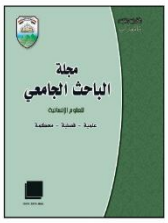
جامعة إب
مجلة الباحث الجامعي
ISSN: 2079-5068 ISSN (online): 2663-3930



حوكمة مخاطر تكنولوجيا المعلومات وتأثيرها على موثوقية النظم المحاسبية الإلكترونية (دراسة ميدانية في البنوك اليمنية)

حمدان حميد قايد عبد الإله*، محمد حمود احمد السمحي
قسم المحاسبة، كلية العلوم الإدارية، جامعة إب، اليمن
***Email: elhamdan82@gmail.com**

الكلمات المفتاحية:
حوكمة مخاطر تكنولوجيا المعلومات، النظم المحاسبية، موثوقية النظم، البنوك اليمنية،

الملخص

هدفت الدراسة إلى معرفة تأثير حوكمة مخاطر تكنولوجيا المعلومات على موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية. اعتمدت الدراسة على المنهج الوصفي التحليلي لملاءمته لطبيعتها؛ حيث استندت إلى خلفية نظرية إضافة إلى الاستفادة منها في تصميم استبانة أعدّت لجمع البيانات الأولية. وتم إجراء الدراسة الميدانية على موظفي البنوك اليمنية التي مثلت مجتمع الدراسة، حيث تم توزيع الاستبانة على عينة قصدية من شاغلي الوظائف المالية في البنوك اليمنية. وقد بلغ عدد الاستمارات الموزعة (114) استمارة، استجاب منها (107) موظفاً. وبعد مراجعة الاستجابات، تم استبعاد (7) استمارات لعدم صلاحيتها للتحليل الإحصائي، ليصبح عدد الاستمارات الصالحة للتحليل (100) استمارة.

أظهرت نتائج تحليل الدراسة أن تطبيق حوكمة مخاطر تكنولوجيا المعلومات يسهم بشكل فعّال في تعزيز موثوقية النظم المحاسبية الإلكترونية، من خلال تحسين دقة البيانات المحاسبية وضمان سلامة التقارير المالية. كما أظهرت النتائج وجود علاقة إيجابية حوكمة المخاطر والممارسات المحاسبية السليمة في بيئة الأنظمة الإلكترونية.

أوصت الدراسة بتعزيز إجراءات الحوكمة والرقابة على النظم المحاسبية الإلكترونية، من خلال تطوير السياسات الأمنية، وتحسين نظم الحماية والضبط الداخلي، بما يضمن الحفاظ على سرية البيانات وسلامتها، ويعزز ثقة مستخدمي التقارير المالية.

حوكمة مخاطر تكنولوجيا المعلومات وتأثيرها على موثوقية النظم المحاسبية الإلكترونية (دراسة ميدانية في البنوك اليمنية)

Information Technology Risk Governance and Its Impact on the Reliability of Electronic Accounting Information Systems: A Field Study on Yemeni Banks

Hamdan Hamid Qaid Abdulelah*, Mohammed Hamoud Ahmed Alsamhi
Department of Accounting, Faculty of Administrative Sciences, Ibb University, Yemen
*** Emai: elhamdan82@gmail.com.**

Keywords:

Information Technology Risk Governance, Accounting Systems, Reliability, Yemeni Banks,

Abstract

The study aimed to examine the impact of information technology risk governance on the reliability of electronic accounting systems in Yemeni banks. To achieve the study objective, the descriptive-analytical approach was adopted, drawing upon a theoretical framework that informed the design of a questionnaire used for primary data collection. The field study targeted employees of Yemeni banks, with the questionnaire distributed to a purposive sample of employees occupying financial positions within these institutions. A total of (114) questionnaires were distributed, of which (107) were returned; after excluding (7) invalid responses, the final sample consisted of (100) valid questionnaires suitable for statistical analysis. The findings revealed that the implementation of information technology risk governance contributes significantly to enhancing the reliability of electronic accounting systems by improving the accuracy of accounting data and ensuring the integrity of financial reports. The results further demonstrated a positive relationship between risk governance practices and sound accounting practices within electronic systems environments. In light of these findings, the study recommended strengthening governance and control procedures related to electronic accounting systems through the development of security policies and the enhancement of protection and internal control systems to ensure data confidentiality and integrity and to reinforce users' confidence in financial reporting.

1- المقدمة:

تشهد بيئة الأعمال المعاصرة تطوراتٍ متسارعةً وتحولاتٍ نوعيةً في ظل التقدم التكنولوجي المتلاحق، وما يصاحبه من توسّعٍ غير مسبوقٍ في استخدام تطبيقات تكنولوجيا المعلومات على مستوى الأنشطة المحاسبية والمالية. وقد أسهم هذا التحول في انتقال المؤسسات من الاعتماد على النظم التقليدية إلى تبنّي نظم إلكترونية متقدمة تعتمد على تقنيات ذكية تُوفّر معلومات عالية الجودة، مما يُعزز فاعلية اتخاذ القرارات ويدعم بناء الميزة التنافسية.

وفي هذا السياق، تبرز نظم المعلومات المحاسبية الإلكترونية كأحد مقومات البنية التحتية الرقمية، إذ تمثل أداةً فعالةً لمعالجة البيانات المالية وتوفير معلومات موثوقة تدعم عملية اتخاذ القرار. ومع ذلك، فإن هذه النظم، على الرغم من مزاياها، تظل عرضةً لمخاطر تقنية وأمنية متنامية تهدد سلامة البيانات وموثوقية النتائج المحاسبية، الأمر الذي يستدعي وجود إطار حوكمي متكامل يضمن الاستخدام الرشيد للتقنية، ويحقق التوازن بين الكفاءة التشغيلية والرقابة الفاعلة (حسن، علي 2021، ص 82).

أما في السياق اليمني، فتتجلّى هذه التحديات بوضوح في ظل الظروف الاستثنائية التي تمر بها بيئة الأعمال على المستويين الاقتصادي والتشغيلي، والتي ألقت بظلالها على أداء القطاع المصرفي، بوصفه أحد أكثر القطاعات تأثرًا بالتغيرات التقنية المتسارعة. ويُواجه هذا القطاع تحديات متزايدة تشمل ضعف البنية التحتية، وارتفاع التهديدات الأمنية، وتفاوت جاهزية المؤسسات المصرفية. ومن ثم، فإن تطبيق حوكمة تكنولوجيا المعلومات يُعد خيارًا استراتيجيًا لا غنى عنه للبنوك والمؤسسات المالية.

