أثر الأمن السيبراني على تعزيز التحول الرقمي المحاسبي في الشركات الصناعية

أ. عيده جمعة ياسين
كليه الاقتصاد / جامعة طبرق
eidagm59@yahoo.com

الملخص:

يتمثل الهدف الرئيسي في دراسة " دراسة أثر الأمن السيبراني على تعزيز التحول الرقمي في بيئة الأعمال المحاسبية في الشركات الصناعية الليبية"؛ يسعى هذا البحث للإجابة عن السؤال الرئيسي التالي: ما أثر الأمن السيبراني على تعزيز التحول الرقمي في بيئة الأعمال المحاسبية في الشركات الصناعية الليبية؟، تم إتباع المنهج الوصفي التحليلي، أجريت الدراسة الميدانية على الشركات الصناعية في دولة ليبيا تم إعداد هذا الدراسة خلال عام 2024، وتوصلت نتائج البحث هناك تأثير لإدارة مخاطر الأمن السيبراني على تعزيز الاستقرار المالي والشمول، تدرك إدارة الشركات الصناعية الليبية أن التهديدات للأمن السيبراني وتسريب البيانات يمكن أن تقوض الاستقرار المالي وتؤدي إلى خسائر مالية يمكن أن تتعرض لها، وتقلل من تعرضها وتؤمن ضد مثل هذه المخاطر من خلال تبني تدابير الأمن السيبراني للأمن المالي، يوجد في الشركات الصناعية الليبية فريق استجابة لحوادث الأمن السيبراني لدعم زيادة الجهود لزيادة الكفاءة وتحسين استخدام القدرات والنمو المستمر لنظام الأمن السيبراني، حيث تطور الشركات الصناعية الليبية وتحدد استراتيجيات التخفيف من المخاطر السيبرانية التي يتم تنفيذها من خلال تحديد المصدر والذي يؤدي إلى مثل هذه المخاطر واحتمال حدوثها، حيث تديرها من خلال الاستفادة من تدابير الأمن الصحيحة في المجال الذي يمكن من تعزيز المدخلات المالية، وتقوم الشركات الصناعية الليبية بوضع استراتيجيات وسياسات للتخفيف من المخاطر السيبرانية مع تفصيل المهام ورفع معدل المشاركة في التعامل مع التهديدات السيبرانية والتعافي منها في وقت قياسي، وهذا يؤدي إلى الاستقرار والإصلاح المالي، وعلى نحو مماثل، حيث تستخدم معايير وإطار عمل دولي راسخ في إدارة المخاطر للتخفيف من المخاطر السيبرانية، و تقدم تقريرًا يحتوي على معلومات أساسية حول المخاطر السيبرانية بالإضافة إلى طرق السيطرة عليها لحماية العملاء.

الكلمات المفتاحية: الأمن السيبراني؛ التحول الرقمي؛ الشمول المالي؛ الاستقرار المالي؛ الإصلاح المالي.

Abstract:

The main objective is to study “The impact of cybersecurity on enhancing digital transformation in the accounting business environment in Libyan industrial companies." This research seeks to answer the following main question: What is the impact of cybersecurity on enhancing digital transformation in the accounting business environment in Libyan industrial companies? The descriptive-analytical approach was followed. The field study was conducted on industrial companies in the State of Libya. This study was prepared during the year 2024. The research results showed that there is an impact of cybersecurity risk management on enhancing financial stability and inclusion. The management of Libyan industrial companies realizes that threats to cybersecurity and data leakage can undermine financial stability and lead to financial losses that they may be exposed to. It reduces its exposure and insures against such risks by adopting cybersecurity measures for financial security. Libyan industrial companies have a cybersecurity incident response team to support increased efforts to increase efficiency, improve capacity utilization, and ensure continuous growth of the cybersecurity system. Libyan industrial companies develop and identify cyber risk mitigation strategies that are implemented by identifying the source that leads to such risks and the likelihood of their occurrence. They manage them by utilizing the right security measures in the field that can enhance financial inputs. Libyan industrial companies develop strategies and policies to mitigate risks Cyber with detailed tasks and raising the rate of participation in dealing with cyber threats and recovering from them in record time, which leads to financial stability and reform, similarly, the use of established international standards and frameworks in risk management to mitigate cyber risks and provide a report containing basic information about cyber risks as well as ways to control them to protect customers.

Keywords: Cybersecurity; Digital Transformation; Financial Inclusion; Financial Stability; Financial Reform.

1. مقدمة:

شهدت السنوات الأخيرة تطورًا هائلًا في تكنولوجيا المعلومات، مما أدى إلى إحداث ثورة معرفية واسعة تُعرف باسم الثورة الصناعية الرابعة. وقد امتد تأثير هذا التحول إلى مختلف المجالات، وخاصة بيئة الأعمال المحاسبية، حيث أصبح تقييم متطلبات الأمن السيبراني ضرورة ملحّة لضمان حماية المعلومات المالية والمحاسبية في الشركات الصناعية. يهدف هذا التقييم إلى تحليل المخاطر الأمنية التي تهدد أنظمة المعلومات المحاسبية، بالإضافة إلى تحديد الأساليب الفعالة للتعامل معها.

في العصر الرقمي، تُعد أنظمة المعلومات والإنترنت من الأصول الحيوية لأي مؤسسة، حيث تحتوي على بيانات حساسة تتعلق بالجوانب التجارية والشخصية والمالية. ومع تصاعد التهديدات السيبرانية، بات من الضروري تعزيز أمن المعلومات لضمان استمرارية العمل وحماية البيانات من الاختراق والاستغلال. تُعتبر أنظمة التحول الرقمي عنصرًا أساسيًا في الشركات الصناعية، مما يجعل أمن هذه الأنظمة عاملًا حاسمًا في ضمان استدامة العمليات وسلامة التقارير المالية وغير المالية. ومع تطور التقنيات الحديثة، تواجه أنظمة المحاسبة تحديات متزايدة في مجال الأمن السيبراني، مثل الهجمات الإلكترونية الناتجة عن ضعف الأنظمة ووجود ثغرات برمجية، أو بسبب عدم مواكبة التحديثات التكنولوجية المستمرة، فضلًا عن تعقيد الأنظمة المحوسبة الذي قد يجعلها أكثر عرضة للمخاطر.

كل هذه التحديات تطرح تساؤلات حول أهمية ودور تقنيات الأمن السيبراني في حماية المعاملات المالية والبيانات من الانتهاكات والاختراقات. لذا، أصبح من الضروري اعتماد مناهج جديدة لفهم البيئة التنظيمية المحاسبية، وتحديد الشروط الضرورية والكافية التي يجب أن يلتزم بها المحاسبون ضمن إطار الأمن السيبراني للمؤسسات.

1.1. مشكلة البحث:

باتت دراسة الأمن السيبراني للنظام المحاسبي القائم على التحول الرقمي ضرورة ملحّة، إذ يُعد الأمن السيبراني الركيزة الأساسية لحماية المعلومات المحاسبية وضمان سلامتها. فكلما ازدادت العمليات المحاسبية تعقيدًا، زادت معها التهديدات السيبرانية، سواء كانت تهديدات خارجية مثل سرقة البيانات المحاسبية والسرية التجارية، أو تهديدات داخلية مثل التلاعب غير القانوني في البيانات المحاسبية (Mahmood, et al., 2022).

تُعد الشركات الصناعية من أكثر المؤسسات حرصًا على إدارة مخاطر الأمن السيبراني، نظرًا للآثار

السلبية المحتملة التي قد تنتج عن الهجمات السيبرانية، والتي تشمل الخسائر المالية المباشرة وغير المباشرة، وتعطيل العمليات التشغيلية، والإضرار بالسمعة المؤسسية. كما أن الشركات الصناعية الليبية، نظرًا لدورها الحيوي في الوساطة المالية، تُعد هدفًا جذابًا للهجمات السيبرانية، مما قد يؤثر على الاستقرار المالي والشمول المالي.

