دور حوكمة تكنولوجيا المعلومات فى إدارة المخاطر السيبرانية للقطاع المصرفي

إعـــــــداد

الباحث/ نواف متعب بنيه متعب الخرينج

إشـــــراف

أ.د/ يـاسر إبراهيـم داود
أستاذ مساعد بقسم الاقتصاد والمالية ووكيل الكلية لشئون التعليم والطلاب - جامعة مدينة السادات

د/ مروة أحمد عبد الرحمن
مدرس بقسم المحاسبة – كلية التجارة جامعة مدينة السادات

- **ملخص البحث**

يُمثل الهدف الرئيس للبحث الحالي فى التعرف على دور حوكمة تكنولوجيا المعلومات فى إدارة المخاطر السيبرانية للقطاع المصرفي, واستخدمت المنهج الاستقرائي والاستنباطي, وتم تطبيق الاستبيان على عينة بلغت (٩٦) من المدراء الماليين وخبراء تكنولوجيا المعلومات, ومسئولي إدارة المخاطر السيبرانية, وتوصلت النتائج إلى:

١. تتمثل أهم معوقات تطبيق حوكمة تكنولوجيا المعلومات في: لا توجد لجنة لتكنولوجيا المعلومات تابعة لمجلس إدراة القطاع المصرفي. السماح لغير المصرح لهم بالدخول إلى برامج القطاع المصرفي المختلفة.
٢. تتمثل أهم محددات المخاطر السيبرانية بالقطاع المصرفي في: قيام المصارف بتعزيز حماية المؤسسة من الهجمات الإلكترونية بكافة أشكالها. قيام المصارف بالتأكد من صحة المعاملات والمسؤولية من خلال العمليات الإلكترونية.
٣. تسهم حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي, حيث توفر حوكمة التكنولوجيا الاعتماد على مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات, كما تقدم حوكمة التكنولوجيا الاستشارات اللازمة عند تصميم وتحسين إستراتيجيات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات.

- **الكلمات الدالة:**

حوكمة تكنولوجيا المعلومات- إدارة المخاطر السيبرانية- للقطاع المصرفي.

Abstract:

The main objective of the current research is to identify the role of information technology governance in managing cyber risks for the banking sector, and used the inductive and deductive approach, and the questionnaire was applied to a sample of (96) financial managers, information technology experts, and cyber risk management officials, and the results reached:

1. The most important obstacles to the application of information technology governance are: There is no information technology committee affiliated to the banking sector board of directors. Allowing unauthorized persons to enter the various banking sector programs.

2. The most important determinants of cyber risks in the banking sector are represented in: Banks strengthening the institution's protection from all forms of cyber-attacks. Banks verify the validity of transactions and liability through electronic operations.

3. Technology governance contributes to managing cyber risks in the banking sector, as technology governance provides reliance on licensed and trusted sources of application development tools, and technology governance provides the necessary advice when designing and improving cyber risk management strategies in light of information technology governance.

Keywords: Information Technology Bovernance- Cyber Risk Management - The Banking Sector.

المقدمة:

يشهد العالم في كافة المجالات تغيرات جذرية سريعة ومتتابعة، فأصبحت السمة الغالبة على بيئة العمل المحيطة بنا هى التغير الديناميكي السريع، هذا بالإضافة إلى تميز هذا التغير بالتقدم التقني، مما أدى إلى تغير معادلة النمو الاقتصادي حيث ظهرت عوامل جديدة حديثة تدخل وبصفة أساسية في هذه المعادلة.

أثرت الطفرة النوعية في العقدين الأخيرين من القرن الماضي في مجال التكنولوجيا على شكل المنظمات، فأصبحت تكنولوجيا المعلومات العصب الرئيس للمنظمات فقد ساعدت على ظهور شكل جديد من المنظمات يتمتع بالمرونة والقوة، وبالنظر إلى الأخطار الملازمة لاستخدام تكنولوجيا المعلومات نجد أن هذه التكنولوجيا سلاح ذو حدين فإن تم استخدامه بالشكل المناسب الصحيح الذي يؤدي إلى دعم المنظمة في تحقيق أهدافها الإستراتيجية ويساعدها على الاستقرار والتقدم والاستدامة ويسهم في خلق مميزات تنافسية، وبالمقارنة بهذه الميزات فإن التهديدات التي تتعرض لها تكنولوجيا المعلومات آخذة في الازدياد والتي قد تهدد حاضر ومستقبل المنظمة (أمين, ٢٠١٥).

وتهتم حوكمة تكنولوجيا المعلومات بنوعين أساسيين: الأول هو إضافة قيمة للمؤسسة، والثاني هو إدارة المخاطر المرتبطة بتكنولوجيا المعلومات, ويمكن تحقيق النوع الأول من خلال تحقيق المحاذاة بين إستراتيجية تكنولوجيا المعلومات مع الإستراتيجية العامة للمؤسسة، كما يمكن تحقيق النوع الثاني من خلال تطبيق محاسبة المسئولية داخل المؤسسة وكلاهما يحتاج إلى عملية القياس وتقييم الأداء (السواح, ٢٠٢٠).

وبذلك يتحدد موضوع البحث الحالي في معرفة أثر حوكمة تكنولوجيا المعلومات فى إدارة المخاطر السيبرانية للقطاع المصرفي.

مشكلة البحث:

تتجسد مشكلة البحث الحالي فى السؤال الرئيس التالي: ما أثر حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي ؟

ويتفرع من هذا السؤال عدة أسئلة فرعية تتمثل في:

١. ما هى أهم محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات؟
٢. ما هى طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي؟
٣. إلى أي مدى تسهم حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي ؟

الدراسات والبحوث السابقة

١. **تناولت دراسة مراد (٢٠١٦)** اختبار أثر تطبيق آليات حوكمة تكنولوجيا المعلومات على الأداء المالي والقدرة التنافسية في الشركات المساهمة المصرية، وفي سبيل تحقيق ذلك الهدف قامت الباحثة باختبار عينة قدرها (٦٠) شركة من مجتمع الشركات المساهمة المصرية، وإجراء دراسة ميدانية عن طريق الاستقصاءات والمقابلات الشخصية مع جميع مفردات عينة الدراسة، وتوصلت الدراسة إلى العديد من النتائج من أهمها: معرفة الشركات المطبقة وغير المطبقة لآليات حوكمة تكنولوجيا المعلومات، ثم قامت الباحثة من خلال نماذج الانحدار المتعدد باختبار أثر تطبيق تلك الآليات على الأداء المالي والقدرة التنافسية لشركات العينة وتم قياس الأداء المالي باستخدام معدل العائد على الأصول (ROA)، وتم قياس القدرة التنافسية من خلال معدل نمو المبيعات (SGR)، وتوصلت الباحثة إلى أن هناك أثر معنوي لتطبيق آليات حوكمة تكنولوجيا المعلومات على الأداء المالي والقدرة التنافسية، وأن الشركات التي يرتفع فيها تطبيق آليات حوكمة تكنولوجيا المعلومات، يزداد أدائها وقدرتها التنافسية مقارنة بالشركات ضعيفة التطبيق، وأن الآثار اللاحقة لتطبيق آليات حوكمة تكنولوجيا المعلومات أعلى وأفضل من الآثار الفورية.

٢. **أما دراسة السعداوي (٢٠١٧)** فهدفت إلى إبراز واقع منظمات الأعمال في العصر الحديث -عصر العولمة- وحاجتها الماسة إلى حوكمة الشركات، والأبعاد المحاسبية للحوكمة, وتحديد المتطلبات الأساسية لحوكمة نظم تكنولوجيا المعلومات, وتوصلت الدراسة إلى العديد من النتائج من أهمها: أنه لا توجد علاقة ذات دلالة معنوية بين تطبيق تكنولوجيا المعلومات وتعرض المعلومات للمخاطر في شركات المساهمة الليبية". ولا توجد علاقة ذات دلالة معنوية بين تدنية مخاطر نظام المعلومات المحاسبي الذي يعتمد على تطبيق تكنولوجيا المعلومات وجودة المعلومات في شركات المساهمة الليبية". لا توجد علاقة ذات دلالة معنوية بين تطبيق إجراءات حوكمة نظم تكنولوجيا المعلومات وبين تخفيض مخاطر المعلومات في شركات المساهمة الليبية". لا يؤثر تطبيق إجراءات حوكمة نظم المعلومات في نظام المعلومات المحاسبي على عدد مرات تكرار المخاطر. والالتزام بتطبيق حوكمة نظم المعلومات من شأنه أن يعمل على رفع مستوى جودة الأداء لمهنة المحاسبة والمراجعة، وتوسيع لنطاق ومسؤوليات عمل المحاسب والمراجع. وتطبيق إجراءات حوكمة نظم المعلومات يؤدى إلى جودة المعلومات المحاسبية وتحقيق الثقة في تلك المعلومات. كلما زادت إجراءات حوكمة نظم المعلومات الخاصة بتوصيل السياسات المحددة إلى الأفراد الذين لهم الحق في الإطلاع على تلك السياسات وتنفيذ الإجراءات لتحقيق الأهداف طبقاً للسياسات المحددة من قبل ومراقبة النظام للحفاظ على الإلتزام بالسياسات المحددة كلما قلت نشأة مخاطر المعلومات بسبب أفراد من داخل الشركة.

٣. **تناولت دراسة غنيمي (٢٠١٧)** أهم الآثار المترتبة على التطورات في تكنولوجيا المعلومات على مهنة المحاسبة والمراجعة، بالإضافة إلي المخاطر والتهديدات التي واجهت مهنة المحاسبة من استخدام تكنولوجيا المعلومات في النظم المحاسبية لمنظمات الأعمال وعملية النشر الإلكتروني للمعلومات عبر المواقع الإلكترونية على الإنترنت، الأمر الذي فرض على الهيئات العلمية والمهنية المسئولة عن مهنة المحاسبة ضرورة تبني فكرة تطبيق آليات حوكمة تكنولوجيا المعلومات، ووصلت درجة الاهتمام إلى المطالبة بصياغة معيار محاسبي لحوكمة تكنولوجيا المعلومات، كنتيجة طبيعة للآثار السلبية والتهديدات التي صاحبت استخدام تكنولوجيا المعلومات في منظمات الأعمال. وأجريت الدراسة الميدانية على عينة من أعضاء هيئات التدريس بالجامعات المصرية في، مجال التخصص، وعينة أخرى من خبراء تكنولوجيا المعلومات والحوكمة بالشركات والمؤسسات المالية، وتوصلت الدراسة إلى عدد من النتائج منها: أن حوكمة تكنولوجيا المعلومات تسهم بدرجة كبيرة في الحد من المخاطر والتهديدات المصاحبة لاستخدام تكنولوجيا المعلومات وتدعم تحسين الأداء المالي في منظمات الأعمال، وقد كانت أبرز التوصيات: ضرورة اهتمام مجلس معايير المحاسبة الدولية ومعهد حوكمة تكنولوجيا المعلومات بإصدار معيار خاص بحوكمة تكنولوجيا المعلومات مع وضع الإرشادات التي تضمن الإلتزام بتطبيق المعيار في منظمات الأعمال في بيئة الأعمال الحديثة.

٤. **دراسة Asanza (٢٠١٧)** فهدفت إلى دراسة إدارة حوكمة تكنولوجيا المعلومات فى البيئة المستدامة القائمة على معيار COBIT 5 كمعيار دولى لحوكمة تكنولوجيا المعلومات معترف به دولياً منذ صدوره كما تحدد الدراسة أنشطة البيئة وتكنولوجيا المعلومات وتم إجراء رسم الخرائط التوضيحية لتحديد الأنشطة البيئية المتعلقة بحوكمة تكنولوجيا المعلومات, وتوصلت أهم النتائج إلى تعزيز النموذج المستدام مع أنشطة حوكمة تكنولوجيا المعلومات والأنشطة البيئية الجديدة التى تمت إضافتها إلى

٥. **في حين تناولت دراسة Safari etal (2018)** ممارسة نموذج النضج وإستراتيجيات حوكمة تكنولوجيا المعلومات بالتطبيق على البنوك الإيرانية, وتم تصميم قائمة استقصاء وتوزيعها على (٣٩) من البنوك الكبيرة العامة والخاصة بالاعتماد على مجموعة من الأساليب الإحصائية الوصفية، وتوصلت الدراسة إلى مجموعة من النتائج من أهمها: دور مواءمة إستراتيجيات العمل مع إستراتيجيات تكنولوجيا المعلومات، كما أن البنوك التي تستخدم حوكمة تكنولوجياً رئيساً وإستراتيجيات في المعلومات تتميز بميزة تنافسية حيث تعتبر حوكمة تكنولوجيا المعلومات جزءاً تطوير أعمال تكنولوجيا المعلومات.