استنادًا إلى ما سبق، تُعد حوكمة مخاطر تكنولوجيا المعلومات إطارًا مرجعيًا ضروريًا لتحقيق الاستخدام الرشيد للتقنية، بما ينسجم مع الأهداف المؤسسية ويُقلل من المخاطر المرتبطة بها.

انطلاقًا من ذلك، وبالنظر إلى محدودية الدراسات المحلية، خصوصًا في بيئة مصرفية تتسم بتحديات مركبة مثل اليمن، تبرز الحاجة الملحة إلى دراسة حوكمة مخاطر تكنولوجيا المعلومات وتأثيرها على موثوقية نظم المعلومات المحاسبية الإلكترونية في البنوك اليمنية.

2- مشكلة الدراسة:

تواجه البنوك اليمنية تحدياً متزايداً يتمثل في ضمان موثوقية نظم المعلومات المحاسبية الإلكترونية، والتي باتت تشكل عنصراً محورياً في دعم الأنشطة والوظائف واتخاذ القرارات. ففي عام 2018م، وصل ترتيب اليمن عالمياً في مجال الأمن السيبراني إلى (172) من أصل (175) ورقمها القياسي (0.019) (International Telecommunication Union (ITU),2019,68) وقد أعطت أكاديمية الحوكمة الإلكترونية e-Governance Academy (eGA) اليمن درجة متدنية في مجال الأمن الإلكتروني، حيث كان

ترتيبها (148) من أصل (161)، وكان مؤشر الأمن السيبراني (7.79) (NCSI 2020)، وبالتالي يتضح أن هناك قصوراً كبيراً في الجوانب التشريعية والتنظيمية المتعلقة بأمن المعلومات في اليمن، وهذا ما أكدته أكاديمية الحوكمة الإلكترونية (EGA) (السريحي وآخرون، 2025، ص، 3).

أصبحت النظم المحاسبية الإلكترونية عرضة لمخاطر وتهديدات متعددة، بدءاً بمخاطر الاختراقات الأمنية، والتحريفات المتعمدة أو غير المقصودة، ومروراً بالأخطاء وتعقيد بيئة التشغيل، ووصولاً إلى أوجه القصور في ضوابط الرقابة الداخلية، وانتهاكات الخصوصية؛ وهذه المخاطر تُضعف أمن وسلامة المعالجة المحاسبية، وتُهدد انتظام أداء النظام، مما يعرض موثوقية النظم للتشويه أو الفقدان، ويقلل من ثقة المستخدمين ومتخذي القرار في نتائجها، وبالتالي ينعكس سلباً على فعالية العمل المصرفي واستقراره.

في ظل هذه التحديات، تبرز حوكمة مخاطر تكنولوجيا المعلومات، كإطار استراتيجي متكامل السياسات والإجراءات والضوابط التي تُعنى بتحقيق الاستخدام الأمثل للتقنية وتخفيف المخاطر المرتبطة بها.

3- تساؤلات الدراسة:

تتمثل تساؤلات الدراسة الآتي:

1. ما دور حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية؟
2. ما مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية؟
3. ما تأثير حوكمة مخاطر تكنولوجيا المعلومات في موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية؟

4- أهمية الدراسة:

تتمثل أهمية الدراسة بالآتي:

4- 1- الأهمية العلمية: تبرز في الآتي:

- أنها تسلط الضوء على تأثير حوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية نظم المعلومات المحاسبية الإلكترونية.
- الحاجة الماسة لنتائج مثل هذه الدراسات في تطوير نظم معلومات محاسبية فاعلة تمكن إدارة البنوك من اتخاذ القرارات وأداء الأنشطة.
- أنها تسهم في رفع مستوى الوعي في البنوك اليمنية والأطراف ذات العلاقة, وتعزز الاتجاه نحو تطبيق حوكمة مخاطر تكنولوجيا المعلومات لما لها من دور في تحقيق موثوقية النظم المحاسبية. الإلكترونية.

4- 2- الأهمية العملية: تنبع من الآتي:

- من أهمية موضوع حوكمة مخاطر تكنولوجيا المعلومات, موثوقية النظم المحاسبية الإلكترونية في قطاع البنوك اليمنية، لما لها دور في ادارة ورقابة نشاط البنوك وانعكاس ذلك على النهوض بالاقتصاد الوطني.
- مما ستقدمه من نتائج وتوصيات تخدم البنوك اليمنية؛ إذ يمكن الاستفادة منه في بلورة أسس سليمة تساعدها في تطوير نظمها وتحقيق أهدافها.

- مما تسهم به في خفض المخاطر وتعزيز موثوقية النظم المحاسبية الإلكترونية.
- أنها قد تُسهِم في رفع أداء العمليات المصرفية, وزيادة الثقة لدى أصحاب المصالح والأطراف الأخرى بالمعلومات.

5- أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف الآتية:

1. تقيم تأثير حكومة مخاطر تكنولوجيا المعلومات في البنوك اليمنية.
2. تقييم مستوى موثوقية نظم المعلومات المحاسبية الإلكترونية واقتراح آليات لتحسينها وفقاً لممارسات الحوكمة الفعالة.
3. تحليل تأثير حوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية نظم المعلومات المحاسبية الإلكترونية في البنوك اليمنية.

6- منهجية الدراسة:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، لملاءمته لطبيعتها بشقيها النظري والميداني؛ حيث تم استخدام البيانات الثانوية المستمدة من الدراسات السابقة ذات الصلة في بناء الإطار النظري، والاستفادة منه في إعداد استمارة الاستبانة لجمع البيانات الأولية للدراسة الميدانية التي أُجريت في البنوك اليمنية.

7- فرضيات الدراسة:

تتمثل فرضيات الدراسة بالآتي:

1. "لا توجد فروق دالة إحصائية عند مستوى دلالة أقل من أو يساوي (0.05) حول حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية".
2. "لا توجد فروق دالة إحصائية عند مستوى دلالة أقل من أو يساوي (0.05) حول موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية".
3. "لا توجد فروق دالة إحصائية عند مستوى دلالة أقل من أو يساوي (0.05) حول تأثير حوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية".

8- حدود الدراسة:

- **الحدود الموضوعية:** اقتصرت الدراسة على تناول تأثير حوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية نظم المعلومات المحاسبية الإلكترونية في البنوك اليمنية.
- **الحدود الزمانية والمكانية:** أجريت الدراسة الميدانية في البنوك اليمنية خلال العام 2025م.

