مجلة البحوث المحاسبية

https://com.tanta.edu.eg/abj-journals.aspx

اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الأمن السيبراني على قرار منح الائتمان، الدور المعدل لنوع وخبرة مانح الائتمان : دراسة تجريبية.

السادة: نيفين صلاح علي علي مطر

مدرس، بقسم المحاسبة والمراجعة،كلية التجارة،جامعة الاسكندرية،مصر

تاريخ النشر الالكتروني: سبتمبر- 2024

للتأصيل المرجعي: مطر، نيفين صلاح علي علي. **اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الأمن السيبراني على قرار منح الائتمان، الدور المعدل لنوع وخبرة مانح الائتمان : دراسة تجريبية.**

، مجلة البحوث المحاسبية ، المجلد 11 (3)،

المعرف الرقمي: abj.2024.375921/10.21608

للتواصل مع المؤلف: Neveensalah@yahoo.com

اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الأمن السيبراني على قرار منح الائتمان، الدور المعدل لنوع وخبرة مانح الائتمان : دراسة تجريبية.

نيفين صلاح علي علي مطر

مدرس، بقسم المحاسبة والمراجعة،كلية التجارة، جامعة الاسكندرية،مصر

تاريخ المقال

تم استلامه 8 يوليو 2024، وتم قبوله في6 اغسطس 2024، هو متاح على الإنترنت سبتمبر 2024

ملخص البحث

استهدف البحث دراسة واختبار اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الأمن السيبراني على قرار منح الائتمان. وكذلك اثر نوع وخبرة مانح الائتمان كمتغيرين مُعدلين على العلاقة سالفة الذكر. ولتحقيق هدف البحث تم تحليل الدراسات السابقة لاشتقاق فروض البحث وفرعياته ثم تم اجراء دراسة تجريبية على عينة من المسئولين عن اتخاذ قرار منح الائتمان في البنوك التجارية المصرية. واظهرت نتائج **التحليل الأساسي** أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني لشركات تكنولوجيا المعلومات يؤثر **بصورة معنوية** على قرار منح الائتمان من حيث الموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه، **وبصورة غير معنوية** على معدل الفائدة على القرض. وأن الاثر المعدل لنوع وخبرة مانح الائتمان على العلاقة التأثيرية محل البحث في بيئة الأعمال المصرية كان معنوياً للموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه وغير معنوي على معدل الفائدة على القرض. وقد تم تعزيز تلك النتيجة من خلال إجراء التحليلات الأخرى.

الكلمات المفتاحية: الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني؛ قرار منح الائتمان؛ نوع مانح الائتمان وخبرته.

Abstract:

The research aimed to study and test the effect of of information technology companies' disclosure of Cybersecurity Risk Management Report on Credit Granting Decisions, **as well as** the effect of gender and experience of the credit grantor as a moderating variable on the aforementioned relationship. To achieve the aim of the research, previous studies were analyzed to derive the research hypotheses and its sub-hypotheses. Then, an experimental study was conducted on a sample of those responsible for making the decision to grant credit in Egyptian commercial banks. The results of **the main analysis** showed that disclosure the cybersecurity risk management report to information technology companies significantly affects Credit Granting Decisions in terms of approval to granting the credit loan and the amount of the loan that can be obtained, and in a non-significant the interest rate on the loan. And that The modifying effect of the gender and experience of the credit grantor on the influence relationship under study in the Egyptian business environment was significant for approval to granting the credit loan and the amount of the loan and insignificant for the interest rate on the loan. This result was reinforced by conducting **other analyzes.**

Keywords: Disclosure of the cybersecurity risk management report - Credit Granting Decisions - gender of credit grantor and his experience.

1- مقدمة البحث وأهدافه ومشكلته وحدوده وخطته

اصبح الآن الأمن السيبراني قضية حيوية لكل مؤسسة، وذلك نظراً لانتشار استخدام المؤسسات لتكنولوجيا المعلومات. إذ تعتمد العديد من الصناعات على الانترنت بما في ذلك الاتصالات السلكية واللاسلكية والخدمات المصرفية والمالية والطاقة والنقل وغيرها من الخدمات الحكومية الاساسية. كما ان القطاعين العام والخاص اصبحوا اكثر اعتماداً على التقنيات والشبكات القائمة على الويب في انظمة الإدارة المالية الخاصة بها (e.x., Harris et al., 2023). ونتيجة لذلك قد تتعرض الشركات للمخاطر والاختراقات السيبرانية أثناء المسار الطبيعي لأعمال الشركة (Sheneman, 2017; Harris et al., 2023). إذ في السنوات الاخيرة ارتفعت كمية وشدة اختراقات الأمن السيراني مثل؛ (1) اختراق Equifax في يوليو 2017 للمعلومات الشخصية 145 مليون فرد، (2) هجوم برنامج الفدية wannacry في مايو 2017عبر 150 دولة والذي ادى إلى اغلاق اكثر من 300 الف جهاز، (3) اختراق capital one في يوليو 2019 والذي اثر على بيانات 106 مليون عميل، (4) هجوم برامج الفدية في عام 2021 والذي اثر على حزمة برمجيات طورتها شركة kasya وهي شركة امريكية لتكنولوجيا المعلومات موزعة على 800 إلى 1500 شركة على مستوى العالم (Harris et al., 2023).

وتنشأ اختراقات الأمن السيبراني نتيجة فشل الشركات في حماية معلومات الملكية الخاصة بالعملاء والموظفين والموردين وأصحاب المصالح الآخرين. إذ تعتبر تلك المعلومات أصولاً غير ملموسة تسجل خارج الميزانية العمومية (مثل علاقات العملاء)، كما تعد تلك المعلومات ضرورية لأداء الشركة في المستقبل (Sheneman, 2017; Sheneman, 2022; Demek and Kaplan, 2023). وتكون الشركات اكثر عرضة للهجمات السيبرانية عندما تكون كبيرة الحجم، واقل عرضه للقيود المالية، واكثر قيمة، وعاملة في صناعات اقل قدرة على المنافسة، ولديها المزيد من الأصول غير الملموسة (Kamiya et al., 2021; Harris et al., 2023).

وتؤدي اختراقات الأمن السيبراني إلى العديد من الآثار السلبية مثل؛ خسائر في سمعة الشركة، وخسائر في ثروة المساهمين، وانخفاض فرص النمو المستقبلية للشركة، وانخفاض اسعار اسهم الشركات النظيرة Peer في الصناعة (Havakhor et al., 2020; Kamiya et al., 2021; Sheneman, 2022; Harris et al., 2023)، والحاق الضرر بالعملاء (إذ يؤدي إلى تعريض العملاء لخسائر في الخصوصية والتي يمكن ان تتراوح من الازعاج مثل تغيير كلمة المرور إلى الاحتيال مثل استخدام بيانات العملاء لارتكاب عمليات الاحتيال (Sheneman, 2017; Sheneman, 2022)، وارتفاع تكلفة التمويل (Demek and Kaplan, 2023)، وارتفاع تكليف التقاضي والغرامات، والتأثير السلبي على بقاء واستمرارية الشركات، وفقدان الملكية الفكرية، وانخفاض قيمة العلامة التجارية، وفقدان العلاقات مع العملاء (Sheneman, 2017; Sheneman, 2022; Demek and Kaplan, 2023).

ونتيجة لتزايد عدد اختراقات الأمن السيبراني ولما لها من آثار سلبية عديدة، قامت الشركات بالاستثمار بدرجات متفاوتة في مبادرات استراتيجية لإدارة مخاطر الامن السيبراني، حيث تهدف تلك المبادرات إلى حماية سرية[1] المعلومات وسلامتها[2] وتوافرها[3]، كما تشير هذه المبادرات أن الإدراة على دراية بمخاطر الامن السيبراني واتخذت الخطوات اللازمة لمعالجة والحد من هذه المخاطر. وعلى الرغم من أن هذه المبادرات تساعد على تقليل مخاطر الامن السيبراني إلا انها لاتقضي عليها بشكل تام. إذ إن اتخاذ خطوات لإدارة مخاطر الامن السيبراني لايضمن عدم حدوث اختراقات حتى مع وجود سياسات واجراءات قوية، حيث يمكن للمهاجمين المتطورين استغلال التهديدات ونقاط الضعف الجديدة، كما ان من المحتمل ان الشركة لم تقوم بتقييم المخاطر بشكل مناسب او لم يكن لدى الشركة موظفين مدربين بشكل مناسب للقيام بإدارة مخاطر الامن السيبراني مما يجعل الشركة عرضة للهجمات السيبرانية (Demek and Kaplan, 2023) ومن ثم فأن الشركات التي تتولى اهتماماً اكبر بإدارة مخاطر الامن السيبراني (من حيث وجود لجنة لإدارة المخاطر في مجلس الإداة) تكون اقل عرضة للهجمات السيبرانية ولكن لم تقم بمنعها تماماً (Kamiya et al., 2021).

وينظر اصحاب المصالح لمخاطر الأمن السيراني على انها تهديد متزايد يؤثر على الاداء المستقبلي للشركة، ومن ثم يطلب اصحاب المصالح معلومات اضافية حول حوادث الامن السيبراني وتحديداً تلك التي تنطوي على انتهاكات فعلية (Sheneman, 2022; Demek and Kaplan, 2023). فعلى سبيل المثال؛ يأخذ **المستثمرين غير المحترفين** في الاعتبار مخاطر الامن السيبراني عند اتخاذ قرار الاستثمار (Frank et al., 2023)، كما يقدر المستثمرين جهود الشركات في الانخراط بمبادرات إدارة مخاطر الامن السيبراني إذ يميلون إلى التفاعل بشكل إيجابي عند الاعلان عن الاستثمار في الامن السيبراني (شرف، 2023 ;2020 ,.Yang et al). وكذلك يأخذ البنوك في الاعتبار اختراقات الامن السيبراني للشركات عند تحديد كلاً من تكلفة الاقتراض وحجم وقيمة الضمانات المقدمة للقروض (e.x., Huang and Wang, 2021; Wang et al., 2023; Chatterjee et al., 2024)، كما يقدر البنوك جهود الشركات في الانخراط بمبادرات إدارة مخاطر الامن السيبراني، حيث يميل البنوك إلى انخفاض تكلفة الاقتراض وزيادة حجم القروض وتقليل حجم الضمانات المقدمة عند الحصول على القرض، وذلك عند الاعلان عن الاستثمار في الامن السيبراني (Havakhor et al., 2020).

[1] هي عدم اتاحة المعلومات أو اطلاع الاطراف غير المصرح لها على تلك المعلومات او عدم حصول الاطراف غير المسموح لها عليها (علي وفرج، 2024).

[2] وتعني ضمان ان تكون المعلومات دقيقة وصحيحة ومكتملة اثناء تخزينها ونقلها وان يتم تشغيلها بطرقة صحيحة، كما تتضمن السلامة خاصية امكانية الاعتماد على المعلومات اي لم يحدث بها اي تحريف ولم يتم التلاعب بها (علي وفرج، 2024).

[3] يعني ضمان ان تكون المعلومات متاحة للأطراف المصرح لها في الوقت المناسب والمكان المناسب (علي وفرج، 2024).

وقد اتضح للباحثة ان تلك الدراسات السابقة تمت في بيئات مختلفة عن البيئة المصرية، **ومن ثم تتمثل مشكلة البحث** في الإجابة على عدة تساؤلات رئيسة، نظريًا وعمليًا، هل يؤثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان؟ وهل يختلف تأثير افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان بإختلاف خبرة ونوع مانح الائتمان كمتغيرين مُعدلين للعلاقة محل البحث؟

ولذا **يستهدف هذا البحث** دراسة واختبار العلاقة بين افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان، وذلك في ظل وجود خبرة ونوع مانح الائتمان كمتغيرين معدلين للعلاقة سالفة الذكر، وسيتم تحقيق هذه الأهداف من خلال دراسة تجريبية.

وفي ضوء مشكلة البحث والهدف منه **تنبع أهمية هذا البحث** من تناوله لموضوع مهم؛ ألا وهو تأثير افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان، وذلك من خلال دراسة تجريبية. ويكتسب البحث أهميته الأكاديمية من خلال ندرة البحوث –في حدود علم الباحثة– التي تناولت تأثير الاختلافات والتشابهات في السمات النوعية والفنية لمانحي الائتمان وتحديداً نوع وخبرة مانح الائتمان على العلاقة محل الدراسة خاصة على المستوى المحلي، والتي ليست بنفس القدر من الاهتمام الذي حظي به في كثير من الدول المتقدمة.

وتتمثل اهم **دوافع البحث** في مسايرة الجدل الاكاديمي حول مدى تأثير افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان، والتغلب على الندرة الملموسة في البحوث التي تناولت الاثر التفاعلي لبعض السمات الفنية لمانحي الائتمان، كمتغيرات معدلة للعلاقة محل الدراسة، وكذلك ايجاد دليل عملى على مدى صحة تلك العلاقة من عدمه من خلال اتباع منهجية بحث متكاملة تشمل كلاً من التحليل الاساسي، والتحليلات الاخرى.

ويقتصر البحث على دراسة واختبار اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان، وذلك في بيئة الاعمال المصرية، ومدى تأثر هذه العلاقة ببعض السمات النوعية والفنية لمانح الائتمان مثل نوعه وخبرته وبالتالي **يخرج عن نطاق** هذا البحث باقي السمات الفنية الأخرى لمانحي الائتمان على العلاقة سالفة الذكر(مثل عمر مانح الائتمان، وحالته المزاجية وجوانبه النفسية). كما يخرج عن نطاق البحث مردود ومنفعة الافصاح عن تقرير إدارة مخاطر الامن السيبراني على باقي اصحاب المصالح الآخرين. وأيضاً، يخرج عن نطاق الدراسة تعرض الشركة لحوادث سيبرانية سابقة والاختلافات في انواعها واهميتها النسبية. واخيراً يخرج عن نطاق الدراسة باقي القطاعات.

ولتحقيق هدف البحث ومعالجة مشكلته، وفي ضوء حدوده، تم تنظيم المتبقي منه على النحو التالي:

2- الافصاح عن تقرير إدارة مخاطر الامن السيبراني : المفهوم، والمردود

3- تحليل الدراسات السابقة واشتقاق فروض البحث.

4- منهجية البحث.

5- النتائج والتوصيات ومجالات البحث المقترحة

2- الافصاح عن تقرير إدارة مخاطر الأمن السيبراني : المفهوم والمردود.

بالتركيز على **مفهوم الأمن السيبراني**، فقد تم تعريفه من قبل الهيئة الوطنية للامن السيبراني (2018) بأنه حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. كما تم تعريفه على انه تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء الالكتروني والانظمة التي تدعم الفضاء الالكتروني من الاحداث التي لاتتوافق بحكم القانون مع حقوق الملكية الفعلية (Craigen et al., 2014). وكذلك اعتبرت دراسة Santhosh and Thiyagu (2021) الامن السيبراني على انه احد فروع امن المعلومات، اي ان الامن السيبراني جزء من امن المعلومات، وعرفته على انه مجموعة التدابير الامنية التي يمكن اتخاذها لحماية الفضاء الالكتروني واصول المستخدم من الوصول والهجمات غير المصرح بها. كما عرفه البعض (Public Safety Canada, 2014 as cited in Craigen et al., 2014) على انه مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجمات أو الضرر أو الوصول غير المصرح به. وايضاً عرفه آخرون (ITU, 2009 as cited in Craigen et al., 2014) على انه مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم. وتتمثل **أهداف الأمن السيبراني** في سرية وسلامة وتوافر المعلومات، كما أن من **السياسات والاجراءات التي يمكن استخدامها لتحقيق الامن السيبراني** التشفير، واجراءات الحماية ضد الفيروسات، واعداد نسخ احتياطية، واستخدام الحوائط النارية[4]، وإدارة كلمات المرور (فرج، 2022).

[4] عبارة عن مجموعة برامج مترابطة تقع على حدود شبكة الحاسب، وتهدف إلى التأكد من هوية اي شخص يحاول الدخول إلى النظام اي يطلب منه الاسم وكلمة السر الخاصة به، حيث يتم مطابقتها مع الاسم وكلمة السر المحفوظين بقاعدة بيانات النظام لتحديد الاشخاص المصرح لهم بالوصول والدخول إلى النظام (علي وفرج، 2024)..

وبشأن **مخاطر الامن السيبراني،** فتعرف على انها مزيج من احتمالية وقوع حدث يهدد شبكة أنظمة المعلومات وعواقب هذا الحدث على أصول وسمعة الشركة (WEF, 2012: World Economic Forum as cited in Cains et al., 2022) كما تشير على انها المخاطر التي تنشأ نتيجة وجود احداث تؤدي إلى فقدان سرية أو نزاهة أو توفر المعلومات أو أنظمة المعلومات والتي تؤثر سلباًعلى العمليات التنظيمية للشركة (بما في ذلك مهمة الشركة أو أو صورتها أو سمعتها أو اصولها أو ادارتها) (CNSS, 2015: United States Committee on National Security System, as cited in Cains et al., 2022). وتعرف **الاختراقات السيبرانية** cyber breaches بأنها اي اجراء او انتهاك امني على البيانات المحمية والتي تؤدي إلى وصول البيانات إلي كيانات غير مصرح بها. وقد يكون هذا الانتهاك نتيجة لهجوم الكتروني او سرقة الاجهزة او فقدانها او سرقة او تسريب بيانات الموظفين مثل بيانات بطاقات الائتمان security credentials او الاخطاء البشرية human error (Algarni et al., 2021). **ويتم الاختراقات والهجمات السيبرانية** من خلال عدة وسائل منها (1)التصيد الاحتيالي phishing[5] (2) برامج الفدية Ransomware[6] (3) الهجوم بكلمة المرور (4)هجمات التنصت Eavesdropping (5)هجمات البرامج الضارة Malware Attacks[7] Trojan(6)[8] (7)هجوم رفض

[5] هو نوع من هجمات الهندسة الاجتماعية، ويُستخدم غالباً لسرقة بيانات المستخدم. يبدأ هذا الهجوم عندما يتمكن المجرم الإلكتروني من خداع ضحية ما بعد تنكره على شكل كيان موثوق به، حيث يصل للضحية بريد إلكتروني أو رسالة نصية تحفزه على النقر فوق ارتباط ضار (Cheng et al., 2017).