٦. **وتناولت دراسة البلقاسي, (٢٠١٨),** إيضاح مفهوم حوكمة تكنولوجيا المعلومات ودراسة إمكانية استخدام كوبت (٥) كأحد أطر هذه الحوكمة ودراسة التأثير الناتج عن تطبيق مفهوم الحوكمة على تخفيض فجوة المخاطر في نظم المعلومات الإلكترونية، وتم تصميم استبيان تم تطبيقه على عينة من المستثمرين والعاملين في المؤسسات التعليمية الخاصة كأحد نماذج منظمات الأعمال التي تستخدم تكنولوجيا المعلومات بشكل دائم حيث تم تطبيق الاستبيان علي عينة عشوائية مكونة من (١٤٠) مفردة، هدف الاستبيان إلى معرفة آراء عينة البحث حول حوكمة تكنولوجيا المعلومات ودورها الفاعل في معالجة فجوة المخاطر، وتوصلت الدراسة إلى عدة نتائج من أهمها: أن استخدام مفاهيم حوكمة تكنولوجيا المعلومات يؤدي إلى انخفاض فجوة المخاطر وما هو فعلي في نظم المعلومات الإلكترونية بالإضافة إلى القدرة علي اتخاذ القرار المناسب والاستفادة القصوى من الموارد المتاحة وفاعلية استخدامها، توصي الباحثة بتبني المفاهيم الحديثة مثل التعلم بالهاتف الذكي والكتاب الإلكتروني وغيره من المفاهيم التي تعد الاستثمار وترفع هامش الربح لدي المستثمرين بشرط استخدام اطر الحوكمة.

٧. **أما دراسة Muda & Landau (٢٠١٩),** فهدفت إلى معرفة أثر تطبيق نظرية المحاسبة التراكمية على جودة نظم المعلومات المحاسبية, واستخدمت المنهج الوصفي التحليلي والاستقرائي, وتوصلت النتائج إلى أن متغير تكنولوجيا المعلومات له أثر إيجابي على جودة المعلومات المحاسبية، وكان من أهم التوصيات ضرورة العمل على استخدام تكنولوجيا المعلومات بشدة علاقتها الرئيسة بجودة المعلومات المحاسبية.

٨. **وتناولت دراسة Al Abbadi (٢٠٢٠)** توضيح تأثير حوكمة تقنية المعلومات على ربحية (١٦) بنكاً تجارياً أردنياً بما فى ذلك البنوك الإسلامية المدرجة فى سوق عمان المالى حيث تمت دراسة المجتمع بأكمله باستخدام المنهج الوصفي التحليلي وتم اعداد استبيان تم توزيعه على شاغلى المناصب الإدارية والعاملين فى خدمة تكنولوجيا المعلومات فتم توزيع (١٨٣) استبانة حيث تم استرجاع (١٦٠) استبانة تم تحليليها بالكامل, وتوصلت الدراسة إلى العديد من النتائج من أهمها: فعالية حوكمة تكنولوجيا المعلومات على ربحية البنوك الأردنية.

أهداف البحث:

هدف البحث الحالي إلى:

١. التعرف على أهم محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات.
٢. التعرف على طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي.
٣. تحديد مدى إسهام حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي.

أهمية البحث:

وتنقسم أهمية البحث إلى ما يلي:

١- **أهمية علمية:**

وتتمثل فيما يلي:

- ترجع أهمية البحث فى ندرة البحوث التطبيقية الخاصة بدراسة الآثار المُتعلقة بتطبيق آليات حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية بالقطاع المصرفي بالرغم من حاجة البيئة الكويتية لهذه النوعية من البحوث وأهميته على المستوى: المحلي والإقليمي.
- يأمل الباحث أن يكون للبحث الحالي دور كبير في إدارة المخاطر السيبرانية بالقطاع المصرفي.
- حداثة مفهوم حوكمة تكنولوجيا المعلومات وعلاقته إدارة المخاطر السيبرانية.
- تبرز أهمية هذا البحث فى الحاجة إلى استخدام حوكمة تكنولوجيا المعلومات فى إدارة المخاطر السيبرانية بالقطاع المصرفي.

٢- **أهمية عملية:**

وتتمثل فيما يلي:

- عدم تفعيل الإجراءات المناسبة لمواجهة المخاطر السيبرانية وكيفية معالجتها, والتصدي لها من خلال استخدام حوكمة تكنولوجيا المعلومات.
- عدم وجود أي دراسة تطبيقية تناولت أثر حوكمة تكنولوجيا المعلومات على إدارة المخاطر السيبرانية بالقطاع المصرفي.

حدود البحث:

وتتمثل الحدود فيما يلي:

الحدود المكانية: اقتصر البحث الحالي على القطاع المصرفي بمنطقة الفروانية بدولة الكويت.

الحدود الزمانية: تم تطبيق الاستبيان فى العام الدراسي ٢٠٢١/ ٢٠٢٢م.

الإطار النظري

المبحث الأول: ماهية حوكمة تكنولوجيا المعلومات:

وفيه تناول الباحث مفهوم حوكمة تكنولوجيا المعلومات وأهدافها وأهميتها, وركائزها, متطلباتها, معوقاتها, وضوابطها, وأخيراً معاييرها, وسوف يتم تناول ذلك بالتفصيل في الاتي:

أولاً: مفهوم حوكمة تكنولوجيا المعلومات:

تم تناول مفهوم حوكمة تكنولوجيا المعلومات في عدة تعريفات على النحو التالي:

التعريف الأول: عرف معهد حوكمة تكنولوجيا المعلومات ITGI حوكمة تكنولوجيا المعلومات بأنها: هيكل العلاقات والعمليات لتوجيه المؤسسة والرقابة عليها, وخلق قيمة من خلال تحقيق التوازن بين المخاطر من ناحية والعوائد من تكنولوجيا المعلومات والعمليات المرتبطة بها من ناحية أخرى, إذ تعمل تكنولوجيا المعلومات على وضع الهيكل الذى يربط بين العمليات المُتعلقة بتكنولوجيا المعلومات وموارد تكنولوجيا المعلومات والمعلومات وبين أهداف وإستراتيجيات المؤسسة (بن سعيد, ٢٠١٥).

التعريف الثاني: أما المعهد الاسترالي للحوكمة فعرف حوكمة تكنولوجيا المعلومات بأنها: النظام الذى يتم من خلاله توجيه ورقابة الاستخدامات: الحالية والمستقبلية لتقنية المعلومات وتقييم وتوجيه الخطط لاستخدام تكنولوجيا المعلومات فى دعم المؤسسة, ومتابعة هذا الاستخدام لإنجاز الخطط والأهداف المقررة (السمان؛ عبدالجبوري, ٢٠١٦).

التعريف الثالث: تعرف حوكمة تكنولوجيا المعلومات بأنها: وصف كيفية قيام الأفراد المكلفين بالشركة بالاهتمام بتكنولوجيا المعلومات عند ممارسة عمليات الرقابة على استثمارات الشركة في الأنظمة المختلفة, وأنها تعتبر مسئولية الإدارات التنفيذية ومجلس الإدارة بالدرجة الأولى، بحيث تضمن لتكنولوجيا المعلومات أن تكون قادرة على تحقيق الأهداف الاستراتيجية للشركة (غنيمي, ٢٠١٧).

التعريف الرابع: تعرف حوكمة تكنولوجيا المعلومات بأنها: سلسلة من العمليات التي تساعد المؤسسات على استخدام نظام من القرارات لنقل تكنولوجيا المعلومات من مركز تكلفة إلى مركز ربح (السواح, ٢٠٢٠).

ويرى الباحث من التعريفات السابقة أن حوكمة تكنولوجيا المعلومات تعرف بأنها: جزء مهم ومكمل لحوكمة المؤسسات يتم من خلاله التركيز على تكنولوجيا المعلومات بواسطة مجلس الإدارة والإدارة التنفيذية, وإدارة تكنولوجيا المعلومات من أجل تحقيق التنسيق والتكامل بين أهداف تكنولوجيا المعلومات وأهداف المؤسسات, وتأسيس المساءلة.

ثانيًا: أهداف حوكمة تكنولوجيا المعلومات:

تناولت العديد من الدراسات والأدبيات أهداف حوكمة تكنولوجيا المعلومات, ومنها: (Aasi, 2018), (Shuaibu, 2019), (السواح, ٢٠٢٠), وقد استخلص منهم الباحث أن أهداف حوكمة تكنولوجيا المعلومات تتمثل فيما يلي:

١. رفع مستوى جدوى استخدام تكنولوجيا المعلومات, وإضافة القيمة للمؤسسة من خلال منع إعاقة الأعمال وزيادة كفاءة التشغيل وزيادة القوى الدافعة الإيجابية وإنشاء وتقوية الأصول الإستراتيجية وتحقيق المزايا التنافسية.
٢. تطوير وإدارة إستراتيجية نظم تكنولوجيا المعلومات والشروع في الفحص: التشغيلي والإستراتيجي.
٣. ضمان أن مشروعات الأعمال قد تم استكمالها.
٤. تحديد الأساليب والوسائل والعمليات المرتبطة بتكنولوجيا المعلومات.
٥. تحديد أفضل الممارسات في مجال التطوير التكنولوجي.
٦. إدارة تنمية وتطوير تطبيقات تكنولوجيا المعلومات.
٧. ضمان فعالية خدمات تكنولوجيا المعلومات لتوصيل الإستراتيجية لأقسام أنشطة الأعمال التي تؤدي إلى فعالية وكفاءة الإنتاجية الداخلية.
٨. زيادة قدرة تكنولوجيا المعلومات لجذب الاختراعات والابتكارات وتوصيل المنافع المرجوة.
٩. الاستخدام المسئول لمصادر تكنولوجيا المعلومات.
١٠. الإدارة المناسبة لمخاطر تكنولوجيا المعلومات.
١١. التنسيق والتكامل بين أهداف التكنولوجيا وأهداف المؤسسة وإدراك المنافع المرجوة.
١٢. استخدام تكنولوجيا المعلومات لمساعدة المؤسسة من خلال استعراض الفرص وزيادة المنافع لأقصى درجة ممكنة.
١٣. فرض الرقابة الفعالة على أدء تكنولوجيا المعلومات وتطوير مؤشرات الأداء الرئيسة.
١٤. تعظيم العائد من الاستثمار في تكنولوجيا المعلومات مما يؤدي إلى تمتع المؤسسة بمركز تنافسي متميز بالنسبة للشركات المنافسة لها.
١٥. فهم الأدوار والمسئوليات من جانب مجلس الإدارة والإدارة التنفيذية المسئولين عن وضع نظام الحوكمة وتطبيقه.
١٦. التأكد من الإفصاح الكامل عن التقارير المالة للمؤسسة، والمخاطر الحالة والمتوقعة لتقنية المعلومات، وأن مصادر تكنولوجيا المعلومات يتم إدارتها واستخدامها بكفاءة .
١٧. ضمان فعالة خدمات تكنولوجيا المعلومات لتوصيل الإستراتيجية لجميع أقسام المؤسسة مما يؤدي إلى كفاءة وفعالية عمليات التشغيل الداخلية.

ثالثًا: أهمية حوكمة تكنولوجيا المعلومات:

تناولت العديد من الدراسات والأدبيات أهمية حوكمة تكنولوجيا المعلومات, ومنها: (Lunardi et al 2017), (Bianchi, 2020) وقد استخلص منهم الباحث أن أهمية حوكمة تكنولوجيا المعلومات تتمثل فيما يلي:

١- الاستفادة من مميزات تكنولوجيا المعلومات في نشر التقارير المالية غبر شبكة الإنترنت بالجودة الملائمة وبالأساليب الحديثة للنشر.
٢- الموازنة بين التكاليف الكبيرة والمتزايدة لتكنولوجيا المعلومات والقيمة الكبيرة للمعلومات وذلك من أجل تحصيل عائد مناسب من الاستثمارات في تكنولوجيا المعلومات.
٣- إدارة مخاطر القيام بممارسة العمل التجاري عبر الإنترنت (التجارة الإلكترونية) وخفض مخاطر النشر الإلكتروني للتقارير المالية.
٤- إدارة تكنولوجيا المعلومات في استمرارية العمل في المؤسسة, وذلك نظراً للاعتماد المتزايد على المعلومات وتكنولوجيا المعلومات في جميع مجالات المؤسسة.
٥- الحفاظ على قدرة تكنولوجيا المعلومات في بناء المعرفة اللازمة, وذلك لضمان نمو المؤسسة وصيانتها.
٦- نجاح مشاريع تكنولوجيا المعلومات وتجنب فشلها الذي يؤثر تأثيراً كبيراً في قيمة المؤسسة وسمعتها.
٧- الاعتماد بشكل جوهري على تقنية المعلومات كشرط أساسي تفرضه الجهات الرقابية والجهات الاشرافية والتطبيقات الجيدة لحوكمة المؤسسات وزيادة قدرتها التنافسية .
٨- الإدارة الفعالة لاحتياجات ومتطلبات العملاء في إطار الإستراتيجية العامة للمؤسسة كزيادة جودة المعلومات المالية المنشورة للعملاء عبر الشبكة العالمية للإنترنت.
٩- تحسن وتحسين وتطوير تقنية المعلومات المستخدمة باستمرار للوفاء بالمتطلبات المتغيرة بالبيئة المحيطة.
١٠-تعميق وتعزيز دور الرقابة على تقنية المعلومات ومخرجاتها.
١١-ظهور العديد من التشريعات والقوانين المنظمة لاستخدام التكنولوجيا الحديثة: كالتوقيع والنشر الإلكتروني, والاتصالات, وأيضاً تداول المعلومات.