9- الدراسات السابقة:

اولاً: الدراسات العربية:

1. دراسة شادي (2021) بعنوان: دور حوكمة تكنولوجيا المعلومات في تعزيز أمن المعلومات.

هدفت هذه الدراسة إلى تحديد تأثير أبعاد حوكمة تكنولوجيا المعلومات ممثلة بـ (التخطيط والتنظيم، الاكتساب والتنفيذ، الدعم والتوصيل، المتابعة والتقييم) في تعزيز أمن المعلومات في المصارف المدرجة في سوق دمشق للأوراق المالية، تم الاعتماد على المنهج الوصفي التحليلي، وقد ضم مجتمع الدراسة العاملين في المصارف الخاصة السورية المدرجة في سوق

دمشق للأوراق المالية البالغ عددها أربعة عشر مصرفاً، وقد تم توزيع 100 استبانة على العاملين في القسم المالي في المصارف عينة الدراسة, وتم استرداد 85 استبانة صالحة للتحليل.

توصلت الدراسة إلى وجود تأثير ذي دلالة معنوية لأبعاد حوكمة تكنولوجيا المعلومات في تعزيز أمن المعلومات في المصارف المدرجة في سوق دمشق للأوراق المالية.

2. دراسة خليفة، زين؛ وضيف الله (2021). بعنوان: أثر حوكمة تكنولوجيا المعلومات على الحد من مخاطر نظام المعلومات المحاسبي.

هدفت هذه الدراسة إلى تسليط الضوء على المخاطر التي تواجه نظام المعلومات المحاسبي، وأثر تطبيق حوكمة تكنولوجيا المعلومات في الحد من تلك المخاطر. وتكون مجتمع الدراسة من فئة مستعملي نظام المعلومات المحاسبي في مكاتب المحاسبة والشركات على المستوى الوطني، أما العينة فقد بلغ عددها 100 فرد، تم توزيع قائمة الاستقصاء عليهم بوصفها من أهم الأدوات البحثية الناجعة للتحليل، فكانت عدد الاستمارات الصالحة للتحليل 82 استمارة. وخلصت الدراسة إلى جملة من النتائج أهمها: أن تفعيل آليات حوكمة تكنولوجيا المعلومات بشكل متكامل سيؤدي حتماً إلى التقليل من المخاطر التي تواجه نظام المعلومات المحاسبي، وهو ما يؤدي إلى تحسين جودة المعلومات المحاسبية.

3. دراسة غالي وحسين ومحمد (2024) بعنوان: تأثير حوكمة تكنولوجيا المعلومات في تقليل مخاطر نظم المعلومات المحاسبية السحابية.

هدفت الدراسة إلى التعرف على تأثير حوكمة تكنولوجيا المعلومات في تقليل مخاطر نظم المعلومات المحاسبية السحابية. تم إجراء الدراسة من خلال استمارة استبانة؛ إذ تم توزيع (110) استبانة على عينة من المصارف، وتم جمع (100) منها، ووجد أن (92) منها كانت صالحة للتحليل.

وتوصلت الدراسة إلى مجموعة من النتائج أهمها: توجد علاقة ارتباط وتأثير بين حوكمة تكنولوجيا المعلومات ونظم المعلومات المحاسبية السحابية.

4. دراسة التكريتي والزواري (2024). بعنوان: دور حوكمة تكنولوجيا المعلومات في تعزيز أداء نظم المعلومات المحاسبية.

هدفت الدراسة إلى قياس أثر حوكمة تكنولوجيا المعلومات على نظم المعلومات المحاسبية للمصارف التجارية العراقية. واعتمدت الدراسة على أداة الاستبانة كأداة أساسية لجمع البيانات، تم توزيعها على عينة عشوائية من العاملين بالإدارة العليا والوسطي والتنفيذية في مصارف تجارية عراقية، وعليه تم التوصل إلى عينة نهائية تبلغ (335) استبانة صالحة. وقد توصلت الدراسة إلى وجود مستوي مرتفع نسبياً لحوكمة تكنولوجيا المعلومات، ونظم المعلومات المحاسبية بهذه المصارف وذلك من وجهة نظر المستقصين وإلى وجود أثر إيجابي لحوكمة

تكنولوجيا المعلومات في تعزيز نظم المعلومات المحاسبية على المستوى الكلي. أما على المستوى الفرعي اتضح أن التأثير يأتي من بعدي الامتلاك، والتنفيذ والمتابعة، والتقييم، حيث كان هناك تأثير إيجابي مباشر لبعدي الامتلاك والتنفيذ، المتابعة والتقييم على نظم المعلومات المحاسبية. وفي المقابل، كان لبعد التوصيل والدعم، تأثير مباشر سلبي على نظم المعلومات المحاسبية. في حين لم يكن لبعد التخطيط والتنظيم أي تأثير.

ثانياً الدراسات الأجنبية:

1. دراسة Mahdi (2021). بعنوان: حوكمة تكنولوجيا المعلومات وأمن المعلومات في أنظمة المعلومات المحاسبية: دراسة حالة.

هدفت الدراسة إلى تحديد مستوى حوكمة تكنولوجيا المعلومات المتاحة في المصرف التجاري (بنك عودة – فرع النجف) باستخدام مكونات COBIT السبعة الممثلة في المبادئ والسياسات، والأطر والعمليات، والهيكل التنظيمي، والثقافة والأخلاقيات والسلوكيات، والمعلومات والمهارات والخبرة، والخدمات، والبنية التحتية. تم إجراء الدراسة الميدانية من خلال استطلاع رأي الإداريين والمدراء في بنك عودة – فرع النجف، لتحديد مستوى حوكمة تكنولوجيا المعلومات المتاحة ومقارنتها بنموذج COBIT. أظهرت النتائج أن تطبيق آليات حوكمة تكنولوجيا المعلومات في المصارف التجارية العراقية يمكن أن يقلل من مخاطر التدقيق التي يقيمها المدققون الخارجيون، ويزيد من موثوقية أنظمة المعلومات المحاسبية، ويدعم أمن المعلومات في ضوء أنظمة المحاسبة الإلكترونية. وأخيرًا، فإن تطبيق نموذج لقياس حوكمة تكنولوجيا المعلومات في المصارف التجارية العراقية إطار COBITسيكون مقياسًا قياسيًا لمستوى حوكمة تكنولوجيا المعلومات, ويساعد هذه المصارف على تقليل المخاطر.

2. دراسة .ELshoorbagy & et (2025). بعنوان: العلاقة بين حوكمة تكنولوجيا المعلومات ومخاطر أنظمة المعلومات المحاسبية السحابية.