[6] في هذا النوع من الهجمات، يضطر الضحية إلى حذف جميع المعلومات الضرورية من نظامه إذا فشل في دفع فدية ضمن الجدول الزمني الذي قدمه مجرمو الإنترنت، حيث أنهم غالباً يبتزون المستخدم بنشر ملفاته الهامة بحال لم يتم دفع الفدية (Cheng et al., 2017).

[7] هي أي نوع من البرامج الضارة المصممة لإحداث ضرر أو تلف لجهاز كمبيوتر أو خادم أو عميل أو شبكة دون معرفة المستخدم النهائي يتم استخدامها لسرقة المعلومات الشخصية أو المالية أو التجارية (Cheng et al., 2017).

[8] وهو نوع من البرامج الضارة يتم إخفاؤه عادةً كمرفق في رسالة بريد إلكتروني أو ملف مجاني للتنزيل ، ثم ينتقل إلى جهاز المستخدم. بمجرد التنزيل، سينفذ الكود الضار المهمة التي صممها المهاجم من أجلها، مثل الوصول إلى الباب الخلفي لأنظمة الشركة أو التجسس على نشاط المستخدمين عبر الإنترنت، أو سرقة البيانات الحساسة (Cheng et al., 2017).

او حجب الخدمة (DDOS: Distributed Denial-OF-Service)[9](8) حقن SQL Injection SQL[10] (9) الفيروسات[11] (10) التهديدات من الداخل[12] (Cheng et al., 2017; Algarni et al., 2021).

ويعرف **برنامج إدارة مخاطر الامن السيبراني** على انه قيام الشركة بمجموعة من السياسات والعمليات والضوابط لحماية المعلومات والانظمة من الحوادث السيبرانية التي يمكن ان تهدد اهداف الامن السيبراني للشركة، وايضاً من الحوادث السيبرانية التي لم يتم منعها ومحاولة اكتشافها والاستجابة لها وتخفيضها في الوقت المناسب (AICPA, 2017).

وفيما يتعلق بالافصاح عن تقرير إدارة مخاطر الامن السيبراني، **فمن ناحية طبيعته**، يعد افصاح غير مالي. **ومن حيث درجة الالزام به**، فيكون افصاح اختيارياً، والذي تستخدمه الشركة كوسيلة لتوصيل جهودها في إدارة مخاطر الامن السيبراني لأصحاب المصالح. **وبشأن موقع الافصاح** ، فقد يكون الإفصاح في تقرير مجلس الإدارة أو في تقرير منفصل أو في تقرير الحوكمة والاستدامة. **وبشأن مصداقية الافصاح**، يجب اجراء توكيد مهني من جانب مراقبي الحسابات لإضفاء المصداقية على معلوماته، وذلك وفقاً للإطار الذي قدمه AICPA.

وبشأن اطار الافصاح عن إدارة مخاطر الامن السيبراني من منظور محاسبي وفني، فقد تعددت جهود المنظمات المهنية استناداً إلى لجنة بورصة الاوراق المالية الامريكية (SEC)، والمعهد الامريكي للمحاسبين القانونيين (AICPA)، والمعهد الوطني للمعايير والتكنولوجيا NIST national institute of standards and technology، ISO/IEC :27001 International Organization for Standardization and the International Electrotechnical Commission، ولجنة COSO، والهيئة الوطنية للامن السيبراني في السعودية، والاستراتيجية الوطنية للامن السيبراني في مصر.

[9] . تتم ببساطه بان يقوم المهاجم بإطلاق أحد البرامج التي تزحم المرور للموقع الخاص بك وبالتالي تمنع أي مستخدم آخر من الوصول إليه (Cheng et al., 2017).

[10] هذه الثغرات ممكن أن .(Database Layer) الهدف هو استغلال أي ثغرة أمنية موجودة بطبقة قاعدة البيانات التابعة لأي برنامج المضمنة داخل (Escape Characters) تكون حاضرة عندما لا يتم تصفية مدخلات المستخدم لبعض الحروف والرموز الخاصة مما يسبب عدم (Strongly Typed) جمل لغة الاستعلام البنيوية، أو ان لا يتم مراجعة نوعية المدخلات ان كانت نصية ام عددية التكهن بنتيجة تنفيذها (Cheng et al., 2017).

[11] برامج يتم تشغيلها وإلحاقها ضمن برامج النظام الاساسية دون علم مستخدمي النظام، وتعمل تلك البرامج بصورة تلقائية لإحداث ضرر بالنظام (Cheng et al., 2017).

[12] وجود شخص من الداخل يشارك في العملية لمساعدة مجرمي الإنترنت في الحصول على معلومات حول منظمتهم، ويتم ذلك من خلال تزويد أولئك المجرمين بكل المعلومات الضرورية، مما يؤدي إلى عواقب كبيرة على المنظمة. وتعتبر التهديدات من الداخل احد التهديدات الشائعة للهجمات السيبرانية على البنوك والمؤسسات المالية(Cheng et al., 2017).

وفيما يتعلق **بلجنة بورصة الاوراق المالية الامريكية SEC**، قامت SEC في عام 2011 بإصدار ارشادات حول الافصاح عن مخاطر الامن السيبراني. إذ يجب على الشركات الافصاح عن مخاطر الهجمات السيبرانية المحتملة والحوادث السيبرانية المالية المعروفة والتي حدثت بالفعل بما في ذلك التكاليف والعواقب المحتملة، بحيث يتضمن تلك الافصاح معلومات محددة حول طبيعة المخاطر وكيفية تأثير كل خطر على اعمال الشركة. وبعد خرق Equifax عام 2017 وخرق قاعدة بيانات SEC EDGAR اصدرت SEC عام 2018 ارشادات محدثة لتوجية الشركات العامة لإعداد افصاحات عن مخاطر الامن السيبراني، وقامت بتوسيع تلك الارشادات، حيث تم تناول موضوعين: أولاً قامت SEC بالتأكيد على اهمية واجراءات ضوابط الامن السيبراني لتمكين الافصاح عن مخاطر وحوادث الامن السيبراني في الوقت المناسب، ثانياً حظرت SEC التداول الداخلي prohibited the insider trading لحوادث الامن السيبراني. واوصت الشركات بمراجعة المجالات التالية عند تقييم مخاطر وحوادث الامن السيبراني والافصاح عن (أ) وقوع الحوادث السيبرانية. (ب) احتمال وقوع حوادث سيرانية محتملة. (ج) الاجراءات الوقائية للحد من مخاطر الامن السيبراني. (د) مخاطر الامن السيبراني المتعلقة بطبيعة عمل الشركات او عملياتها. (هـ) الاضرار بالسمعة. (و) التكاليف المرتبطة بالانظمة الجديدة القائمة او المحتملة. (ي) مخاطر التقاضي (e.x., Sheneman, 2022; Harris et al., 2023; Demek and Kaplan, 2023). وفي عام 2022 قامت SEC باقتراح تعديلات لإعلام المستثمرين بشكل افضل حول إدارة المخاطر وتقديم اخطار في الوقت االمناسب بحوادث الامن السيبرانية الجوهرية، وكذلك الافصاح بشكل دوري عن الاستراتيجية والسياسات والاجراءات المتبعة في حوكمة مخاطر الامن السيبراني (شرف، 2023).

وقام **AICPA** في عام 2017 بوضع اطار للتقرير عن إدارة مخاطر الامن السيبراني يتضمن ثلاثة مكونات؛ (1) وصف الإدارة لبرنامج إدارة مخاطر الامن السيبراني. (2) تأكيد الإدارة بأن وصف البرنامج يتوافق مع معايير الوصف وايضاً تأكيدات الإدارة حول فعالية ضوابط الامن السيبراني. (3) رأي مراقب الحسابات في إفصاحات الإدارة وفعالية ضوابط الشركة. ويتضمن هذا الاطار مجموعتين من المعايير، اولهما **معايير الوصف description criteria** لوصف برنامج إدارة مخاطر الامن السيبراني، ثانيهما **معايير الرقابة control criteria** لتقييم فعالية الضوابط داخل البرنامج (AICPA, 2017).

وتشمل **معايير الوصف** ما يلي: (1) طبيعة اعمال الشركة وعملياتها. (2) الانواع الرئيسية للمعلومات المعرضة للخطر. (3) اهداف برنامج إدارة مخاطر الامن السيبراني والتي تتمثل في الاهداف العامة للامن السيبراني وهي الحفاظ على سرية وسلامة وتوافر المعلومات. (4) العوامل التي لها تأثير كبير على المخاطر المتلازمة بالامن السيبراني مثل الخصائص والبيئة التكنولوجية والتغيرات التنظيمية التي حدثت خلال فترة وصف الشركة. (5) هيكل حوكمة إدارة مخاطر الامن السيبراني مثل التقرير عن النزاهة والاخلاق واشراف مجلس الإدارة على برنامج مخاطر

الامن السيبراني. (6) عملية تقييم مخاطر الامن السيبراني. (7) قنوات اتصال الامن السيبراني وجودة معلومات الامن السيبراني وتشمل عملية الاتصال الداخلي بمعلومات الامن السيبراني. (8) عملية رقابة برانامج إدارة مخاطر الامن السيبراني من خلال اجراء تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الاخرى للرقابة الداخلية المتعلقة بالامن السيبراني. (9) عملية رقابة الامن السيبراني من خلال عمليات تطوير الاستجابة السريعة للمخاطر المتوقعة. وبالنسبة **لمعايير الرقابة،** حافظت AICPA منذ عام 1997 على مجموعة من المعايير المستخدمة لتقييم والافصاح عن الضوابط المتعلقة بأمن وتوافر وسلامة معالجة وسرية وخصوصية المعلومات والنظام system. ويجوز للشركات استخدام معايير خدمات الثقة Trust service criteria للامن والتوافر والسرية كمعايير رقابية يتم من خلالها تحديد فعالية تلك الخدمات. ويتميز هذا الاطار بالمرونة حيث يسمح للإدارة باستخدام معايير اخرى غير معايير خدمات الثقة كمعايير رقابة (AICPA, 2017).

وبشأن **اطار NIST** فانه يوفر مجموعة من الارشادات التي تستخدمها المؤسسات لإدارة المخاطر السيبرانية بجميع انواعها والحد منها بشكل افضل بما في ذلك البرامج الضارة malware، سرقة كلمات المرور، هجمات التصيد الاحتيالي phishing attack، DDOS، الهندسة الاجتماعية social engineer، وغيرها. ويتكون الاطار من خمسة عناصر وهم (1) identify تحديد: اي تحديد الموقف الامني الاساسي للمنظمة وتحديد المخاطر. (2) protect الحماية: اي تنفيذ الضوابط الامنية للحماية من المخاطر المحددة. (3) detect الكشف: اي تطوير وتنفيذ عمليات الكشف لتحديد حوادث الامن السيبراني.(4) respond الاستجابة: اي انشاء وتنفيذ خطط الاستجابة لحوادث الامن السيبراني المحددة. (5) recover الاسترداد: اي وضع وتنفيذ خطط الاستفادة والانظمة والبيانات بعد احداث events الامن السيبراني. وفيما يتعلق **بمعيار ISO/ IEC: 27001** فأنه يحدد السياسات والاجراءات والموارد التي تقوم بها المؤسسات لإنشاء وتنفيذ ومراجعة وصيانة وتحسين نظام إدارة امن المعلومات ISMS information security management system، وذلك وفقاً لاحتياجات واهداف المنظمة عبر العمليات والمواقع المختلفة، وكذلك تنفيذ الضوابط الامنية واجراءات تقييمات المخاطر (Giuca et al., 2021).

وقامت لجنة COSO في عام 2017 بتطوير إطار عمل إدارة المخاطر المؤسسية، وكان أحد الدوافع الأساسية وراء تحديث تلك الإطار هو الحاجة إلى معالجة تطور إدارة المخاطر في العصر السيبراني، وحاجة المؤسسات إلى تحسين نهجها في إدارة المخاطر السيبرانية لتلبية متطلبات بيئة الأعمال المتطورة. وتم دمج ملف تعريف المخاطر السيبرانية الخاص بالمنطمة في المكونات الخمس للإطار **(1) الحوكمة والثقافة:** يجب أن يقوم مجلس الإدارة بزيادة الكفاءات السيبرانية لفهم المخاطر السيبرانية وتقييم البرامج والمبادرات السيبرانية للمؤسسة وتقييم مدى المخاطر السيبرانية التي تواجه العالم، ويجب قيام مجلس الإدارة بالإشراف على الإستراتيجية وينفذ مسؤوليات الحوكمة لدعم الإدارة في تحقيق الإستراتيجية أهداف العمل، كما يجب أن تكون ثقافة الأمن السيبراني جزءا لا يتجزأ

من ثقافة المنظمة[13]، كما يجب ان تُظهِر المنظمة التزامًا بالقيم الأساسية للكيان، كما يجب أن تسعى الإدارة إلى بناء ثقة الموظفين وحثهم على إدراك أهمية اليقظة السيبرانية vigilance **(2) الإستراتيجية وتحديد الأهداف:** تدرس المنظمة التأثيرات المحتملة لسياق الأعمال على ملف تعريف المخاطر، تحدد المنظمة الرغبة في المخاطرة في سياق خلق القيمة والحفاظ عليها وتحقيقها، تقوم المنظمة بتقييم الاستراتيجيات البديلة والتأثير المحتمل على ملف المخاطر، تأخذ المنظمة في الاعتبار المخاطر أثناء تحديد أهداف العمل على مختلف المستويات التي تتوافق مع الاستراتيجية وتدعمها. **(3) الأداء:** تحدد المنظمة المخاطر التي تؤثر على أداء الإستراتيجية وأهداف العمل، تقوم المنظمة بتحديد أولويات المخاطر كأساس لاختيار الاستجابات للمخاطر، تحدد المنظمة وتختار الاستجابات للمخاطر. **(4) المراجعة:** ستحتاج المنشأت إلى مراجعة استراتيجياتها التشغيلية والمالية والتقنية الحالية لمعالجة مخاطر الأمن السيبراني التي تنشأ. ويمكن أن تنطوي المراجعة على تحليل التكلفة والفوائد لتطوير برنامج قوي لإدارة المخاطر السيبرانية، توظيف متخصصين مؤهلين في مجال المخاطر السيبرانية أو إعادة تدريب الموظفين الحاليين، أو إجراء تقييمات مستمرة للثغرات الأمنية الجديدة. بالإضافة إلى ذلك، يمكن إجراء التأكد من فعالية الرقابة المتعلقة بالمخاطر السيبرانية (أي كيفية مراقبة واختبار ضوابط المخاطر بشكل دوري) من قبل قسم المراجعة الداخلية أو من قبل مراجع خارجي لأغراض إعداد التقارير المستقلة.**(5) المعلومات والاتصالات وإعداد التقارير:** تعمل المنظمة على الاستفادة من أنظمة المعلومات والتكنولوجيا الخاصة بالمنظمة لدعم إدارة مخاطر المؤسسة، توصيل معلومات المخاطر من خلال قنوات الاتصال، تقدم المنظمة تقارير عن المخاطر والثقافة والأداء على مستويات متعددة وعبر المنشأة (COSO, 2019).

وفي السعودية، قامت **الهيئة الوطنية للأمن السيبراني** بوضع نموذج سياسة لإدارة مخاطر للأمن السيبراني، والغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المبنية على افضل الممارسات والمعايير لإدارة مخاطر الامن السيبراني وتشمل بنود السياسة بأنه يجب ان تغطي منهجية إدارة مخاطر الامن السيبراني ما يلي (تحديد الاصول ومعرفة اهميتها، وتحديد وتقييم المخاطر، وتحديد التهديدات والثغرات المتعلقة بالامن السيبراني التي قد تؤثر على الاصول المعلوماتية والتقنية وتقييمها، وتحديد اساليب التعامل مع المخاطر السيبرانية، ترتيب التدابير الحد من المخاطر السيبرانية حسب الاولوية ووفق لأجراءات محددة، تصنيف مستويات المخاطر السيبرانية وتعريفها بناءً على مستوى التأثير واحتمالية حدوث التهديد، انشاء سجل مخاطر الامن السيبراني لتويثق المخاطر ومتابعتها، تحديد الأدوار والمسئوليات لإدارة مخاطر الامن السيبراني والتعامل معها)، كما يجب تنفيذ تقييم المخاطر

[13] إذ ان المنظمات ذات الثقافة القوية التي تركز على الإنترنت والوعي الأمني والتدريب ومنع فقدان البيانات قد يقلل من التعرض لمحاولات التصيد الاحتيالي والهندسة الاجتماعية، وغيرها من أشكال الهجمات السيبرانية (COSO, 2019)

دورياً لضمان حماية الاصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الاولوية، وكذلك يجب ان تكون إدارة مخاطر الامن السيبراني متوافقة مع إدارة المخاطر المؤسسية (الهيئة الوطنية للامن السيبراني، 2018).

وفي مصر، تم وضع الاستراتيجية الوطنية للأمن السيبراني (2017–2021) من قبل المجلس الأعلى للامن السيبراني التابع لرئاسة مجلس الوزراء وبرئاسة وزير الاتصالات وتكنولوجيا المعلومات، وذلك نتيجة للمادة (31) من الدستور المصري (يناير 2014) والتي نصت على ان أمن الفضاء المعلوماتي جزء اساسي من منظومة الاقتصاد والامن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، وعلى النحو الذي ينظمه القانون. وتتضمن تلك الاستراتيجية توضيح اهم التحديات والاخطار السيبرانية[14]، وايضاً اهم القطاعات الحيوية المستهدفة[15]، وكذلك اهم البرامج المستهدفة في المرحلة الحالية[16] (الاستراتيجية الوطنية للامن السيبراني، 2017). وفي يناير، 2024 **تم وضع الاستراتيجية الوطنية للأمن السيبراني** (2023–2027)، وتتمثل أهمية الاستراتيجية (1) التصدي للحوادث السيبرانية التي تزايدت من حيث العدد والمصدر. (2) خلق فرص للسوق المصرية عن طريق بناء كوادر بشرية واقامة صناعة وطنية تسهم في زيادة الناتج المحلي الاجمالي. واشارت الاستراتيجية لتزايد عدد الهجمات السيبرانية في الاعوام السابقة بشكل كبير. وذكرت الاستراتيجية ان من مصادر التهديدات السيبرانية الجريمة السيبرانية، والحرب السيبرانية cyber war[17]، والارهاب terrorists، والتهديدات الداخلية[18]، والهواة[19](الاستراتيجية الوطنية للامن السيبراني، 2024).