رابعاً: منهجية تطبيق حوكمة تكنولوجيا المعلومات:

وتناولها الباحث فيما يلي:

١- **مبادئ حوكمة تكنولوجيا المعلومات:**
ونعرضها في ستة مبادىء فيما يلي:

- **المسؤولية:** حيث أن الأشخاص والفرق يفهمون ويقبلون مسؤولياتهم مع احترام العرض من والطلب لتكنولوجيا المعلومات، كما لديهم السلطة الكافية لأداء مسؤولياتهم .
- **الإستراتيجية:** حيث أن إستراتيجية الأعمال تأخذ في الحسبان القدرات الراهنة والمستقبلية لتكنولوجيا المعلومات؛ الخطط الإستراتيجية المرتبطة بتكنولوجيا المعلومات ترضى الاحتياجات الآنية والآجلة لإستراتيجية الأعمال.
- **الاكتساب:** أي أن إكتساب تكنولوجيا المعلومات يكون لسبب مبرر؛ يعتمد على تحليل منطقى مع إتخاذ قرار شفاف وواضح, كما أن هناك موازنة بين الفوائد، الفرص، التكاليف، الأخطار، وعلى المستويين القصير والطويل الأمد.
- **الأداء:** تستخدم تكنولوجيا المعلومات لدعم المؤسسات وتوفير الخدمات، والمستويات المناسبة ونوعية الخدمات يجب أن تقابل الاحتياجات الراهنة والمستقبلية.
- **المطابقة:** تكنولوجيا المعلومات يجب أن تستجيب لكل أنواع التشريع والتعليمات, السياسات والتطبيقات محددة بوضوح، معززة وأيضاً قابلة للتطبيق .
- **السلوك الإنساني:** سياسات تكنولوجيا المعلومات، والتطبيقات والقرارات لا بد أن تحترم السلوك الإنسانى، وتتضمن الاحتياجات الراهنة والمتطورة لكل الأشخاص في العمليات (Julianti, et al).
2021

٢- **إجراءات تطبيق حوكمة تكنولوجيا المعلومات:**

وتتمثل فيما يلي:

- الموائمة بين الإستراتيجية العامة للمنظمة وخطط التشغيل اللازمة لتحقيق الأهداف الإستراتيجية وبين الخطة الإستراتيجية لتكنولوجيا المعلومات.
- وضع خطة تشغيل لتكنولوجيا المعلومات.
- وضع خطة مالية وتمويلية لتكنولوجيا المعلومات.
- وضع إطار عام لتطبيق حوكمة لتكنولوجيا المعلومات والرقابة عليها مأخوذاً في الاعتبار ما تصدره جهات الرقابة والإشراف والتشريعات المنظمة للعمل بالمنظمات واختيار البدائل العملية المطروحة.
- لا بد من القيام بتشكيل اللجان المتخصصة في تشجيع تكنولوجيا المعلومات ووضع التخطيط الإستراتيجي الخاصة بها ويتعين أن يكون مستوى هذه اللجان من أعضاء مجلس الإدارة.
- مشاركة مدير إدارة تكنولوجيا المعلومات فى إستراتيجية المؤسسة.
- ممارسة الإلتزام.

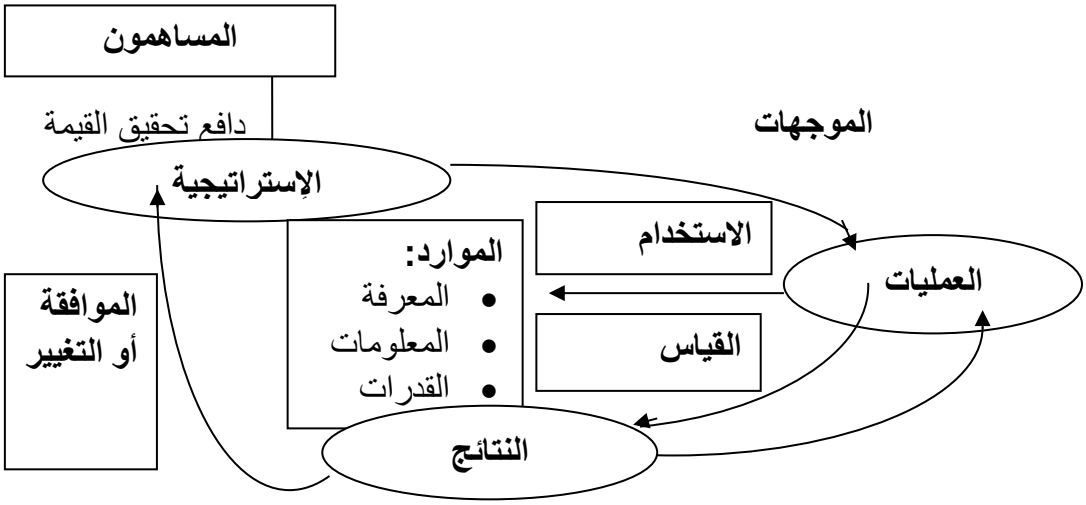
٣- **النماذج المفاهيمية لتطبيق حوكمة تكنولوجيا المعلومات:**

النموذج الأول: نموذج معهد حوكمة تكنولوجيا المعلومات

بحيث يعتبر المعهد حوكمة تكنولوجيا المعلومات ليس تخصصاً مستقلاً، بل جزء من النظام العام للحوكمة فى المؤسسة، تتضمن تحقيق المسؤوليات الآتية:

١. الأخذ فى الحسبان قيم المساهمين عند وضع الإستراتيجية.
٢. إعطاء التوجيهات للعمليات التي تنفيذ الإستراتيجية.
٣. التاكد من أن تلك العمليات توفر نتائج قابلة للقياس.
٤. ضمان التصرف وفق ما يضمن تحقيق النتائج المتوقعة.

ويوضح شكل (١) نموذج معهد حوكمة تكنولوجيا المعلومات لتطبيق حوكمة تكنولوجيا المعلومات فيما يلي:



شكل (١) نموذج معهد حوكمة تكنولوجيا المعلومات

فحوكمة تكنولوجيا المعلومات تتضمن تطبيق إستراتيجياً لتوجيه ومراقبة تكنولوجيا المعلومات، فلا بد من التركيز على ما يلى:

١. توقعية تكنولوجيا المعلومات في تعزيز رافعة تاثير الأصول اللاملموسة (المعلومات، المعارف، الثقة).

٢. الانسجام بين تكنولوجيا المعلومات وإستراتيجية الأعمال.
٣. ضمان شفافية أخطار الاستثمار في تكنولوجيا المعلومات.
٤. قياسية أداء تكنولوجيا المعلومات.

إذن هى مسؤولية مجلس الإدارة، وهم ليسوا في حاجة لأن يكونوا خبراء في تقنية المعلومات، بل يحتاجون بدرجة أولى إلى فهم على أعلى مستوى فيما يتعلق بالأدوار والمسؤوليات المُتعلقة بتكنولوجيا المعلومات والرقابة عليها، وبالتاكيد ينبغي تعزيز مهاراتهم. ولابد أن يبدأوا بالتساؤل حول مدى انسجام التكنولوجيا، تكاليفها، أخطارها، فرصها، وقياس فعاليتها وأدائها، ومدى قدرتها فيما يتعلق بالحفاظ على المعلومات وخطر ضياعها، خاصة في ظل التطور المستمر للتكنولوجيا في ظل عصر المعلومات. كما على مجلس الإدارة تبني إلتزام إستراتيجي، بخصوص الأهداف التي يجب تحقيقها، وكل الأطراف المرتبطة بذلك، وتعزيز إستراتيجية لتكنولوجيا المعلومات، وقدر عالي من مستويات الرقابة على أخطارها.

خامساً: ركائز حوكمة تكنولوجيا المعلومات

إن فهم قيمة وكلفة تقنية المعلومات تُعد مهمة بالنسبة للمدير ومجلس الإدارة وإدارة تقنية المعلومات على حد سواء, حيث تتطلب تحقيق التوافق الناجح بين المؤسسة وتكنولوجيا المعلومات أن تتوافق أهداف وأغراض المؤسسة مع احتياجات المؤسسة من نظم المعلومات, وعندما تكون تقنية المعلومات قادرة على تلبية تلك الاحتياجات بالتعاون مع الإدارة على هذا الأساس يقع على عاتق الإدارة مسؤولية الاهتمام بركائز حوكمة تكنولوجيا المعلومات والتي تتمثل فيما يلي:

١. **التوافق الإستراتيجي:** Strategic Alignment وهى التحقق من الموائمة بين الإستراتيجية العامة للمنظمة وبين الخطة الإستراتيجية لتكنولوجيا المعلومات, حيث تعتني حوكمة تكنولوجيا المعلومات بتشكيل إستراتيجية معلوماتية للمنظمة تتطابق أهدافها مع الإستراتيجية العامة لتلك المنظمة, وتوفير الإجراءات الخاصة والقوانين والسياسات الكفيلة وعدم خروجها عن الإسترتيجية العامة للمنظمة.
٢. **القيمة المضافة:** Value Addedحيث التأكد والعمل على أن قسم تكنولوجيا المعلومات يفعل ما هو ضروري لتحقيق الفوائد والمنافع والأهداف المسيطرة في بداية الاستثمار في مجال تكنولوجيا المعلومات في المنظمة.
٣. **إدارة المخاطر:** Risk Management وهو وضع إطار رسمى للمخاطر التي تواجه معلومات وبيانات المنظمة نتيجة استخدامها للتكنولوجيا الحديثة, وكذلك العمل على حماية هذه المعلومات وتوفير الأمن اللازم لها, وتهتم بمعالجة احتياجات الامتثال القانوني, والتنظيمي, وفهم وإدارة مخاطر العمليات الرئيسة. إن الدفع لإدارة المخاطر هو حاجة الإدارة لإثبات وجود حوكمة في الشركة لمختلف المُستخدمين مثل: (المساهمين, المنظمين, المستخدمين, العملاء, المجهزين) لذلك ينبغي على مجلس الإدارة التأكد من وجود شفافية ترتبط بالمخاطر الجوهرية على المؤسسة, وهذا يتضمن تحديد تقبل وتحمل المخاطرة, تقدير المعرفة بمخاطر تقنية المعلومات وتحديد الحالات المعرضة للمخاطر. وفي ضوء إدارة المخاطر توصلت نتائج دراسة (رشيد؛ علي, ٢٠٢٠) إلى أن آليات حوكمة تكنولوجيا المعلومات لها دور فى تفعيل إدارة مخاطر تقنية المعلومات المحاسبية.
٤. **مقاييس الأداء:** Performance Indicators ويتم القياس من خلال استخدام بطاقة الآداء المتوازن فهي تُعد أداة غاية في الفاعلية لمجلس الإدارة, وذلك لتحقيق التوافق بين نظم المعلومات وإستراتيجية المؤسسة كما ينبغى على الإدارة استخدام بيانات الوقت الحقيقي أو البيانات الفورية, وذلك لتحسين عملية الإبلاغ الفوري للمعلومات في نظم تكنولوجيا المعلومات.
٥. **إدارة الموارد البشرية:** Human Resources Management إدارة الموارد البشرية والتقنية على نحو أكثر فعالية, وتنظيمها بشكل أكثر كفاءة وذلك بوضع خطة مالية وتمويلية لتكنولوجيا المعلومات (عبيدلي, ٢٠١٨).

سادساً: متطلبات حوكمة تكنولوجيا المعلومات:

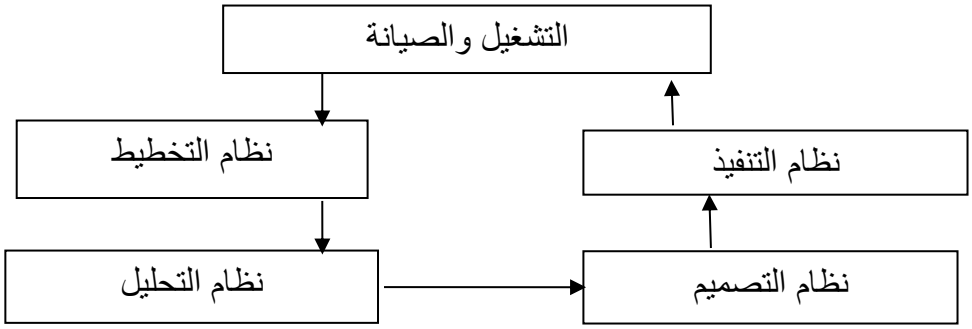
وتتمثل متطلبات حوكمة تكنولوجيا المعلومات في النقاط التالية:

١. **وجود لجنة حوكمة تكنولوجيا المعلومات:**

وتقوم بتحديد النظم تكنولوجيا المعلومات التي تساعد على تحقيق أهداف المنظمة, كما تقوم بالحكم على ردود الفعل الناتجة عن استخدام تكنولوجيا المعلومات ومناقشة التقارير الواردة من التشغيل لهذه النظم لتقييمها والتعرف على مدى ملائمتها مع الأهداف الإستراتيجية للمنظمة.

٢. **التطوير المستمر لدورة حياة النظم (SDLC):**

وهى عملية منهجية لإدارة عملية تخطيط وتحليل وتصميم وتنفيذ وكذلك استخدام تكنولوجيا المعلومات كما هو بالشكل رقم (٢) (أمين, ٢٠١٥).