هدفت الدراسة إلى معرفة مدى المساهمة المحتملة لحوكمة تكنولوجيا المعلومات في التخفيف من المخاطر المرتبطة بأنظمة معلومات المحاسبة السحابية. وتم استخدام التحليل الكمي بناءً على خمسة وتسعين استبيانًا لدراسة كيفية قدرة شركة ITG على الحد من المخاطر المرتبطة بأنظمة معلومات المحاسبة السحابية. حيث أُرسلت الاستبيانات إلى 215 مشاركًا، من بينهم أعضاء هيئة التدريس في الجامعات المصرية، ومحاسبون، ومهندسو تنفيذ السحابة، ومديرو مخاطر تكنولوجيا المعلومات. وتم تحليل 95 استبيانًا صحيحًا وقابلًا للاستخدام. وأشارت النتائج إلى أن المخاطر التي تواجه بيئة الأعمال المصرية تزداد من خلال تطبيق أنظمة معلومات المحاسبة السحابية. علاوة على ذلك، أظهرت النتائج أن تطبيق تقنية المعلومات (ITG) يُقلل من المخاطر المحتملة المرتبطة بأنظمة معلومات الذكاء الاصطناعي السحابية في مصر.

ما يميز الدراسة الحالية عن الدراسات السابقة:

تُعد الدراسة الحالية امتداد للدراسات السابقة إلا أنها تختلف عنها في أبعاد قياس المتغيرات فضلاً عن بيئة التطبيق, وتناولت هذه المواضيع من زوايا مُتعددة، ومن أدوار مختلفة, ويمكن إيضاح ذلك بالآتي:

1. التركيز على البيئة المحلية وتطبيق النموذج في سياق البنوك اليمنية.

تُعنى الدراسة بتطبيق نموذج حوكمة مخاطر تكنولوجيا المعلومات في البنوك في اليمن، وهو سياق خاص لم يتم تسليط الضوء عليه بشكل كافٍ في الدراسات السابقة؛ حيث تناولت بعض الدراسات الإطار النظري أو تم تطبيقه على بيئات مصرفية في دول أخرى مثل (Mahdi، 2021؛ غالي، 2024).

2. منهجية بحثية تجمع بين التحليل الكمي والمراجعة الأدبية:

ترتكز هذه الدراسة على أسلوب وصفي تحليلي باستخدام بيانات ميدانية (عن طريق استبانة) تستهدف أصحاب الوظائف المالية في البنوك اليمنية، وهو نهج يوفر بعدًا عمليًا لتقييم مستوى التطبيق الفعلي لحوكمة مخاطر تكنولوجيا المعلومات. كما تم تصميم الاستبانة بناءً على مراجعة شاملة للأدبيات والدراسات السابقة مثل دراسات شادي (2021) ودراسة ELshoorbagy (2025) والتجارب المعمول بها في إطار (COBIT)و(ISO/IEC 38500) مما يضمن انطلاق الدراسة من قاعدة نظرية راسخة تُضيف إليها البيانات الميدانية قيمة تطبيقية. هذا الجمع بين المراجعة الأدبية المتعمقة والتحليل الكمي يجعل الدراسة قابلة للمقارنة مع أبحاث سابقة.

3. **تحديد مستوى موثوقية نظم المعلومات المحاسبية الإلكترونية:**

التي تعتمدها البنوك محل الدراسة من خلال الأبعاد الخمسة؛ لتأكيد الثقة المتمثلة في (الأمن، السرية، الخصوصية، سلامة العمليات، الجاهزية).

10- الإطار النظري للدراسة:

10 – 1- مخاطر تكنولوجيا المعلومات

تعد مخاطر تكنولوجيا المعلومات من التحديات البارزة التي تواجه المؤسسات الحديثة في عصر التحول الرقمي. وتشمل هذه المخاطر تهديدات متعددة مثل الاختراقات الأمنية، وفقدان البيانات، وتعطل الأنظمة. ومن الضروري أن تعتمد المؤسسات استراتيجيات فعّالة لإدارة هذه المخاطر لضمان استمرارية الأعمال وحمايتها من الآثار السلبية المترتبة عليها (Aven, 2016,p. 32).

10 – 2- مفهوم تكنولوجيا المعلومات:

تُعرّف بأنها استخدام الأجهزة الحاسوبية، البرمجيات، وشبكات الاتصال في معالجة البيانات وتحويلها إلى معلومات مفيدة لصناع القرار (Laudon & Laudon, 2020, p. 35). ويشمل ذلك تطبيقات إدارة البيانات، النظم الإلكترونية، وتقنيات الأمن السيبراني التي تهدف إلى تعزيز الكفاءة التشغيلية للمؤسسات.

ووفقًا لـ Turban، فإن تكنولوجيا المعلومات تمثل البنية التحتية الأساسية التي تعتمد عليها المؤسسات في عملياتها المحاسبية، إذ تساعد في تسريع العمليات، وتحقيق التكامل بين الوظائف المختلفة(Turban et al. 2018, p. 122) .

كما تعرف تكنولوجيا المعلومات بأنها مجموعة الأدوات والأنظمة الحاسوبية المستخدمة في معالجة البيانات، تخزينها، وتحليلها لدعم اتخاذ القرار (عبد الحميد، 2019، 22).

10 – 3 – أنواع مخاطر تكنولوجيا المعلومات:

رغم الأهمية الكبيرة لتكنولوجيا المعلومات، إلا أنها تنطوي على العديد من المخاطر. وتتمثل هذه المخاطر بالآتي:

1. الاختراقات الأمنية: تعد الجرائم الإلكترونية من أكبر المخاطر التي تواجه تكنولوجيا المعلومات، إذ يمكن للقراصنة اختراق البيانات، وسرقتها، أو تغييرها (Kshetri, 2017, p. 105).
2. الأخطاء البرمجية: قد تؤدي أخطاء البرمجيات في تكنولوجيا المعلومات إلى فقدان البيانات أو حدوث تلاعب (Hall, 2018, p. 142).
3. انقطاع الخدمة: قد تتعرض تكنولوجيا المعلومات لعطل مفاجئ نتيجة لأخطاء فنية أو هجمات إلكترونية، وهو ما يعيق الوصول إلى البيانات المهمة (مسعود، 2020، 119).
4. مخاطر الامتثال التنظيمي: عدم توافق تكنولوجيا المعلومات مع القوانين، والمعايير الدولية، قد يؤدي إلى تعرض المؤسسات لعقوبات قانونية (الربيعي، 2021، 49). والجدول رقم (1) الآتي يوضح أنواع مخاطر تكنولوجيا المعلومات.