وبشأن **مردود الافصاح عن تقرير إدارة مخاطر الامن السيبراني** على فئات اصحاب المصالح. **وبالنسبة للمستثمرين** اشارت دراسة Frank et al. (2023) ان المستثمرين غير المحترفين يأخذون في الاعتبار مخاطر الامن السيبراني عند اتخاذ قرار الاستثمار، ويعتبرون تلك المخاطر واحدة من اكبر المخاطر التي تهدد اسواق رأس

[14] مثل خطر اختراق وتخزين البنية التحتية للاتصالات وتكنولوجيا المعلومات، وخطر الارهاب والحرب السيبرانية، وخطر سرقة الهوية الرقمية والبيانات الخاصة (الاستراتيجية الوطنية للامن السيبراني، 2017).

[15] مثل قطاع الاتصالات وتكنولوجيا المعلومات، وقطاع الخدمات المالية، وقطاع الطاقة، وقطاع الخدمات الحكومية، وقطاع النقل والمواصلات، وقطاع الصحة وخدمات الاسعاف العاجل، وقطاع الاعلام والثقافة (الاستراتيجية الوطنية للامن السيبراني، 2017)

[16] مثل برنامج لتطوير الاطار التشريعي الملائم لامن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية، وبرنامج تطوير منظومة وطنية متكاملة لحماية امن الفضاء السيبراني وتأمين البنية التحتية للاتصالات وتكنولوجيا المعلومات، وبرنامج لحماية الهوية الرقمية وتفعيل البنية التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخجمات الحكومية الالكترونية بوجه هاص، وبرنامج لإعداد الكوادر البشرية والخدمات اللازمة لتفعيل منظومة الامن السيبراني في مختلف القطاعات(الاستراتيجية الوطنية للامن السيبراني، 2017).

[17] هي تهديدات تقوم بها دول، وذلك لإختراق القطاعات الحرجة في الدول الاخرى مثل قطاعات الطاقة والاتصالات والبنوك(الاستراتيجية الوطنية للامن السيبراني، 2024)

[18] تكون من جانب الموظفين الذي لهم تصريح الدخول عن انظمة المعلومات(الاستراتيجية الوطنية للامن السيبراني، 2024).

[19] مجموعة اشخاص اصحاب مهارات سيبرانية محدودة، ولكنهم يستخدمون برامج مجهزة ذات قدرات تخريبية عالية(الاستراتيجية الوطنية للامن السيبراني، 2024).

المال في الولايات المتحدة، كما ان تقديم افصاحات اضافية حول تقرير إدارة مخاطر الامن السيبراني يقلل من عدم التأكد لدى المستثمرين. كما خلصت دراستا (Yang et al. 2020; Kelton, 2021) إلى انه يؤثر افصاح الشركات عن تقرير إدارة مخاطر الامن السيبراني تأثير ايجابي على تحسين قرارات المستثمرين ويساهم في زيادة ثقة المستثمرين في تلك الشركات عن طريق انخفاض عدم تماثل المعلومات. كما توصلت دراسة (Cheng et al., 2022) ان المستثمرين غير المحترفين هم اقل عرضة للاستثمار في الشركات المخترقة والتي افصحت عن تقارير إدارة مخاطر الامن السيبراني. إذ اشارت الدراسة ان المستثمرين يلقوا اللوم blame على الشركات التي ادعت فعالية تلك التقرير او الضوابط الخاصة بها، ولكنها تعرضت لاحقاً لانتهاكات سيبرانية.

وبالنسبة للمحللين الماليين، اشارت دراسة Bui (2023) بأن المديرين على استعداد لاخفاء الهجمات السيبرانية إذا كان احتمال اكتشافها منخفض، مما يؤدي ذلك إلى زيادة كلاً من عدم تماثل المعلومات وعدم التأكد بشأن بيئة المعلومات، الامر الذي ينعكس على زيادة تشتت توقعات المحللين الماليين. وكذلك اشارت دراسة (Havakhor et al., 2020) انه يؤدي الافصاح عن الاستثمارات في الامن السيبراني إلى انخفاض عدم تماثل المعلومات، مما يؤدي إلى تقليل اخطاء توقعات المحللين الماليين. **وبالنسبة للمقرضين،** يقدر البنوك جهود الشركات في الانخراط بمبادرات إدارة مخاطر الامن السيبراني (Havakhor et al., 2020)، وهذا ما سوف يتم تناوله بشئ من التفصيل في النقطة التالية.

وتخلص الباحثة مما سبق، أن برنامج إدارة مخاطر الامن السيبراني هو عبارة عن مجموعة من السياسات والاجراءات التي تضعها الشركة لحماية المعلومات والانظمة من الحوادث السيبرانية التي يمكن ان تهدد اهداف الأمن السيبراني للشركة. كما تعددت جهود المنظمات المهنية بشأن الإفصاح عن مخاطر الأمن السيبراني وإداراتها. كما ان الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني له محتوى معلوماتي على فئات اصحاب المصالح خاصةً، المستثمرين، والمحللين الماليين، والمقرضين.

3-تحليل الدراسات السابقة واشتقاق فروض البحث

ويشمل تحليل الدراسات السابقة التي تناولت العلاقة بين مستوى افصاح الشركات عن تقرير إدارة مخاطر الامن السيبراني وقرار منح الائتمان، وكذلك الدراسات السابقة التي تناولت اثر نوع وخبرة مانح الائتمان على العلاقة بين مستوى افصاح الشركات عن تقرير إدارة مخاطر الامن السيبراني وقرار منح الائتمان، وذلك على النحو التالي:

3-1-تحليل العلاقة بين الافصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار منح الائتمان، واشتقاق الفرض الأول وفرعياته

يوجد العديد من العوامل التي يعتمد عليها البنك عند اتخاذ قرار منح الائتمان ومنها، مستوى المخاطر التي تتعرض إليها الشركات المقترضة. فتفترض نظرية سوق الائتمان Loan pricing theory انه كلما زادت مخاطر المقترض كلما ارتفعت اسعار الفائدة على القروض، ووفقاً لنظرية الاشارة The Signaling Theory يجب على الشركات الجيدة أرسال اشارات للبنوك تفيد انها ذو مخاطر قليلة حتى تحصل على اسعار فائدة اقل مقارنة بالشركات ذات المخاطر الاعلى. ووفقاً لنظرية تسعير القروض Loan Pricing Theory يجب على البنوك ان تأخذ في الاعتبار مشكلة الاختيار العكسي والمخاطر الاخلاقية عند تحديد اسعار الفائدة على المقترض، لأنه من الصعب التنبؤ بنوع المقترض في بداية العلاقة المصرفية. إذ يكون المقترض ذو المخاطر العالية على استعداد قبول معدلات فائدة مرتفعة مما يجعل في بعض الاحيان ان سعر الفائدة الذي يحدده البنوك لايتناسب مع مخاطر المقترضين (Olokoyo, 2011; Ladime et al., 2013). ومن ثم تميل الشركات إلى الافصاح عن إدارة المخاطر لكي تستطيع الحصول على القروض بشروط افضل من حيث أسعار الفائدة وحجم القرض وقيمة الضمانات المقدمة عليه (Rahmawati et al., 2024).

وبالتركيز على **الافصاح عن الاختراقات السيبرانية**، خلصت دراسة (Binfarè, 2020; Boasiako and michael, 2021; Huang and Wang, 2021; Singh, 2023; Rincon and Ordóñez, 2023; Evans et al., 2023; Wang et al., 2023; Chatterjee et al., 2024) إلى ان الشركات التي افصحت عن تعرضها لاختراقات البيانات تواجه اسعار فائدة اعلى على القروض وايضاً تواجه ارتفاع مخاطر الائتمان وانخفاض تصنيفها الائتماني مقارنة بالشركات التي لم تتعرض للأختراقات. إذ ان الاختراقات تؤدي إلى زيادة التكاليف المباشرة وغير المباشرة مثل خسارة سمعة الشركة وخسارة كبار العملاء وارتفاع مخاطر التقاضي، مما يؤدي إلى ارباح اقل واكثر تقلباً وانخفاض كلاً من الأداء التشغيلي للشركة المخترقة وحصتها السوقية وتدفقاتها النقدية، مما يؤدي إلى زيادة مخاطر التخلف عن السداد. كما ان انخفاض السمعة الناتجة عن اختراق البيانات تؤثر سلباً على علاقة الشركة مع اصحاب المصالح الاخرى مثل الموردين والمديرين التنفيذين والمساهمين، مما يؤدي إلى زيادة المخاطر التشغيلية.

كما يعتمد الدائنون مثل البنوك على المعلومات التشغيلية والمحاسبية بما في ذلك المعلومات الداخلية التي يتم الحصول عليها مباشرة من الشركة لتقييم صحتها وقدرتها على الاستمرار واتخاذ قرارات بشأن الاقراض لها. ويشير تعرض الشركات لاختراق البيانات إلى وجود ضعف في نظام المعلومات والذي يؤدي بدوره إلى زيادة مخاطر الرقابة التشغيلية وانخفاض موثوقية التقارير المالية، مما يؤدي إلى ارتفاع مخاطر المعلومات لتلك الشركات

المخترقة، مما ينعكس سلباً على شروط القروض المصرفية من حيث قيمة القرض ومعدل الفائدة وقيمة الضمانات المقدمة. كما ان الشركات المخترقة يُمكن ان تقلل من العواقب السلبية لشروط القروض من خلال اتخاذ المزيد من الاجراءات التصحيحية بعد الاختراق (مثل توظيف خبير خارجي في أمن البيانات، وتحسين نظام تكنولوجيا المعلومات، ومراجعة السياسات المتعلقة بأمن البيانات) (Binfarè, 2020; Boasiako and michael, 2021; Huang and Wang, 2021; Chatterjee et al., 2024).

ووفقاً لنظرية التعاقد غير المكتملة incomplete contracting theory يستخدم المقرضون شروط تعاقدية للتعويض عن الاحداث السلبية او غير المؤكدة المحتملة والحماية منها. ويعتبر اختراقات الامن السيبراني من الاحداث السلبية التي قد تؤثر على زيادة تكلفة الديون للحد الذي يصبح فيه المقرضون اكثر قلقاً من ان المقترض لن يفي بألتزاماته المالية. وعند حدوث الانتهاك قد يكون عدد اقل من المقرضين على استعداد لإقراض الشركات المخترقة (Sheneman, 2017). كما ان اصحاب المصالح (الدائنين) يقرضوا الشركات التي تعرضت للهجوم الالكتروني بشروط اعلى من نظيراتها ويرجع ذلك إلى مخاوفهم بشأن ضعف المركز المالي للشركة وارتفاع مخاطر التخلف عن السداد وزيادة احتمالية افلاس الشركات بعد التعرض للهجوم (Kamiya et al., 2021).

وتوصلت دراسة (Sheneman, 2017; Ashraf and Sunder, 2023; Chatterjee et al., 2024) ان هناك تأثير إيجابي بين افصاح الشركة عن تعرضها لاختراقات الامن السيبراني وتكلفة الديون وذلك بالمقارنة بالقروض التي حصلت عليها الشركة قبل الانتهاكات. وهذه العلاقة الايجابية تكون اكثر وضوحاً بالنسبة للشركات التي تتمتع بتصنيفات ائتمانية منخفضة قبل الانتهاك (اي مخاطر ائتمانية عالية)، والشركات ذات المخاطر الاعلى لتكنولوجيا المعلومات. واضافت دراسة Chatterjee et al. (2024) ان العلاقة الايجابية تكون اكثر وضوحاً بالنسبة للشركات التي تنتمي للصناعات المعرضة للانتهاكات السيبرانية والشركات التي تفصح عن نقاط ضعف في هيكل الرقابة الداخلية والتي تفصح عن مخاطر الامن السيبراني. كما اضافت دراسة Ashraf and Sunder, 2023; Chatterjee et al., 2024) ان العلاقة الايجابية يمكن ان تنخفض في الشركات التي تركز على تدابير الامن السيبراني مثل الشركات التي تقوم بالاستثمار في الامن السيبراني او الشركات التي تقوم بتعيين مسئول تكنولوجي في مجلس إدارته او عندما تقوم الشركات بتعيين لجنة فنية لإدارة المخاطر السيبرانية.

كما استهدفت دراسة Sheneman (2022) التعرف على تأثير هجمات الامن السيبراني للشركات النظيرة في الصناعة على تكلفة الديون للشركات الاخرى في الصناعة (الشركات غير المخترقة) او ما يعرف بتأثير العدوى. وتوصلت الدراسة إلى وجود تأثيرات تنافسية لأحداث هجمات الامن السيبراني، حيث يستفيد المقترضين غير المنتهكين من الهجمات السيبرانية للشركات النظيرة في الصناعة وذلك من خلال تخفيض تكلفة القروض. إذ اعتبر المقرضون حدث الاختراق حدثاً ايجابياً للشركات غير المخترقة. كما خلصت الدراسة إلى ان التأثيرات التنافسية

اكثر وضوحاً بالنسبة للقروض قصيرة الاجل وللشركات ذات النمو المرتفع والشركات ذات الرفع المالي المنخفض. وخلصت دراسة (2023) .Harris et al إلى ان انخفاض جودة الافصاح عن مخاطر الامن السيبراني (مقاسة بزيادة عدد كلمات وزيادة تعقيد قراءة التقرير) يؤدي إلى ارتفاع تكلفة الديون.

وبالتركيز على **تقرير إدارة مخاطر الامن السيبراني**، يوفر افصاح الشركات عن تلك التقرير معلومات مفيدة لأصحاب المصالح (المستثمرون والدائنين) حول الجهود المبذولة في مجال الامن السيبراني، وحول قدرتهم على منع واكتشاف حوداث الامن السيبراني والاستجابة لها (Yang et al., 2020; Kelton, 2021)، وحول استراتيجية الشركات فيما يتعلق بإدارة المخاطر السيبرانية (Eijkelenboom and Nieuwesteeg, 2021)، مما ينعكس على تحسين سمعة وقيمة تلك الشركات وادائها المالي وتدفقاتها النقدية في المستقبل (Gatzert and Schubert, 2022; Kejwang, 2022)، الامر الذي يؤدي إلى تخفيض تكلفة الاقتراض (Anginer et al., 2011) وفي هذا السياق، توصلت دراستا (Gordon et al., 2015; Havakhor et al., 2020) انه يقدر البنوك جهود الشركات في الانخراط بمبادرات إدارة مخاطر الامن السيبراني، حيث يميل البنوك إلى انخفاض تكلفة الاقتراض وزيادة حجم القروض وتقليل حجم الضمانات المقدمة عند الحصول على القرض، وذلك بمجرد الاعلان عن الاستثمار في الامن السيبراني. كما خلصت دراسة (Kamiya et al., 2021) ان الشركات التي تتولى اهتماماً اكبر بإدارة مخاطر الامن السيبراني (من حيث وجود لجنة لإدارة المخاطر في مجلس الإداة) تكون اقل عرضة للهجمات السيبرانية ولكن لم تقم بمنعها تماماً، الامر الذي يؤدي بدوره إلى تخفيض تكلفة الاقتراض (e.x., Sheneman, 2017; Ashraf and Sunder, 2023; Chatterjee et al., 2024). ونفس السياق، هدفت دراسة (يوسف، 2022) إلى التعرف على واقع الافصاح عن تقرير إدارة مخاطر الامن السيبراني وأثره على قراراي الاستثمار ومنح الائتمان. وخلصت الدراسة إلى عدم افصاح الشركات المقيدة بسوق المال عن مخاطر الامن السيبراني، مما يؤثر ذلك سلباً على اسعار الاسهم وأحجام التداول.

وتخلص الباحثة من تتبع التطور التاريخي للدراسات (Sheneman, 2017; Binfarè, 2020; Boasiako and michael, 2021; Kamiya et al., 2021; Huang and Wang, 2021; Sheneman, 2022; Singh, 2023; Harris et al., 2023; Rincon and Ordóñez, 2023; Ashraf and Sunder, 2023; Evans et al., 2023; Wang et al., 2023; Chatterjee et al., 2024) ذات الصلة بأثر تعرض الشركة لأختراقات سيبرانية على تكلفة الاقتراض إلى وجود اتفاق بين معظمها على وجود علاقة إيجابية بين هذين المتغيرين، وكذلك دراسات (يوسف، 2022؛ Gordon et al., 2015; Havakhor et al., 2020) ذات الصلة بأثر افصاح الشركات عن الاستثمارات في الامن السيبراني على تكلفة رأس المال المقترض إلى وجود اتفاق على وجود علاقة سلبية بين هذين المتغيرين. **وقد اتضح للباحثة** من تحليل تلك الدراسات إلى

تعدد البيئات التي أجريت فيها هذه الدراسات، وان معظمها تمت في بيئات الدول المتقدمة مثل الولايات المتحدة الامريكية (e.x., Havakhor et al., 2020; Singh, 2023)، والقليل منها تمت في الدول النامية مثل مصر (يوسف، 2022). **ومن الناحية المنهجية**، اتضح اعتمادها على اسلوب تحليل المحتوى بينما اتبع البعض إلى اسلوب قائمة الاستقصاء مثل دراسة (يوسف، 2022). **وبناءً على ما تقدم، تتوقع الباحثة إمكانية تأثير افصاح الشركات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان. وبالتالي يمكن اشتقاق الفرض الأول للبحث في صورته البديلة على النحو التالي:**

H1: يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على قرار منح الائتمان

ويمكن اختبار هذا الفرض من خلال اختبار اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان المتعلقة بالموافقة على او رفض منح الائتمان، وشروط منح الائتمان من حيث معدل الفائدة وقيمة القرض (يوسف، 2022)، وذلك على النحو التالي:

H_{1a}:يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على الموافقة على منح الائتمان.