ومن هذا المنطلق، تنبثق مشكلة الدراسة من الحاجة إلى فهم تأثير الأمن السيبراني على التحول الرقمي في بيئة الأعمال المحاسبية، وهو ما يدفعنا إلى طرح السؤال الرئيسي التالي:

ما مدى تأثير الأمن السيبراني على تعزيز التحول الرقمي في بيئة الأعمال المحاسبية في الشركات الصناعية الليبية؟

ويتفرع عن هذا السؤال الرئيسي مجموعة من التساؤلات الفرعية، وهي:

1. ما المقصود بالتحول الرقمي وما هي تطبيقاته؟
2. ما مفهوم الأمن السيبراني وما أهميته في مهنة المحاسبة؟
3. كيف تؤثر إدارة مخاطر الأمن السيبراني على الاستقرار المالي في الشركات الصناعية الليبية؟
4. ما دور إدارة مخاطر الأمن السيبراني في تعزيز الشمول المالي داخل الشركات الصناعية الليبية؟

1.2. أهمية البحث:

تكتسب هذه الدراسة أهمية أكاديمية لكونها تسعى إلى تقديم رؤية حديثة حول تأثير إدارة مخاطر الأمن السيبراني على تعزيز التحول الرقمي في المحاسبة، وذلك من خلال دعم الاستقرار المالي والشمول المالي في الشركات الصناعية الليبية. وتزداد أهمية الدراسة من خلال قدرتها على تشخيص واقع إدارة مخاطر الأمن السيبراني، مما يسهم في تعزيز تطبيق الشمول المالي لدعم الاستقرار المالي، خصوصًا في الشركات الصناعية المدرجة في البورصة الليبية، وتنقسم أهمية الدراسة إلى قسمين رئيسيين:

الأهمية العلمية: تنبع الأهمية العلمية للدراسة من كونها تتناول أحد المواضيع الحديثة والمهمة في مجال التحول الرقمي لمهنة المحاسبة والأمن السيبراني، مما يساهم في إثراء المعرفة الأكاديمية وفتح آفاق جديدة أمام الباحثين. كما توفر الدراسة مرجعًا علميًا يتيح للباحثين فرصة التوسع في دراسة تأثير التحول الرقمي على مهنة المحاسبة، إلى جانب استكشاف دور إدارة مخاطر الأمن السيبراني في دعم الاستقرار المالي والشمول المالي. وبالتالي، قد تكون هذه الدراسة نقطة انطلاق للعديد من الأبحاث المستقبلية ذات الصلة.

الأهمية العملية: تتجلى الأهمية العملية للدراسة في تقديم رؤى واضحة حول كيفية إدارة مخاطر الأمن السيبراني في الشركات الصناعية الليبية، مما يساعد على تعزيز التحول الرقمي في المحاسبة. كما تساهم نتائج الدراسة في اقتراح توصيات عملية تهدف إلى دعم الاستقرار المالي وتعزيز الشمول المالي، مما يساهم في تطوير استراتيجيات أكثر فاعلية لمواجهة التحديات السيبرانية في بيئة الأعمال المحاسبية.

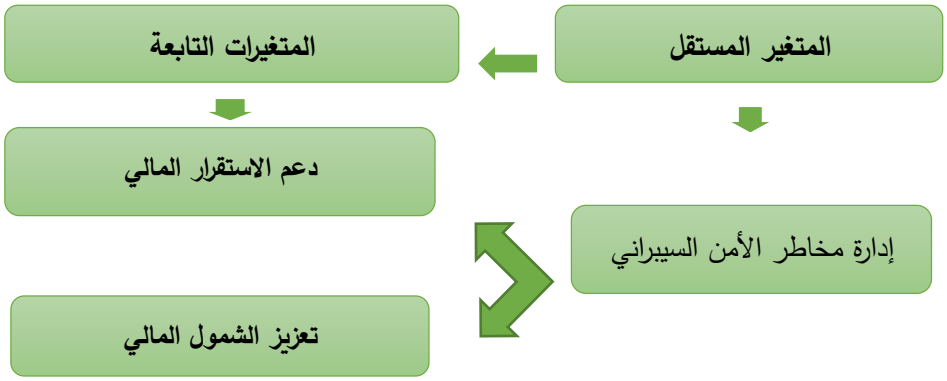
1.3. أهداف البحث: يهدف هذا البحث إلى دراسة أثر الأمن السيبراني على تعزيز التحول الرقمي في بيئة الأعمال المحاسبية في الشركات الصناعية الليبية، ومن هذا الهدف الرئيسي تتفرع الأهداف الفرعية التالية:

1. تحليل تأثير تطبيق تقنيات التحول الرقمي على بيئة الأعمال المحاسبية.
2. تحديد المخاطر السيبرانية التي تواجه الممارسات المحاسبية التقليدية، وفهم دورها في تسريع رقمنه بيئة الأعمال المحاسبية نحو التحول الرقمي.
3. دراسة أثر إدارة مخاطر الأمن السيبراني في دعم الاستقرار المالي داخل الشركات الصناعية الليبية.
4. توضيح دور إدارة مخاطر الأمن السيبراني في تعزيز الشمول المالي في الشركات الصناعية الليبية.

1.4. فروض البحث: بناءً على مشكلة الدراسة وأهدافها، يمكن صياغة الفرضيات التالية:

1. توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha < 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي في الشركات الصناعية الليبية.
2. توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha < 0.05$) بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في الشركات الصناعية الليبية.

1.5. نموذج متغيرات الدراسة:



شكل رقم (1) نموذج لمتغيرات الدراسة

1.6. حدود البحث: تمثلت حدود الدراسة فيما يلي:

1. **الحدود الزمانية:** تم إعداد هذا الدراسة خلال عام 2024.
2. **الحدود المكانية:** يطبق هذا الدراسة على الشركات الصناعية الليبية.
3. **الحدود البشرية:** تتكون من محاسبين في الشركات الصناعية الليبية
4. **الحدود العلمية:** دراسة أثر إدارة الأمن السيبراني على تعزيز التحول الرقمي المحاسبي لدعم الاستقرار والشمول المالي للشركات الصناعية الليبية.

1.7. الدراسات السابقة:

دراسة Polishchuk et al. (2024): هدفت هذه الدراسة إلى تحليل أثر الأمن السيبراني على استقرار المؤسسات المالية، مع التركيز على فعالية التدابير الأمنية في تعزيز مرونة المؤسسات المالية الأوكرانية ضد التهديدات السيبرانية. استخدمت الدراسة الأساليب النوعية لفحص تجارب المؤسسات الأوكرانية التي تعتمد على استراتيجيات دفاعية رقمية متطورة للحفاظ على استمراريتها، خصوصًا في ظل النزاعات العسكرية العالمية، توصلت الدراسة عدة نتائج منها: أكدت الدراسة على أهمية أنظمة الأمن السيبراني القوية في ضمان الاستدامة التشغيلية والمالية للمؤسسات، كما شددت على ضرورة تحديث البرامج والأجهزة، إلى جانب تحسين الحلول الإدارية لمواجهة التهديدات السيبرانية المتزايدة. وأوصت بضرورة الابتكار المستمر لتعزيز الأمن السيبراني.

دراسة Abrahams et al. (2024): ركزت هذه الدراسة على العلاقة بين المحاسبة والأمن السيبراني، من خلال تحليل التكامل بينهما لتحقيق الامتثال والشفافية في المؤسسات. استخدمت الدراسة النماذج التحليلية والأساليب الإحصائية، ومن نتائج الدراسة انها توصلت:إلى أن التكامل الفعّال بين المحاسبة والأمن السيبراني يعزز حماية البيانات المالية والشفافية، ويحد من المخاطر القانونية، مما يسهم في تحسين الأداء المؤسسي والامتثال التنظيمي. كما اقترحت استراتيجيات شاملة تشمل التعاون بين الفرق المختلفة، والتحديث المستمر للتقنيات والإجراءات الأمنية.

دراسة Daoud & Serag (2022): هدفت هذه الدراسة إلى تطوير إطار لدراسة تأثير الأمن السيبراني على البيانات المحاسبية، بهدف زيادة الثقة في التقارير المالية، في ظل تطورات مثل البيانات الضخمة، وإنترنت، وتكامل أنظمة الحوسبة، وزيادة والتقنيات الافتراضية. كما سعت إلى تمكين الممارسين من تقييم تهديدات الأمن السيبراني وفهم استراتيجيات الاستجابة، من خلال نهج الحدث–التأثير–الاستجابة.

النتائج: أكدت الدراسة على دور الأمن السيبراني في حماية البيانات المالية والمعلومات المحاسبية مع الإشارة إلى ضرورة استجابة فعالة من قبل الإدارة، المستثمرين، المراجعين، والجهات التنظيمية. كما قدمت مجموعة من الاستراتيجيات المقترحة لتعزيز الأمن السيبراني، من أبرزها: تقييم المخاطر: تحديد الثغرات والتهديدات المحتملة من خلال تقييم شامل للمخاطر، وتدريب الموظفين: رفع الوعي الأمني عبر برامج تدريبية متخصصة، وتطوير استراتيجيات استجابة: وضع خطط فعالة للاستجابة للحوادث السيبرانية، وتعزيز التعاون الداخلي: توثيق التعاون بين فرق الأمن السيبراني والمراجعة الداخلية لتعزيز الحماية. وتظهر هذه الدراسات أهمية الأمن السيبراني كعنصر محوري في تعزيز التحول الرقمي للمحاسبة، وتحقيق الاستقرار المالي، وتعزيز الشمول المالي، مما يؤكد الحاجة إلى تبني استراتيجيات قوية لإدارة المخاطر السيبرانية.