جدول(1): أنواع مخاطر تكنولوجيا المعلومات

م	النوع	البيان
1	المخاطر الأمنية	تشمل الهجمات السيبرانية، البرمجيات الضارة، وسرقة الهوية، التي قد تؤدي إلى فقدان أو تلف البيانات (Whitman & Mattord, 2020, p. 76).
2	المخاطر التقنية	تشمل أعطال البرمجيات، الفشل في تكامل الأنظمة، أو التحديثات غير المتوافقة التي قد تؤدي إلى تلف البيانات (عبد الحميد، 2019، ص 58)
3	مخاطر التشغيل	تشمل الأخطاء الناتجة عن الإدخال غير الصحيح للبيانات أو خلل في تشغيل البرمجيات أو فقدان البيانات أثناء النقل أو التخزين (Weber, 2019, p. 55).
5	المخاطر القانونية	المخاطر القانونية والتنظيمية: تتضمن عدم الامتثال للمعايير المحاسبية أو القوانين المحلية، وهو ما قد يعرض الشركات لعقوبات قانونية (Otim et al., 2016, p. 132).

المصدر: الباحثان بتصرف: عن (Otim et al، 2016؛ Weber،2019؛ عبد الحميد، 2019؛ Mattord & Whitman, 2020)

10-4- إدارة مخاطر تكنولوجيا المعلومات: تشير إدارة مخاطر تكنولوجيا المعلومات إلى العملية المنهجية لتحديد، وتحليل، وتقليل المخاطر

المرتبطة باستخدام التكنولوجيا في المؤسسات. وتهدف هذه الإدارة إلى حماية البيانات، تحسين استمرارية الأعمال، وضمان الامتثال للمعايير القانونية والتنظيمية (Aven, 2016, p. 45). حيث تتم إدارة مخاطر تكنولوجيا المعلومات من خلال الآتي:

- **تحديد المخاطر وتحليلها:** تقييم التهديدات التقنية المحتملة وتأثيرها على العمليات المؤسسية (ISACA, 2012, p. 90).
- **تخفيف المخاطر:** تطوير استراتيجيات وإجراءات للحد من التأثير السلبي للمخاطر التقنية (ISO/IEC 31000, 2018, p. 30).
- **تحسين استمرارية الأعمال:** إنشاء خطط للطوارئ والتعافي من الكوارث لضمان عدم تعطل العمليات (NIST, 2014, p. 22).
- **تعزيز الأمن السيبراني:** تطبيق ضوابط أمنية لحماية الأنظمة من الهجمات الإلكترونية (ISO/IEC 27001, 2013, p. 55).

10- 5- آليات الحماية من مخاطر تكنولوجيا المعلومات:

تتطلب مواجهة مخاطر تكنولوجيا المعلومات اتباع مجموعة من الإستراتيجيات الوقائية والتصحيحية لضمان حماية البيانات، واستمرارية الأعمال، وتقليل التأثيرات السلبية على الأنظمة التكنولوجية، تتمثل هذه الآليات بالآتي:

1. تطبيق أنظمة الحماية الإلكترونية.

استخدام أنظمة الحماية الإلكترونية يسهم بشكل كبير في الحد من مخاطر تكنولوجيا المعلومات والاتصال، إذ تُحسن هذه الأنظمة من مستوى الأمان السيبراني، وتحمي البيانات الحساسة من الاختراقات (عبد القادر، 2019، 112).

2. تنفيذ آليات حوكمة تكنولوجيا المعلومات

تطبيق آليات الحوكمة يمكن أن يُعزز من فعالية إدارة المخاطر من خلال الفحص الدوري للمخاطر، وتطوير استراتيجيات استباقية للتعامل مع التهديدات التقنية (حسن، 2021، 87).

3. تعزيز أمن المعلومات والرقابة الداخلية.

تعزيز الرقابة الداخلية عبر تكنولوجيا المعلومات يساعد في تقليل الأخطاء التشغيلية، والاستخدام غير المشروع للبيانات (الجابري، 2020، 134).

4. تطوير سياسات أمن سيبراني شاملة.

وجود سياسات أمن سيبراني متكاملة، تشمل التقييمات الأمنية الدورية والتدريب المستمر للموظفين، يقلل من نقاط الضعف التقنية، ويحسن استجابة المؤسسات للهجمات الإلكترونية (NIST, 2020, p. 55).

5. تقييم مخاطر التكنولوجيا لتحسين أنشطة الرقابة.

تحليل مخاطر التكنولوجيا بشكل دوري لتعزيز أنشطة الرقابة الداخلية، وتحقيق استجابة أسرع للتهديدات السيبرانية (ISO/IEC, 2019, p. 40).

10- 6- حوكمة مخاطر تكنولوجيا المعلومات

تشير حوكمة مخاطر تكنولوجيا المعلومات إلى الإطار الذي يحدد كيفية إدارة المخاطر

المرتبطة بالتكنولوجيا داخل المؤسسات، من خلال وضع سياسات، وإجراءات لضمان الامتثال للمعايير الأمنية، وتقليل التهديدات المحتملة، وتعزيز استدامة العمليات التقنية(عبد القادر، 2019، ص 112).

10-6-1- أهمية حوكمة مخاطر تكنولوجيا المعلومات: تُعد حوكمة المخاطر عاملاً أساسياً في نجاح المؤسسات الرقمية، إذ تسهم في الآتي (NIST, 2020, p. 55):

- **تحسين الأمن السيبراني:** من خلال تنفيذ ضوابط وقائية واستراتيجية لمكافحة الهجمات الإلكترونية.

- **تحقيق الامتثال التنظيمي:** يساعد الالتزام بمعايير مثل ISO 31000 و COBITعلى تقليل المخاطر القانونية والتشغيلية.

- **تعزيز ثقة المستثمرين والعملاء:** إذ يؤدي التحكم الفعّال في المخاطر إلى رفع مستوى الشفافية والمصداقية.

10- 6- 2- مكونات حوكمة مخاطر تكنولوجيا المعلومات: تتألف حوكمة مخاطر تكنولوجيا المعلومات من مجموعة عناصر، أبرزها الآتي (العلي، 2016، 95):

- **التقييم المستمر للمخاطر:** تحليل نقاط الضعف التكنولوجية المحتملة.