شكل (٢) نظرة عامة حول تطوير دورة حياة النظم

سابعاً: معوقات تبني حوكمة تكنولوجيا المعلومات

وتتمثل المعوقات فيما يلي:

١. **عدم كفاية مساهمة أصحاب المصالح:**

أ. معوقات في الحصول على مشاركة كافية في مبادرات حوكمة تكنولوجيا المعلومات.
ب. ضعف الدعم: الداخلي والخارجي.
ج. السياسات الداخلية.
د.مقاومة التغير والتغيير.
ه.مقاومة متعلقة بتقبل السياسات والمعايير والمسؤوليات الجديدة.
و. ضعف دعم إدارة الموارد البشرية.
ز. غياب الملكية.

٢. **غياب وضوح مبادئ وسياسات متُعلقة بحوكمة تكنولوجيا المعلومات:**

أ. فشل المديرين التنفيذيين في دعم تكنولوجيا المعلومات.
ب. غياب الدعم لإدارة تكنولوجيا المعلومات.
ج.مدى وضوح مبادئ حوكمة تكنولوجيا المعلومات.
د. التحليل التنظيمى.

٣. **عدم ملائمة الثقافة التنظيمية:**

أ. أولويات تكنولوجيا المعلومات غير محددة جيداً.
ب. الثقافة المجتمعية- الثقافة الداخلية.

٤. **غياب التواصل والاتصال:**

أ. لا توجد علاقات متقاربة بين الأعمال وتكنولوجيا المعلومات.
ب. لا يوجد تفهم واضح لمنطق الأعمال من قبل تكنولوجيا المعلومات.

ج. غياب الاتصال المناسب.

٥. **غياب وضوح لعمليات المُتعلقة بحوكمة تكنولوجيا المعلومات:**

أ. غياب وضوح لعمليات حوكمة تكنولوجيا المعلومات.

ب. دعم عمليات حوكمة تكنولوجيا المعلومات.

٦. **عدم كفاية دعم الموارد المالية:**

أ. محدودية الميزانيات المالية.

٧. **عدم كفاية الوقت المخصص للمشروع (Abdollahbeigi, Salehi, 2020).**

ثامناً: ضوابط حوكمة تكنولوجيا المعلومات

وتتمثل فيما يلي:

١. **ضوابط المبادئ والسياسات وأطر العمل:**

أ. على المجلس أو من يفوض من لجانه، اعتماد منظومة المبادئ والسياسات وأطر العمل وبالأخص المرتبطة بإدارة مخاطر تكنولوجيا المعلومات، وإدارة أمن المعلومات، وإدارة الموارد البشرية اللازمة لتحقيق الإطار العام لإدارة موارد ومشاريع تكنولوجيا المعلومات والاتصالات، وضبطها ومراقبتها،وبما يلبي متطلبات الأهداف وعمليات حوكمة تكنولوجيا المعلومات والاتصالات.

ب. على المجلس اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حوكمة تكنولوجيا المعلومات وعد منظومة السياسات هذه حداً أدنى مع إمكانية الجمع والدمج لتلك السياسات بحسب ما تقتضيه طبيعة العمل، على أن يتم تطوير سياسات أخرى ناظمة مواكبة لتطور أهداف المنظمة وآليات العمل، وعلى أن تحدد كُل سياسة الجهة المالكة، ونطاق التطبيق، ودورية المراجعة والتحديث وصلاحيات الإطلاع، والتوزيع، والأهداف، والمسؤوليات وإجراءات العمل المرتبطة بها, والعقوبات فى حال عدم الامتثال وآليات فحص الامتثال.

ج. يراعى لدى إنشاء السياسات مساهمة جميع الشركاء: الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها بوصفها مراجع لصياغة تلك السياسات مثل: (ISO,2/27001 IEC/ISO, COBIT ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL,...etc)

٢. **ضوابط الهياكل التنظيمية:**

أ. على المجلس اعتماد الهياكل التنظيمية (الهرمية واللجان) وبصورة خاصة تلك المرتبطة بإدارة موارد وعمليات ومشاريع تكنولوجيا المعلومات، وإدارة أمن المعلومات، وإدارة الموارد البشرية التي تلبي متطلبات عمليات حوكمة تكنولوجيا المعلومات وتحقيق أهداف المنظمة بكفاءة عالية وفعالية.

ب. يراعي ضمان فصل المهام المتعارضة بطبيعتها ومتطلبات الحماية التنظيمية المرتبطة بالرقابة الثنائية حدًا أدنى وكفاية وتحديث الوصف الوظيفى لدى اعتماد الهياكل التنظيمية للمنظمة وتعديلها (البنك المركزى العراقي, ٢٠١٩).

٣. **ضوابط المعلومات والتقارير:**

أ. على المجلس والإدارة التنفيذية العليا تطوير البنية التحتية ونظم المعلومات اللازمة لتوافر المعلومات والتقارير لمُستخدميها بصفته مرتكزاً لعمليات إتخاذ القرار في المنظمة، وعليه يجب أن تتوافر متطلبات جودة المعلومات والمتمثلة بالمصداقية والنزاهة والتكامل والدقة والتوافرية ومتطلبات السرية بحسب سياسة تصنيف البيانات والامتثال لتلك المعلومات والتقارير، فضلاً عن المتطلبات الأخرى الواردة في المعيار COBIT–Information Enabling والمتمثلة بالموضوعية، والمصداقية، والسمعة، والملاءمة، والمبالغ المناسبة، والتمثيل المختصر، والتمثيل المتناسق، والتفسير، والفهم، والوصول المقيد.

ب. على المجلس اعتماد منظومة المعلومات والتقارير الواردة وعد تلك المنظومة حداً أدنى مع مراعاة تحديد مالكين لتلك المعلومات والتقارير تُحدَّد من خلالهم، وتُفوض صلاحيات الاطلاع والاستخدام

بحسب الحاجة للعمل والشركاء المُعنيين على أن تتم مراجعتها وتطويرها بشكل مستمر لمواكبة تطوير أهداف وعمليات المنظمة وبما يوافق أفضل الممارسات الدولية المقبولة بهذا الشأن.

وفي ضوء ذلك توصلت نتائج دراسة (بن سعيد, ٢٠١٥) الى فاعلية حوكمة تكنولوجيا المعلومات على جودة التقارير المالية, حيث ان زيادة الثقة فى نظام المعلومات المحاسبي للمنظمة مما ينعكس بصورة مباشرة على القوائم المالية والمحاسبية التي يصدرها النظام.

٤. **ضوابط الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات :**

أ. على المجلس والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات، وعد تلك المنظومة حداً أدنى على أن يتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف المنظمة وعملياتها، وبما يوافق أفضل الممارسات الدولية المقبولة بهذا الشأن.

ب. على المجلس الإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات، ومن ثم المعلومات والتقنية المصاحبة لها، والأهداف المؤسسية .

٥. **ضوابط المعارف والمهارات والخبرات:**

أ. على المجلس اعتماد مصفوفة المؤهلات وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حوكمة تكنولوجيا المعلومات، ومتطلبات هذه الضوابط بشكل عام، وضمان وضع الفرد المناسب في المكان المناسب.

ب. على إدارة المنظمة توظيف العنصر البشري المؤهل والمدرب من الأفرد ذوي الخبرة في مجالات إدارة موارد تكنولوجيا المعلومات وإدارة المخاطر وإدارة أمن المعلومات وإدارة تدقيق تكنولوجيا المعلومات بالإستناد إلى معايير الخبرات: الأكاديمية والفنية والمهنية, وذلك من خلال تأشيرها من جهات ذات اختصاص، على أن تتم إعادة تأهيل وتدريب الكوادر الموظفة حالياً لتلبية المتطلبات المذكورة خلال سنتين من تاريخ هذه الضوابط .

ج. على الإدارة التنفيذية في المنظمة الاستمرار برفد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق عمليات حوكمة تكنولوجيا المعلومات.

د. على الإدارة التنفيذية في المنظمة تضمين آليات التقييم السنوي للكوادر بمعايير قياس موضوعية تأخذ بالحسبان المساهمة من خلال المركز الوظيفي بتحقيق أهداف المنظمة (البنك المركزى العراقي, ٢٠١٩).

تاسعاً: معايير حوكمة تكنولوجيا المعلومات :

يمكن تحديد أهم المعايير التي سهمت فى الحد من المخاطر وتحقيق أمن المعلومات فى المؤسسات الشركات حسب ما ذكرته بعض الدراسات والتى من الممكن أن تسهم فى تحقيق نفس الأهداف فى البنوك التجارية وفقاً لنظام المعلومات فيما يلي:

١- **معيار الكوبيت: COBIT** هذا أصدره معهد حوكمة تكنولوجيا المعلومات (ITGI) في عام (١٩٩٥)، وهو يُمثل إطار للتحكم والسيطرة يمكن عن طريقه الربط بين تكنولوجيا المعلومات وبين متطلبات العمل بهدف تنظيم أنشطة تكنولوجيا المعلومات وفقاً لنموذج العملية المقبولة، حيث يتم تحديد الموارد الرئيسة لتكنولوجيا المعلومات وأهداف الرقابة التى يجب أخذها في الاعتبار.

٢- **معايير أيزو: ISO** الصادرة عن منظمة أيزو ISO المسئولة معن صياغة ووضع المعايير الخاصة بأمن وحماية تكنولوجيا المعلومات، وقد قامت هذه المؤسسة منذ إنشائها وحتى الآن، بإصدار العديد من المعايير كان من بينها:

أ- معيار ISO 27001: أصدر عام (٢٠٠٥) بهدف وضع القواعد الخاصة بنظام إدارة أمن وحماية المعلومات، حيث أوضحت تلك القواعد كيفية التصميم والتطبيق والرقابة والتطوير المستمر لأداء هذه الإدارة، هذا بالإضافة إلى تقييم المخاطر الإلكترونية التى قد تتعرض لها، ويقوم معيار ISO 27001 على نموذج يسمى PDCA، حيث تمر عملية تطبيق المعيار وفقاً لهذا النموذج بأربعة مراحل أساسية وهى:

- الخطة: Plan إنشاء نظام لإدارة أمن المعلومات ووضع خطة واضحة لتشغيل هذا النظام.

- التنفيذ: Do وهو البداية الفعلية في تنفيذ الخطط الموضوعة وتشغيلها.
- التحقق: Check مراجعة دورية للتنفيذ لقياس القدرة على تحقيق الأهداف.
- العمل: Act ويعنى إتخاذ الإجراءات اللازمة لصيانة وتحسين أداء النظام .

ب. معيار ISO 27001: والصادر عن منظمة الأيزو ISO عام (٢٠٠٥)، لتوضيح كيفية التطبيق الفعلى لأسس وقواعد التطبيق الخاصة بمعيار ISO 27001 الذى يوضح النقاط الأساسية التى يجب القيام بها بعد التطبيق، لتأمين وحماية الأصول التكنولوجية لتجنب مخاطر التشغيل الإلكترونى:

ج. معيار ISO 38500 ويقوم على مجموعة من القواعد تتمثل فيما يلي :

- التحديد الواضع والدقيق لمهام ومسئوليات إدارة تكنولوجيا المعلومات.
- وضع إستراتيجية كاملة للتخطيط بما يتفق مع أهداف ومتطلبات المؤسسة .
- أن يتم اقتناء تكنولوجيا المعلومات المناسبة وفقاً لأسباب منطقية ومحددة .
- التأكد من أن الأداء التكنولوجى يسير وفقاً خطوات الموضوعة.
- تحقيق التوافق بين تكنولوجيا المعلومات والقوانين واللوائح ذات العلاقة بها
- مراعاة الموارد المالية والكفاءات البشرية اللازمة لإدارة وتشغيل النظام.

المبحث الثاني إدارة المخاطر السيبرانية

وفيه تناول الباحث مفهوم الأمن السيبراني, طبيعة مخاطر الأمن السيبراني أهم نماذج الأمن السيبراني, إدارة مخاطر الأمن السيبراني, وسوف يتم تناول ذلك بالتفصيل في الاتي:

أولاً: مفهوم الأمن السيبراني:

يعرف الأمن السيبراني بأنه: "النشاط الذي يحمي الموارد: المالية والبشرية التي ترتبط بالاتصالات، ويخفف من حدة الأضرار والخسائر التي تحدث في حالة وجود قرصنة أو مخاطر أو تهديدات ويحاول تصليح ما أفسدته هذه الهجمات" (جبور، ٢٠١٦).

ويعرف الباحث الأمن السيبراني بأنه: حماية الأفراد لبياناتهم وحساباتهم وأجهزتهم من الهجمات الإلكترونية.

ثانياً: طبيعة مخاطر الأمن السيبراني:

وتتمثل المخاطر السيبرانية فيما يلي:

٢-١ المخاطر التقنية

تترافق طبيعة التكنولوجيا والاتصالات، مع أخطار خاصة، مرتبطة بهندستها الخاصة، وبالبيئة التي تعمل في إطارها، أي الفضاء السيبيرى. واذا كانت التقنية، والرقمنة، تتحكم بتوسع تقنيات المعلومات والاتصالات، وبالولوج إلى الفضاء السيبيري، ورسم حدوده، بما جعل البعض يعتبرونها قادرة على لعب دور القانون فى تنظيم الفضاء السيبرانى، وضبط الأعمال المخلة بأمنه وصولاً إلى إنكارهم على المشرع، وحق الاضطلاع بمهمة هذا التنظيم .