التعليق على الدراسات السابقة :يرى الباحث أن معظم الدراسات السابقة التي تناولت العلاقة بين التحول الرقمي والأمن السيبراني قد ركزت على تعزيز الأمن والخصوصية من خلال توفير منصات آمنة وشفافة للمعاملات الرقمية ومشاركة البيانات. ومع ذلك، لم يتوصل الباحث إلى دراسات تناولت الدور المتبادل بين التحول الرقمي المحاسبي والأمن السيبراني بشكل مباشر، أو تلك التي ناقشت متطلبات الأمن السيبراني التي يجب أخذها بعين الاعتبار لضمان الاستفادة القصوى من المزايا التكنولوجية في مهنة المحاسبة. لذا، تسعى هذه الدراسة إلى سد هذه الفجوة البحثية من خلال تحليل التكامل بين التحول الرقمي في المحاسبة وإدارة مخاطر الأمن السيبراني، وتحديد العوامل التي تساهم في تعزيز الحماية السيبرانية دون المساس بكفاءة العمليات المالية والمحاسبية.

1.8. خطة البحث:

القسم الأول: الإطار العام للبحث من خلال عرض المقدمة ومشكلة البحث، وأهميته وأهدافه، وحدود البحث ومنهجيته، والدراسات السابقة

القسم الثاني: الإطار النظري للبحث

القسم الثالث: الإطار المنهجي للبحث ونموذج عرض وتحليل البيانات

القسم الرابع: يعرض الخلاصة والنتائج والتوصيات، ويقدم مقترح لأبحاث مستقبلية

2. الإطار النظري

2.1. تعريف التحول الرقمي

يُعرَّف التحول الرقمي (Digital Transformation) من منظور محاسبي، وفقًا لما ذكره Khanon (2020)، على أنه عملية تغيير جذري وتطوير للبنية التحتية لنماذج أداء الأعمال من خلال تطبيق التقنيات التكنولوجية الحديثة، سواء كان ذلك بشكل جزئي أو كلي، بهدف تحقيق مزايا تنافسية وإضافة قيمة حقيقية، مع السعي نحو تحقيق الأهداف الاستراتيجية للمؤسسات.

أما شحاته (2020)، فقد أوضح أن التحول الرقمي قد تطور عبر ثلاث مراحل أساسية في بيئة الأعمال المحاسبية، وهي:

- **النمذجة (الرقمنة):Digitization -** تشير إلى تحويل البيانات التناظرية التقليدية إلى بيانات رقمية يمكن تخزينها ومعالجتها باستخدام أنظمة الحاسب الآلي. ويتم ذلك من خلال دمج تقنيات تكنولوجيا المعلومات مع العمليات المحاسبية التقليدية.
- **التمثيل الرقمي:Digitalization -** يُعبّر عن كيفية الاعتماد على التكنولوجيا في تنفيذ العمليات التشغيلية وتعزيز التواصل بين الأطراف ذات الصلة، مثل إنشاء قنوات اتصال رقمية تُسهّل التفاعل بين المؤسسات والعملاء.
- **التحول الرقمي:Digital Transformation -** يتضمن إعادة تصميم نماذج الأعمال الحالية أو تبني نماذج جديدة لتحقيق ميزة تنافسية وإضافة قيمة حقيقية للمنظمة، سواء كانت هذه النماذج قائمة بالفعل لدى شركات أخرى أو تم تطويرها بشكل مبتكر.

حيث شهدت بيئة الأعمال المحاسبية تطورًا ملحوظًا في تطبيقات التحول الرقمي، ومن أبرزها:

سلاسل الكتل :(Blockchain) تتيح تسجيل المعاملات بشكل آمن وشفاف.

البيانات الضخمة :(Big Data) توفر تحليلات معمقة لاتخاذ قرارات مالية دقيقة.

الحوسبة السحابية :(Cloud Computing) تسهّل تخزين البيانات والوصول إليها عبر الإنترنت.

الذكاء الاصطناعي :(Artificial Intelligence) يساهم في تحليل البيانات وأتمتة العمليات المحاسبية.

العملات المشفرة :(Cryptocurrency) تسهم في التحويلات المالية الرقمية.

العقود الذكية :(Smart Contracts) تعمل على تنفيذ الاتفاقيات تلقائيًا دون الحاجة إلى وسطاء.

تحديات التحول الرقمي في المحاسبة

على الرغم من المزايا العديدة التي يوفرها التحول الرقمي، إلا أنه يواجه عددًا من التحديات، من أبرزها:

- ضرورة تدريب المحاسبين والمراجعين على استخدام التقنيات الحديثة، لضمان امتلاكهم المهارات اللازمة للتكيف مع الأدوات الرقمية.
- الحاجة إلى تأمين البيانات المالية ضد الاختراقات والانتهاكات التي قد تؤثر على موثوقية النظام المحاسبي، مما قد يؤدي إلى زعزعة الثقة في التحول الرقمي.
- تزايد المخاطر السيبرانية مع الاعتماد المتزايد على التكنولوجيا، مما يجعل المؤسسات عرضة لهجمات إلكترونية وتسريب البيانات الحساسة.
- ضرورة تبني استراتيجيات أمن سيبراني متقدمة لضمان حماية البيانات وتعزيز الأمان والثقة في بيئة الأعمال الرقمية.

لذلك، يتوجب على المؤسسات إدراك المخاطر الأمنية المحيطة بالتحول الرقمي واتخاذ التدابير اللازمة لضمان استدامة العمليات المحاسبية وحماية المعلومات المالية من التهديدات السيبرانية المحتملة.

2.2. مفهوم الأمن السيبراني

عرّف المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) الأمن السيبراني بأنه مجموعة من الممارسات والإجراءات المصممة لحماية البيانات والمعلومات من التهديدات السيبرانية (Daoud & Serag, 2022). وفي هذا الإطار، قام AICPA بتطوير مجموعة من المعايير التي تساعد المحاسبين في تأمين بيئة الأعمال الرقمية وتعزيز الثقة في الأنظمة والعمليات التي تدعم تقديم الخدمات المهنية. ومن أبرز هذه المعايير بيانات المعايير الخاصة بخدمات المحاسبة والمراجعة (SSARS)، بالإضافة إلى مبادئ خدمات الثقة والمراجعة (Trust Services Principles and Review Services)، والتي تهدف إلى تمكين المؤسسات من تطبيق تدابير فعالة لحماية البيانات وضمان استمرارية الأعمال (www.aicpa.org).

ومن أهم معايير الأمن السيبراني وفق AICPA:

- تقييم المخاطر: تحليل التهديدات المحتملة وتحديد المخاطر المرتبطة بالأنظمة والبيانات.
- التحكم في الوصول: وضع آليات تحدد من يمكنه الوصول إلى المعلومات الحساسة وكيفية استخدامها.
- التشفير: استخدام تقنيات التشفير لحماية البيانات أثناء التخزين والنقل.
- التوعية والتدريب: تقديم برامج تدريبية للموظفين لرفع الوعي بالأمان السيبراني وتمكينهم من التعرف على التهديدات المحتملة.
- الاستجابة للحوادث: تطوير خطط فعالة للاستجابة الفورية عند وقوع أي اختراقات أمنية.

من ناحية أخرى، يعرّف إطار عمل COBIT (Control Objectives for Information and Related Technologies) الأمن السيبراني بأنه نظام شامل لإدارة وحوكمة تكنولوجيا المعلومات في المؤسسات، وقد تم تطويره بواسطة جمعية المراجعة والتحكم في نظم المعلومات (ISACA) كأداة قياسية تساعد المؤسسات في تحقيق الأهداف التجارية من خلال إدارة فعالة لتكنولوجيا المعلومات.

ومن فوائد إطار COBIT في الأمن السيبراني:

- تحسين إدارة المخاطر: يتيح للمؤسسات إمكانية تحديد وإدارة المخاطر المرتبطة بتكنولوجيا المعلومات بفعالية.
- تعزيز الكفاءة التشغيلية: من خلال توفير إطار عمل منظم يساعد على تحسين الأداء والفعالية في العمليات التقنية.
- تحقيق الأهداف التجارية: يضمن توافق استراتيجيات تكنولوجيا المعلومات مع الأهداف المؤسسية، مما يسهم في تحقيق النجاح التنظيمي.