H_{1b}:يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على مبلغ القرض الذي يمكن الحصول عليه.

H_{1c}:يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على معدل الفائدة على القرض.

3-2-تحليل اثر نوع مانح الائتمان على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان، واشتقاق الفرض الثاني وفرعياته

خلص البعض (Bellucci et al., 2010; Beck et al., 2010) ان نوع جنس موظفي القروض له تأثير على قرار منح الائتمان. إذ يميل النساء إلى تجنب المخاطرة وأقل ثقة بالنفس من الرجال، خاصة في مجالات اتخاذ القرارات المالية والاستثمارات. وقد تميل موظفات القروض إلى استخدام معايير أكثر صرامة عند اتخاذ قرار منح الائتمان من عدمه لتجنب حالات التخلف عن السداد، وتوليد خسائر أقل للبنك، ومن ثم اشارت الدراسة إلى انخفاض احتمالية المقترض عن التأخير في سداد قروضه التي تم فحصها ومراقبتها من قبل مسؤولي القروض الأناث، لأن النساء يمنحن القروض بشكل أكثر تقييدًا. كما انهم يميلون إلى تقييد إتاحة الائتمان للمقترضين الجدد غير المستقرين أكثر من نظرائهم الذكور. كما تكون النساء أقل أنانية وانتهازية ويميلون إلى إظهار سلوك تعاوني أكبر مدفوعًا بنوع من أخلاق المسؤولية morality of responsibility مقارنة بالذكور. وايضاً يميل النساء إلى

إظهار التعاطف مع مصالح الآخرين (مثل المقترضون)، ومن ثم يمنحوا الائتمان بشروط أسهل. وعلى الجانب الاخر، لم تتوصل دراسة (2015) Baklouti لوجود تأثير لجنس موظف القرض أو جنس طالب القرض على التقييم عند اتخاذ قرار منح الائتمان.

ومن ناحية اخرى، اهتمت دراسة (2017) .Anwar et al باختبار إلى أي مدى يلعب نوع جنس موظفي الشركات في زيادة الوعي لديهم بأهمية الأمن السيبراني والانخراط في سلوكيات الأمن السيبراني. **وبناءً عليه، ترى الباحثة وفقاً للدراسات السابق عرضها ان نوع مانحي الائتمان قد تؤثر على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان، وبالتالي يمكن اشتقاق الفرض الثاني للبحث في صورته البديلة على النحو التالي:**

H2: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف جنس مانح الائتمان.

ويمكن اختبار هذا الفرض من خلال اختبار اثر نوع مانح الائتمان على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان المتعلقة بالموافقة على او رفض منح الائتمان، وشروط منح الائتمان من حيث معدل الفائدة وقيمة القرض (يوسف، 2022)، وذلك على النحو التالي:

H_{2a}:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على الموافقة على منح الائتمان باختلاف جنس مانح الائتمان.

H_{2b}: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على مبلغ القرض الذي يمكن الحصول عليه باختلاف جنس مانح الائتمان.

H_{2c}: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على معدل الفائدة على القرض باختلاف جنس مانح الائتمان.

3-3-تحليل اثر خبرة مانحي الائتمان على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان، واشتقاق الفرض الثالث وفرعياته

يوجد وجهتا نظر بشأن اثر خبرة مانحي الائتمان على قرار منح الائتمان، **إذ تشير وجهة النظر الاولى** إلى وجود تأثير إيجابي للعلاقة المشار إليها سلفاً. إذ انه وفقاً لنموذج اتخاذ القرار الطبيعي naturalistic decision making paradigm بأن اداء مانحي الائتمان ذو الخبرة أفضل من أداء مانحي الائتمان ذو الخبرة المحدودة، حيث يُمكن لمانحي الائتمان ذو الخبرة من استخلاص النتائج من المواقف السابقة ويمكن مطابقة هذه المواقف مع المواقف الحالية ومن ثم يتعلموا من خبراتهم السابقة. كما يميل مسئولي القروض ذو الخبرة من استخدام النهج

البديهي intuitive approach كمكمل للنهج العقلاني rational approach عند الموافقة على القروض، كما ان هناك مواقف يجب فيها تقليل استخدام البديهة مثل اتخاذ قرارات عالية المخاطر، ووجود قيود تنظيمية على مانحي الائتمان كضغط المساءلة accountability pressure (Trönnberg and Hemlin, 2012).

كما اشارت دراسة Baklouti (2015) ان مانحي الائتمان ذوي الخبرة يصبحوا اكثر تأهيلاً لتجنب التحيز في الاحكام، الامر الذي من شأنه تحسين دقة توقعاتهم وتحسين جودة قراراتهم. إذ ان سلوك المتنبأ سوف يتحسن مع مرور الوقت ومن ثم يؤدي إلى احكام اكثر دقة، كما انهم عندما يصبحون اكثر خبرة يمكنهم تطبيق ما تعلموه من خلال العمل لتحقيق المزيد من الكفاءة لأغراض معالجة المعلومات، وبالتالي تجنب التحيز في الحكم، وايضاً التعلم من التجربة يساعد على القضاء على التحيزات السلوكية من خلال اداء المهام المماثلة والمتكررة. كما ترى الدراسة بأن استخدام الاستدلال التمثيلي[20] representativeness heuristics من قبل مانحي الائتمان ذو الخبرة يساعده على اتخاذ أحكامًا جيدة وسريعة على الفور وايضاً يساعده على حل المشكلات بسرعة أكبر وبأخطاء أقل. كما ان مانحي الائتمان ذوي خبرة يكتسبون المزيد من المهارات ويصبحون قادرين على تطوير مفاهيم أكثر ملاءمة ويمكنهم العودة إلى تحيزاتهم الأولية المعتادة في المواقف والأحكام. فمانحي الائتمان ذوي الخبرة يمكنه مقايضة trade off الجهد المبذول في إصدار حكم معين مقابل الوصول إلى دقة الاختيار من خلال اختيار استراتيجية بسيطة وموفرة للوقت لاتخاذ قرارات معينة. كما يمكن لموظفي القروض ذوي الخبرة من تجميع المعلومات بسرعة أكبر وقد يتوصلون إلى نتيجة أسرع من زملائهم المبتدئين ذو الخبرة الاقل.

و**تشير وجهة النظر الثانية** إلى انه لا يختلف قرار منح الائتمان بأختلاف خبرة مانحي الائتمان. إذ انه وفقاً لنموذج الاكتشاف والتحيز heuristic and bias paradigm ان الخبراء غالباً ما يكونوا ضحايا victims للتحيزات مثلهم مثل المبتدئين ذو الاقل خبرة، وبالتالي لا يمكن ان يتفوقوا على المبتدئين إلا في حالات محددة، اي ان المجموعة الأكثر خبرة لم يكن ادائها أفضل بأستمرار في مهمة قرار منح الائتمان (Trönnberg and Hemlin, 2012). كما خلصت دراسة Miller and Smith (2002) إلى وجود تأثير إيجابي لخبرة مانح الائتمان على قرار منح الائتمان من حيث قبوله او رفضه، بينما لم يؤثر على القرار من حيث تحديد مقدار الائتمان او معدل الفائدة. **وبناءً عليه، ترى الباحثة وفقاً للدراسات السابق عرضها ان خبرة مانحي الائتمان قد تؤثر على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان، وبالتالي يمكن اشتقاق الفرض الثالث للبحث في صورته البديلة على النحو التالي:**

[20] هي مجموعة القواعد والاساليب التي يمكن من خلالها تبسيط التقييمات اي ان يكون لديه خلفية ومعرفة واضحة فيما يتعلق بحدث معين.

H3: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف خبرة مانح الائتمان

ويمكن اختبار هذا الفرض من خلال اختبار اثر خبرة مانح الائتمان على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان المتعلقة بالموافقة على او رفض منح الائتمان، وشروط منح الائتمان من حيث معدل الفائدة وقيمة القرض (يوسف، 2022)، وذلك على النحو التالي:

H_{3a}:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على الموافقة على منح الائتمان باختلاف خبرة مانح الائتمان.

H_{3b}: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على مبلغ القرض الذي يمكن الحصول عليه باختلاف خبرة مانح الائتمان.

H_{3c}: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على معدل الفائدة على القرض باختلاف خبرة مانح الائتمان.

4-منهجية البحث

تستهدف الباحثة في هذه الجزئية عرض لمنهجية البحث تمهيداً لاختبار فروض البحث تجريبياً, ولذلك سيتم تناول كل من؛ الهدف من الدراسة التجريبية، ومجتمع وعينة الدراسة، ونموذج البحث وقياس متغيرات الدراسة، وأدوات واجراءات الدراسة التجريبية، والتصميم التجريبي المستخدم والمعالجات والمقارنات التجريبية، والاساليب الاحصائية المستخدمة لتحليل نتائج الدراسة، ونتائج اختبار فروض البحث، واخيراً التحليلات الاخرى ونتائجها، وذلك على النحو التالي:

4-1-الهدف من الدراسة التجريبية

تستهدف الدراسة التجريبية اختبار فروض البحث في بيئة الاعمال المصرية، لقياس ما إذا كان هناك تأثير لافصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخامر الامن السيبراني على قرار منح الائتمان، وكذلك اختبار اثر خبرة ونوع مانح الائتمان على قوة العلاقة محل الدراسة، وذلك قياساً على دراستا (Gordon et al., 2015; Havakhor et al., 2020).

4-2-مجتمع وعينة الدراسة التجريبية:

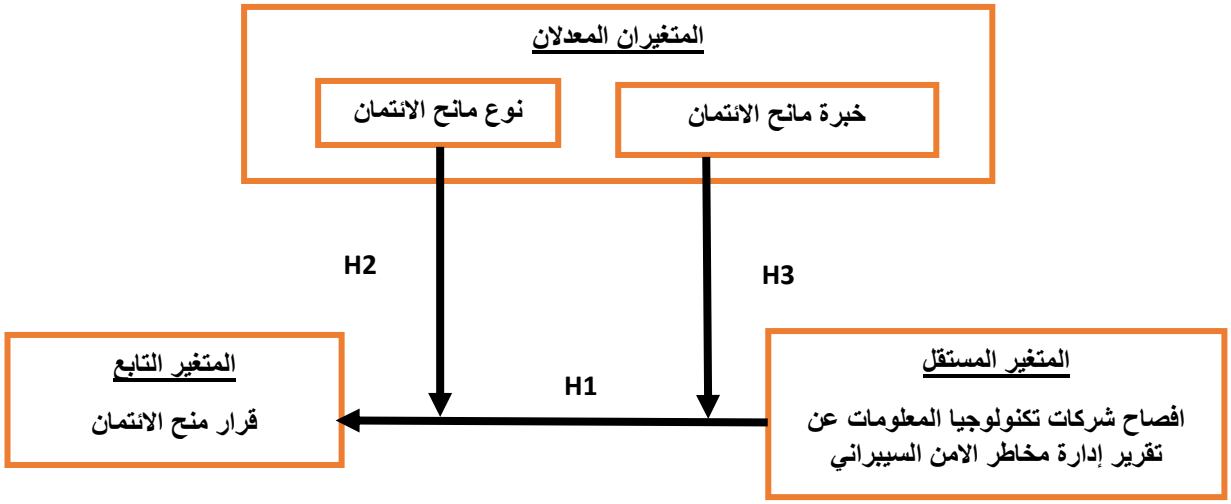
يتمثل مجتمع الدراسة التجريبية **لأغراض التحليل الاساسي** من المسئولين عن اتخاذ قرار منح الائتمان في البنوك االتجارية المصرية، وقد قامت الباحثة بتوزيع الحالات الافتراضية على عينه تحكمية من هذا المجتمع، كما

هو موضح بالجدول رقم (1)، وذلك قياساً على البعض (Nguyen and Dung, 2020؛ الصباغ، 2021). ويتكون مجتمع الدراسة **لأغراض التحليلات الاخرى من الأكاديميين** من اعضاء هيئة التدريس والمدرسين المساعدين والمعيدين بقسم المحاسبة والمراجعة وقسم إدارة اعمال مسار استثمار بكلية التجارة جامعة الاسكندرية، وقد تم اختيار عينة تحكمية من هذا المجتمع. وفيما يلي بيان بالحالات الموزعة والمستلمة:

جدول1 : بيان بالحالات التجريبية الموزعة والمستلمة

بيان بالحالات التجريبية الموزعة والمستلمة في ظل التحليل الاساسي على المسئولين عن اتخاذ قرار منح الائتمان في البنوك التجارية	
اجمالي الحالات الموزعة	**عدد الحالات المستلمة**
72	45 بنسبة 62.5%من الحالات الموزعة
بيان بالحالات التجريبية الموزعة والمستلمة في ظل تحليل الآخر على الاكاديميين	
اجمالي الحالات الموزعة	**عدد الحالات المستلمة**
65	51 بنسبة 78.5% من الحالات الموزعة

4-3-نموذج البحث وقياس متغيرات الدراسة



شكل 1: نموذج البحث في ظل التحليل الاساسي

جدول 2: قياس متغيرات الدراسة

المتغيرات	نوع المتغير	قياس المتغيرات	المرجع
قرار منح الائتمان	تابع	يتم قياسه من خلال ردود المشاركين على حالتي الدراسة التجريبية عن قبول او رفض منح القرض للشركة، وقيمة القرض، ومعدل الفائدة	الصباغ، 2021 Ruhnke et al., 2018
الافصاح عن تقرير إدارة مخاطر الامن السيبراني	مستقل	يتم قياسه من خلال امداد افراد العينة من مانحي الائتمان بقوائم مالية مرفق بها تقرير الادارة بشان مخاطر الامن السيبراني مقارنة بقوائم مالية فقط بدون تقرير إدارة مخاطر الامن السيبراني.	Cheng et al., 2022
نوع جنس مانح الائتمان	مُعدل	يتم قياسه بمتغير وهمي ياخذ القيمة (1) إذا كان مانح الائتمان ذكر، ويأخذ القيمة (صفر) اذا كان مانح الائتمان انثى	Baklouti, 2015
مستوى خبرة مانح الائتمان	مُعدل	يتم قياسه بمتغير وهمي ياخذ القيمة (1) إذا كان مانح الائتمان ذو خبرة مرتفعة، ويأخذ القيمة (صفر) اذا كان مانح الائتمان ذو خبرة منخفضة. ويعتبر مانح الائتمان ذو خبرة مرتفعة اذا كان عدد سنوات عملة يزيد عن 10 ويكون مانح الائتمان ذو خبرة منخفضة اذا كان عدد سنوات عمله 10 سنوات.	Baklouti, 2015

4-4-أدوات واجراءات الدراسة التجريبية

اعتمدت الدراسة التجريبية على الحالات الافتراضية والاسئلة المرافقة لها، ثم تم عرضها على المشاركين في العينة وقامت الباحثة بإجراء مقابلات شخصية مع بعض افراد العينة بجانب تصميم قائمة باستخدام تقنية Google وارسالها بالبريد الالكتروني. اما بشأن **اجراءات الدراسة التجريبية** تم صياغة الحالات الافتراضية، Forms والتي اشتملت على ثلاثة اقسام؛ تضمن القسم الاول التعرف على بعض خصائص المشاركين في التجربة من خلال الاستفسار عن نوع جنس المشاركين ومستوى خبرتهم المهنية ودرجتهم الوظيفية وعمرهم ومستوى تأهيلهم العلمي. ويتعلق القسم الثاني ببعض المصطلحات الفنية ذات الصلة التي قد يصعب على بعض مفردات العينة إدراك المقصود بها. واخيراً تضمن القسم الثالث الحالات التجريبية. إذ اشتملت الحالة التجريبية الاولى ملخصاً للقوائم المالية لأحدى شركات تكنولوجيا المعلومات لسنتين 2022، 2023 بالإضافة لبعض الايضاحات المتممة. اما الحالة التجريبية الثانية فتضمنت نفس القوائم المالية بجانب تقرير إدارة الشركة عن إدارة مخاطر الامن السيبراني لعام 2023. وقد طُلب من المشاركين في العينة الاجابة على الثلاث اسئلة التي تضمنتها كل حالة افتراضية والمتعلقة بقرار منح الائتمان والذي يقيس درجة الموافقة على او رفض منح الائتمان، وقيمة القرض، ومعدل الفائدة. وبعد ذلك تم استلام الردود وتم فحصها واستبعاد غير المكتمل منها تمهيداً لتحليلها احصائياً.

4-5-التصميم التجريبي والمعالجات والمقارنات التجريبية

يظهر التصميم التجريبي لاختبار فروض البحث من خلال الجدول التالي، حيث تم اجراء تصميم تجريبي (2×2×2)، وذلك على النحو التالي:

جدول 3 : التصميم التجريبي (2×2×2)

سمات مانح الائتمان / الافصاح	خبرة مانحي الائتمان		نوع مانحي الائتمان	
	مرتفعة	منخفضة	ذكر	انثى
قوائم مالية بدون الافصاح عن تقرير إدارة مخاطر الامن السيبراني	المعالجة (1) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة	المعالجة (2) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة	المعالجة (3) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة	المعالجة (4) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة
قوائم مالية بالاضافة إلى الافصاح عن تقرير إدارة مخاطر الامن السيبراني	المعالجة (5) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة	المعالجة (6) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة	المعالجة (7) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة	المعالجة (8) أ-منح القرض ب-مبلغ القرض ج-معدل الفائدة

وفي ضوء ذلك **تضمنت التجربة 8 معالجات** على النحو التالي:

المعالجة (1) : قوائم مالية لشركة تكنولوجيا المعلومات بدون الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان ذو خبرة مرتفعة / ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

المعالجة (2) : قوائم مالية لشركة تكنولوجيا المعلومات بدون الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان ذو خبرة منخفضة / ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

المعالجة (3) : قوائم مالية لشركة تكنولوجيا المعلومات بدون الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان ذكر / ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

المعالجة (4) : قوائم مالية لشركة تكنولوجيا المعلومات بدون الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان انثى / ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

المعالجة (5) : قوائم مالية لشركة تكنولوجيا المعلومات بالاضافة إلى الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان ذو خبرة مرتفعة / ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

المعالجة (6) : قوائم مالية لشركة تكنولوجيا المعلومات بالاضافة إلى الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان ذو خبرة منخفضة / ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

المعالجة (7) : قوائم مالية لشركة تكنولوجيا المعلومات بالاضافة إلى الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان ذكر/ ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

المعالجة (8) : قوائم مالية لشركة تكنولوجيا المعلومات بالاضافة إلى الافصاح عن تقرير إدارة مخاطر الامن السيبراني / مانح ائتمان انثى/ ويطلب منه الموافقة على او رفض منح الائتمان وتحديد كُلاً من قيمة القرض ومعدل الفائدة.