٢-٢ المخاطر القانونية:

وتتمثل فى غياب الهيكل التشريعى والتنظيمى المناسب للتعامل مع نتائج الأعمال القانونية وغير القانونية منها، والتى تتم فى الفضاء السيبرانى. فالنشاط الاقتصادى والتجارى وغيره، يتطلب تحديداً واضحاً للحقوق والواجبات بما يسهم فى تعزيز الثقة بقدرات تكنولوجيا المعلومات والاتصالات، فى مجال الخدمات عبر الفضاء الإلكتروني, وعليه، فإن المخاطر القانونية تتمثل في: غياب الأمن القانونى، وتناقض الأحكام والقوانين وتنازع الأنظمة القانونية من جهة، وفى إتساع إمكانات انتشار الجريمة الإلكترونية من جهة أخرى, حيث يرتفع نسبة

هذه المخاطر مع انعدام أو ضعف التعاون بين الدول المختلفة فى ملاحقة مرتكبي تتلاءم الاعتداءات الإلكترونية التي لا تقتصر على الأفراد فحسب بل تمتد لتطول أمن الدول واستقرارها (البغدادي, ٢٠٢١).

ثالثاً: أهم نماذج الأمن السيبراني:

لقد بدأت المؤسسات الأكاديمية ومراكز البحوث والمجتمع التقنى بالمساهمة, وقد اقترحت منهجيات متنوعة لتسريع الجاهزية السيبرانية للدول والمنظمات, هذا بالإضافة إلى مستويات نضوجها, وتتمثل هذه النماذج فيما يلي:

١- فريق من الخبراء فى معهد بوتاماك للدراسات السياسية:

في عام (٢٠١٥) تم نشر مؤشر الجاهزية السيبرانية CRI (2.0) وهو يبنى على مؤشر الجاهزية السيبرانية (1.0) الذى صدر عام (٢٠١٣) والذى قدم إطار عمل منهجى لتقييم الجاهزية السيبرانية, ويقدم مؤشر الجاهزية السيبرانية CRI (2.0) منهجية شاملة ونسبية وقائمة على التجارب لتقييم إلتزام الدول ومستوى النضج في سد الفجوة بين وضعها الحالى بالنسبة للأمن السيبراني, وبين القدرات السيبرانية الوطنية اللازمة لدعم مستقبلها الرقمى, ويستخدم المؤشر أكثر من (٧٠) مؤشر فريد من نوعه موزعين على (٧) عناصر أساسية لتمييز النشاطات الجاهزة من الناحية التشغيلية ولتحديد المجالات التي ينبغي تحسينها فى الفئات التالية: (١) الإستراتيجية الوطنية. (٢) الاستجابة للحوادث. (٣) الجريمة الإلكترونية وتطبيق القانون. (٤) تبادل المعلومات. (٥) الاستثمار فى البحث والتطوير. (٦) الدبلوماسية والتجارة. (٧) الدفاع والاستجابة للأزمات. ويوفر المخطط الناتج والقابل للتنفيذ خريطة طريق لخفض المخاطر لتتبعها الدول. ويربط مؤشر الجاهزية السيبرانية (2.0) بين النمو الاقتصادى والتنمية وبين سياسات الأمن الوطنى. كما يقر بأن تحقيق القدرة الكاملة لاقتصاد الإنترنت من ناحية نمو الناتج المحلى الإجمالى، وزيادة الإنتاجية والكفاءة، وتحسين مهارات القوى العامة، وتحسين الوصول للأعمال التجارية والبيانات يتطلب الموائمة بين إستراتيجيات التنمية الاقتصادية وبين أولويات الأمن الوطنى. بمعنى آخر، تقنيات المعلومات والاتصالات لا يمكنها تحقيق النمو الاقتصادى فى حال عدم وضع سياسات وعمليات وتقنيات لحماية وتأمين البنية التحتية السيبرانية والخدمات التى يعتمد عليها مستقبل الدولة الرقمى ونموها. ويركز مؤشر الجاهزية السيبرانية (2.0) على الأدوات التى يمكن لقادة العالم الاستفادة منها، بما فى ذلك السياسات، والتشريعات والقوانين، والأنظمة، والمعايير، وحوافز السوق، والمبادرات الأخرى لحماية قيمة استثماراتهم الرقمية ولمعالجة التآكل الاقتصادى المستمر الناجم عن انعدام الأمن السيبراني (Hathaway, 2020) .

٢- نموذج أوكسفورد لنضج قدرات الأمن السيبراني (CMM)

في عام (٢٠١٦) تم نشر نموذج أوكسفورد لنضج قدرات الأمن السيبراني (CMM) بواسطة مركز قدرات الأمن السيبرانى (GCSCC) فى جامعة أوكسفورد، وهو يصور مستويات متفاوتة لنضج الأمن السيبراني لدى الدول المختلفة وذلك بالاعتماد على خمسة أبعاد للقدرات: (١) سياسة وإستراتيجية الأمن السيبرانى؛ (٢) الثقافة السيبرانية والمجتمع؛ (٣) الأمن والتعليم والتدريب والمهارات السيبرانية؛ (٤) أطر العمل القانونية والتنظيمية؛ المعايير والمنظمات والتقنيات. وكل واحدة من تدل هذه الأبعاد ينقسم إلى عوامل ومؤشرات أكثر تحديداً، عند النظر إليها جميعاً, على مستوى نضج قدرات الأمن السيبرانى الخاصة بالدولة, ويستخدم نموذج أوكسفورد لنضج قدرات الأمن السيبراني (CMM) وسيلتين للمساعدة فى تشخيص الجاهزية السيبرانية. تستخدم الوسيلة الأولى أداة للاستقصاء (شبيهة بالاتحاد الدولى للاتصالات ITU)حيث يمكن للدول تشخيص جاهزياتها بذاتها. ومن ثم تتم مراجعة إجابات الاستقصاء وتشارك إحدى الفرق فى ورشة عمل تقنية مع أصحاب المصلحة السيبرانيين الرئيسين من الحكومة والمؤسسات الأكاديمية ومن القطاعين الحكومي والخاص لتقييم مستوى القدرات السيبرانية بشكل أفضل على خمس مستويات من النضج السيبراني هى: (المستوى الابتدائي، التكويني، القائم، الإستراتيجي، الديناميكى). نموذج أوكسفورد لنضج قدرات الأمن السيبراني (CMM) هو عبارة عن أداة ممتازة لقياس مستوى فهم أصحاب المصلحة الرئيسين للوضع الحالى للقدرات السيبرانية ولمستوى نضج الدولة مما يوفر أساساً لأهداف السياسات المُستقبلية ولنتائج خفض المخاطر (Hathaway, 2020).

رابعاً: إدارة مخاطر الأمن السيبراني:

لإدارة أمن المعلومات مجموعة من المُتغيرات الداخلية التى تعمل على نجاح برامج أمن نظم المعلومات, وهذه المُتغيرات هى:

١-سياسة أمن المعلومات: IS Policy

وهى مزيج من المبادئ والأنظمة والمنهجيات والتقنيات والأدوات التى أنشئت لحماية المنظمة من التهديات كما تعرف بأنها: وثيقة إستراتيجية بمعنى أنها تنشأ قبل القيام بأي نشاط من أنشطة أمن المعلومات فهى تتكون من الأهداف والاتجاهات والقواعد التى يجب وضعها واتباعها من قبل الموظفين والأطراف الأخرى التى تتعامل مع المؤسسة، لذا يجب أن تكون هذه السياسة واضحة في تحديد الأهداف والأدوار ومسئوليات الموظفين والأطراف الأخرى ذات المصلحة، كما يجب أن تكون شاملة بمعنى أنها تغطى جميع جوانب متطلبات وضوابط أمن المعلومات وأن تكون متناسقة مع سياسة المؤسسة ورؤيتها.

وتُمثل سياسة أمن المعلومات حجر الزاوية في إدارة أمن المعلومات الجيدة، كما أن هذه السياسة ليست ثابتة أي يجب أن يتم مراجعتها بإنتظام على الأقل مرة واحدة فى السنة للتأكد من أنها ذات صلة باحتياجات الوقت الحاضر, ويتم إرسالها إلى كامل الموظفين والأطراف الأخرى ذات المصلحة مع مراعاة أنه عند قيام المؤسسة بإحلال أساليب أمن تكنولوجية حديثة بدلاً من أساليب أمن المعلومات العادية يجب المفاضلة من حيث درجة الاستفادة ونجاح برامج أمن المعلومات بين البقاء على الأساليب العادية لأمن المعلومات مع تكاملها مع أساليب أمن المعلومات الحديثة أم الإحلال التام أكثر إفادة وينبغى لسياسة أمن المعلومات على المستوى المؤسسي أن تعالج أساسيات هيكل إدارة أمن المعلومات في المؤسسة, بما في ذلك أدوار ومسئوليات أمن المعلومات، بيان خط الأساس للضوابط الأمنية وقواعد تجاوز خط الأساس، وقواعد السلوك التى من المتوقع أن يتبعها مستخدمو المؤسسة والحد الأدنى من العواقب المترتبة على عدم الامتثال. وفيما يلي بعض المعايير التى ينبغى على المؤسسة اتباعها من أجل تنفيذ سياسة أمن فعالة :

- يجب أن تكون سياسة أمن المعلومات واضحة ومفهومة من قبل جميع الأطراف المُعنية وأن يتم متابعة هذه السياسة بانتظام لمعرفة ما إذا كان يتم انتهاكها كما يجب وجود مبادئ توجيهية إجرائية محددة بشكل جيد للتعامل مع حوادث انتهاك السياسة.
- أن تكون ملائمة للثقافة التنظيمية، وملائمة للنمط الذى يتسق مع أسلوب الاتصال العام فى المؤسسة.
- استخدام لغة بسيطة لضمان سهولة فهمها، وتحديد الغرض من السياسة ونطاق المؤسسة وشرح ما هو النشاط المقبول وما هو غير مقبول .
- ينبغى وضع سياسة أمن المعلومات على أساس الاحتياجات الأمنية والأهداف التجارية للمؤسسة .

٢-إجراءات أمن المعلومات: IS Procedures

يرتبط أمن المعلومات بمجموعة من الإجراءات المصممة لحماية المعلومات, فالإجراءات هى المبادئ التوجيهية لتنفيذ العمليات والأنشطة القائمة على أساس الاحتياجات الموضحة في سياسة أمن المعلومات بمعني أنها إرشادات التشغيل التى تشرح كيفية تنفيذ سياسة أمن المعلومات, حيث يتم اشتقاق الإجراءات من سياسة الأمن, وذلك لضمان تنفيذ ISM بشكل مناسب وصحيح. كما يجب أن تكون الإجراءات واضحة ومحددة فى وصف الخطوات اللازمة لإنجاز العمليات والأنشطة، وينبغى استعراضها بطريقة دورية أو عند تغيرات بيئة الأمن نتيجة التطورات التكنولوجية المستمرة, لذلك فإنه من الضرورى وجود إدارة مسئولة عن إدارة برنامج التغير وقادرة على رسم إجراءات وخطوات ملائمة لإدارة ذلك التغير, حيث إنه قبل إجراء أى تغيير لا بد من وضع تخطيط جيد يضمن أن إقتناء التقنيات الجديدة لن يؤثر سلبياً على سلامة أمن المعلومات ومدى الاستفادة منها.

يتضح مما سبق أن إجراءات أمن المعلومات أقرب إلى المُستخدمين والأجهزة من السياسة الأمنية حيث إنها توفر الخطوات التفصيلية للتركيب والإعداد والتهيئة، فهى تعمل على تحويل السياسات والتوجيهات إلى أرض الواقع ومن البيئة النظرية إلى بيئة تشغيلية حقيقية.

٣- فريق إدارة أمن المعلومات: ISM Team

ويتكون الفريق من الموظفين المشاركين فى معظم أنشطة أمن المعلومات، حيث يجب أن يتمتع هذا الفريق بالمعرفة والمهارات الواسعة والتعاون في تنفيذ عمليات ISM وأن يكون دائم التحديث مع القضايا الأمنية الحالية، كما ينبغى أن يمتلك المهارة التقنية التى تؤهله للقيام بالأعمال والمهام الجديدة.

٤- فريق تنسيق إدارة أمن المعلومات: Coordinator Team

يعمل الفريق كحلقة وصل بين كل من الإدارة العليا وفريق ISM ومراجعى أمن المعلومات والموظفين، فهو المسئول عن تنظيم التدريب والتوعية بالبرامج وإدارة الموارد المالية والبشرية وتقديم تقرير عن التقدم في ISM إلى الإدارة العليا، كما ينبغى أن يتوافر فى أفراد فريق التنسيق مهارات التواصل الجيدة مع الآخرين والمعرفة الكاملة بأنشطة ISM حيث القدرة على التواصل بفعالية مع جميع المستويات في المؤسسة (Zammani, Razali, 2016).

٥- فريق مراجعة أمن المعلومات IS Audit Team

هو فريق مسئول عن ضمان ضوابط الرقابة، وأنه يتم تنفيذ العمليات والإجراءات والأنشطة بشكل صحيح، فينبغى أن يتمتع هذا الفريق بمهارات الاتصال الجيدة والإلتزام بالوقت المحدد لإنهاء عملية مراجعة أمن المعلومات، ولكي يغم نجاح برامج أمن المعلومات يجب أن يكون لدى فريق مراجعة أمن المعلومات فهم جيد لعمليات ISM حيث إن نقص المعرفة قد تؤدى إلى طرح الأسئلة بطريقة خاطئة وبذلك وجود معلومات خاطئة.