يُعد كل من AICPA وCOBIT من الأطر المرجعية الأساسية التي تعتمد عليها المؤسسات في حماية بياناتها وتعزيز الأمن السيبراني، مما يضمن استدامة الأعمال وسلامة المعلومات المحاسبية والمالية في ظل التهديدات الرقمية المتزايدة.

2.3. أهداف الأمن السيبراني:

يهدف تطبيق الأمن السيبراني إلى تحقيق مجموعة من الأهداف الأساسية التي تساهم في حماية نظم المعلومات وتعزيز الأمان الرقمي، والتي يمكن تلخيصها على النحو التالي (الجنابي، 2017):

- ضمان استمرارية تشغيل نظم المعلومات، مما يتيح للمؤسسات العمل بكفاءة دون انقطاع.
- حماية خصوصية وسرية البيانات الشخصية، سواء للأفراد أو للمؤسسات العامة والخاصة، من الاختراقات أو الاستغلال غير القانوني.
- اتخاذ التدابير الوقائية اللازمة لحماية المستخدمين من المخاطر المحتملة عند تصفح الإنترنت.
- تأمين الأجهزة التقنية والتشغيلية ضد الهجمات السيبرانية التي قد تؤثر على أدائها.
- المحافظة على شبكات المعرفة والمعلومات، وضمان عدم تعرضها للتلاعب أو الاختراق.

وبذلك، يُعد الأمن السيبراني عنصرًا أساسيًا في حماية الأنظمة التكنولوجية، حيث يعمل على تفعيل آليات الأمان لحماية الأفراد والمؤسسات من التهديدات الرقمية المتزايدة.

2.4. أقسام الأمن السيبراني وأهميتها:

قسّم Moore (2018) الأمن السيبراني إلى عدة مجالات رئيسية، تهدف جميعها إلى حماية البنية التحتية الرقمية والمعلوماتية من التهديدات السيبرانية. يمكن تلخيص هذه الأقسام على النحو التالي:

- **أمن الاتصالات (Communications Security)**: يهدف إلى حماية البنية التحتية والتقنية للاتصالات من التهديدات السيبرانية، وضمان عدم التلاعب أو الاختراق.
- **أمن العمليات (Operations Security)**: يركز على حماية العمليات التشغيلية داخل المؤسسة، ومنع أي تلاعب قد يؤثر على سير العمل أو يعرضه للخطر.
- **أمن المعلومات (Information Security)**: يعنى بحماية المعلومات من الوصول غير المصرح به، والحفاظ على خصوصيتها وسلامتها، ومن أبرز تقنياته استخدام التشفير لضمان سرية البيانات.
- **الأمن المادي (Physical Security)**: يشمل حماية الأصول المادية المرتبطة بالأمن السيبراني، مثل الخوادم ومكونات الشبكة، لمنع الوصول غير المصرح به أو التخريب المادي.
- **أمن التطبيقات (Application Security)**: يهدف إلى حماية التطبيقات من التهديدات الناجمة عن العيوب البرمجية في مراحل التصميم، التطوير، التثبيت، التحديث، والصيانة، مما يعزز أمان البرامج المستخدمة في بيئات العمل الرقمية.

- **الأمن العسكري (Military Security)**: يعنى بحماية الأصول المعلوماتية ذات البعد السياسي أو العسكري أو الاستراتيجي، لضمان عدم تعرضها للاختراق أو الاستخدام غير القانوني.
- **أمن الشبكات (Network Security)**: يهدف إلى تأمين الشبكات وضمان سلامتها واستمرارية استخدامها، وحماية المكونات المرتبطة بها من الهجمات السيبرانية. من أمثلته برامج مكافحة الفيروسات وبرامج مكافحة التجسس.

تساهم هذه الأقسام مجتمعة في بناء نظام أمني شامل يضمن حماية الأفراد والمؤسسات من المخاطر السيبرانية، ويعزز استدامة العمليات الرقمية في مختلف القطاعات.

2.5. متطلبات تطبيق مبادئ الأمن السيبراني:

تتطلب تطبيقات الأمن السيبراني مجموعة من العناصر الأساسية والمتطلبات الضرورية لضمان فعاليته وكفاءته، ويمكن تلخيصها وفقًا لـ Kennedy (2017) على النحو التالي:

- **العناصر المادية (Hardware)**: تشمل الأجهزة والمعدات الإلكترونية التي تشكل البنية التحتية الأساسية لتشغيل نظم المعلومات، مثل الخوادم، أجهزة الحاسوب، معدات الشبكات، وغيرها من الأدوات التقنية.
- **العناصر البرمجية (Software)**: تتضمن الأنظمة والبرمجيات التي تتيح تشغيل وإدارة نظم المعلومات، مثل أنظمة التشغيل، برامج الحماية، تطبيقات تحليل البيانات، وبرامج الأمان السيبراني.
- **القوى البشرية (Human Resources)**: يشكل العنصر البشري ركيزة أساسية في إدارة الأمن السيبراني، حيث يعتمد نجاح النظام على كفاءة الأفراد العاملين في مجال تكنولوجيا المعلومات، ومدى قدرتهم على تشغيل النظم وصيانتها وتطويرها باستمرار.
- **دعم الإدارة العليا**: يُعد التأييد القوي من الإدارة العليا ضروريًا لإنجاح عمليات تطبيق نظم المعلومات والأمن السيبراني داخل المؤسسات، مع أهمية التحلي بالصبر وعدم استعجال النتائج حتى تكتمل عمليات .

- **إعادة تصميم الهيكل التنظيمي:** يتطلب التحول الرقمي إعادة هيكلة الوظائف الإدارية داخل المؤسسة بما يتماشى مع التطورات التكنولوجية، من خلال استحداث وظائف جديدة أو إلغاء وظائف غير متوافقة مع بيئة الأعمال الرقمية، لضمان تطبيق أمن سيبراني فعّال.
- **الشبكات والاتصالات:** تُعد الشبكات والبنية التحتية للاتصالات أساسًا لنقل البيانات بين مختلف الأنظمة والمستخدمين، مما يستدعي توفير شبكات آمنة لحماية تدفق المعلومات من الاختراقات والهجمات السيبرانية.

على الرغم من أهمية كافة العناصر السابقة، إلا أن العنصر البشري يُعتبر العامل الأكثر تأثيرًا في إدارة الأمن السيبراني، حيث يعتمد نجاح النظام الأمني على تدريب الأفراد وتحسين مهاراتهم في التعامل مع المخاطر السيبرانية واتخاذ التدابير الوقائية اللازمة.

2.6. مزايا تطبيق الأمن السيبراني:

يركز الأمن السيبراني على حماية سرية المعلومات وخصوصيتها من خلال منع الوصول غير المصرح به، بحيث لا يتمكن أي شخص من الاطلاع على المعلومات إلا إذا كان مخوّلًا بذلك، ويتم التحقق من ذلك عبر هوية المستخدم (الجنابي، 2017). كما يضمن الأمن السيبراني سلامة وتجانس البيانات من خلال منع التلاعب أو التغيير غير المشروع، إلى جانب ضمان توافر المعلومات عند الطلب بعد التأكد من هوية المستخدم، ومن مزايا تطبيق الأمن السيبراني (الوكيل، 2017):

- **تحقيق وفورات مالية مع نتائج دقيقة:** يساهم الأمن السيبراني في تقليل التكاليف التشغيلية، مع ضمان نتائج دقيقة وعالية الجودة، مما يعزز الجدوى الاقتصادية للمؤسسات.
- **إمكانية العمل عن بُعد:** يتيح للمراقبين أداء مهامهم دون الحاجة إلى التواجد الفعلي في موقع العمل، مما يقلل من المخاطر المرتبطة بالتنقل أو التواجد في بيئات غير آمنة.
- **تحليل الأداء وكشف الانحرافات:** يوفر الأمن السيبراني أدوات رقابية متقدمة تساعد في تحليل الأداء وتحديد الانحرافات عن الأهداف المحددة، مما يسهل اتخاذ القرارات التصحيحية.

يساهم الأمن السيبراني بشكل كبير في تحقيق وفورات في الوقت، مع توفير نتائج أكثر شمولية وتكاملًا مقارنة بالأنظمة التقليدية اليدوية، مما يعزز من كفاءة وفعالية العمليات الرقمية في المؤسسات.

2.7. أثر الأمن السيبراني على تعزيز التحول الرقمي لحماية البيانات المالية والمحاسبية

يُساهم إطار عمل تقانة المعلومات (COBIT) بشكل كبير في تعزيز الأمن السيبراني من خلال التركيز على عدة محاور رئيسية، وهي:

- تحديد نتائج أمان المعلومات، بما في ذلك السرية، النزاهة، وتوافر البيانات.
- إدارة العمليات والموارد، لضمان اتخاذ تدابير أمنية فعالة تحمي الأنظمة الرقمية.
- استجابة الحوادث، من خلال تقديم إرشادات للتعامل مع التهديدات السيبرانية والتعافي منها بكفاءة.