وتضمن التجربة **ثلاث مقارنات تجريبية:**

المقارنة الاولى : بين المعالجات{ (1+2+3+4) مع المعالجات (5+6+7+8) } وذلك لقياس تأثير الافصاح وذلك لإختبار الفرض الاول(H1).عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان،

المقارنة الثانية : بين المعالجات {(7مقابل3) مع المعالجات(8مقابل4)} وذلك لقياس مدى اختلاف تأثير الافصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان، باختلاف نوع مانح الائتمان وذلك لإختبار الفرض الثاني (H_2)

المقارنة الثالثة: بين المعالجات {(5مقابل1) مع المعالجات (6مقابل2)} وذلك لقياس مدى اختلاف تأثير الافصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان، باختلاف خبرة مانح الائتمان وذلك لإختبار الفرض الثالث (H_3)

4-6-الاساليب الاحصائية المستخدمة لتحليل نتائج الدراسة

تم استخدام **اختبار الاعتدالية Normality test** وذلك من خلال اجراء **اختبار-Kolmogorov Smirnov** لتحديد نوع المجتمع الذي سحبت من العينة اي معرفة ما اذا كان هذا المجتمع يتبع التوزيع الطبيعي ام لا، وذلك لتحديد نوع الاختبارات الاحصائية المناسبة التي يمكن استخدامها في اختبار الفروض، وقد اتضح من الجدول رقم (4) ان العينة لا تتبع التوزيع الطبيعي، حيث ان قيمة P-value لكل اسئلة البحث مساوية 0.000 (اقل من 0.05)، ومن ثم تم رفض فرض العدم القائل بأن المجتمع الذي سحبت من العينة يتبع التوزيع الطبيعي، وفي هذه الحالة يتم الاعتماد على الاساليب الاحصائية اللامعلمية Nonparametric لاختبار فروض البحث.

جدول4 : نتائج اختبار الاعتدالية

Kolmogorov-Smirnov			
	Statistic	df	P-value
Q01	0.310	45	0.000
Q02	0.489	45	0.000
Q03	0.375	45	0.000
Q11	0.233	45	0.000
Q12	0.399	45	0.000
Q13	0.344	45	0.000

كما تم استخدام **اختبار الصدق والثبات Reliability test**، وذلك من خلال اجراء اختبار **Cronbach Alpha** لاختبار درجة ثبات ومصداقية الاسئلة ذات الاجابات الترتيبية. إذ تم الاعتماد على قياس المتغير التابع (قرار منح الائتمان سواء الموافقة على او رفض منح الائتمان وتحديد مبلغ القرض ومعدل الفائدة) من خلال مجموعة من الاسئلة ذات الاجابات الترتيبية، فبالنسبة لسؤال الموافقة والرفض على منح الائتمان تم الاعتماد على سؤال ذات خمس درجات تتدرج من موافق تماماً تأخذ القيمة (5) إلى غير موافق تماماً تأخذ القيمة (1)، اما بشأن سؤال تحديد مبلغ القرض ومعدل الفائدة فلجأت الباحثة إلى تحويله من سؤال كمي إلى سؤال ترتيبي، وذلك نظراً لأن غالبية المشاركين في العينة لم يقوموا بتحديد مبلغ القرض او معدل الفائدة بل اكتفوا بالاختيار فقط من ضمن الاختيارات المتاحة لهم، لذا تم الاعتماد على الاجابات الترتيبية ذات ثلاث درجات تتدرج من قيمة القرض اكبر من مليار و300 مليون جنية تأخذ القيمة (3) إلى قيمة القرض اقل من مليار جنيه تأخذ القيمة (3) بالنسبة لقيمة القرض، وايضاً تتدرج من اكبر من 22.25% تأخذ القيمة (3) إلى اقل من 22.25% تأخذ القيمة (1) بشان معدل الفائدة. وقد اتضح من الجدول رقم (5) انه تبلغ قيمة معامل كرونباخ الفا (0.845،0.641،0.702،0.619) على التوالي، وهي اكبر من 60%، وهو ما يمثل مستوى جيد من الصدق والثبات.

جدول 5: نتائج اختبار الصدق والثبات

	Cronbach Alpha		N of items
	عينة مانحي الائتمان	عينة الاكاديمين	
الموافقة على منح الائتمان	0.845	0.702	2
قيمة القرض ومعدل الفائدة	0.641	0.619	4

كما تم اجراء **اختبار ويلكوكسون Wilcoxon signed Rank Test** اللامعلمي، وذلك لاختبار فروض البحث. ويتم الاعتماد على هذا الاختبار في حالة وجود عينتين غير مستقلتين من المجموعات التجريبية، وذلك لأجراء المقارنات الثنائية وتحديد مدى الاختلاف بين وسيطي العينتين. ويتم تحديد مدى قبول الفرض من عدمه من خلال مستوى المعنوية P–value فإذا كان مستوى المعنوية 0.05 أو أقل يتم رفض الفرض العدم، وقبول الفرض البديل.

4-7-نتائج اختبار فروض البحث

4-7-1-نتيجة اختبار الفرض الأول وفرعياته

استهدف هذا الفرض اختبار ما إذا كان هناك تأثير معنوي لإفصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان، وذلك من خلال ثلاث فروض فرعية تختبر الاثر على قرار منح الائتمان المتعلقة بالموافقة على او رفض منح الائتمان، وقيمة القرض، ومعدل الفائدة على القرض. ولاختبار هذا الفرض وفرعياته احصائياً تم اعادة صياغته كفرض عدم، وذلك كما يلي:

H_1: لايؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان.

H_{1a}: لايؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على الموافقة على منح الائتمان.

H_{1b}: لايؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على مبلغ القرض الذي يمكن الحصول عليه.

H_{1c}:لايؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على معدل الفائدة على القرض.

ويظهر الفرض الاحصائي الخاص بهذا الاختبار كما يلي:

فرض العدم M2 =H_0:M1 اي لايوجد اختلافات معنوية في وسيط ردود عينة مانحي الائتمان في حالة الافصاح عن تقرير إدارة مخاطر الامن السيبراني مقارنة بحالة عدم الافصاح

الفرض البديل M2 ≠H_1:M1 اي يوجد اختلافات معنوية في وسيط ردود عينة مانحي الائتمان في حالة الافصاح عن تقرير إدارة مخاطر الامن السيبراني مقارنة بحالة عدم الافصاح.

ويظهر الجدول رقم (6) التالي نتائج اختبار الفرض الأول وفرعايته:

Wilcoxon Signed Ranks Test

		N	Mean Rank	Sum of Ranks
Q11-Q01	Negative Ranks	1a	8.50	8.50
	Positive Ranks	17b	9.56	162.50
	Ties	27c		
	Total	45		
Q12-Q02	Negative Ranks	2d	12.25	24.50
	Positive Ranks	15e	8.57	128.50
	Ties	28f		
	Total	45		
Q13-Q03	Negative Ranks	6g	5.92	35.50
	Positive Ranks	5h	6.10	30.50
	Ties	34i		
	Total	45		
a.Q11< Q01		b. Q11> Q01		c. Q11= Q01
d.Q12< Q02		e. Q12> Q02		f. Q12= Q02
g.Q13< Q03		h. Q13> Q03		i. Q13= Q03

Test Statistics

	Q11-Q01	Q12-Q02	Q13-Q03
Z	-3.662b	-2.681b	-0.237c
Asymp.sign.(2-tailed)	0.000	0.007	0.813

a. Wilcoxon Signed Ranks Test
b. Based on negative ranks
c. Based on positive ranks

وبالنسبة للفرض الفرعي الأول، يتضح من الجدول السابق (6) معنوية الاختبار، حيث بلغت قيمة (p-value) لهذا الاختبار (0.000)، مما يعني وجود تأثير للإفصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات معنوياً على الموافقة على منح الائتمان. وعليه فقد تم **رفض فرض العدم وقبول الفرض البديل H_{1a} القائل بأنه يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات تأثيراً معنوياً على الموافقة على منح الائتمان.** ومن ثم تم **قبول الفرض الفرعي الاول (H_{1a}) للبحث.**

وبشأن الفرض الفرعي الثاني، يتضح من الجدول السابق (6) معنوية الاختبار، حيث بلغت قيمة (p-value) لهذا الاختبار (0.007)، مما يعني وجود تأثير للإفصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات معنوياً على مبلغ القرض الذي يمكن الحصول عليه. وعليه فقد تم **رفض فرض العدم وقبول الفرض البديل H_{1b} القائل بأنه يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات تأثيراً معنوياً على مبلغ القرض الذي يمكن الحصول عليه.** ومن ثم تم **قبول الفرض الفرعي الثاني (H_{1b}) للبحث.**

وبالنسبة للفرض الفرعي الثالث، يتضح من الجدول السابق (6) عدم معنوية الاختبار، حيث بلغت قيمة (p–value) لهذا الاختبار (0.813)، مما يعني وجود تأثير للإفصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات ولكنة **تأثير غير معنوي** على معدل الفائدة على القرض. وعليه فقد تم **قبول فرض العدم ورفض الفرض البديل H_{1c} القائل بأنه يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات تأثيراً معنوياً على معدل الفائدة على القرض**. ومن ثم **تم رفض الفرض الفرعي الثالث (H_{1c}) للبحث.**

ويتضح من النتائج السابقة قبول الفرض الفرعي الاول والثاني، وبالتالي تم **قبول الفرض الأول للبحث جزئياً**. مما يشير ان افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني يقدم معلومات هامة لمانحي الامتحان، مما يؤثر على قراراتهم المتعلقة بالموافقة على أو رفض منح الائتمان وقيمة القرض الذي يمكن الحصول عليه. وهو ما يتفق مع نتائج بعض الدراسات (Gordon et al., 2015; Havakhor et al., 2020). **وترى الباحثة** ان تأثير افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قراراتهم المتعلقة بالموافقة على أو رفض منح الائتمان وقيمة القرض الذي يمكن الحصول عليه، يعتبر تأثيراً منطقياً حيث يقدر البنوك جهود الشركات في الانخراط بمبادرات إدارة مخاطر الامن السيبراني، ولذلك يميل البنوك إلى زيادة حجم القروض الممنوحة إليهم وتقليل حجم الضمانات المقدمة، حيث ان الشركات التي تتولى اهتماماً اكبر بإدارة مخاطر الامن السيبراني تكون اقل عرضة للهجمات السيبرانية، ومن ثم تكون سمعتها وادائها المالي أفضل مقارنة بالشركة التي لم تقوم بإدارة مخاطر الامن السيبراني.

4-7-2-نتيجة اختبار الفرض الثاني وفرعياته

استهدف هذا الفرض اختبار ما إذا كان التأثير المعنوي لإفصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان يختلف باختلاف نوع جنس مانح الائتمان، وذلك من خلال ثلاث فروض فرعية تختبر الاثر على قرار منح الائتمان المتعلقة بالموافقة على او رفض منح الائتمان، وقيمة القرض، ومعدل الفائدة على القرض. ولاختبار هذا الفرض وفرعياته احصائياً تم اعادة صياغته كفرض عدم، وذلك كما يلي:

H_2: لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف جنس مانح الائتمان.

H_{2a}: لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على الموافقة على منح الائتمان باختلاف جنس مانح الائتمان.

H_{2b}: لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على مبلغ القرض الذي يمكن الحصول عليه باختلاف جنس مانح الائتمان.

H_{2c}:لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على معدل الفائدة على القرض باختلاف جنس مانح الائتمان.

ويظهر الفرض الاحصائي الخاص بهذا الاختبار كما يلي:

فرض العدم H_0:M1= M2، ويعني هذا الفرض انه لايوجد اختلافات معنوية في وسيط ردود عينة مانحي الائتمان من الذكور عن الاناث في حالة الافصاح عن تقرير إدارة مخاطر الامن السيبراني مقارنة بحالة عدم الافصاح.

الفرض البديل H_1:M1≠ M2، ويعني هذا الفرض انه يوجد اختلافات معنوية في وسيط ردود عينة مانحي الائتمان من الذكور عن الاناث في حالة الافصاح عن تقرير إدارة مخاطر الامن السيبراني مقارنة بحالة عدم الافصاح.

ويظهر الجدول 7:التالي نتائج اختبار الفرض الثاني وفرعايته:

الفرض	الاختبار الاحصائي	N	Z	P–value
H2:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف جنس مانح الائتمان	**اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان من جانب مانحي الائتمان من الذكور**	**29**	**-2.483**	**0.013**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان من من جانب مانحي الائتمان من الاناث	**16**	**-2.828**	**0.005**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان من الذكور	**29**	**-1.155**	**0.248**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان من الاناث	**16**	**-2.714**	**0.007**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على معدل الفائدة على القرض الذي يمكن الحصول عليه من مانحي الائتمان من الذكور	**29**	**-0.707**	**0.480**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على معدل الفائدة على القرض االذي يمكن الحصول عليه من مانحي الائتمان من الاناث	**16**	**-0.333**	**0.739**

وبالنسبة للفرض الفرعي الأول، يتضح من الجدول السابق (7) أن قيمة (p–value) لهذا الاختبار (0.005،0.013)، بالنسبة لجنس مانح الائتمان **على الموافقة على منح الائتمان،** مما يشير إلى وجود تأثير معنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان سواء كان مانحي الائتمان من الذكور أو الاناث. ولتحديد مدى قوة تأثير نوع جنس مانح الائتمان على العلاقة محل الدراسة (H_1). قامت الباحثة بإجراء مقارنة بين الحالتين السابقتين (مانحي الائتمان من الذكور، مانحي الائتمان من الاناث) باستخدام قيمة (Z) المحسوبة، فكلما زادت قيمة (Z) المحسوبة دل ذلك على قوة تأثير نوع جنس مانح الائتمان على العلاقة محل الدراسة. وبالرجوع إلى النتائج في الجدول رقم (7) يتضح ان قيمة (Z) المحسوبة في حالة مانحي الائتمان من الاناث (2.828) اكبر من قيمة (Z) المحسوبة في حالة مانحي الائتمان من الذكور (2.483). مما يعني زيادة قوة التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على الموافقة او رفض منح الائتمان في الاناث عن الذكور، اي بعد الاخذ في الاعتبار جنس مانح الائتمان. وعليه فقد تم رفض فرض العدم وقبول الفرض البديل H_{1a} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على الموافقة على منح الائتمان باختلاف جنس مانح الائتمان.** ومن ثم تم **قبول الفرض الفرعي الاول (H_{2a}) للبحث.**

وبشأن الفرض الفرعي الثاني، يتضح من الجدول السابق (7) أن قيمة (p–value) لهذا الاختبار (0.007،0.248)، بالنسبة لجنس مانح الائتمان **على مبلغ القرض الذي يمكن الحصول عليه،** مما يعني وجود **تأثير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول **عليه من مانحي الائتمان اناث،** ووجود **تأثير غير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه **من مانحي الائتمان ذكور.** كما يتضح ان قيمة (Z) المحسوبة في حالة مانحي الائتمان من الاناث (2.714) اكبر من قيمة (Z) المحسوبة في حالة مانحي الائتمان من الذكور (1.155). مما يعني زيادة قوة التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على مبلغ القرض الذي يمكن الحصول عليه في الاناث عن الذكور، أي بعد الاخذ في الاعتبار جنس مانح الائتمان. وعليه فقد تم رفض فرض العدم وقبول الفرض البديل H_{2b} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على مبلغ القرض الذي يمكن الحصول عليه باختلاف جنس مانح الائتمان.** ومن ثم تم **قبول الفرض الفرعي الثاني (H_{2b}) للبحث.**

وبالنسبة للفرض الفرعي الثالث، يتضح من الجدول السابق (7) أن قيمة (p–value) لهذا الاختبار (0.480،0.739)، بالنسبة لجنس مانح الائتمان **على معدل الفائدة على القرض،** مما يعني ان جنس مانح الائتمان **ليس له تأثير معنوي** على العلاقة محل الدراسة (H_1). وعليه فقد تم قبول فرض العدم ورفض الفرض

البديل H_{2c} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على معدل الفائدة على القرض باختلاف جنس مانح الائتمان.** ومن ثم تم **رفض الفرض الفرعي الثالث (H_{2c}) للبحث.**

ويتضح من النتائج السابقة قبول الفرض الفرعي الاول والثاني، وبالتالي تم **قبول الفرض الثاني للبحث جزئياً. وترى الباحثة** انه يميل مانحي الائتمان من الاناث إلى تجنب المخاطر خاصة في مجال اتخاذ القرارات المالية مقارنة بالرجال، ولذا فإن افصاح الإدارة عن تقرير إدارة مخاطر الامن السيبراني يعتبر مؤشر لمانحي الائتمان من الاناث على جهودهم في تخفيض تلك المخاطر وتقليل تعرضهم للهجمات السيبرانية ومن ثم يفضلوا الموافقة على منح الائتمان وزيادة حجم القروض لتلك الشركات بدون تخفيض معدل الفائدة لهم حتى لايخسر البنك.

4-7-3-نتيجة اختبار الفرض الثالث وفرعياته

استهدف هذا الفرض اختبار ما إذا كان التأثير المعنوي لإفصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان يختلف باختلاف خبرة مانح الائتمان، وذلك من خلال ثلاث فروض فرعية تختبر الاثر على قرار منح الائتمان المتعلقة بالموافقة على او رفض منح الائتمان، وقيمة القرض، ومعدل الفائدة على القرض. ولاختبار هذا الفرض وفرعياته احصائياً تم اعادة صياغته كفرض عدم، وذلك كما يلي:

H_3: لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف خبرة مانح الائتمان.