٦- تقييم إدارة أمن نظم المعلومات:

ويتم هذا التقييم عن طريق: الإدارة المستمرة للأعمال (خطة استمرارية الأعمال)، لذلك يجب على المؤسسة تحديد متطلبات أمن المعلومات وجعلها جزء لا يتجزأ من خطة استمرارية الأعمال، وأن تقوم المؤسسة أيضاً بتحديد خطة العمليات والإجراءات والموارد والمسئوليات للسيطرة على الحوادث والكوارث ولضمان استمرارية الأعمال أثناء الأحداث غير المقصودة وبعدها، ينبغى تطوير خطة استمرارية الأعمال وتوثيقها والموافقة عليها من قبل الإدارة كما يجب اختبارها لمراقبة فعاليتها (صالح؛ أوموسى؛ أبوسعدة, ٢٠٢٠).

الدراسة الميدانية

١- منهج البحث:

اعتمد الباحث على المزج بين المنهجين: المنهج الاستقرائي في إعداد الإطار النظري للبحث الحالى, والمنهج الاستنباطي في التطبيق الميداني على النحو التالي:

- **المنهج الاستقرائي:** حيث تم تحديد إطار لأبعاد مشكلة البحث وأهدافه وتناول التأصيل العلمى لأبعاد مشكلة البحث, وذلك بالاعتماد على الكتب العلمية والمقالات والأبحاث المنشورة والدوريات المختلفة المُتعلقة بموضوع البحث الحالي, وذلك بهدف معرفة أهم محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات, ومعرفة طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي, وتحديد مدى إسهام حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي.
- **المنهج الاستنباطي:** وعن طريقة قام الباحث باختبار فروض البحث وتحديد مدى قبول هذه الفروض من عدمه وتقييم الدور الذى تلعبه حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي الكويتي.

٢- مجتمع وعينة البحث:

تكون مجتمع البحث من جميع المدراء الماليين وخبراء تكنولوجيا المعلومات بالقطاع المصرفي الكويتي, ومسئولي إدارة المخاطر السيبرانية للقطاع المصرفي الكويتي.

وتم اختيار عينة البحث بطريقة عشوائية بسيطة ممثلة لمجتمع البحث بحجم (٩٦) مبحوث: (مدير مالي, وخبير تكنولوجيا المعلومات, ومسئول إدارة المخاطر السيبرانية), وتم توزيع (١٢٠) استبانة وتم استرداد (١٠٤) استبانة منها (٩٦) صالحة و(٨) غير صالحة للتحليل.

جدول (١)

تجميع استمارات الاستقصاء الخاصة بالبحث

م	الفئات	إجمالي عدد الاستمارات	
		الموزعة	الصالحة
١	المدراء الماليين.	٤٨	٤٣
٢	خبراء تكنولوجيا المعلومات بالمصارف.	٣٢	٢٧
٣	مسئولى إدارة المخاطر السيبرانية.	٤٠	٢٦
الإجمالي		**١٢٠**	**٩٦**

المصدر: من إعداد الباحث

وفى ضوء الجدول السابق (١) يتضح أن معدل القوائم الصالحة للتحليل الإحصائى لفئات البحث معدلاً مناسباً.

جدول (٢)

الخصائص الديموغرافية لعينة البحث

المتغير	الفئات	العدد	النسبة المئوية
الإدارة التابع لها	مدير مالي	٤٣	٤٤,٨
	خبير تكنولوجيا المعلومات.	٢٧	٢٨,٢
	مسئول إدارة المخاطر السيبرانية.	٢٦	٢٧

	الإجمالي	**٩٦**	**١٠٠**
المؤهل العلمي	بكالوريوس	٦٦	٦٨,٨
	ماجستير	١٥	١٥,٦
	دكتوراه	١٥	١٥,٦
	الإجمالي	**٩٦**	**١٠٠**
عدد سنوات الخبرة الوظيفية	أكبر من ٥ سنوات وأقل من ١٠ سنة	٣٨	٣٩,٦
	أكبر من ١٠ سنوات وأقل من ١٥ سنة	٢٨	٢٩,٢
	أكبر من ١٠ سنوات وأقل من ٢٠ سنة	٣٠	٣١,٢
	الإجمالي	**٩٦**	**١٠٠**

المصدر: من إعداد الباحث

٣- أداة البحث:

قام الباحث بتصميم أداة البحث الميداني, والمُتمثلة في استمارة تعرف دور حوكمة تكنولوجيا المعلومات فى إدارة المخاطر السيبرانية للقطاع المصرفي, والمتضمنة ثلاثة محاور, وتم وضع مجموعة من العبارات التي تُعبر عن كل محور وتُمثله, وعرضها على مجموعة من السادة الخبراء في مجال المحاسبة والمراجعة من أجل تحكيم المحاور, والعبارات الممثلة لكل محور من حيث وضوحها ومناسبتها, وذلك بهدف التأكد من أن العبارات الواردة في الاستطلاع تُمثل المحور الخاص بها وتعبر عنه.

وبعد عرض الاستبيان على الخبراء للتحكيم وبلغ عددهم (١٠) محكمين من الجامعات الكويتية وبعد إجراء التعديلات اللازمة على الاستبيان في ضوء اقتراحات السادة الخبراء والمحكمين, تكونت الاستبانة في صورتها النهائية من (٣١) عبارة موزعة على ثلاثة محاور كما يلي:

- **المحور الأول:** محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات, وشمل (١٠) عبارات.
- **المحور الثاني:** طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي, وشمل (٩) عبارات.
- **المحور الثالث:** مساهمة حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي, وشمل (١٢) عبارة.

صدق محتوى الأداة وثباتها:

- **صدق الأداة:**

يشير مفهوم الصدق إلى الاستدلالات الخاصة التي يمكن الخروج بها في درجات القياس من حيث مناسبتها وفائدتها, لذلك يشير صدق المحتوى للأداة إلى صلاحيتها في القيام بتفسيرات معينة, وأنها تقيس ما وضعت لقياسه أي قدرتها على تمثيل المحتوى المراد دراسته.

٣- **صدق المحكمين:** لقد تم عرض أداة البحث - الاستبيان - على مجموعة من الخبراء المتخصصين في مجال المحاسبة والمراجعة ومن خلال آراء, وتعديلات الخبراء تم صياغة الاستبيان فى صورته النهائية.

٤- **صدق التكوين:** تم حساب صدق التكوين في هذا البحث من خلال حساب الاتساق الداخلي, وذلك عن طريق حساب ارتباط كل عبارة بالدرجة الكلية للمحور:

جدول (٣)

معاملات ارتباط بيرسون بين الاسئلة والدرجة الكلية للمحور

المتغير	عدد العبارات	الدالة	غير الدالة
المحور الأول: محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات.	١٠	١٠	٠
المحور الثاني: طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي.	٩	٩	٠
المحور الثالث: مساهمة حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي.	١٢	١٢	٠

ونظرًا لاشتمال الاستمارة على عدة محاور، فقد تم حساب ارتباط كل محور مضمَّن مع الدرجة الكلية للاستمارة كما يلي:

جدول (٤)

معاملات ارتباط بيرسون بين محاور الاستمارة والدرجة الكلية للاستمارة

المحور	معامل الإرتباط بالدرجة الكلية	مستوى الدلالة
المحور الأول: محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات.	٠,٩٥٠	أقل من .0001
المحور الثاني: طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي.	٠,٩٣٥	أقل من .0001
المحور الثالث: مساهمة حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي.	٠,٩٤٣	أقل من .0001
الدرجة الكلية للاستمارة	٠,٩٧١	أقل من .0001

المصدر من إعداد الباحث

يتبين من الجدول السابق (٤) ارتفاع عدد الفقرات الدالة مما يدل على وجود قدر مقبول من الاتساق الداخلي بالاستمارة, كما أن جميع محاور البحث ترتبط ارتباطاً دالاً بالدرجة الكلية للاستمارة بلغت (٠,٩٧١) مما يؤكد أن الاستمارة تتمتع بدرجة عالية من الصدق يُطمْئِن الباحث أنها صالح للتطبيق على مفردات البحث.

- **ثبات الأداة:**

الثبات في أبسط معانيه يعني الوصول لنفس النتائج عند اتباع نفس الإجراءات المطبقة على مادة معينة بمعنى أنه يشير إلى درجة استقرار نتائج أداة القياس إذا ما أعيد تطبيقها على نفس الأفراد وفي نفس الظروف.

وتم حساب الثبات بمعامل "ألفا كرونباخ Cronbach's Alpha" لدراسة ثبات أسئلة الاستمارة بالتطبيق على العينة الاستطلاعية، وجدير بالذكر أنه من أكثر الطرق شيوعاً لقياس الثبات، وتعتمد هذه الطريقة على قيمة ألفا المقبولة في العلوم الإنسانية (٠,٦) أو أكبر لمجموعة الفقرات، وفيما يلي حساب معامل ألفا كما في الجدول التالي:

جدول (٥)

معامل "ألفا كرونباخ Cronbach's Alpha" لمحاور البحث

المحور	عدد البنود	معامل ألفا
المحور الأول: محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات.	١٠	٠,٩٠٣
المحور الثاني: طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي.	٩	٠,٨٧٥

المحور الثالث: مساهمة حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي.	١٢	٠,٨٩١
الدرجة الكلية للاستمارة	٣١	٠,٩٤٤

المصدر من إعداد الباحث

ويلاحظ في الجدول السابق (٥) أن قيمة معامل ألفا مرتفعة حيث بلغت (٠,٩٤٤) مما يدل على قبول درجة الثبات لجميع محاور البحث.

٤-المعالجة الإحصائية للبيانات:

لمعالجة بيانات الاستبيان باستخدام الحاسوب اعتمد البحث على برنامج الحزمة الإحصائية للعلوم الاجتماعية SPSS (Statistical Package for Social Sciences), حيث تم تفريغ استجابات أفراد عينة البحث, وترميزها من خلال تقدير الدرجات التالية لاستجابات الأفراد على درجة الموافقة لعبارات الاستبيان وفقاً لمقياس ليكرت الخماسي كما يلي:

جدول (٦)

استجابات الأفراد على درجة الموافقة لعبارات الاستبيان وفقاً لمقياس ليكرت الخماسي

بدائل الإجابة	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
الدرجة	(٥)	(٤)	(٣)	(٢)	(١)

وتم استخدام التكرارات والنسب المئوية لتحليل إجابات العينة على كل عبارة من عبارات الاستمارة, كما اعتمد البحث على المتوسطات الحسابية, والانحرافات المعيارية, وتحليل التباين الأحادي (ANOVA), لمقارنة العبارات ببعضها البعض, وكذلك تم الاستعانة بمعامل ألفا كرونباخ ومعاملات ارتباط بيرسون للتأكد من صدق وثبات استمارة البحث المستخدمة, وبذلك تم تحليل نتائج الأداة في ضوء تلك العمليات وتفسيرها, وذلك على النحو التالي:

نتائج البحث ومناقشتها

الفرض الأول: لا يوجد اختلاف ذو دلالة إحصائية بين متوسط آراء عينة البحث على محددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات.

وللتحقق من صحة الفرض تم استخراج المتوسطات الحسابية والانحرافات المعيارية للفقرات المرتبطة بمحددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات وجدول (٧) يوضح ذلك:

جدول (٧)

نتائج التحليل الإحصائي لمحددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات

م	الفقرة	المتوسط الحسابي	الانحراف المعيارى
١	خطة تكنولوجيا المعلومات في القطاع المصرفي ثابتة لا تتغير.	٤,٠٣	١,٢٨
٢	تنظيم وهيكلية تكنولوجيا المعلومات لا يتم وفق خطة القطاع المصرفي المتطورة.	٣,٧٧	١,١٠
٣	لا يوجد تقييم مستمر ومتتالي لإستراتيجية القطاع المصرفي المُتعلقة بأساليب تكنولوجيا المعلومات.	٣,٥٦	١,٢٣
٤	لا تدرج إدارة استثمارات تكنولوجيا المعلومات وتطويرها وإقرارها ضمن موازنة تكنولوجيا المعلومات للقطاع المصرفي.	٤,١٠	٠,٩١

٥	السماح لغير المصرح لهم بالدخول إلى برامج القطاع المصرفي المختلفة.	٤,١٧	٠,٧٢
٦	تأكيد المصارف على أن مخاطر تكنولوجيا المعلومات يتم إدارتها بكفاءة.	٣,٨١	١,٢٨
٧	لا توجد دورات مستمرة للعاملين بالقطاع المصرفي على تكنولوجيا المعلومات.	٣,٩٣	١,٠٩
٨	افتقار عدد من أعضاء مجلس إدارة القطاع للخبرة في مجال تكنولوجيا المعلومات.	٣,٩٠	١,٠٠
٩	لا توجد لجنة لتكنولوجيا المعلومات تابعة لمجلس إدراة القطاع المصرفي.	٤,٢١	٠,٨٠
١٠	ضعف السياسات الداخلية في القطاع المصرفي بشأن تفعيل آليات تكنولوجيا المعلومات.	٣,٩٨	١,١١
	الاجمالي	**٣,٩١**	**٠,٨٥**

يبين الجدول السابق (٧) الإحصاءات الوصفية: (المتوسطات الحسابية وتراوحت بين (٣,٥٦ - ٤,٢١), والانحرافات المعيارية وتراوحت بين (٠,٧٢- ١,٢٨)) لإجابات عينة البحث عن أسئلة الاستقصاء المرتبطة بمحددات ومعوقات تطبيق حوكمة تكنولوجيا المعلومات, ويبدو ذلك في ارتفاع قيم المتوسط الحسابى لكل فقرة (أكبر من ٣) وقد جاء ترتيب أهم الفقرات على النحو التالي:

١. لا توجد لجنة لتكنولوجيا المعلومات تابعة لمجلس إدراة القطاع المصرفي, وأخذت المرتبة الأولى بمتوسط حسابي (٤,٢١).
٢. السماح لغير المصرح لهم بالدخول إلى برامج القطاع المصرفي المختلفة, وأخذت المرتبة الثانية بمتوسط حسابي (٤,١٧).