يُعد المعهد الوطني للمعايير والتكنولوجيا (NIST) من أبرز المؤسسات التي تقدم إرشادات وأطر عمل في مجال الأمن السيبراني.

إطار عمل الأمن السيبراني NIST (NIST Cybersecurity Framework)، الذي يهدف إلى تحسين إدارة مخاطر الأمن السيبراني، ويشمل العناصر الأساسية التالية (Krumay et al., 2018):

- التحديد (Identify): فهم الأصول والموارد التي تحتاج إلى حماية، وتقييم المخاطر المرتبطة بها.
- الحماية (Protect): تنفيذ التدابير الأمنية المناسبة لضمان سلامة الأنظمة والمعلومات.
- الكشف (Detect): تطوير أنظمة مراقبة لاكتشاف أي تهديدات أو أنشطة مشبوهة.
- الاستجابة (Respond): وضع خطط فعالة للتعامل مع الحوادث السيبرانية وتقليل تأثيرها.
- الاستعادة (Recover): إعداد استراتيجيات لاستعادة العمليات إلى وضعها الطبيعي بعد التعرض لحادث أمني.

وضعت منظمة المعايير الدولية (ISO) مجموعة من المعايير التي تهدف إلى تعزيز الأمن السيبراني، وأحد أكثر هذه المعايير شهرة هو معيار ISO/IEC 27001، والذي يحدد متطلبات نظام إدارة أمن المعلومات (ISMS)، لضمان إدارة آمنة للأصول المعلوماتية. ومن أبرز عناصره:

- تقييم المخاطر: إجراء تحليل شامل لتحديد المخاطر المحتملة ووضع إجراءات لإدارتها.
- سياسات أمن المعلومات: تطوير سياسات واضحة تحدد كيفية حماية وإدارة المعلومات.

- التوعية والتدريب: تدريب الموظفين على التعرف على التهديدات الأمنية وتعزيز ثقافة الأمن السيبراني.
- تقييم الأداء: قياس وتحليل مدى كفاءة نظام أمن المعلومات بشكل دوري.

يرى الباحث أن التحول الرقمي المدعوم بتقنيات الأمن السيبراني يسهم بشكل كبير في تعزيز أمن وشفافية بيئة الأعمال المحاسبية، من خلال:

- تحقيق أمان المعاملات المالية وضمان خصوصية وسرية البيانات.
- تقليل المخاطر السيبرانية التي قد تؤثر على النظم المالية والمحاسبية.
- الاستفادة من تقنيات الذكاء الاصطناعي لتعزيز الدفاعات السيبرانية وتحسين كفاءة إدارة الأمن الرقمي.

وبذلك، يُعد تكامل التحول الرقمي مع الأمن السيبراني عنصرًا أساسيًا لضمان استدامة الأعمال المحاسبية وحمايتها من التهديدات السيبرانية المتزايدة.

3. الدراسة الميدانية:

3.1. منهج الدراسة: تم اعتماد المنهج الوصفي التحليلي في هذه الدراسة، نظرًا لكونه من أكثر المناهج استخدامًا في البحوث الاجتماعية والإنسانية، حيث يتيح تحليل الظواهر واستنتاج العلاقات بينها بطريقة علمية دقيقة، ومن مصادر البيانات في الدراسة

- **المصادر الثانوية:** تضمنت مراجعة الأبحاث العلمية السابقة ذات الصلة بموضوع الدراسة، بالإضافة إلى المقالات المنشورة في الدوريات المتخصصة، كما تم الاستناد إلى القوانين والتشريعات المتعلقة بالأمن السيبراني والتحول الرقمي في بيئة الأعمال المحاسبية.
- **المصادر الأولية:** اعتمد الباحث على استبانة تم تصميمها وتوزيعها خصيصًا لأغراض الدراسة، لجمع البيانات من الفئة المستهدفة، وتم تحليل بيانات الاستبانة باستخدام برنامج SPSS الإحصائي، حيث تم استخراج الاختبارات الإحصائية المناسبة لضمان دقة النتائج ومدى توافقها مع أهداف الدراسة.

3.2. مجتمع وعينة الدراسة:

1. **مجتمع الدراسة:** شمل مجتمع الدراسة (120) مشاركًا من المديرين العامين، مديري الفروع، مديري الدوائر المالية، ومديري إدارات المخاطر في الشركات الصناعية الليبية.

2. **عينة الدراسة:** تم اختيار عينة عشوائية مكونة من (90) مشاركًا من نفس الفئات الإدارية، حيث تم توزيع الاستبانة عليهم بهدف جمع البيانات اللازمة للدراسة. وقد تم تحليل النتائج واستخلاص الاستنتاجات بناءً على الردود الواردة من العينة المستهدفة:

المتغير	البيان	العدد	النسبة المئوية
المؤهل العلمي	بكالوريوس	70	77.8%
	ماجستير	17	18.9%
	دكتوراه	3	3.3%
	المجموع	90	100.0%
المسمى الوظيفي	محاسبين	20	22.3
	مراجعين خارجيين	31	34.5
	مراجعين داخلين	22	24.5
	مديري المخاطر	17	18.9
	المجموع	90	100.0%
سنوات الخبرة	أقل من 5 سنوات	13	14.4%
	5-10 سنوات	17	18.9%
	10-15 سنة	33	36.7%
	أكثر من 15 سنوات	27	30.0%
	المجموع	90	100%

3.3. أداة الدراسة:

لقد تم تقسيم الاستبانة إلى جزأين كما يلي:

- **الجزء الأول:** ويتكون من البيانات الديمغرافية لعينة الدراسة ويتكون من 3 فقرات.
- **الجزء الثاني:** ويتناول أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في الشركات الصناعية الليبية، وقد تم تقسيم هذه الاستبانة إلى ثلاثة محاور.

وقد اعتمد الباحث على المقياس الخماسي للإجابة عن الفقرات، حسب ما هو موضح في الجدول رقم (1)

جدول رقم (1) مقياس ليكرت الخماسي

التصنيف	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

3.4. صدق وثبات الاستبانة:

تم تقنين فقرات الاستبانة وذلك للتأكد من صدق وثبات فقراتها كالتالي:

صدق الاتساق الداخلي: يقصد بصدق الاتساق الداخلي مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إليه هذه الفقرة، وقد قامت الباحثة بحساب الاتساق الداخلي للاستبانة وذلك من خلال حساب معاملات الارتباط بين كل فقرة من فقرات مجالات الاستبانة والدرجة الكلية للمجال نفسه.

جدول (2) معامل الارتباط بين كل فقرة من فقرات المجال الأول إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سيبرمان	القيمة الاحتمالية (Sig)
1	تؤدي مخاطر الأمن السيبراني إلى اختراقات للبيانات التي تتم من خلالها الوصول إلى معلومات سرية عن أعمال الشركات الصناعية.	0.60	دالة عند مستوى دلالة 0.05
2	تدرك إدارة الشركة أن مخاطر أمن المعلومات يمكن أن تزعزع الاستقرار المالي وتحقق خسائر مالية يمكن أن يتكبدها الشركات الصناعية.	0.74	دالة عند مستوى دلالة 0.05
3	تقوم الشركات بضبط المخاطر السيبرانية وتخفيف الأثر المالي والتحوط منها من خلال وضع الإجراءات والتدابير للأمن السيبراني بهدف دعم الاستقرار المالي له.	0.81	دالة عند مستوى دلالة 0.05
4	يوجد فريق للاستجابة لحوادث الأمن السيبراني على مستوى الشركة بما يساهم في تكثيف الجهود للاستغلال الأمثل للطاقات لتطوير منظومة الأمن السيبراني لتعزيز الاستقرار المالي للشركات.	0.55	دالة عند مستوى دلالة 0.05
5	تصدر الشركات تعليمات لكيفية إدارة المخاطر السيبرانية، ووضع السياسات لإدارة أمن المعلومات والأمن السيبراني.	0.69	دالة عند مستوى دلالة 0.05
6	يعتبر إدماج المخاطر السيبرانية بصورة أفضل في تحليل الاستقرار المالي من شأنه تحسين القدرة على فهم المخاطر على مستوى النظام وتخفيف حدتها.	0.66	دالة عند مستوى دلالة 0.05
7	يؤدي تقليل المخاطر النظامية المرتبطة بالشركات إلى دور إيجابي على الاستقرار المالي.	0.68	دالة عند مستوى دلالة 0.05

الارتباط دال إحصائياً عند مستوى دلالة $\alpha=0.05$.