H_{3a}: لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على الموافقة على منح الائتمان باختلاف خبرة مانح الائتمان.

H_{3b}: لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على مبلغ القرض الذي يمكن الحصول عليه باختلاف خبرة مانح الائتمان.

H_{3c}:لايختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على معدل الفائدة على القرض باختلاف خبرة مانح الائتمان.

ويظهر الفرض الاحصائي الخاص بهذا الاختبار كما يلي:

فرض العدم H_0:M1= M2، ويعني هذا الفرض انه لايوجد اختلافات معنوية في وسيط ردود عينة مانحي الائتمان من ذوي الخبرة عن قليل الخبرة في حالة الافصاح عن تقرير إدارة مخاطر الامن السيبراني مقارنة بحالة عدم الافصاح.

الفرض البديل H_1:M1≠ M2 اي يوجد اختلافات معنوية في وسيط ردود عينة مانحي الائتمان من ذوي الخبرة عن قليل الخبرة في حالة الافصاح عن تقرير إدارة مخاطر الامن السيبراني مقارنة بحالة عدم الافصاح.

ويظهر الجدول 8: التالي نتائج اختبار الفرض الثالث وفرعايته:

الفرض	الاختبار الاحصائي	N	Z	P–value
H3:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف خبرة مانح الائتمان	**اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان من جانب مانحي الائتمان ذوي الخبرة**	**34**	**-2.840**	**0.005**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان من من جانب مانحي الائتمان قليل الخبرة	**11**	**-2.333**	**0.02**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان ذوي الخبرة	**34**	**-2.138**	**0.033**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان قليل الخبرة	**11**	**-1.667**	**0.096**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على معدل الفائدة على القرض الذي يمكن الحصول عليه من مانحي الائتمان ذوي الخبرة	**34**	**-0.632**	**0.527**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على معدل الفائدة على القرض االذي يمكن الحصول عليه من مانحي الائتمان قليل الخبرة	**11**	**-1.134**	**0.257**

وبالنسبة للفرض الفرعي الأول، يتضح من الجدول السابق (8) أن قيمة (p–value) لهذا الاختبار (0.02،0.005)، بالنسبة لخبرة مانح الائتمان على **الموافقة على منح الائتمان**، مما يشير إلى وجود **تأثير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان **سواء كان مانحي الائتمان من ذوي الخبرة أو قليل الخبرة**. ولتحديد مدى قوة تأثير خبرة مانح الائتمان على العلاقة محل الدراسة (H_1). قامت الباحثة بإجراء مقارنة بين الحالتين السابقتين (مانحي الائتمان ذوي الخبرة، مانحي الائتمان قليل الخبرة) باستخدام

قيمة (Z) المحسوبة، فكلما زادت قيمة (Z) المحسوبة دل ذلك على قوة تأثير خبرة مانح الائتمان على العلاقة محل الدراسة. وبالرجوع إلى النتائج في الجدول رقم (8) يتضح ان قيمة (Z) المحسوبة في حالة مانحي الائتمان ذوي الخبرة (2.840) اكبر من قيمة (Z) المحسوبة في حالة مانحي الائتمان قليل الخبرة (2.333). مما يعني إلى زيادة قوة التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على الموافقة او رفض منح الائتمان في ذوي الخبرة عن قليل الخبرة ، اي بعد الاخذ في الاعتبار خبرة مانح الائتمان. وعليه فقد تم رفض فرض العدم وقبول الفرض البديل H_{3a} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على الموافقة على منح الائتمان باختلاف خبرة مانح الائتمان.** ومن ثم تم **قبول الفرض الفرعي الاول (H_{3a}) للبحث.**

وبشأن الفرض الفرعي الثاني، يتضح من الجدول السابق (8) أن قيمة (p–value) لهذا الاختبار (0.096،0.033)، بالنسبة لخبرة مانح الائتمان على مبلغ القرض الذي يمكن الحصول عليه، مما يعني وجود **تأثير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من **مانحي الائتمان ذوي الخبرة،** ووجود **تأثير غير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من **مانحي الائتمان قليل الخبرة.** كما يتضح ان قيمة (Z) المحسوبة في حالة مانحي الائتمان ذوي الخبرة (2.138) اكبر من قيمة (Z) المحسوبة في حالة مانحي الائتمان قليل الخبرة (1.667). مما يعني زيادة قوة التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان ذوي الخبرة عن قليل الخبرة، أي بعد الاخذ في الاعتبار خبرة مانح الائتمان. وعليه فقد تم رفض فرض العدم وقبول الفرض البديل H_{3b} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على مبلغ القرض الذي يمكن الحصول عليه باختلاف خبرة مانح الائتمان.** ومن ثم تم **قبول الفرض الفرعي الثاني (H_{3b}) للبحث.**

وبالنسبة للفرض الفرعي الثالث، يتضح من الجدول السابق (8) أن قيمة (p–value) لهذا الاختبار (0.257،0.527)، بالنسبة لخبرة مانح الائتمان على معدل الفائدة على القرض، مما يعني ان خبرة مانح الائتمان **ليس له تأثير معنوي** على العلاقة محل الدراسة (H_1). وعليه فقد تم قبول فرض العدم ورفض الفرض البديل H_{3c} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على معدل الفائدة على القرض باختلاف خبرة مانح الائتمان.** ومن ثم تم **رفض الفرض الفرعي الثالث (H_{3c}) للبحث.**

ويتضح من النتائج السابقة قبول الفرض الفرعي الاول والثاني، وبالتالي تم **قبول الفرض الثالث للبحث جزئياً. وترى الباحثة** ان مانحي الائتمان ذوي خبرة لديهم المزيد من المهارات، الامر الذي يُحسن من دقة توقعاتهم

وتحسين جودة قراراتهم، لذا يميل مانحي الائتمان ذو الخبرة من الموافقة على منح الائتمان وزيادة حجم القروض للشركات التي تتولى اهتماماً اكبر بإدارة مخاطر الامن السيبراني. اذ يكونوا اقل عرضة للهجمات السيبرانية، ومن ثم تكون سمعتها وادائها المالي أفضل مقارنة بالشركة التي لم تقوم بإدارة مخاطر الامن السيبراني.

4-8-التحليلات الاخرى

ولإضفاء المزيد من الوضوح أو الفهم على العلاقات الرئيسية للبحث بتحليله الأساسي وتقييم مدى قوة ومتانة Solidity النتائج التي تم التوصل إليها في ذلك الصدد، تم اجراء مجموعة من التحليلات الإضافية والمتمثلة في حالة تغيير معالجة المتغيرين المعدلين كمتغيرين رقابيين، وحالة اختبار تأثير كلا المتغيران المعدلان معاً (وهم نوع جنس وخبرة مانحي الائتمان معاً) على العلاقة محل الدراسة، وحالة إدخال متغير معدل جديد (مستوى التأهيل العلمي لمانحي الأئتمان) بخلاف المتغيرين المعدلين المستخدمين في التحليل الأساسي، وحالة الاعتماد على عينة ومجتمعين مختلفيين، وذلك على النحو التالي:

(أ) حالة تغيير معالجة المتغيرين المعدلين كمتغيرين رقابيين

يستهدف هذا التحليل التحقق من مدى أفضلية معالجة المتغيران المعدلان بنموذج البحث بالتحليل الأساسي وهما نوع جنس وخبرة مانحي الائتمان، كمتغيران رقابيان بدلاً من كونهما متغيران معدلان للعلاقة التأثيرية مجال البحث، وذلك بغرض تأييد أو عدم تأييد ما توصل إليه البحث من نتائج، قياساً على دراستا (Sarang et al., 2022). واستنادًا إلى ما سبق تم **اشتقاق السؤال الأول والثاني للبحث (Q1,Q2) والقائل هل يؤثر** نوع جنس مانح الائتمان **على قرار منح الائتمان، في سياق العلاقة التأثيرية بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان؟، وهل يؤثر** خبرة مانح الائتمان **على قرار منح الائتمان، في سياق العلاقة التأثيرية بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان؟**، وتتم الإجابة "بنعم" على هذان التساؤلان إذا كانت القيمة الاحتمالية للمتغير الرقابي أقل من (0.05)، وفيما يلي توضيح للنتائج في ظل معالجة المتغير المعدل كمتغير الرقابي، وذلك على النحو التالي:

جدول 9: نتائج اختبار سؤال البحث الأول (معالجة المتغير المعدل (جنس مانح الائتمان) كمتغير رقابي) في ظل التحليل الاخر

حالة اعتبار جنس مانح الائتمان متغير رقابي في ظل التحليل الاخر		حالة اعتبار جنس مانح الائتمان متغير مُعدل في ظل التحليل الاساسي	
قرار مانح الائتمان	p-value	قرار مانح الائتمان	p-value
بالنسبة للموافقة على منح الائتمان	0.465	بالنسبة للموافقة على منح الائتمان	0.005
بالنسبة لمبلغ القرض الذي يمكن الحصول عليه	0.322	بالنسبة لمبلغ القرض الذي يمكن الحصول عليه	0.007
بالنسبة لمعدل الفائدة على القرض	0.012	بالنسبة لمعدل الفائدة على القرض	0.739

جدول 10: نتائج اختبار سؤال البحث الثاني (معالجة المتغير المعدل (خبرة مانح الائتمان) كمتغير رقابي) في ظل التحليل الاخر

حالة اعتبار خبرة مانح الائتمان متغير رقابي في ظل التحليل الاخر		حالة اعتبار خبرة مانح الائتمان متغير مُعدل في ظل التحليل الاساسي	
قرار مانح الائتمان	p-value	قرار مانح الائتمان	p-value
بالنسبة للموافقة على منح الائتمان	0.630	بالنسبة للموافقة على منح الائتمان	0.005
بالنسبة لمبلغ القرض الذي يمكن الحصول عليه	0.201	بالنسبة لمبلغ القرض الذي يمكن الحصول عليه	0.033
بالنسبة لمعدل الفائدة على القرض	0.733	بالنسبة لمعدل الفائدة على القرض	0.527

وبتحليل النتائج بالجدول رقم (9) اتضح **وجود تأثير معنوي** لأثر نوع مانح الائتمان على معدل الفائدة على القرض، حيث كانت **p-value (0.012)**. كما اتضح **وجود تأثير غير معنوي** لأثر نوع مانح الائتمان على الموافقة أو رفض منح الائتمان وعلى مبلغ القرض الذي يمكن الحصول علية، حيث كانت **p-value (0.322،0.465) على التوالي**. وهذا يعني ان قرار منح الائتمان من حيث تحديد معدل الفائدة على القرض يختلف إذا كان مانحي الائتمان من الإناث او الذكور، **ولكنه لايختلف من حيث الموافقة أو رفض منح الائتمان وعلى مبلغ القرض الذي يمكن الحصول علية. وتتفق هذه النتجة** مع دراسة (Baklouti, 2015). **لذا تمت الإجابة على سؤال البحث الأول Q1 القائل: هل يؤثر نوع مانح الائتمان على قرار منح الائتمان، في سياق العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني وقرار منح الائتمان؟ بـ" نعم بشأن معدل الفائدة على القرض، ولا بشأن الموافقة أو رفض منح الائتمان وعلى مبلغ القرض الذي يمكن الحصول علية ".**

وايضاً بتحليل النتائج بالجدول رقم (10) اتضح **وجود تأثير غير معنوي** لأثر خبرة مانح الائتمان على كلاً من الموافقة أو رفض منح الائتمان ومبلغ القرض الذي يمكن الحصول علية ومعدل الفائدة على القرض، حيث كانت **p-value (0.630،0.201،0.733) على التوالي**. وهذا يعني ان قرار منح الائتمان **من حيث الموافقة أو رفض منح الائتمان ومبلغ القرض الذي يمكن الحصول علية وتحديد معدل الفائدة على القرض** لايختلف إذا كان مانحي الائتمان ذوي الخبرة او قليل الخبرة. **وتتفق هذه النتجة** مع دراسة (Trönnberg and Hemlin, 2012). **لذا تمت الإجابة على سؤال البحث الثاني Q2 القائل: هل يؤثر خبرة مانح الائتمان على قرار منح الائتمان، في سياق العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني وقرار منح الائتمان؟ بـ" لا ".**

ويتضح من تتبع إجابة الأسئلة في ظل مدخل المتغيرات الرقابية ومقارنتها بنتائج اختبار الفروض في ظل مدخل المتغيرات المعدلة، اختلاف نتائج كلا المدخلين بالنسبة لنوع جنس وخبرة مانح الائتمان وكانت في صالح معالجة تلك المتغيرات كمتغيرات معدلة. **وبالتالي ترى الباحثة** أفضلية تبني مدخل المتغيرات المعدلة مقارنة بمدخل

المتغيرات الرقابية فيما يتعلق بأغلبية العلاقات التأثيرية محل الدراسة، وهو ما يدعم وجهة نظر الباحثة واقتناعها بأهمية اختبار وتبني هذا المدخل في اختبار العلاقات محل الدراسة **بالتحليل الأساسي**.

(ب) حالة اختبار تأثير كلا المتغيرين المعدلين معاً (جنس وخبرة مانحي الائتمان معاً) على العلاقة محل الدراسة:

تسعى الباحثة في هذا الاختبار إلى الأجابة عن التساؤل التالي: **هل يختلف أثر المتغيرات المُعدلة معاًعلى العلاقة محل الدراسة مقارنة بأثر كل متغير مُعدل على حده ؟** وللإجابة على هذا التساؤل قامت الباحثة بإختبار هذا الفرض، وفيما يلي توضيح للنتائج:

جدول 11: نتيجة اختبار سؤال البحث الثالث (اختبار نوع جنس وخبرة مانح الائتمان معاً) في ظل التحليل الاخر

الفرض	الاختبار الاحصائي	N	Z	P-value
Q3 :هل يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف نوع وخبرة الائتمان معاً؟	**اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان من جانب مانحي الائتمان الاناث وذوي الخبرة**	**11**	**-2.236**	**0.025**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني الموافقة على منح الائتمان من من جانب مانحي ذكور وقليل الخبرة	**9**	**-1.633**	**0.102**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان الاناث وذوي الخبرة	**11**	**-2.000**	**0.046**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان ذكور وقليل الخبرة	**9**	**-1.000**	**0.317**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني معدل الفائدة على القرض الذي يمكن الحصول من مانحي الائتمان الاناث وذوي الخبرة	**11**	**-0.816**	**0.414**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني معدل الفائدة على القرض االذي يمكن الحصول من مانحي الائتمان ذكور وقليل الخبرة	**9**	**-0.447**	**0.655**

يتضح من الجدول السابق رقم (11) أن قيمة (p-value) لهذا الاختبار (0.025،0.046،0.102 ،0.317) على التوالي، بالنسبة لنوع وخبرة مانح الائتمان معاً على **الموافقة على منح الائتمان وعلى مبلغ القرض الذي يمكن الحصول عليه**، مما يعني وجود **تأثير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على كلاً من الموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان اناث وذوي الخبرة، ووجود **تأثير غير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان ومبلغ

القرض الذي يمكن الحصول عليه من مانحي الائتمان ذكور وقليل الخبرة. كما يتضح ان قيمة (Z) المحسوبة في حالة مانحي الائتمان **من الاناث وذوي الخبرة** (2.236، 2.000) اكبر من قيمة (Z) المحسوبة في حالة مانحي الائتمان **من الذكور وقليل الخبرة** (1.633،1.000). مما يعني زيادة قوة التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على الموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان اناث وذوي خبرة عن الذكور وقليل الخبرة، أي بعد الاخذ في الاعتبار نوع وخبرة مانح الائتمان معاً.

كما يتضح من الجدول السابق رقم (11) أن قيمة (p–value) لهذا الاختبار (0.414،0.655)، بالنسبة لنوع وخبرة مانح الائتمان معاً على معدل الفائدة على القرض، **وجود تأثير غير معنوي** لنوع وخبرة مانح الائتمان معاً على العلاقة محل الدراسة (H_1). **لذا تمت الإجابة على سؤال البحث الثالث Q3 القائل: هل يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف نوع وخبرة مانح الائتمان معاً ." نعم" من حيث الموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه،" لا " من حيث معدل الفائدة على القرض. ويتضح من تتبع** إجابة الأسئلة في ظل اختبار نوع جنس وخبرة مانح الائتمان معاً على العلاقة محل الدراسة ومقارنتها بنتائج اختبار نوع جنس وخبرة مانح الائتمان كلاً على حدا، اتفاق النتائج بالنسبة لمبلغ القرض الذي يمكن الحصول عليه ومعدل الفائدة على القرض، واختلافها بالنسبة للموافقة على منح القرض.

(ج)حالة إدخال متغير معدل جديد (مستوى التأهيل العلمي لمانحي الأئتمان) بخلاف المتغيرين المعدلين المستخدمين في التحليل الأساسي:

وقد قامت الباحثة بإدخال متغير مستوى التأهيل العلمي لمانحي الائتمان (الذي تم قياسه بمتغير وهمي يأخذ القيمة (1) إذا كان مانحي الائتمان حاصل على دراسات عليا سواء دبلومة أو ماجستير أو دكتوراه، والقيمة (صفر) بخلاف ذلك) قياساً على (Baklouti, 2015 الصباغ، 2021)، ونتيجة لإشارة البعض (Trönnberg and Hemlin, 2012; Baklouti, 2015) ان مانحي الائتمان ذو التأهيل العلمي المرتفع يميلوا إلى تجنب التحيز في الاحكام، الامر الذي يؤدي إلى تحسين دقة توقعاتهم وتحسين جودة قراراتهم. كما اشار (الصباغ، 2021) إلى أنه يساعد اختلاف مستوى التأهيل العلمي لمانحي الائتمان على التقييم والتنبؤ بالمخاطر التي قد تواجهها الشركة. وفي سياق اخر، خلصت دراسة Fatokun et al. (2019) إلى ان اختلاف المستوى التعليمي يعطي اشارات ويُمكن من العمل والالمام بالتهديدات السيبرانية. **وبناءً عليه، ترى الباحثة وفقاً للدراسات السابق عرضها ان مستوى التأهيل العلمي لمانحي الائتمان قد تؤثر على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان، وبالتالي يمكن اشتقاق الفرض الرابع للبحث في صورته البديلة على النحو التالي:**

H_4: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف مستوى التأهيل العلمي لمانح الائتمان.

