit by internal audit function an international study Managerial auditing journal , Pp. 377- 409, available at :10.1108/MAJ-07/2017-1595

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

- 28- Jan, A., and Marimuthu, M. (2015), Bankruptcy and Sustainability: A Conceptual Review on Islamic Banking industry. Global business and management research: an international journal, 7(1), Pp.109-138.
- 29- Ji O and All, (2018) ,Evaluation of financial soundness of selected commercial banks in Nigeria An application of Bankometer S-score model 2 (4) Journal – finance-marketing 2 (4) Pp. 22 – 25.
- 30- Kahyaoglu S.B and K. Caliyurt, (2018) ,Cyber security assurance process from the internal audit perspective managerial audit J. 33 (4) Pp. 360 – 376 available at <http://doi.org/10.1108/MAJ-02-2018-1804> .
- 31- Kamiya, S., Kang, J., Kim, J., and Stulz, R., (2021), Risk management, firm reputation, and the impact of successful cyberattacks on target firms, Journal of Financial Economics, Pp. 719–749 .
- 32- Kelton, A. and Pennington, R., (2020) , Do Voluntary Disclosures Mitigate the Cybersecurity Breach Contagion Effect?, Journal of Information Systems, 34 (3), Pp. 133-157.
- 33- Li H. W.G.No and T. Wang , (2018) ,SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors International Journal of Accounting Information Systems, 30, Pp.40 – 55
- 34- Marei, Elbadri and Eralp, Bektaş, (2017), "Measuring the Financial Stability of Islamic and Conventional Banks in Turkey," Springer Proceedings in Business and Economics, in: NESRIN ÖZATAÇ & Korhan K. GÖKMENOGLU (ed.), New Challenges in Banking and Finance, Pp. 115-137.

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

- 35- Onakoya a ., b., and Ayooluwa o.e, (2017) ,Bankruptcy and insolvency an exploration of relevant theories International Journal of economics and financial 7 (3) Pp706 – 712.
- 36- Permata M., and Purwanto E. (2018) ,analysis of CAMEL Z-score and Bankometer in Assessment Soundness of Banking Listed on the Indonesia Stock Exchange IDX from 2012 – 2015 Journal of Applied Economic Sciences 13 (5) 59 , Pp.1311 – 1324
- 37- Price water house Coopers (PWC), (2018) ,Internal Audit Available at www.pwc.org .
- 38- Shahimi S. and N. Mahzan, (2018) ,Building a research model and hypotheses development and findings of Exploratory Interviews International Journal of Management Excellence 10 (2) Pp. 1257 – 1283.
- 39- Steinbart P.J., Raschke R. L. Gal G and Dilla W.N. (2018) the influence of a good relationship between the internal audt and information security functions on information security outcomes accounting organizations and society Vol., 71 Pp. 15- 29 .
- 40- Tuson, O., (2021), Cyber-attacks and stock market activity, International Review of Financial Analysis,Pp.1-15.
- 41- Vighneswara, Swamy, (2014), "Bank regulation, supervision and efficiency during the global financial crisis," , University Library of Munich, Germany, Pp. 1-36 .
- 42- Vuko Tina, Sergeja Slapničar, Marko Čular, Matej Drašček, (2021) ,key drivers of cyber security audit effectiveness the neo- institutional perspective, Pp.1-43 available at <http://ssrn.com/abstract=3932177> .

أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار
المالي في البنوك الإلكترونية (دراسة ميدانية)

- 43- Weijters, Bert, Kobe Millet, and Elke Cabooter. (2021) , "Extremity in Horizontal and Vertical Likert Scale Format Responses. Some Evidence on How Visual Distance Between Response Categories Influences Extreme Responding" . International Journal of Research in Marketing, Vol.38, No.1, Pp .85-103.
- 44- Yang, L., Lau, L. and Jan, H. (2020) . Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management, Vol. 28 No. 1, Pp. 167-183.