يوضح جدول (2) معامل الارتباط بين كل فقرة من فقرات المجال الأول والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha=0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (3) معامل الارتباط بين كل فقرة من فقرات المجال الثاني إدارة مخاطر الأمن السيبراني ودعم الشمول المالي والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سيبرمان	القيمة الاحتمالية (Sig)
1	تقوم الشركات بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي.	0.74	دالة عند مستوى دلالة 0.05
2	تقوم الشركات الصناعية الليبية بإعداد وتصميم معالجات للمخاطر السيبرانية تتم من خلال تحديد مصادر بداية هذه المخاطر واحتمالية حدوثها.	0.80	دالة عند مستوى دلالة 0.05
3	تقوم الشركات الصناعية الليبية بإعداد خطة لإدارة المخاطر السيبرانية والتي تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات السيبرانية والتعافي منها في زمن قياسي، مما يعزز الشمول المالي.	0.86	دالة عند مستوى دلالة 0.05
4	تقوم الشركات الصناعية بدولة ليبيا بالتغلب على المخاطر السيبرانية الناجمة عن التحول المتزايد الى رقمنه العمليات المالية.	0.67	دالة عند مستوى دلالة 0.05
5	تقوم الشركات الصناعية بدولة ليبيا بزيادة التركيز على تعزيز الوعي بالأمن السيبراني بين موظفيه.	0.69	دالة عند مستوى دلالة 0.05
6	تقوم الشركات الصناعية بتطوير أطر الرقابة والاستجابة الفعالة للمخاطرالسيبرانية، بما في ذلك ضمان تنفيذ ممارسات إدارة المخاطر العامة السليمة المتعلقة بالمخاطر السيبرانية.	0.71	دالة عند مستوى دلالة 0.05
7	تقوم الشركات الصناعية بعقد دورات تدريبية لموظفيه تتعلق بالأمن السيبراني والشمول المالي.	0.60	دالة عند مستوى دلالة 0.05

الارتباط دال إحصائياً عند مستوي دلالةα=0.05.

يوضح جدول (3) معامل الارتباط بين كل فقرة من فقرات المجال الثاني والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوي معنوية (0.05 a) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (4) معامل الارتباط بين كل فقرة من فقرات المتغير المستقل مخاطر الأمن السيبراني والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سيبرمان	القيمة الاحتمالية (Sig)
1	تعد الخدمات المالية الإلكترونية في الشركات الصناعية بدولة ليبيا من أكثر الخدمات التي تتعرض للمخاطر المتعلقة بالأمن السيبراني.	0.64	دالة عند مستوى دلالة 0.05
2	تعتبر البرامج الضارة واحدة من أكثر التقنيات المستخدم في تحقيق الهجمات السيبرانية.	0.79	دالة عند مستوى دلالة 0.05
3	تقوم الشركات الصناعية بدولة ليبيا بوضع خطط للتعامل مع أي خطر سيبراني يهدد معاملاته الإلكترونية في المستقبل وكيفية التعامل معه.	0.72	دالة عند مستوى دلالة 0.05
4	تقوم الشركات الصناعية بدولة ليبيا بالاعتماد على المعايير والأطر الدولية المعروفة في إدارة المخاطر للتحوط للمخاطر السيبرانية.	0.67	دالة عند مستوى دلالة 0.05
5	تقوم الشركات الصناعية بدولة ليبيا بشكل مستمر على تطوير وتحديث خطط استمرارية العمل بحيث تأخذ بالاعتبار الهجمات السيبرانية.	0.81	دالة عند مستوى دلالة 0.05
6	تقوم الشركات الصناعية بدولة ليبيا بتقييم مخاطر الأمن السيبراني باستمرار لحماية بياناته من الوصول غير المصرح به أو التدمير.	0.80	دالة عند مستوى دلالة 0.05
7	تقدم إدارة المخاطر لإدارة الشركات الصناعية بدولة ليبيا تقرير يشتمل على معلومات هامة حول المخاطر السيبرانية.	0.76	دالة عند مستوى دلالة 0.05
8	يقوم الشركات الصناعية بدولة ليبيا بوضع إجراءات فعالة للحد من المخاطر السيبرانية لحماية عملائه.	0.75	دالة عند مستوى دلالة 0.05

الارتباط دال إحصائياً عند مستوي دلالةα=0.05

يوضح جدول (4) معامل الارتباط بين كل فقرة من فقرات المتغير التابع والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوي معنوية (α=0.05.) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

الصدق البنائي: يعتبر الصدق البنائي أحد مقاييس صدق الأداة الذي يقيس مدى تحقق الأهداف التي تريد الأداة الوصول إليها، ويبين مدي ارتباط كل مجال من مجالات الدراسة بالدرجة الكلية لفقرات الاستبانة.

وللتحقق من الصدق البنائي قام الطالبان بحساب معاملات الارتباط بين درجة كل مجال من مجالات الاستبانة والمجالات الأخرى، وكذلك درجة كل مجال بالدرجة الكلية للاستبانة كما في جدول (5)

جدول (5) معامل الارتباط بين درجة كل مجال من مجالات الاستبانة والدرجة الكلية للاستبانة

الرقم	المجال	معامل الارتباط سيبرمان	القيمة الاحتمالية (Sig)
1	الاستقرار المالي	0.71	دالة عند مستوى دلالة 0.05
2	الشمول المالي	0.76	دالة عند مستوى دلالة 0.05
3	مخاطر الأمن السيبراني	0.74	دالة عند مستوى دلالة 0.05
الدرجة الكلية		0.73	دالة عند مستوى دلالة 0.05

الارتباط دال إحصائياً عند مستوي دلالة0.05=α.

يتضح من جدول (5) أن جميع معاملات الارتباط في جميع مجالات الاستبانة دالة إحصائياً وبدرجة قوية عند مستوي معنوية (α=0.05.) وبذلك تعتبر جميع مجالات الاستبانة صادقة لما وضعت لقياسه.

تصحيح معامل الارتباط بمعادلة سيبرمان براون: معامل الارتباط المعدل=$\frac{2r}{1+r}$ حيث r معامل الارتباط بين درجات الفقرات الفردية ودرجات الفقرات الزوجية. وتم الحصول على النتائج الموضحة في جدول (6)

جدول (6) طريقة التجزئة النصفية لقياس ثبات الاستبانة

الرقم	المجال	معامل الارتباط سيبرمان	معامل الارتباط سيبرمان المعدل
1	الاستقرار المالي	0.71	0.83
2	الشمول المالي	0.75	0.86
3	مخاطر الأمن السيبراني	0.76	0.87
جميع المجالات		0.74	0.85

واضح من النتائج الموضحة في جدول (6) أن قيمة معامل الارتباط المعدل (سبيرمان براون Spearman Brown) مقبول ودال إحصائيا.

معامل ألفا كرونباخ: استخدم الباحث طريقة ألفا كرونباخ لقياس ثبات الاستبانة وبعد حساب معامل ألفا كرونباخ لثبات الاستبانة تبين أن معاملات ثبات المجالات التي تكونت منها الاستبانة تتمتع بدرجة عالية

من الثبات مما جعل الطالبان يطمئنان إلى تطبيقها، وكانت النتائج كما هي مبينة في جدول (7).

جدول (7) قيمة معامل ألفا كرونباخ لقياس ثبات الاستبانة

م	المجال	معامل ألفا كرونباخ	الثبات *
1	الاستقرار المالي	0.90	0.94
2	الشمول المالي	0.80	0.89
3	مخاطر الأمن السيبراني	0.86	0.92
	جميع المجالات	0.84	0.91

الثبات = الجذر التربيعي الموجب لمعامل ألفا كرونباخ

يتضح من الجدول رقم (7) أن المقياس على درجة مرتفعة من الثبات

3.5. تحليل فرضيات الدراسة:

تم استخدام العديد من الاختبارات الإحصائية لتحليل فقرات الاستبانة واستخراج المتوسط الحسابي، والانحراف المعياري، والوزن النسبي، والرتب.

3.5.1. تحليل فقرات ومحاور الدراسة:

للإجابة على الفرضية الفرعية الأولى للفقرات: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي في الشركات الصناعية الليبية ."