ويمكن اختبار هذا الفرض من خلال اختبار اثر مستوى التأهيل العلمي لمانح الائتمان على العلاقة بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على قرار منح الائتمان المتعلقة بالموافقة على او رفض منح الائتمان، وشروط منح الائتمان من حيث معدل الفائدة وقيمة القرض، وذلك على النحو التالي:

H_{4a}:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على الموافقة على منح الائتمان باختلاف مستوى التأهيل العلمي لمانح الائتمان.

H_{4b}: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على مبلغ القرض الذي يمكن الحصول عليه باختلاف مستوى التأهيل العلمي لمانح الائتمان.

H_{4c}: يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على معدل الفائدة على القرض باختلاف مستوى التأهيل العلمي لمانح الائتمان.

ولاختبار هذا الفرض احصائياً تم الاعتماد على اختبار ويلكوكسون Wilcoxon signed Rank Test اللامعلمي، **وظهرت نتائج اختبار هذا الفرض على النحو التالي:**

جدول 12 : نتيجة اختبار الفرض H_4 في ظل التحليل الآخر

الفرض	الاختبار الاحصائي	N	Z	P-value
H_4:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف مستوى التأهيل العلمي لمانح الائتمان	**اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان من جانب مانحي الائتمان المؤهلين علمياً**	**23**	**-2.887**	**0.004**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان من من جانب مانحي الائتمان غير المؤهلين علمياً	**22**	**-2.309**	**0.021**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان المؤهلين علمياً	**23**	**-2.714**	**0.007**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان غير المؤهلين علمياً	**22**	**-1.081**	**0.279**
	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على معدل الفائدة على القرض الذي يمكن الحصول عليه من مانحي الائتمان المؤهلين علمياً	**23**	**-0.264**	**0.792**

	اثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني على معدل الفائدة على القرض االذي يمكن الحصول عليه من مانحي الائتمان غير المؤهلين علمياً	**22**	**-0.115**	**0.848**

وبشأن الفرض الفرعي الأول، يتضح من الجدول السابق رقم (12) أن قيمة (p–value) لهذا الاختبار (0.004،0.021)، بالنسبة لمستوى التأهيل العلمي لمانح الائتمان **على الموافقة على منح القرض،** مما يشير إلى **وجود تأثير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح القرض من مانحي الائتمان مؤهلين أو غير مؤهلين علمياً. كما يتضح ان قيمة (Z) المحسوبة في حالة مانحي الائتمان ذو مستوى التأهيل العلمي المرتفع (2.887) اكبر من قيمة (Z) المحسوبة في حالة مانحي الائتمان ذو مستوى التأهيل العلمي المنخفض (2.309). مما يعني زيادة قوة التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على الموافقة على منح القرض بعد الاخذ في الاعتبار مستوى التأهيل العلمي لمانح الائتمان. وعليه فقد تم رفض فرض العدم وقبول الفرض البديل H_{4a}القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على الموافقة على منح الائتمان باختلاف مستوى التأهيل العلمي لمانح الائتمان.** ومن ثم **تم قبول الفرض الفرعي الأول (H_{4a}) للبحث.**

وبشأن الفرض الفرعي الثاني، يتضح من الجدول السابق رقم (12) أن قيمة (p–value) لهذا الاختبار (0.007،0.279)، بالنسبة لمستوى التأهيل العلمي لمانح الائتمان **على مبلغ القرض الذي يمكن الحصول عليه،** مما يعني **وجود تأثير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان مؤهلين علمياً، ووجود **تأثير غير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على مبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان غير مؤهلين علمياً. كما يتضح ان قيمة (Z) المحسوبة في حالة مانحي الائتمان ذو مستوى التأهيل العلمي المرتفع (2.714) اكبر من قيمة (Z) المحسوبة في حالة مانحي الائتمان ذو مستوى التأهيل العلمي المنخفض (1.081). مما يعني زيادة قوة التأثير المعنوي للإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على مبلغ القرض الذي يمكن الحصول عليه بالنسبة لمانحي الائتمان ذو مستوى تأهيل علمي مرتفع عن مانحي الائتمان ذو مستوى تأهيل علمي منخفض، اي بعد الاخذ في الاعتبار مستوى التأهيل العلمي لمانح الائتمان. وعليه فقد تم رفض فرض العدم وقبول الفرض البديل H_{4b} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على مبلغ القرض الذي يمكن الحصول عليه باختلاف مستوى التأهيل العلمي لمانح الائتمان.** ومن ثم **تم قبول الفرض الفرعي الثاني (H_{4b}) للبحث.**

وبالنسبة للفرض الفرعي الثالث، يتضح من الجدول السابق رقم (12) أن قيمة (p–value) لهذا الاختبار (0.792،0.848)، بالنسبة لمستوى التأهيل العلمي لمانح الائتمان **على معدل الفائدة على القرض،** مما يعني ان

مستوى التأهيل العلمي لمانح الائتمان **ليس له تأثير معنوي** على العلاقة محل الدراسة (H_1). وعليه فقد تم قبول فرض العدم ورفض الفرض البديل H_{4c} القائل بأنه **يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات على معدل الفائدة على القرض باختلاف مستوى التأهيل العلمي لمانح الائتمان**. ومن ثم تم **رفض الفرض الفرعي الثالث (H_{4c}) للبحث**. ويتضح من النتائج السابقة قبول الفرض الفرعي الاول والثاني، وبالتالي تم **قبول الفرض الرابع للبحث جزئياً**. **وترى الباحثة**، ان مانحي الائتمان ذو مستوي التأهيل العلمي المرتفع لديهم خبرة ومهارة عالية تُمكنهم من اتخاذ قرارات سليمة بشأن منح الائتمان، لذا يميل مانحي الائتمان المؤهلين علمياً من الموافقة على منح الائتمان وزيادة حجم القروض للشركات التي تتولى اهتماماً اكبر بإدارة مخاطر الامن السيبراني. اذ يكونوا اقل عرضة للهجمات السيبرانية، ومن ثم تكون سمعتهم وادائهم المالي أفضل مقارنة بالشركة التي لم تقوم بإدارة مخاطر الامن السيبراني.

(د) حالة الاعتماد على عينة ومجتمعين مختلفين (الأكاديميين):

تسعى الباحثة في هذا الاختبار إلى الأجابة عن التساؤل التالي: هل تختلف النتائج التي تم التوصل إليها فيما يتعلق باختبار فروض البحث من خلال التحليل الأساسي باختلاف مجتمع وعينة الدراسة؟ وللإجابة على هذا التساؤل قامت الباحثة بتوزيع الحالتين التجريبيتين على اعضاء هيئة التدريس والمدرسين المساعدين والمعيدين. ويوضح الجدول رقم (13) مدى اتفاق نتائج اختبار فروض البحث باختلاف مجتمع وعينة الدراسة:

جدول 13:مقارنة ما بين نتائج البحث في التحليل الاساسي والتحليل الآخر

الفروض في صيغتها البديلة	في ظل التحليل الأساسي	في ظل التحليل الآخر
H_1:يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان.	**تم قبوله جزئياً من حيث الموافقة أو رفض منح الائتمان، ومبلغ القرض الذي يمكن الحصول عليه.**	**تم قبوله جزئياً من حيث الموافقة أو رفض منح الائتمان، ومبلغ القرض الذي يمكن الحصول عليه.**
H_2:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف جنس مانح الائتمان.	**تم قبوله جزئياً من حيث الموافقة أو رفض منح الائتمان، ومبلغ القرض الذي يمكن الحصول عليه.**	**تم قبوله جزئياً من حيث الموافقة أو رفض منح الائتمان، ومبلغ القرض الذي يمكن الحصول عليه.**
H_3:يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف خبرة مانح الائتمان.	**تم قبوله جزئياً من حيث الموافقة أو رفض منح الائتمان، ومبلغ القرض الذي يمكن الحصول عليه.**	**تم قبوله جزئياً من حيث الموافقة أو رفض منح الائتمان، ومبلغ القرض الذي يمكن الحصول عليه.**

خلاصة اختبار الفروض، والاجابة على اسئلة البحث فى ظل كل من، التحليل الأساسى، والتحليلات الاخرى

الفرض	صياغة الفرض البديل	نتيجة اختبار الفروض في ظل التحليل الأساسي	حالات التحليلات الاخرى			
			حالة تغيير معالجة المتغير المعدل كمتغير رقابي	حالة اختبار تأثير كلا المتغيرين المعدلين معاً	حالة إدخال متغير معدل جديد (مستوى التأهيل العلمي لمانحي الأئتمان)	حالة الاعتماد على عينة ومجتمعين مختلفين (الأكاديميين)
H_1	يؤثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر معنوياً على قرار منح الائتمان	تم قبوله جزئياً	—	—	—	تم قبوله جزئياً
H_2	يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف جنس مانح الائتمان.	تم قبوله جزئياً	—	—	—	تم قبوله جزئياً
H_3	يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف خبرة مانح الائتمان.	تم قبوله جزئياً	—	—	—	تم قبوله جزئياً
H_4	يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف مستوى التاهيل العلمي لمانح الائتمان.	———	—	—	تم قبوله جزئياً	—
Q1	هل يؤثر جنس مانح الائتمان على قرار منح الائتمان، في سياق العلاقة التأثيرية بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان؟	—	نعم بشأن معدل الفائدة على القرض، ولا بشأن الموافقة على منح الائتمان وعلى مبلغ القرض الذي	—	—	—

			يمكن الحصول علية			
Q2	هل يؤثر خبرة مانح الائتمان على قرار منح الائتمان، في سياق العلاقة التأثيرية بين الافصاح عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان؟	—	لا	—	—	—
Q3	هل يختلف التأثير المعنوي للافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات في مصر على قرار منح الائتمان باختلاف نوع وخبرة مانح الائتمان معاً؟	—	—	تم قبوله جزئياً	—	—

5-النتائج والتوصيات ومجالات البحث المقترحة

استهدف البحث دراسة واختبار اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان. وكذلك اثر نوع وخبرة مانح الائتمان كمتغيرين مُعدلين على العلاقة سالفة الذكر. ولتحقيق هدف البحث تم تحليل الدراسات السابقة لاشتقاق فروض البحث وفرعياته، ثم تم اجراء دراسة تجريبية على عينة من المسئولين عن اتخاذ قرار منح الائتمان في البنوك التجارية المصرية. واظهرت نتائج **التحليل الاساسي** ان الافصاح عن تقرير إدارة مخاطر الامن السيبراني لشركات تكنولوجيا المعلومات يؤثر **بصورة معنوية** على قرار منح الائتمان من حيث الموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه، **وبصورة غير معنوية** على معدل الفائدة على القرض. وان الاثر المعدل لنوع وخبرة مانح الائتمان على العلاقة التأثيرية محل البحث في بيئة الاعمال المصرية كان **معنوياً** للموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه وغير معنوياً على معدل الفائدة على القرض.

كما توصلت الدراسة **في ظل التحليلات الإخرى**، إلى أفضلية تبني مدخل المتغيرات المعدلة مقارنة بمدخل المتغيرات الرقابية فيما يتعلق بأغلبية العلاقات التأثيرية محل الدراسة، وهو ما يدعم وجهة نظر الباحثة واقتناعها بأهمية اختبار وتبني هذا المدخل في اختبار العلاقات محل الدراسة **بالتحليل الأساسي**. كما خلصت الدراسة إلى وجود **تأثير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على كلاً من الموافقة على منح الائتمان

ومبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان اناث وذوي الخبرة، ووجود **تأثير غير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على الموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه من مانحي الائتمان ذكور وقليل الخبرة، **ووجود تأثير غير معنوي** للافصاح عن تقرير إدارة مخاطر الامن السيبراني على معدل الفائدة على القرض سواء كان مانحي الائتمان اناث وذوي خبرة او ذكور وقليل الخبرة.

كما **خلص البحث** إلى ان الاثر المعدل **لمستوى التأهيل العلمي لمانح الائتمان** على العلاقة التأثيرية محل البحث في بيئة الممارسة المهنية كان معنوياً للموافقة على منح الائتمان ومبلغ القرض الذي يمكن الحصول عليه وغير معنوياً على معدل الفائدة على القرض. واخيراً **خلص البحث إلى عدم اختلاف معنوية** العلاقة التأثيرية محل الدراسة في ظل الاعتماد على مجتمع وعينة مختلفة (الاكاديميين)، وهو ما يساهم في اضفاء المزيد من الوضوح والتفسير على العلاقة التأثيرية مجال البحث.

واستنادًا إلى ما سبق، **توصي الباحثة** بضرورة قيام الهيئة العامة للرقابة المالية، بتشجيع الشركات على اهمية الافصاح عن تقرير إدارة مخاطر الامن السيبراني، بهدف زيادة المحتوى المعلوماتي لفئات اصحاب المصالح المختلفة. **كما توصي الباحثة** بإصدار معيار محاسبي مصري لتوفير ارشادات كافية عن محتوى تقرير إدارة مخاطر الامن السيبراني. وايضاً **توصي الباحثة** بضرورة انشاء لجنة لأدارة مخاطر الامن السيبراني في كل شركة، وتوعيه الموظفين دائماً بخطورة الهجمات السيبرانية. واخيراً **توصي الباحثة** بضرورة اهتمام البحوث المحاسبية بمصر والمؤتمرات العلمية بأقسام المحاسبة بالجامعات المصرية بقضية الامن السيبراني عامةً واهمية الافصاح والتوكيد عن تقرير إدارة مخاطر الامن السيبراني من خلال إجراء المزيد من البحوث.

وأخيرًا، تعتقد الباحثة **بأهمية اتجاه البحث المحاسبي في مصر مستقبلاً نحو المجالات التالية: أثر الافصاح عن تقرير إدارة مخاطر الامن السيبراني** على العلاقة بين تعرض الشركة لإختراقات سيبرانية وقرار المستثمرين غير المحترفين – دراسة تجريبية، **أثر توكيد مراقب الحسابات على الافصاح عن تقرير إدارة مخاطر الامن السيبراني** على العلاقة بين تعرض الشركة لإختراقات سيبرانية وقرار منح الائتمان – دراسة تجريبية، **أثر الافصاح عن اختراقات الامن السيبراني** على تكلفة التمويل بالملكية، أثر **الاستثمار في الامن السيبراني** على تكلفة التمويل بالديون، **محددات افصاح** الشركات عن تقرير إدارة مخاطر الامن السيبراني.

المراجع

أولاً: المراجع العربية

الاستراتيجية الوطنية للامن السيبراني، 2017. المجلس الاعلى للأمن السيبراني، رئاسة مجلس الوزراء جمهورية مصر العربية.

الاستراتيجية الوطنية للامن السيبراني، 2024. المجلس الاعلى للأمن السيبراني، رئاسة مجلس الوزراء جمهورية مصر العربية.

الصباغ، احمد عبده الصباغ. 2021. اثر افصاح الشركات المقيدة بالبورصة المصرية عن حدود الاهمية النسبية على قرار منح الائتمان: دراسة تجريبية. **المجلة العلمية للدراسات المحاسبية**. مجلد 3 العدد 4 : 242-296.

الهيئة الوطنية للامن السيبراني.2018. نموذج سياسة إدارة مخاطر الامن السيبراني، السعودية.

شرف، ابراهيم احمد ابراهيم. 2023. اثر افصاح الشركات عن تقرير إدارة مخاطر الامن السيبراني على قرارات المستثمرين غير المحترفين: دراسة تجريبية. **مجلة الاسكندرية للبحوث المحاسبية**. مجلد 7 العدد1 :211-281

علي، عبد الوهاب نصر وفرج، هاني خليل. 2024. الرقابة والمراجعة الداخلية: مدخل نظري تطبيقي معاصر. **قسم المحاسبة كلية التجارة جامعة الاسكندرية** : 1- 418.

فرج، هاني خليل. 2023. اثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الامن الإلكتروني على قرار الاستثمار بالأسهم: دراسة تجريبية. **مجلة المحاسبة والمراجعة لاتحاد الجامعات**. مجلد 7 العدد 2: 129-209.

يوسف، اماني أحمد وهبه. 2022. واقع الافصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرارات الاستثمار ومنح الائتمان في البورصة : دراسة تطبيقية. **المجلة العلمية للدراسات التجارية والبيئية** . كلية التحارة – جامعة قناة السويس. مجلد 13 العدد 2: 28-109

ثانياً: المراجع الاجنبية

Algarni, A. M., Thayananthan, V. & Malaiya, Y. K. (202)1. Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied Sciences.* 11(8): 3678.

American Institute of Certified Public Accountants (AICPA). (2017). Cybersecurity risk management reporting fact sheet: 1-7

Anginer, D., Mansi, S. Warburton, A. J. & Yildizhan, C. (2011). Firm reputation and cost of debt capital. *avaliable at: https://mpra .ub.uni-muenchen.de/64965/1/MPR A_paper_64965.pdf*

Anwar, M., He, W, Ash. Yuan, I. X. Li, L. & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*. 69: 437-443.

Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review* 98(4): 1-32.

Baklouti, I. (2015). On the role of loan officers' psychological traits in predicting microcredit default accuracy. *Qualitative Research in Financial Markets***.** 7(3): 264-289.

Beck, T., Behr, P. & Guettler, A. (2010). Gender and banking: are women better loan officers. *Review of Finance, Forthcoming, European Banking Center Discussion Paper***:** 19-63

Bellucci, A., Borisov, A. & Zazzaro, A. (2010). Does gender matter in bank–firm relationships? Evidence from small business lending. *Journal of Banking & Finance*. 34(12): 2968-2984.