- **وضع سياسات وإجراءات الأمن المعلوماتي:** تطبيق سياسات تحكم الوصول إلى البيانات وحمايتها.

- **التكامل مع إستراتيجيات الأعمال:** مواءمة أهداف الحوكمة مع الخطط الاستراتيجية للمؤسسة.

10-6-3- التحديات التي تواجه حوكمة مخاطر تكنولوجيا المعلومات: تشمل أبرز التحديات في الآتي (مسعود، 2020، 82).

- التطور السريع للتهديدات السيبرانية، يتطلب تحديثًا مستمرًا للسياسات الأمنية.

- ضعف الوعي الأمني لدى الموظفين، وهو ما يزيد من احتمالية وقوع الهجمات

- تكاليف تنفيذ أطر الحوكمة، التي قد تكون مرتفعة لبعض المؤسسات.

11- موثوقية النظم المحاسبية الإلكترونية:

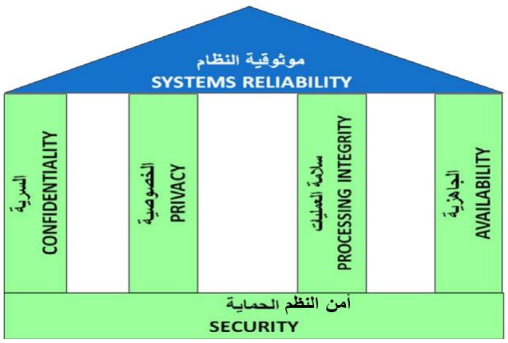
إن توفير المعلومات المفيدة العملية لاتخاذ القرارات إحدى الوظائف الرئيسة لنظام المعلومات المحاسبي، وحتى تكون هذه المعلومات مفيدة فإنه يجب أن تنتجها النظم المحاسبية؛ المتصفة بالأمن، السرية، الخصوصية، سلامة المعالجة، والجهوزية التامة، وهذا ما حدده الإطار الفكري للموثوقية الذي طرح من قبل معهد المحاسبين القانونيين الأمريكي، ومعهد المحاسبين القانونيين الكندي، إذ حددها بخمسة مبادئ رئيسية تسهم في موثوقية الأنظمة وهي:(AICPA/CICA, 2002) .

1. **أمن النظم (الحماية):** تعني التحكم في عملية الوصول للنظام وبياناته.
2. **السرية:** تعني أن المعلومات الحساسة تكون محمية من أن تكون مكشوفة لغير المخولين.

3. **الخصوصية:** تعني أن المعلومات الشخصية عن العملاء تجمع وتستعمل ويفصح عنها وتصان بطريقة مناسبة.

4. **سلامة العمليات:** تعني أن تعالج المعلومات بصورة دقيقة وكاملة وفي الوقت المناسب.

5. **الجاهزية:** تعني أن يكون النظام متاحاً للإيفاء بالمتطلبات التشغيلية والملتزم بها. ويوضح الشكل رقم (1) كيف ترتبط أبعاد موثوقية النظم مع بعضها.



Source: (Romney & Steinbart, 2015, p. 256)

ويمكن **تعريف الموثوقية:** بأنها عبارة عن خدمات مهنية مستقلة تهدف إلى التحقق من المعلومات ومحتواها لأغراض اتخاذ القرار (مشتهي وآخرون، 2011، 24). وعرفت أيضا بأنها أداة مهنية تستخدم بغرض زيادة ثقة المستخدمين (الإدارة، العملاء، الموردين، الملاك، الهيئات الحكومية الجهات الأخرى المعنية في نظام المعلومات الإلكتروني)؛ أي: هي شهادة توكيد يتم منحها للعميل من قبل مكاتب الاستشارات تشهد بتوكيدية وتكامل عمليات النظام وموثوقيتها، وكذلك تماشيه مع مبادئ ومعايير موثوقية النظام. (النسور و الحياري، 2018).

11-1- الأمن:

يقصد بأمن المعلومات: مجموعة الإجراءات والسياسات والبرامج وكذا التجهيزات المادية التي تحقق الحماية لنظام المعلومات المحاسبي من التهديدات المختلفة التي قد يتعرض لها (حجر، 2024، 387). أما العازمي فيرى أن أمن المعلومات المحاسبية الإلكترونية يشير إلى توافر السرية والموثوقية للمعلومات واكتمالها وضمان استمرارية وجودها وإمكانية التحقق من كل تصرف أو كل معالجة مطبقة عليها (العازمي، 2022، 1132).

كما تعد مستويات الأمن الجيدة لنظام المعلومات المحاسبي أداة لتقليل المخاطر المرتبطة بالاستخدام المادي غير المشروع، فأمن المعلومات هي السياسات والممارسات والتكنولوجيا التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال الكترونيا" عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والعملاء والمنظمين وأي شخص آخر يمكن أن يكون معرضاً لمخاطر الاختراق (Al-Salahi, 2018).

ويتمثل أمن نظام المعلومات في المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين. ويلاحظ مما سبق أن هناك تركيزاً على مفهوم أمن المعلومات يتعلق بالنواحي التكنولوجيا، وتهتم بتوفير السياسات والإجراءات اللازمة لحماية هذه المعلومات، وهو

مـا يسـتوجب أن يـتم ذلـك مـن خـلال منظومـة متكاملة من السياسات والتعليمات والإجراءات التي تهدف لحماية المعلومات من أي خطر محتمل، ومنـع أي جهـة غيـر مسموح لهـا بالوصـول لتلـك المعلومـات (AICPA/CICA,2011,23). وحتـى يكون النظام محمياً من الاختراقات غير المصرح بها، يتم الالتزام بالمعايير الموضحة بالجدول رقم (2) الآتي: (أبو الهيجاء، 2017، 20).