جدول (8) دعم الاستقرار المالي

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
1	تؤدي مخاطر الأمن السيبراني إلى اختراقات للبيانات التي تتم من خلالها الوصول إلى معلومات سرية عن أعمال الشركات الصناعية بدولة ليبيا.	3.68	0.79	73.6	3
2	تدرك إدارة الشركات الصناعية بدولة ليبيا أن مخاطر أمن المعلومات يمكن أن تزعزع الاستقرار المالي وتحقق خسائر مالية يمكن أن يتكبدها الشركات.	3.71	0.85	74.2	2
3	تقوم الشركات الصناعية بدولة ليبيا بضبط المخاطر السيبرانية وتخفيف الأثر المالي والتحوط منها من خلال وضع الإجراءات والتدابير للأمن السيبراني بهدف دعم الاستقرار المالي له.	3.68	0.92	73.5	4
4	يوجد فريق للاستجابة لحوادث الأمن السيبراني على مستوى الشركات الصناعية بدولة ليبيا بما يساهم في تكثيف الجهود للاستغلال الأمثل للطاقات لتطوير منظومة الأمن السيبراني لتعزيز الاستقرار المالي للشركات.	3.74	0.85	75.0	1
5	تصدر الشركات الصناعية بدولة ليبيا تعليمات لكيفية إدارة المخاطر السيبرانية، ووضع السياسات لإدارة أمن المعلومات والأمن السيبراني.	3.66	0.76	73.2	5
6	يعتبر إدماج المخاطر السيبرانية بصورة أفضل في تحليل الاستقرار المالي من شأنه تحسين القدرة على فهم المخاطر على مستوى النظام وتخفيف حدتها.	3.66	0.76	73.2	5
7	يؤدي تقليل المخاطر النظامية المرتبطة بالشركات الصناعية بدولة ليبيا إلى دور إيجابي على الاستقرار المالي.	3.58	0.70	72.1	6
	الدرجة الكلية	3.70	0.71	75.9	

يُظهر الجدول السابق أن الفقرة (4)، التي تنص على: "يوجد فريق للاستجابة لحوادث الأمن السيبراني على مستوى الشركات الصناعية في ليبيا، مما يساهم في تكثيف الجهود للاستغلال الأمثل للموارد وتطوير منظومة الأمن السيبراني لتعزيز الاستقرار المالي للشركات الصناعية في ليبيا"، قد حصلت على المرتبة الأولى بوزن نسبي.(75.0%)

ويُعزى ذلك إلى وجود فرق فنية متخصصة داخل الشركات الصناعية الليبية للاستجابة السريعة للحوادث السيبرانية، مما يسهم بشكل مباشر في تعزيز الاستقرار المالي لهذه الشركات.

في المقابل، جاءت الفقرة (7)، التي تنص على: "يؤدي تقليل المخاطر النظامية المرتبطة بالشركات الصناعية إلى دور إيجابي في تعزيز الاستقرار المالي"، في المرتبة الأخيرة بنسبة (72.1%).

أما الدرجة الكلية فقد بلغت (75.9%)، وهي نسبة مرتفعة تعكس مدى إدراك إدارات الشركات الصناعية الليبية لخطورة المخاطر السيبرانية وتأثيرها على الاستقرار المالي. وتسعى هذه الشركات إلى التخفيف من الأثر المالي للمخاطر والتحوط منها عبر تطبيق إجراءات وتدابير الأمن السيبراني لضمان دعم استقرارها المالي.

اختبار الفرضية الفرعية الثانية:

للإجابة على الفرضية الفرعية الثانية، التي تنص على:

"يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في الشركات الصناعية الليبية"

تم تحليل البيانات لاختبار مدى العلاقة الإحصائية بين إدارة مخاطر الأمن السيبراني وتحقيق الشمول المالي في الشركات الصناعية الليبية.

جدول رقم (9) تعزيز الشمول المالي

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
1	تقوم الشركات الصناعية بدولة ليبيا بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي.	3.90	0.85	78.2	3
2	تقوم الشركات الصناعية بدولة ليبيا بإعداد وتصميم معالجات للمخاطر السيبرانية تتم من خلال تحديد مصادر بداية هذه المخاطر واحتمالية حدوثها.	4.00	.087	80.7	2
3	يقوم الشركات الصناعية بدولة ليبيا بإعداد خطة لإدارة المخاطر السيبرانية والتي تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات السيبرانية والتعافي منها في زمن قياسي، مما يعزز الشمول المالي.	3.74	0.86	74.6	5
4	تقوم الشركات الصناعية بدولة ليبيا بالتغلب على المخاطر السيبرانية الناجمة عن التحول المتزايد الى رقمنه العمليات المالية.	3.81	0.88	84.5	1
5	يقوم الشركات الصناعية بدولة ليبيا بزيادة التركيز على تعزيز الوعي بالأمن السيبراني بين موظفيه.	3.81	.088	76.5	4
6	تقوم الشركات الصناعية بدولة ليبيا بتطوير أطر الرقابة والاستجابة الفعالة للمخاطر السيبرانية، بما في ذلك ضمان تنفيذ ممارسات إدارة المخاطر العامة السليمة المتعلقة بالمخاطر السيبرانية.	3.77	0.77	75.4	6
7	تقوم الشركات الصناعية بدولة ليبيا بعقد دورات تدريبية لموظفيه تتعلق بالأمن السيبراني والشمول المالي	4.00	0.87	80.7	2
الدرجة الكلية		3.76	0.83	71.0	

يُظهر التحليل أن الفقرة (4)، التي تنص على: "تقوم الشركات الصناعية في ليبيا بالتغلب على المخاطر السيبرانية الناجمة عن التحول المتزايد نحو رقمنة العمليات المالية"، قد حصلت على المرتبة الأولى بنسبة (84.5%). ويشير ذلك إلى أن الشركات الصناعية الليبية تعمل بشكل مستمر على التحوط من المخاطر السيبرانية وتعزيز استراتيجيات الحماية الرقمية.

في المقابل، جاءت الفقرة (6)، التي تنص على: "تقوم الشركات الصناعية في ليبيا بتطوير أطر الرقابة والاستجابة الفعالة للمخاطر السيبرانية، بما في ذلك ضمان تنفيذ ممارسات إدارة المخاطر العامة السليمة المتعلقة بالمخاطر السيبرانية"، في المرتبة الأخيرة بنسبة.(75.4%)

أما الدرجة الكلية فقد بلغت (71.0%)، وهي نسبة مرتفعة تعكس أهمية إدارة تقنية المعلومات وضرورة تضمينها لمتخصصين في الأمن السيبراني، مما يعزز قدرتها على مواجهة الهجمات السيبرانية المستهدفة، وبالتالي دعم الاستقرار المالي للشركات الصناعية الليبية.

3.5.2.المتغير المستقل: مخاطر الأمن السيبراني

جدول رقم (10) مخاطر الأمن السيبراني

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب
1	تعد الخدمات المالية الإلكترونية في الشركات الصناعية بدولة ليبيا من أكثر الخدمات التي تتعرض للمخاطر المتعلقة بالأمن السيبراني.	3.86	0.80	77.3	4
2	تعتبر البرامج الضارة واحدة من أكثر التقنيات المستخدم في تحقيق الهجمات السيبرانية.	3.76	0.68	75.1	7
3	تقوم الشركات الصناعية بدولة ليبيا بوضع خطط للتعامل مع أي خطر سيبراني يهدد معاملاته الإلكترونية في المستقبل وكيفية التعامل معه.	3.93	0.82	78.5	1
4	تقوم الشركات الصناعية بدولة ليبيا بالاعتماد على المعايير والأطر الدولية المعروفة في إدارة المخاطر للتحوط للمخاطر السيبرانية.	3.91	0.82	78.2	2
5	تعمل الشركات الصناعية بدولة ليبيا بشكل مستمر على تطوير وتحديث خطط استمرارية العمل بحيث تأخذ بالاعتبار الهجمات السيبرانية.	3.88	0.80	77.5	3
6	تقوم الشركات الصناعية بدولة ليبيا بتقييم مخاطر الأمن السيبراني باستمرار لحماية بياناته من الوصول غير المصرح به أو التدمير.	3.71	0.84	74.2	8
7	تقدم إدارة المخاطر لإدارة الشركات الصناعية بدولة ليبيا تقرير يشتمل على معلومات هامة حول المخاطر السيبرانية.	3.77	0.77	73.4	6
8	تقوم الشركات الصناعية بدولة ليبيا بوضع إجراءات فعالة للحد من المخاطر السيبرانية لحماية عملائه	3.79	0.76	75.8	5
الدرجة الكلية		3.76	0.84	77.0	

يُظهر الجدول أن الفقرة (3)، التي تنص على: "تقوم الشركات الصناعية في ليبيا بوضع خطط للتعامل مع أي خطر سيبراني يهدد معاملاتها الإلكترونية في المستقبل وكيفية التصدي له"، قد حصلت على المرتبة الأولى بنسبة (78.5%)، مما يشير إلى أن الشركات الصناعية الليبية تدرك خطورة التهديدات السيبرانية المحتملة وتسعى للاستعداد لمواجهتها بشكل استباقي.