واتفقت هذه النتيجة مع ما توصلت اليه دراسة (البلقاسي, ٢٠١٨), إلى وجود العديد من المعوقات التي تحد من تطبيق حوكمة تكنولوجيا المعلومات.

الفرض الثاني: لا يوجد اختلاف ذو دلالة إحصائية بين متوسط آراء عينة البحث على طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي.

وللتحقق من صحة الفرض تم استخراج المتوسطات الحسابية والانحرافات المعيارية للفقرات المرتبطة بطبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي وجدول (٨) يوضح ذلك:

جدول (٨)

نتائج التحليل الإحصائي طبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي

م	الفقرة	المتوسط الحسابي	الانحراف المعيارى
١	يقوم القطاع المصرفي بالتأكد من صحة المعاملات والمسؤولية من خلال العمليات الإلكترونية.	٤,١٨	.٨٨٩
٢	يقوم القطاع المصرفي بضبط معايير الأنشطة المصرفية الإلكترونية .	٤,١٥	.٨٧٩
٣	يقوم القطاع المصرفي بتحسين الخدمات المصرفية الإلكترونية لإرضاء العملاء.	٤,٠٨	١,٠٨٥
٤	يقوم القطاع المصرفي بالتأكيد على أن مخاطر تكنولوجيا المعلومات يتم إدارتها بكفاءة.	٣,٩٥	.٩٢٩
٥	يقوم القطاع المصرفي بإرشاد وتوجيه العملاء للمخاطر السيبرانية.	٣,٩٢	.٩٦٢
٦	تقوم المصارف بالتعريف بالاطر القانونية والتشريعية من خلال المعاملات الإلكترونية.	٣,٩٠	.٩٥٢

٧	يقوم القطاع المصرفي بالتوسع في تقديم الخدمات والمنتجات المصرفية لمعرفة السوق والتحقق من صحة الضمانات.	٣,٨٨	٩٨٤.
٨	يقوم القطاع المصرفي بتأمين المعلومات والحفاظ على خصوصية البيانات.	٣,٩٤	٩٣٣.
٩	تقوم المصارف بتعزيز حماية المؤسسة من الهجمات الإلكترونية بكافة أشكالها	٤,١٩	٨٨٦.
	الإجمالى	**٣,٩٩**	**٥٧٧.**

يبين الجدول السابق (٨) الإحصاءات الوصفية: (المتوسطات الحسابية تراوحت بين (٣,٨٨- ٤,١٩), والانحرافات المعيارية تراوحت بين (.٨٧٩- ١,٠٨٥)) لإجابات عينة البحث عن أسئلة الاستقصاء المرتبطة بطبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي, ويبدو ذلك في ارتفاع قيم المتوسط الحسابى لكل فقرة (أكبر من ٣) وقد جاء ترتيب أهم الفقرات على النحو التالي:

١. تقوم المصارف بتعزيز حماية المؤسسة من الهجمات الإلكترونية بكافة أشكالها, وأخذت المرتبة الأولى بمتوسط حسابي (٤,١٩).
٢. تقوم المصارف بالتأكد من صحة المعاملات والمسؤولية من خلال العمليات الإلكترونية, وأخذت المرتبة الثانية بمتوسط حسابي (٤,١٨).

الفرض الثالث: توجد علاقة ارتباطية جوهرية بين مساهمة حوكمة التكنولوجيا المعلومات في إدارة المخاطر السيبرانية في القطاع المصرفي.

وللتحقق من صحة الفرض تم استخراج المتوسطات الحسابية والانحرافات المعيارية للفقرات المرتبطة بطبيعة ومحددات المخاطر السيبرانية بالقطاع المصرفي وجدول (٩) يوضح ذلك:

جدول (٩)

نتائج التحليل الإحصائي مساهمة حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية في المصارف

م	الفقرة	المتوسط الحسابي	الانحراف المعيارى
١	توفر حوكمة تكنولوجيا المعلومات تقييماً للمخاطر السيبرانية بصورة دورية.	٣,٥١	١,١٧
٢	تعمل حوكمة تكنولوجيا المعلومات على الحد من مخاطر تكنولوجيا المعلومات وعدم تكرارها.	٣,٥٩	١,٢١
٣	تحسن حوكمة التكنولوجيا أداء المخاطر بالمصرف في ظل بيئة تكنولوجيا المعلومات.	٣,٦٩	١,٢٠
٤	تقدم حوكمة التكنولوجيا الدعم الفعال والمشاركة في عمليات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات.	٤,٠٢	٠,٩٠
٥	تقدم حوكمة التكنولوجيا الاستشارات اللازمة عند تصميم وتحسين إستراتيجيات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات.	٤,١٥	٠,٧٥
٦	تعمل حوكمة التكنولوجيا على وضع مستويات مقبولة وغير مقبولة للمخاطر السيبرانية في ضوء حوكمة تكنولوجيا المعلومات.	٣,٣٥	١,٣٧
٧	توفر حوكمة التكنولوجيا تدريب العاملين في تكنولوجيا المعلومات على التصدي للمخاطر السيبرانية.	٣,٨٦	١,٢١
٨	توفر حوكمة التكنولوجيا تحديث وتطوير نظم الحماية من المخاطر السيبرانية بشكل دوري.	٣,٥٨	٠,٩٨

٩	توفر حوكمة التكنولوجيا الاعتماد على مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات.	٤,٢٢	٠,٧٩
١٠	توفر حوكمة التكنولوجيا إجراء اختبارات موازية للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية ضد مخاطر الهجمات السيبرانية.	٣,٨١	١,٠٦
١١	تحقق حوكمة التكنولوجيا وجود قسم مخصص لإدارة أمن الشبكات ضد المخاطر السيبرانية.	٣,٧٣	١,٣١
١٢	توفر حوكمة التكنولوجيا المراجعة الدورية لأنظمة الحماية ومعالجة البيانات.	٣,٨٦	١,٢٦
	الاجمالي	**٣,٧٧**	**٠,٩٠**

يبين الجدول السابق (٩) الإحصاءات الوصفية: (المتوسطات الحسابية تراوحت بين (٣,٣٥- ٤,٢٢), والانحرافات المعيارية تراوحت بين (٠,٧٥- ١,٣٧)) لإجابات عينة البحث عن أسئلة الاستقصاء المرتبطة بمساهمة حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي, ويبدو ذلك في ارتفاع قيم المتوسط الحسابى لكل فقرة (أكبر من ٣), وقد جاء ترتيب أهم الفقرات على النحو التالي:

١. توفر حوكمة التكنولوجيا الاعتماد على مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات, وأخذت المرتبة الأولى بمتوسط حسابي (٤,٢٢).
٢. تقدم حوكمة التكنولوجيا الاستشارات اللازمة عند تصميم وتحسين إستراتيجيات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات, وأخذت المرتبة الثانية بمتوسط حسابي (٤,١٥).

وتتفق هذه النتيجة مع ما توصلت إليه نتيجة دراسة (كريم, ٢٠١٩) والتي توصلت إلى أهمية حوكمة تكنولوجيا المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية بالقطاع المصرفى الليبى.

التوصيات والمقترحات

وتتمثل فيما يلي:

١- السعى نحو تطبيق حوكمة تكنولوجيا المعلومات بفعالية في القطاعات المصرفية الكويتية للحد من المخاطر السيبرانية.
٢- ضرورة اهتمام الباحثين الجدد بموضوع حوكمة تكنولوجيا المعلومات في القطاع المصرفى.
٣- قيام إدارات المصارف بدولة الكويت بإنشاء لجنة متخصصة بالأمن السيبراني.
٤- قيام إدارات المصارف بدولة الكويت بتامين تعاملاتها الإلكترونية ضد الاختراقات والقرصنة الإلكترونية خصوصاً هناك توسعاً واضحاً في الاعتماد على التكنولوجيا في ظل الثورة الصناعية الرابعة.

قائمة المراجع

أولاً: المراجع العربية

الكتب

١- السواح, نادر شعبان إبراهيم. (٢٠١٦). ***حوكمة تكنولوجيا المعلومات.*** (الإسكندرية, الدار الجامعية).

المجلات

١. بن سعيد, أمين. (٢٠١٥). أثر حوكمة تكنولوجيا المعلومات على جودة وموثوقية القوائم المالية " ***مجلة الدراسات الاقتصادية والمالية***، جامعة الشهيد حمه لخضر الوادي, ٣(٨), ٧- ٣٥.
٢. البلقاسي, منال صبحى على (٢٠١٨). أثر تطبيق حوكمة تكنولوجيا المعلومات وفقا ل Cobit 5 على مخاطر نظم المعلومات الإلكترونية: دراسة ميدانية على المعاهد العالية الخاصة. ***المجلة المصرية للدراسات التجارية***, جامعة المنصورة- كلية التجارة, ٤٢(١), ٧٨-١١٩.
٣. البغدادي, مروة فتحي السيد. (٢٠٢١). اقتصاديات الأمن السيبراني في القطاع المصرفي. ***مجلة البحوث القانونية***, ع(٧٦), يونيو, ١٤٤٧- ١٥١٣.
٤. جبور، منى الأشقر. (٢٠١٦). السيبرانية: هاجس العصر. ***مجلة المكتبات والمعلومات والتوثيق في العالم العربي جامعة الدول العربية***, ١(٥), ديسمبر, ٢٦٢- ٢٦٣.
٥. الحسناوي, عقيل حمزة حبيب؛ الموسري, انعام محسن. (٢٠١٧). دور حوكمة تكنولوجيا المعلومات فى تقليل مخاطر تدقيق نظم المعلومات المحاسبية الإلكترونية في ظل إطار عمل (COBIT) للرقابة الداخلية. ***مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية.*** ٩(٣), ١-٢٤.
٦. رشيد, شلير عبدالرحمن؛ علي, ئاكره يي أسامة حسين. (٢٠٢٠). دور آليات حوكمة تقنيات المعلومات في تفعيل إدارة مخاطر نظم معلومات المحاسبية المحوسب وفق إطار (NIST ٨٠٠-٣٧) للرقابة الداخلية/ دراسة تحليلية لعينة من شركات المساهمة ومراقبي الحسابات في أقليم كوردستان العراق. ***مجلة قهلاي زانست العلمية***, ٥(٣), ٤٩٨- ٥٣١.
٧. الزيود, أحمد محمود. (٢٠٢٠). إدارة مخاطر الأمن السيبراني في البنوك الأردنية. بنك لبنان والمهجر, ٦- ١٤.
٨. السعداوي, محمد عبدالله فرج. (٢٠١٧). تفعيل أثر تطبيق حوكمة نظم المعلومات في الحد من مخاطر المعلومات. ***المجلة العلمية للاقتصاد والتجارة***, كلية التجارة, جامعة عين شمس, ١(٢), يونيو, ٢٩٥- ٣٢٨.
٩. السمان, ثائر أحمد سعدون؛ عبدالجبوري, مراد موسى. (٢٠١٦). متطلبات حوكمة تقنية المعلومات ودورها في تحسين جودة الخدمات: دراسة حالة في المديرية العامة لإنتاج الطاقة الكهربائية. ***المجلة العربية للإدارة***, ٣٦(١), يونيو, ١٢٥- ١٤١.
١٠. السواح, نادر شعبان إبراهيم. (٢٠٢٠). أثر تطبيق حوكمة تكنولوجيا المعلومات علي بطاقة الأداء المتوازن لتعزيز الريادة والنمو في البنوك المصرية "دراسة ميدانية". ***المجلة العلمية التجارة والتمويل***- جامعة طنطا. (١), يونيو, ٤٣٧- ٥٠٠.
١١. صالح, رضا ابراهيم؛ أبوموسى, أحمد عبدالسلام؛ أبوسعدة, ندا حامد توفيق. (٢٠٢٠). دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية: مع دراسة ميدانية على الشركات المصرية. ***مجلة الدراسات التجارية المعاصرة***, ٦(١٠), ج١, ١٠٥- ١٤٢.
١٢. الطويل, عصام محمد؛ نشوان, إسكندر محمود؛ شحادة, محمد ماهر. (٢٠١٨). دور حوكمة تكنولوجيا المعلومات في تحسين جودة المعلومات المحاسبية المنشورة في التقارير المالية دراسة ميدانية على الشركات الخدمية الفلسطينية. ***مجلة جامعة الأزهر***, سلسلة العلوم الإنسانية, ٢٠(عدد خاص), ديسمبر.
١٣. عبيدني, عصام. (٢٠١٨). حوكمة تكنولوجيا المعلومات كأداة للنهوض بالمؤسسات العمومية الاقتصادية. ***الملتقى العلمي الدولى الأول حول: تفعيل الدور التنموي للقطاع العام كآلية للنهوض بالاقتصاد خارج قطاع المحروقات, يومي***٢٧- ٢٨ نوفمبر.