الجدول(2): معايير أمن نظم المعلومات المحاسبية

المعيار	بالمعيار الخاصة الأمن إجراءات
السياسات	. وضع سياسات أمان لحماية البيانات وحفظها، مع تحديد المسؤوليات بوضوح. . تنفيذ إجراءات تحقق صارمة للمستخدمين، مع تسجيل عمليات الدخول والخروج من النظام. . تحديث السياسات الأمنية بشكل دوري لضمان الامتثال للمتطلبات الحديثة. . مراقبة أنشطة المستخدمين لمنع أي استخدام غير مصرح به. . وضع سياسات لعملية التدريب الخاصة بسياسات الحماية.
شبكات الربط	. تعريف المؤسسة بشبكات الربط في النظام. . مسؤولية حماية النظام مربوطة بشبكة اتصال مع الأشخاص المعنيين بوضع سياسات الحماية. . ربط آلية التبليغ عن اختراقات النظام مباشرة مع المصرح لهم بالتعامل ومعالجة الاختراقات. . ربط التغيرات التي تحدث على نظم الحماية بين كل من الإدارة والمستخدم.
الإجراءات	. احتواء النظام على إجراءات منطقية كتسجيل المستخدم الجديد والصلاحيات الممنوحة له. . احتواء النظام على إجراءات فعلية ملموسة تحدد آلية الحد من الوصول لغير المصرح لهم. . احتواء النظام على إجراءات وآليات لمنع دخول الفيروسات والبرامج غير المصرح لها. . احتواء النظام على تكنولوجيا تحمي بيانات المدخلات التي تتم خلال إتمام العمليات على الشبكة. . احتواء النظام على الإجراءات الخاصة بكل من عملية التصميم والتملك والتفعيل وآلية إدارة البنية التحتية وبرامج الحماية وبشكل يتماشى مع السياسات الموضوعة لمنع الدخول غير المصرح لهم. . احتواء النظام على إجراءات تحدد المصرح لهم بفحص وتوثيق التغيرات التي تحدث على النظام. . احتواء النظام على إجراءات خاصة بآلية التغيرات الطارئة التي تحدث للنظام.
الرقابة	. أن يتم تقييم نظام الحماية بشكل دوري ومطابقته بالسياسات الموضوعة. . ايجاد آلية تمكن المؤسسة من خلالها مراقبة نظام الحماية للتأكد من أنه يؤدي المهام المنوطة له. . مراقبة التغييرات التكنولوجية التي تحدث على بيئة نظام الحماية ومواكبتها بشكل مستمر.

المصدر: الباحثان بتصرف عن (أبو الهيجاء، 2017: 20؛ Whitman & Mattord 2017)

11-2- السرية:

يعـرف هـذا المبـدأ بأنـه مجموعـة الإجـراءات التـي تسـهم فـي الحفـاظ علـى سـرية المعلومـات الخاصـة بالمؤسسـة سـواءً بعمليـة جمعهـا، أو معالجتها، أو تخزينها. يتطلب تنفيذ هذا المبدأ أن تقوم الإدارة بتحديد أي المعلومات ستكون سرية وتحتاج إلى حماية. (Abu Mahdi, 2017, p. 42)، و يرى حجر أن السرية: هي المصطلح المستخدم

لمنع الكشف عن معلومات لأشخاص غير مصرح لهم الاطلاع عليها أو الكشف عنها، وحصر الوصول إليها وعدم استخدامها إلا من قبل المخول لهم ذلك؛ وهو ما تؤكد عليه (COBIT) عندما أشارت إلى ضرورة حماية المعلومات الحساسة على امتداد دورة التعامل معها بما في ذلك توزيعها والتخلص منها (تدميرها) وسواء كانت في صورة الكترونية أم في صورة ورقية. (حجر، 2024، 416).

متطلبات تحقيق سرية النظم:

إن تحقيق سرية النظم يتطلب مجموعة إجراءات رئيسية لضمان عدم تسرب البيانات الحساسة أو اختراقها، حددها (Romney and Steinbart, 2009, P.398-400) بالآتي:

1. تحديد المعلومات السرية وتصنيفها: ينبغي على الإدارة تحديد البيانات الحساسة التي تحتاج إلى الحماية، والتي تشمل المعلومات الداخلية وتلك المتبادلة مع الأطراف الأخرى.

2. تشفير البيانات أثناء التخزين والنقل: يُعد التشفير أحد الإجراءات الأساسية لحماية المعلومات، حيث يضمن عدم قراءتها إلا من قبل الأطراف المصرح لهم.

3. حماية الأجهزة المحمولة: نظرًا لسهولة فقدان الأجهزة المحمولة أو سرقتها، فإن تشفير البيانات المخزنة عليها يُعد إجراءً ضروريًا لمنع تسرب المعلومات الحساسة.

4. التحكم في الوصول: لا يقتصر تأمين البيانات على التشفير فقط، بل يجب تعزيز أنظمة التحقق من الهوية لمنع غير المخولين من الوصول إلى المعلومات، خاصة مع إمكانية تجاوز بعض تقنيات التشفير الحديثة.

5. تعزيز توثيق المستخدمين: يتطلب الأمر استخدام أنظمة مصادقة قوية، مثل تقنيات المصادقة متعددة العوامل، لضمان وصول الأفراد المخولين فقط.

6. رقابة الوصول إلى مخرجات الأنظمة.

7. التخلص الآمن من البيانات: يجب تمزيق الوثائق الحساسة قبل التخلص منها، وكذلك استخدام تقنيات متقدمة لإتلاف البيانات المخزنة لمنع استعادتها.

8. إجراء مراجعات أمنية دورية: يساعد التقييم الدوري لإجراءات الحماية في الكشف عن الثغرات الأمنية المحتملة والعمل على تحسينها باستمرار.

11-3- الخصوصية:

إن المبدأ الذي تقوم عليه حماية الخصوصية هو المبدأ نفسه الذي تقوم عليه السرية، فيما عدا انه يتم التركيز بالنسبة للخصوصية على المعلومات الشخصية للعملاء، أو الموظفين، أو شركاء العمل، أو غيرهم بدلاً من التركيز على بيانات المؤسسة. ومن ثم فإن الرقابة المطلوبة لحماية الخصوصية هي الرقابة المطلوبة نفسها لحماية السرية، والمتمثلة في التشفير ورقابة الدخول، وتدريب الأفراد وغير ذلك من الإجراءات الرقابية، فضلاً عن حسن الاستخدام والإفصاح

عن المعلومات الشخصية التي يتم جمعها عن العملاء (حجر، 2024، 434).

وفي ضوء ما سبق فقد أصبح تعزيز خصوصية النظم في بيئة الأعمال الحديثة ضرورة لضمان استمرار المؤسسات في سوق يعتمد على البيانات الرقمية. ومن خلال الالتزام بالمعايير العالمية لحماية الخصوصية، مما يسهم في تحقيق استدامة نظم المعلومات المحاسبية وموثوقيتها (المرزوقي، 2021). والجدول رقم (3) الآتي: يوضح مجموعة الممارسات المثلى لحماية خصوصية بيانات العملاء.