في المقابل، جاءت الفقرة (7)، التي تنص على: "تقدم إدارة المخاطر في الشركات الصناعية الليبية تقارير تشمل معلومات هامة حول المخاطر السيبرانية"، في المرتبة الأخيرة بنسبة.(73.4%)

أما الدرجة الكلية فقد بلغت (77.0%)، وهي نسبة مرتفعة تدل على وجود وعي واضح بمخاطر الأمن السيبراني، كما تعكس قدرة الشركات الصناعية الليبية على مواجهة التهديدات السيبرانية من خلال توفير بيئة آمنة تدعم الشمول المالي وتعزز الاستقرار المالي.

3.6. معامل الانحدار لفرضيات الدراسة:

- **الإجابة على الفرضية الفرعية الأولى:** يوجد أثر ذو دلالة إحصائية عند مستوى معنوية($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي في الشركات الصناعية الليبية ".
- **الإجابة على الفرضية الفرعية الثانية:** يوجد أثر ذو دلالة إحصائية عند مستوى معنوية($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في الشركات الصناعية الليبية ".

جدول رقم (11) معامل الارتباط بين مخاطر الأمن السيبراني ودعم الاستقرار المالي، وتعزيز الشمول المالي

المحاور	مخاطر الأمن السيبراني	
	معامل الارتباط	(sig)
الاستقرار المالي	0.80	*0.00
الشمول المالي	0.71	*0.01

يُظهر الجدول أن معامل الارتباط للاستقرار المالي بلغ (0.80)، بينما كانت القيمة الإحصائية (sig)تساوي (0.00)، وهي أقل من (0.05)، مما يشير إلى وجود علاقة ذات دلالة إحصائية بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي.

واستنادًا إلى نتائج التحليل، يستخلص الباحث رفض الفرض الصفري وقبول الفرض البديل، مما يؤكد أن: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي في الشركات الصناعية الليبية".

كذلك، يُظهر الجدول أن معامل الارتباط للشمول المالي بلغ (0.71)، في حين كانت القيمة الإحصائية (sig) تساوي (0.01)، وهي أيضًا أقل من (0.05)، مما يدل على وجود علاقة ذات دلالة إحصائية بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي.

استنادًا إلى نتائج التحليل الإحصائي، يستخلص الباحث رفض الفرض الصفري وقبول الفرض البديل، مما يشير إلى أن:

"يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في الشركات الصناعية الليبية."

4. النتائج والتوصيات

4.1. النتائج

النتائج التي توصلت إليها الدراسة:

1. أكدت الدراسة وجود تأثير مباشر لإدارة مخاطر الأمن السيبراني على تعزيز الاستقرار المالي والشمول المالي في الشركات الصناعية الليبية.
2. أظهرت النتائج أن إدارات الشركات الصناعية الليبية تدرك خطورة التهديدات السيبرانية، مثل تسريب البيانات، وتأثيرها السلبي على الاستقرار المالي، وما قد تسببه من خسائر مالية كبيرة.
3. تتبنى الشركات الصناعية الليبية استراتيجيات فعالة لإدارة المخاطر السيبرانية، مما يحد من تعرضها للتهديدات ويعزز الأمن المالي من خلال تطبيق تدابير حماية متقدمة.
4. تمتلك الشركات الصناعية الليبية فرقًا متخصصة للاستجابة لحوادث الأمن السيبراني، مما يسهم في تحسين الكفاءة التشغيلية، وتعزيز استخدام الموارد، وتطوير منظومة الأمن السيبراني لدعم الاستقرار المالي.
5. تعمل الشركات على تطوير استراتيجيات واضحة للتخفيف من المخاطر السيبرانية، تعتمد على تحديد مصادر التهديد وتحليل احتمالات حدوثها، بهدف تقليل الأضرار المحتملة.
6. تتبنى الشركات تدابير أمنية متطورة لإدارة المخاطر السيبرانية، مما يساهم في حماية الأصول المالية وتعزيز استدامة العمليات المحاسبية.
7. تضع الشركات الصناعية الليبية سياسات واضحة للتعامل مع المخاطر السيبرانية، مع التركيز على توزيع المسؤوليات ورفع كفاءة الاستجابة السريعة، مما يعزز الاستقرار المالي والإصلاح المؤسسي.
8. تعتمد الشركات على معايير وأطر عمل دولية معترف بها في إدارة المخاطر السيبرانية، لضمان اتباع أفضل الممارسات العالمية في هذا المجال.
9. تقوم إدارات المخاطر في الشركات الصناعية الليبية بإعداد تقارير دورية تحتوي على معلومات تفصيلية حول التهديدات السيبرانية، إلى جانب استراتيجيات الحد منها، بهدف حماية العملاء وتعزيز الثقة في البيئة الرقمية.

4.2. التوصيات

استنادًا إلى النتائج التي توصلت إليها الدراسة، يوصي الباحث بما يلي:

- تعزيز حلول الأمن السيبراني في الشركات الصناعية الليبية، من خلال تبني أنظمة وتقنيات متطورة لحماية البيانات المالية والإدارية، مما يضمن الحفاظ على الجدوى المالية وسهولة الوصول إلى المعلومات، ويساعد الشركات على تحقيق أهدافها بكفاءة.
- نشر ثقافة الاستدامة المالية والتكامل المؤسسي، من خلال التركيز على تقليل الوقت والجهد والتكاليف التشغيلية، حيث تُعد هذه العوامل الثلاثة من الركائز الأساسية لجودة تقديم الخدمات، مما يعزز رضا العملاء ويساهم في تحسين الأداء العام للشركات.
- تطوير نماذج متقدمة لإدارة المخاطر السيبرانية، بحيث تتيح مراقبة مستمرة للتهديدات المحتملة التي قد تؤثر على الاستقرار المالي، مع ضرورة تبني آليات استباقية لحماية البنية التحتية لتكنولوجيا المعلومات في الشركات الصناعية الليبية.
- إطلاق برامج تدريبية وورش عمل متخصصة في الأمن السيبراني، تستهدف الموظفين والعملاء على حد سواء، لرفع مستوى الوعي بأفضل الممارسات في الأمن السيبراني وتكنولوجيا المعلومات، مما يعزز قدرة الشركات على التصدي للهجمات السيبرانية بفعالية.

5. المراجع:

5.1. المراجع العربية:

1- الجنابي، ليلى، (2017)، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، بحث منشور على الموقع: https://www.ssrcaw.org.

2- شحاته، محمد موسى. 2020 . قياس أثر تفعيل أنشطة المراجعة الداخلية لآليات التحول الرقمي على تعزيز المساءلة والشفافية وتحسين الأداء الحكومي مع دليل ميداني بالبيئة المصرية. المجلة العلمية للدراسات المحاسبية، كلية التجارة جامعة قناة السويس 1(2): 703 – 787.

3- مراح، نور الهدى، طويلب، محمد (2022). مستقبل مهنة المحاسبة في ظل تقنيات التحول الرقمي تقنية البلوكشين نموذجا – مجلة الميادين الاقتصادية، 5(1) ، 23-48.

4- الوكيل سامي (2017)، الأمن السيبراني. حماية وطنية لأمن الفرد والمجتمع في المملكة، وكالة الأنباء السعودية، متاح على الموقع الإلكتروني: https://www.spa gov.sa

5.2. المراجع الأجنبية:

5-Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu ،S. O. (2024). Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. Computer Science & IT Research Journal, 5(1), 120-140. Doi: 10.51594/csitrj.v5i.709

6-American Institute of Certified Public Accountants (AICPA, 2018a), "Cybersecurity risk management available reporting fact sheet ،"at : www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices /downloadabledocuments/cybersecurity-factsheet. pdf (accessed 13 January 2025).

7-Daoud, M. M., & Serag, A. A. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. Trade and Finance, 42(1), 20-61

8-Kennedy, C., (2017), The internet of things: how to protect against them, security risks and munication Revolution: https://www.itproportal.com.

9-Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018 ،Proceedings 23 (pp. 369-384). Springer International Publishing.

10-Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. Human Behavior and Emerging Technologies, 2022(1), 7384000.

11-Moore, M,(2018), Adversarial Tactics, Techniques & Welcome Knowledge. to ATT&CK., Common https://attack.mitre.org/wiki/Main.

12-Polishchuk, V., Fedirko, N., Grytsyshen, D., Ohdanskyi, K., & Kotkovskyy, V . .(2024)Analysis of the Impact of Cybersecurity on The Stability of Financial Institutions. International Journal of Religion, 5(9), 302-309. doi: 10.61707/hfrv6059