١٤. غنيمي, سامي محمد أحمد. (٢٠١٦). دور حوكمة تكنولوجيا المعلومات فى تحسين جودة الأداء المالى وزيادة القدرة التنافسية بالبنوك المصرية: دراسة ميدانية. ***مجلة البحوث المحاسبية,*** جامعة طنطا- كلية التجارة. ع١, يونيو, ١٦١- ٢٠٢.
١٥. غنيمي, سامي محمد أحمد. (٢٠١٧). نحو معيار محاسبي لحوكمة تكنولوجيا المعلومات في ضوء تطور تكنولوجيا الإتصالات وتبادل المعلومات: دراسة ميدانية. ***مجلة الفكر المحاسبي,*** ٢١(٥), ٤٢٠-٤٩٠.
١٦. كريم, حمزة محمد محمود (٢٠١٩). "أهمية حوكمة تكنولوجيا المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية بالقطاع المصرفي: دراسة تطبيقية علي المصارف الليبية"، ***المجلة العلمية للدراسات التجارية والبيئية،*** جامعة قناة السويس– كلية التجارة بالاسماعيلية، ١٠(١), الجزء الثاني، ص ١-٣٥.
١٧. مراد، ممدوح هاشم محمد. (٢٠١٦). تأثير حوكمة تكنولوجيا المعلومات على الأداء المالي والقدرة التنافسية في الشركات المساهمة المصرية: دراسة إمبريقية. ***مجلة البحوث التجارية,*** جامعة الزقازيق- كلية التجارة, ٣٨(٢), يوليه, ٢٦٩- ٣٠٢.
١٨. وهدان, محمد علي؛ سعادة, طارق إبراهيم؛ كشك, إيمان حسن. (٢٠٢١). أثر حوكمة تكنولوجيا المعلومات فى فعالية الرقابة الداخلية دراسة ميدانية. ***المجلة العلمية للبحوث التجارية,*** إبريل, ع(٢), ١١٣- ١٤٢.
١٩. وهدان, محمد علي؛ مصطفى, محمود عبدالوهاب؛ شراره, سمير علي زكي. (٢٠٢١). أثر حوكمة تكنولوجيا المعلومات على جودة التقارير المالية بقطاع الجمارك المصرية في ضوء المعايير المهنية الدولية- دراسة ميدانية. ***المجلة العلمية للبحوث التجارية***, ٤٢(٣), ٢٤٢- ٢٠٧.

الرسائل العلمية

١- أبوالهيجاء، أحمد عدنان. (٢٠١٧). "أثر موثوقية نظم المعلومات المحاسبية في ظل تطبيق حوكمة تكنولوجيا المعلومات على ربحية البنوك الأردنية المدرجة في بورصة عمان". ***رسالة دكتوراه,*** كلية الدراسات العليا, جامعة العلوم الإسلامية العالمية.
٢- الجزولي, رفقة الأمين حمدالنيل. (٢٠١٧). "دور حوكمة تكنولوجيا المعلومات في زيادة جودة التقارير المالية (دراسة ميدانية علي مصرف الإدخار والتنمية)". ***رسالة ماجستير,*** كلية التجارة.
٣- الرشيدي, محمد بشير رجا. (٢٠١٥). "دور إدارة مخاطر نظم المعلومات المحاسبية المحوسبة على جودة التقارير المالية في البنوك التجارية الكويتية". ***رسالة ماجستير,*** كلية الاقتصاد والعلوم الإدارية, جامعة آل البيت.
٤- سليمان، حنان زكريا محمد. (٢٠١٩). "أثر حوكمة تكنولوجيا المعلومات علي جودة التقارير المالية". ***رسالة ماجستير,*** كلية التجارة, جامعة بنها.

ثانياً: المراجع الأجنبية

1. Aasi, P. (2018). Information Technology Governance: *The Role of Organizational Culture and Structure.* Stockholm University.
2. Asanza, W. B. R., Roman, R. F. M., Cueva, E. L. L., Calva, J. J. C., & Sarmiento, R. (2017).Administration of Sustainable Environmental Information Technologies based on COBIT5 ESGE21. *International Journal of Applied Environmental Sciences*, Volume12, Number1, pp99-131.
3. Al Abbadi, Abeer Fouzan. (2020). "The Effect of the Information Technology Governance on the Profitability of the Jordanian Banks (2015-2017)" .*Al-mithqal Journal of Economic and Management Sciences*, 6(2), 119– 155.

4. Abu Sina, M., Chowdhury, S., Sakib, T., Akter, S., Arafat, Y. (2021). The Role of Information Technology In Improvement Of Quality Of The Financial Reports Prepared By The Commercial Banks In Bangladesh. *Indian Journal of Finance and Banking*, 5(2), 85- 97.
5. Abdollahbeigi, B., Salehi, F. (2020**)**. The critical factors of IT governance and its impact on organizational performance in Malaysian manufacturing industry. *Serbian Journal of Management*, 15 (1) 81 - 99.
6. Awwad, B., El Khoury, R. (2021). Information technology governance and bank performance: evidence from Palestine. *Journal of Decision Systems*, 1-26.
7. Bianchi, I., Sousa, R., Pereira, R., Souza, I. (2020). Effective IT governance Mechanisms in Higher Education Institutions: An empirical study. *Revista Ibérica de Sistemas e Tecnologias de Informação Iberian Journal of Information Systems and Technologies*, 412- 423.
8. Julianti, R., Gaol, F., Ranti, B., Supangkat, S., (2021). IT Governance Framework for Academic Information System at Higher Education Institutions: A Systematic Literature Review. *International Conference on ICT for Smart Society (ICISS)*.
9. Lunardi, G., Macada, A., Becker, J., Grembergen, W. (2017). Antecedents of IT Governance Effectiveness: An Empirical Examination in Brazilian Firms. *Journal of Information Systems American Accounting Association*, 31(1), 41- 57.
10. Muda, I, and Landau, S. (2019). The Implementation Theory of Conservative Accrual Accounting to the Quality of Accounting Information Systems. *Journal of Southwest Jiaotong University*, 54 (1).
11. Safari, M., Giang, T. (2018). "The theory and Practice of IT Governance Maturity and Strategies Alignment: Evidence from Banking Industry". *Journal of global Information Management*, 26, (2), 127-130.
12. Shuaibu, H., (2019).MIT Governance Implementation in Enterprise: A Review. *International Journal of Electrical and Computer Engineering·* August, 3129- 3134.
13. Su, R., Yang, Z., &Dutta, A. "Accounting Information Comparability and Debt Capital Cost Empirical Evidence from Chinese Listed Companies", ***Asian Economic and Financial Review,*** (8) (1), 2018, 90-102
14. Zammani, M and Razali, R, (2016), "An Empirical Study of Information Security Management Success Factors". *International Journal on Advanced Science Engineering information Technology*, 6 (6).

استبيان

تحية طيبة وبعد...

يقوم الباحث بإجراء دراسة بعنوان: **"دور حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي"**، راجيًا التكرم بالإجابة عن فقرات المقياس ووضع إشارة (/) أمام العبارة التي تتفق مع وجهة نظركم.

وستكون الإجابة وفقًا لمقياس ليكرت الخماسي المبين

العبارة	درجة التوافر درجة الموافقة				
	أوافق بشدة	أوافق	محايد	لاأوافق	لا أوافق بشدة

يأمل الباحث الإجابة بدقة والتعبير عن رأيكم علمًا بأن هذه المعلومات لن تستخدم إلا لأغراض البحث العلمي. وتفضلوا بقبول خالص الشكر والتقدير على تعاونكم الهادف والمثمر.

الباحث

القسم الأول: البيانات الأساسية:

١-الإدارة التابع لها

- الإدارة المالية ☐
- خبراء تكنولوجيا المعلومات ☐
- مسئولى إدارة المخاطر السيبرانية ☐

٢- المؤهل العلمي:

- بكالوريوس ☐
- ماجستير ☐
- دكتوراه ☐

٣-عدد سنوات الخبرة الوظيفية:

- أكبر من ٥ سنوات وأقل من ١٠ سنة ☐
- أكبر من ١٠ سنوات وأقل من ١٥ سنة ☐
- أكبر من ١٠ سنوات وأقل من ٢٠ سنة ☐

القسم الثاني: فقرات الاستبيان

المرجو قراءة كل عبارة بعناية ووضع علامة (√) أمام كل عبارة، وتحت الاستجابة التي تعبر عن رأيكم، علمًا بأنه لا توجد عبارة سليمة وأخرى خاطئة.

المحور الأول: معوقات ومحددات تطبيق حوكمة المعلومات

م	العبارة	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
١	خطة تكنولوجيا المعلومات في القطاع المصرفي ثابتة لا تتغير.					
٢	تنظيم وهيكلية تكنولوجيا المعلومات لا يتم وفق خطة القطاع المصرفي المتطورة.					
٣	لا يوجد تقييم مستمر ومتتالي لإستراتيجية القطاع المصرفي المُتعلقة بأساليب تكنولوجيا المعلومات.					
٤	لا تدرج إدارة استثمارات تكنولوجيا المعلومات وتطويرها وإقرارها ضمن موازنة تكنولوجيا المعلومات للقطاع المصرفي.					
٥	السماح لغير المصرح لهم بالدخول إلى برامج القطاع المصرفي المختلفة.					
٦	تأكيد المصارف على أن مخاطر تكنولوجيا المعلومات يتم إدارتها بكفاءة.					
٧	لا توجد دورات مستمرة للعاملين بالقطاع المصرفي على تكنولوجيا المعلومات.					
٨	افتقار عدد من أعضاء مجلس إدارة القطاع للخبرة في مجال تكنولوجيا المعلومات.					
٩	لا توجد لجنة لتكنولوجيا المعلومات تابعة لمجلس إدراة القطاع المصرفي.					
١٠	ضعف السياسات الداخلية في القطاع المصرفي بشأن تفعيل آليات تكنولوجيا المعلومات.					

المحور الثاني: طبيعة ومحددات المخاطر السيبرانية في القطاع المصرفي

م	العبارة	اوافق بشدة	اوافق	محايد	لا اوافق	لا اوافق بشدة
١	يقوم القطاع المصرفي بالتأكد من صحة المعاملات والمسؤولية من خلال العمليات الإلكترونية.					
٢	يقوم القطاع المصرفي بضبط معايير الأنشطة المصرفية الإلكترونية .					
٣	يقوم القطاع المصرفي بتحسين الخدمات المصرفية الإلكترونية لإرضاء العملاء.					
٤	يقوم القطاع المصرفي بالتأكيد على أن مخاطر تكنولوجيا المعلومات يتم إدارتها بكفاءة.					
٥	يقوم القطاع المصرفي بإرشاد وتوجيه العملاء للمخاطر السيبرانية.					

٦	تقوم المصارف بالتعريف بالاطر القانونية والتشريعية من خلال المعاملات الإلكترونية.					
٧	يقوم القطاع المصرفي بالتوسع في تقديم الخدمات والمنتجات المصرفية لمعرفة السوق والتحقق من صحة الضمانات.					
٨	يقوم القطاع المصرفي بتأمين المعلومات والحفاظ على خصوصية البيانات.					
٩	تقوم المصارف بتعزيز حماية المؤسسة من الهجمات الإلكترونية بكافة أشكالها.					

المحور الثالث: مساهمة حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي

م	العبارة	اوافق بشدة	اوافق	محايد	لا اوافق	لا اوافق بشدة
١	توفر حوكمة تكنولوجيا المعلومات تقييماً للمخاطر السيبرانية بصورة دورية.					
٢	تعمل حوكمة تكنولوجيا المعلومات على الحد من مخاطر تكنولوجيا المعلومات وعدم تكرارها.					
٣	تحسن حوكمة التكنولوجيا أداء المخاطر بالمصرف في ظل بيئة تكنولوجيا المعلومات.					
٤	تقدم حوكمة التكنولوجيا الدعم الفعال والمشاركة في عمليات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات.					
٥	تقدم حوكمة التكنولوجيا الاستشارات اللازمة عند تصميم وتحسين إستراتيجيات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات.					
٦	تعمل حوكمة التكنولوجيا على وضع مستويات مقبولة وغير مقبولة للمخاطر السيبرانية في ضوء حوكمة تكنولوجيا المعلومات.					
٧	توفر حوكمة التكنولوجيا تدريب العاملين في تكنولوجيا المعلومات على التصدي للمخاطر السيبرانية.					
٨	توفر حوكمة التكنولوجيا تحديث وتطوير نظم الحماية من المخاطر السيبرانية بشكل دوري.					
٩	توفر حوكمة التكنولوجيا الاعتماد على مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات.					
١٠	توفر حوكمة التكنولوجيا إجراء اختبارات موازية للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية ضد مخاطر الهجمات السيبرانية.					
١١	تحقق حوكمة التكنولوجيا وجود قسم مخصص لإدارة أمن الشبكات ضد المخاطر السيبرانية.					
١٢	توفر حوكمة التكنولوجيا المراجعة الدورية لأنظمة الحماية ومعالجة البيانات.					