Binfarè, M. (2020). The real effects of operational risk: Evidence from data breaches. *A Thesis Submitted for The Degree of Doctor of Philosophy, The University of North Carolina at Chapel Hill.*

Boasiako, K., & O'Connor Keefe, M. (2021). Data breaches and firm credit risk. *Available at SSRN 3782111.*

Bui, T. L. (2023). Cybersecurity Events, Financial Analysts, and Earnings Forecast Uncertainty. *A Thesis Submitted for The Degree of Doctor of Philosophy, Concordia University.*

Cains, M. G., Flora, L. Taber, King, D. Z. & Henshe, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*. 42(8): 1643-1669.

Chatterjee, C., Agarwal, N. & Agarwal, S. (2024). Data Breach Notification Laws and Cost of Debt. *Available at SSRN 4812852.*

Cheng, X., Hsu, C. & Wang, T. D. (2022). Talk too much? The impact of cybersecurity disclosures on investment decisions. *Communications of the Association for Information Systems*. 50(1): 26.

Cheng, L., Liu, F. & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*. 7(5):1211

Committee of Sponsoring Organizations of the Treadway Commission(COSO). (2019). Governance and Enterprise Risk Management .*avalible at:* https://www.coso.org/files/ugd/3059 fccd21b48f95a748fb908882bb1ec96278.pdf

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*. 4(10): 13-21.

- Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems.* 49:1-15.

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review*. 40: 1-15.

Evans, C. A., Beyer, B. Mason, T. W. & West, A. N. (2023). Data Breach Severity and Debt Market Responses. *Accounting and the Public Interest.* 23(1): 76-109.

Fatokun, F. B., Hamid, S. Norman, A & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. *In Journal of Physics: Conference Series.* 1339 (1): 1-14.

Frank, M. L., Grenier, J. H. Pyzoha, J. S. & Zielinski, N. B. (2023). Implications of Enhanced Cybersecurity Risk Management Reporting and Independent Assurance. *Current Issues in Auditing***.** 17(1) :11-18.

Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value**.** *Journal of Risk and Insurance*. 89(3): 725-763.

Giuca, O., Popescu, T. M. A. Popescu, M. Prostean, G. & Popescu, D. E. (2021). A survey of cybersecurity risk management frameworks. *In Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications. Springer International Publishing.* I (8): 240-272

Gordon, L. A., Loeb, M. P. Lucyshyn, W. & Zho, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity***.** 1(1): 3-17.

Harris, D., Kuzey, C. Naaman, C. & Sahyoun, N. (2023). Cybersecurity Risk Disclosure Quality: Does it Affect the Cost of Debt? *Journal of Forensic and Investigative Accounting*. 15(2):1-21.

Havakhor, T., Rahman, M. S. & Zhang, T. (2020). Cybersecurity investments and the cost of capital. *SSRN Electronic Journal*: 1-48.

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches? *The Accounting Review*. 96(3): 261-286.

Kamiya, S., Kang, J. K. Kim, J. Milidonis, A. & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139(3): 719-749.

Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. *International Journal of Research in Business and Social Science.* 11**(**6): 334-340.

Kelton, A. S. (2021). How to reduce the cybersecurity breach contagion effect? *Current Issues in Auditing*. 15(2): 1-9.

Ladime, J., Sarpong-Kumankoma, E. & Osei, K. A. (2013). Determinants of bank lending behavior in Ghana. *Journal of Economics and Sustainable Development*. 4(17): 42-47.

Miller, J., & Smith, L. (2002). The Effects of the Level of Assurance, Accounting Firm, Capital Structure, and Bank Size on Bank Lending Decisions. *Journal of Accounting, Auditing & Finance* 17: 51 – 71.

Nguyen, A. H., & Nguyen, D. D. (2020). The Impact of Cash Flow Statement on Lending Decision of Commercial Banks: Evidence from Vietnam. *Journal of Asian Finance Economics and Business* 7(6):85-93

Olokoyo, F. O. (2011). Determinants of commercial banks' lending behavior in Nigeria. *International journal of financial research*. 2(2): 61.

Rahmawati, W., Siregar, S. Shauki, V. R. E. & Anggraita.V. 2024. Enterprise risk management and cost of debt: the moderating role of crisis. *Cogent Business & Management***.** 11(1), 2296702.

Rincon A .C, & Ordóñez.G. (2023). The impact of cybersecurity management practices on the likelihood of cyber events and its effect on financial risk**.** *Available at https://www. moodysanalytics. com/ -/media/whitepaper/2023/The-Impact-Of-Cyber-Security-Management-Practices.pdf*

Ruhnke, K., Pronobis, P. & Michel.M. (2018). Effects of audit materiality disclosures: evidence from credit lending decision adjustments. *Betriebswirtschaftliche Forschung und Praxis (BFuP).* 70(4): 440-471.

Santhosh, T. & Thiyagu.K. 2021. Cognizing Scams and Frauds in Cyber Space and its Preventive Measures. *Available at: Academia Letters, Article 1170, https://doi.org/10.20935/AL1170*

Sheneman, A. (2022). Contagion or Competitive Effects? Lenders' Response to Peer Firm Cyberattacks. *Working Paper. Available at https://weis2022.econinfosec.org/wp-content/uploads/sites/ 10/2022/06/weis22-sheneman.pdf*

Sheneman, A. (2017). Cybersecurity risk and the cost of debt. *Available at SSRN 3406217.*

Singh, A. (2023). Data breaches (hacking) and trade credit. *Global Finance Journal*. 57:1-13.

Trönnberg, C. C., & Hemlin.S. (2012). Banker's lending decision making: a psychological approach**.** *Managerial Finance.* 38(11): 1032-1047.

- Wang, J., Huang, X. Ni, X. & Chan.K. C. (2023). Meeting with Creditors in Front of the Black Mirror: Information Security Certification and Corporate Debt Structure**.** *Available at SSRN 4404033.*

- Yang, L., Lau, L. & Gan.H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management.* 28(1): 167-183.

ملحق (1)

الدراسة التجريبية

السيد الاستاذ الفاضل،،

تحية طيبة وبعد....

تقوم الباحثة باجراء تجربة على حالة عملية فعلية لأحدى الشركات بهدف اتمام بحث بعنوان " اثر افصاح الشركات عن تقرير إدارة مخاطر الامن السيبراني على قرار منح الائتمان – الدور المعدل لخبرة ونوع مانح الائتمان – دراسة تجريبية".

وتقدر الباحثة لكم مسبقاً حسن تعاونكم في اثراء المعرفة المحاسبية، لذلك المرجو من سيادتكم التكرم بقراءة الحالة المرفقة والرد على الاسئلة المرافقة لها بدقة. وتؤكد الباحثة ان جميع البيانات والآراء سوف تكون محل سرية تامة ولن تستخدم إلا لأغراض البحث العلمي.

وتقبلوا بقبول فائق الاحترام والتقدير

الباحثة/ نيفين صلاح علي علي

مدرس المحاسبة والمراجعة – كلية الاعمال جامعة الاسكندرية

أولاً: البيانات الشخصية

الاسم (اختياري) : .....

اسم البنك (اختياري): .....

النوع:

- ذكر
- انثى

العمر (اختياري): .....

الوظيفة : .....

المؤهل الدراسي:

- بكالوريوس محاسبة
- دبلوم دراسات عليا في .....
- ماجستير (o اكاديمي o مهني)
- دكتواره (o اكاديمية o مهنية)
- شهادات اخرى (برجاء ذكرها).....

عدد سنوات الخبرة:

- اقل من 5 سنوات
- من 5 سنوات إلى اقل من 10 سنوات
- من 10 سنوات إلى اقل من 15 سنة
- من 15 سنة إلى اقل من 20 سنة
- من 20 سنة فأكثر

ثانياً: المصطلحات الفنية ذات الصلة بموضوع البحث :

الامن السيبراني: هي مجموعة التقنيات والعمليات والممارسات المصممة لحماية الشبكات والانظمة واجهزة الكمبيوتر والبرامج والشبكات وقواعد البيانات من الهجمات الالكترونية والوصول غير المصرح به او التعطيل او سوء استخدام او الاستغلال غير المشروع.

إدارة مخاطر الامن السيبراني: هي تنفيذ الشركة مجموعة من السياسات والعمليات والاجراءات الرقابية والضوابط المصممة لحماية معلوماتها وانظمتها الالكترونية من الاحداث والتهديدات السيبرانية التي يمكن ان تعوق تحقيق اهداف الشركة.

الحالة التجريبية الاولى

أولاً: نبذة عن المنشأة

تنتمي المنشأة س لقطاع تكنولوجيا المعلومات وهي شركة مساهمة مصرية طبقاً لأحكام القانون رقم 159 لسنة 1981. والغرض منها هو تقديم خدمات التشغيل المخصصة لأنظمة تكنولوجيا المعلومات والاتصالات وإدارة وتشغيل وصيانة اجهزة معدات وشبكات الحاسب الالي.

ثانياً: البيانات المالية

وفيما يلي ملخص للقوائم المالية للشركة عن السنة المنتهية في 2023/12/31، 2022/12/31:

قائمة المركز المالي في ٢٠٢٣/١٢/٣١

البيان	٢٠٢٣/١٢/٣١	٢٠٢٢/١٢/٣١
الاصول		
اجمالي الاصول غير المتداولة	١,٥٧٧,٠٣٩,٩٠٢	١,١١٥,١٤٤,١٧١
اجمالي الاصول المتداولة	٤,١٩٣,٢٥٠,٠١٥	٢,٦٤٤,٥٤٧,١٤٣
اجمالي الاصول	٥,٧٧٠,٢٨٩,٩١٧	٣,٧٥٩,٦٩١,٣١٣
حقوق الملكية		
رأس المال المصدر والمدفوع	١,٦٥٣,٦٥٢,٠٦٠	٨٥٣,٦٥٢,٠٦٠
احتياطيات	٥٣,١٥٠,٠٢٣	٤٧,١٢٩,٠٢٤
ارباح محتجزة	٣٥٩,٥٤٠,٥٥١	٢٦٧,٢٤٤,٧٤١
صافي ارباح العام	١٧٧,٧٨٥,٣٤٩	١٢٠,٤١٩,٦٢٥
اجمالي حقوق الملكية	٢,٣٧٦,٠٢٨,٠٦٦	١,٣٣٨,٠٠٧,٧٣٢
الالتزامات غير المتداولة	٨٥,٧٦٣,٧٣٠	٥٠,٢٤٥,١٨٧
الالتزامات المتداولة	٣,٣٠٨,٤٩٨,١٢١	٢,٣٧١,٤٣٨,٤٠٤
اجمالي حقوق الملكية والالتزامات	٥,٧٧٠,٢٨٩,٩١٧	٣,٧٥٩,٦٩١,٣١٣

قائمة الدخل عن السنة المنتهية في ٢٠٢٣/١٢/٣١

البيان	٢٠٢٣/١٢/٣١	٢٠٢٢/١٢/٣١
ايرادات النشاط	١,٤٩٣,٤٥٣,٨٠٤	١,١١٦,٢٦٦,٠٧٧
تكلفة النشاط	(٦٠٦,٣١٤,٦١٦)	(٤٩٢,٤٢٤,٧٦٣)
مجمل الربح	٨٨٧,١٣٩,١٨٨	٦٢٣,٨٤١,٣١٤
صافي الربح التشغيلي	٢٠٤,٣٢٨,٢٤٩	١٤٣,١٢٧,٢١٣
صافي الربح بعد الضريبة	١٧٧,٧٨٥,٣٤٩	١٢٠,٤١٦,٦٢٥

قائمة التدفقات النقدية عن السنة المنتهية في ٢٠٢٣/١٢/٣١

البيان	٢٠٢٣/١٢/٣١	٢٠٢٢/١٢/٣١
صافي التدفقات النقدية من الانشطة التشغيلية	١,٣٥٥,٨٥٤,٦٣١	٨٢٠,٩٢٣,٣٧٩
صافي التدفقات النقدية من الانشطة الاستثمارية	-٢١٣,٩٩٥,٢٨٨	-٩٢,٠١٤,٩٧٣
صافي التدفقات النقدية من الانشطة التمويلية	٤٥,٩٣٧,١١٣	٥٥٥,٤٢٣,٩٠٩
النقدية اخر المدة	٢,٦٨٦,٨٦٨,٨٧٤	١,٠٧٣,٣٨٩,٣٧٢

نبذة عن الايضاحات المتممة:

تم إعداد القوائم المالية المجمعة في 31 ديسمبر 2023 طبقاً لمعايير المحاسبة المصرية وفي ضوء القوانين واللوائح المصرية ذات العلاقة.

المخاطر التي تواجهها الشركة:

خطر الائتمان: يشير إلى خطر عدم وفاء الطرف المقابل لإلتزاماته التعاقدية، والتي ينتج عنها خسائر مالية للشركة، وينشأ هذا الخطر بصفة رئيسية من عملاء الشركة والمدينين الاخرين.

خطر السيولة: يشير إلى خطر عدم وفاء الشركة بإلتزاماتها في تاريخ استحقاقها.

خطر السوق: يشيرإلى خطر التغيرات في اسعار السوق مثل اسعار صرف العملات الاجنبية وسعر الفائدة وأسعار أدوات حقوق الملكية

مخاطر الامن السيبراني: يشير إلى الهجمات السيبرانية التي يمكن ان تؤدي إلى تخفيض الايرادات أو زيادة المصروفات أو الحاق الضرر بسمعة الشركة.

في ضوء قراءتك للقوائم المالية والايضاحات المتممة السابقة، وبإعتبارك مسئول عن منح الائتمان في احد البنوك التجارية، وتقدمت الشركة للحصول على قرض بضمان الاصول الثابتة في 2023/12/31 لمدة 6 سنوات :-

1-هل توافق على منح القرض (ضع علامة امام √ الاجابة المناسبة)؟

1 غير موافق تماما	2 غير موافق لحد ما	3 موافق	4 موافق بدرجة كبيرة	5 موافق تماماً

2-في حالة الموافقة على منح الشركة القرض، في تقديرك ما هو قيمة القرض الذي يمكن ان توافق على اقراضة للشركة:

أ-تتراوح قيمة القرض ما بين مليار إلى مليار و 300 الف جنيه(حدد المبلغ .....)

ب-قيمة القرض اقل من مليار (حدد المبلغ .....)

ج- قيمة القرض اكبر من مليار و 300 الف جنيه (حدد المبلغ .....)

3-اذا علمت ان سعر الفائدة على مثل هذا القرض المعلن من البنك المركزي هو (22.25%) ، ما هو تقديرك لمعدل الفائدة الذي تطلبه من الشركة

أ-22.25%

ب-اقل من 22.25% (حدد المعدل .....)

ج- اكبر من 22.25% (حدد المعدل .....)

الحالة التجريبية الثانية

افترض في الحالة السابقة ما يلي:

ان الشركة لديها إدارة مخاطر بها قسم خاص بإدارة مخاطر الامن السيبراني وقد ظهر تقرير إدارة مخاطر الامن السيبراني للشركة لعام 2023 كما يلي:

تقرير إدارة مخاطر الامن السيبراني للشركة (س) لعام 2023

السادة / الهيئة العامة للرقابة المالية

إدارة البورصة المصرية

مجلس إدارة الشركة

يتمثل برنامج إدارة مخاطر الأمن السيبراني في مجموعة من السياسات والعمليات والضوابط المصممة لحماية المعلومات والأنظمة من الأحداث والهجمات الاللكترونية والوصول غير المصرح به ، التي من الممكن أن تؤثر على اداء عملها بشكل فعال وكفء، كما يلي:

-قام مجلس إدارة الشركة بأنشاء إدارة خاصة للامن السيبراني، وتكوين فريق إدارة المخاطر الإلكترونية متعدد الوظائف.

-قامت الشركة بتصميم هيكل رقابة للامن السيبراني لمواجهة المخاطر وتقوم بعمل تقييم مستمر للتأكد من فاعلية وتصميم وتشغيل الضوابط الداخلية.

-تقوم الشركة بتحديد وتقييم المخاطر السيبرانية التي قد تواجهها، والنظر في احتمالية وقوعها

-يتم عمل تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالامن السيبراني واتخاذ الاجراءات التصحيحية.

ولم تتعرض الشركة لأي هجمات سيبرانية في السنة المالية المنتهية في 2023/12/31 ، وذلك بفضل فعالية برنامج الأمن السيبراني لديها، والذي تمكنت الشركة من خلاله تحقيق اهداف الامن السيبراني المتمثلة في الحفاظ على سلامة وسرية وتوافر المعلومات

التاريخ 2024/3/25

التوقيع

عضو مجلس الإدارة المنتدب

▪ **تتبنى إدارة الشركة الافصاح عن تقرير إدارة المخاطر بما فيها مخاطر الامن السيبراني ضمن مرفقات القوائم المالية. ولذلك تم ارسال هذا التقرير إلى هيئة الرقابة المالية وإدارة البورصة مرفقاً بالقوائم المالية سنة 2023.**

في ضوء قراءتك للقوائم المالية والايضاحات المتممة وتقرير إدارة مخاطر الامن السيبراني وبإعتبارك مسئول عن منح الائتمان في احد البنوك التجارية، وتقدمت الشركة للحصول على قرض بضمان الاصول الثابتة في 2023/12/31 لمدة 6 سنوات:-

1-هل توافق على منح القرض (ضع علامة امام √ الاجابة المناسبة)؟

1	2	3	4	5
غير موافق تماما	**غير موافق لحد ما**	موافق	**موافق بدرجة كبيرة**	**موافق تماماً**

2-في حالة الموافقة على منح الشركة القرض، في تقديرك ما هو قيمة القرض الذي يمكن ان توافق على اقراضة للشركة:

أ-تتراوح قيمة القرض ما بين مليار إلى مليار و300 الف جنيه (حدد المبلغ .....)

ب-قيمة القرض اقل من مليار (حدد المبلغ .....)

ج- قيمة القرض اكبر من مليار و 300 الف جنيه (حدد المبلغ .....)

3-اذا علمت ان سعر الفائدة على مثل هذا القرض المعلن من البنك المركزي وهو (22.25%) ، ما هو تقديرك لمعدل الفائدة الذي تطلبه من الشركة

أ-22.25%

ب-اقل من 22.25% (حدد المعدل .....)

ج- اكبر من 22.25% (حدد المعدل .....)