جدول(3): الممارسات المثلى لحماية الخصوصية

الممارسة	التعريف
الإدارة	توثيق وتحديد الجهات المسؤولة عن سياسات وإجراءات الخصوصية.
الإشعار	توفير بيان رسمي حول سياسة الخصوصية، يوضح أسباب جمع البيانات وآلية استخدامها والاحتفاظ بها.
الاختيار والموافقة	منح العملاء حق تقرير ما إذا كانوا يوافقون على جمع بياناتهم الشخصية واستخدامها والإفصاح عنها.
التجميع	جمع المعلومات الضرورية واستخدامها بما يتماشى مع السياسات المعلنة في الإشعار.
الاستخدام والاحتفاظ	توظيف البيانات للأغراض المحددة مسبقًا، بناءً على الإشعار المقدم للعملاء وموافقتهم.
الدخول	توفير آلية تتيح للعملاء الوصول إلى بياناتهم الشخصية لتحديثها أو مراجعتها.
الإفصاح	الامتناع عن مشاركة بيانات العملاء إلا وفقًا لما تم توضيحه في الإشعار وبموافقتهم الصريحة أو الضمنية.
الأمن	ضمان حماية البيانات الشخصية للعملاء من التلاعب أو الوصول غير المصرح به.
الجودة	الحفاظ على دقة، صحة، واكتمال المعلومات الشخصية بما يتماشى مع الإشعار.
الرقابة التنفيذ	متابعة تنفيذ سياسات الخصوصية والتأكد من معالجتها لشكاوى العملاء بشكل فعال.

إعداد الباحثان بتصرف عن (أبو مهادي،2017: 45)

11-4- سلامة العمليات:

تتمثل سلامة المعالجة في وجوب تجهيز البيانات بشكل صحيح وشامل، وفي الوقت المناسب، ومن قبل المخول لهم ذلك. وهذا يتطلب الرقابة على المدخلات من البيانات، وعملية التجهيز لتلك البيانات للتأكد من أن التجهيز يتم بالصورة المحددة له وأنه لا يوجد إهمال أو إدخال غير صحيح، كما يجب الرقابة على المخرجات لضمان سلامة تجهيز البيانات (حجر، 2024، 436). إن ضمان سلامة المعالجة في نظم المعلومات المحاسبية لا يقتصر فقط على تنفيذ العمليات بطريقة صحيحة، بل يشمل أيضًا تطبيق إجراءات الحماية الأمنية لضمان عدم الوصول غير المصرح به إلى البيانات. إن تعزيز الضوابط الأمنية من خلال استخدام تقنيات التشفير، والمصادقة المتعددة، وتطبيق آليات التدقيق الدوري، يؤدي دورًا حيويًا في الحفاظ على سلامة العمليات المحاسبية ومنع أي تلاعب أو احتيال

مـــالي. (عبـــد الله، 2023). والجـــدول رقـــم (4) والإجراءات الوقائية لسلامة العمليات.
الآتـــي: يوضـــح الضـــوابط الأمنيـــة والمخـــاطر

الجدول(4): الضوابط الامنية والمخاطر والإجراءات الوقائية لضمان لسلامة العمليات

الضوابط	المخاطر	الوصف	إجراءات الرقابة
الرقابة على البيانات الأولية	البيانات غير دقيقة، غير مكتملة، ضياع بيانات.	في حالة فقدان البيانات في أثناء المعالجة، قد يؤدي ذلك إلى بيانات غير دقيقة أو غير كاملة.	تدقيق البيانات. الاحتفاظ بنسخ احتياطية. فرض ضوابط وصول.
الرقابة على إدخال البيانات	أخطاء في المعالجة، نتائج غير صحيحة.	أخطاء في المعالجة يمكن أن تنتج عن إدخال بيانات غير صحيحة أو أخطاء برمجية.	التحقق من صحة البيانات، مراجعة العمليات، اختبار الأنظمة بانتظام.
الرقابة على نقل البيانات	تسريب معلومات، انتهاك خصوصية.	تسرب المعلومات الحساسة قد يؤدي إلى انتهاك الخصوصية وسرقة البيانات.	تشفير البيانات، التحكم في صلاحيات الوصول، تدريب الموظفين على الأمان.
الرقابة على المعالجة	المعلومات غير دقيقة، تلاعب مالي.	عدم اكتمال العمليات المحاسبية يسبب أخطاء في التقارير المالية.	مراجعة العمليات، تدقيق دوري، تحسين الأنظمة المحاسبية.
الرقابة على المخرجات	اختراق النظام، ضياع بيانات. استعمال تقارير غير دقيقة.	توفر عملية اختبار مخرجات النظام سيطرة إضافية على سلامة المعالجة	مراجعة المخرجات، إجراءات التسوية، استخدام جدران الحماية، أنظمة كشف التسلل، تحديث البرامج باستمرار.

اعداد الباحثان بتصرف عن (Romney & Steinbart, 2018:407-414).

11-5- جاهزية النظام:

تعرف جاهزية النظم بقدرة المستخدم النهائي لنظام المعلومات المحاسبي على الوصول إليه وتشغيله في الوقت المناسب، بما يضمن تنفيذ المتطلبات التشغيلية للشركات بكفاءة وفاعلية. وتشمل هذه الجاهزية القدرة على تنفيذ دورة معالجة العمليات المحاسبية من إدخال البيانات وتخزينها ومعالجتها وإعداد التقارير بمستويات عالية من الكفاءة (النسور والحياري، 2018: 107). وتوافر النظام يتطلب تحقيق هدفين: أولهما تدنية مخاطر توقف النظام. وثانيهما الحاجة إلى وضع الرقابة التي تتمكن من خلالها المنشأة من استعادة تشغيل النشاط في حالة تعرض النظام للمخاطر وخروجه عن الجاهزية (حجر، 2024، 440). وأهم الإجراءات الرقابية لضمان جاهزية النظم تحدد في الجدول رقم (5) الآتي:

جدول(5): إجراءات الرقابة لضمان جاهزية النظام

الهدف	المخاطر	الرقابة
تقليل ركود النظام.	توقف النظام، فقدان أو تدمير المعلومات المهمة بسبب الكوارث الطبيعية، الفيروسات، الهجمات المتعمدة.	الصيانة الوقائية، تجاوز الخطأ، تجهيز الطاقة دون انقطاع، الموقع المادي وتصميم الغرف التي تضم مصادر الحوسبة، التدريب، التأسيس، المعالجة، حفظ البرامج الصوتية والمرئية،
التعافي.	فقدان الاتصال بمصادر أنظمة معلومات العمل الجوهرية، عدم القدرة على القيام بالعمليات التجارية الرئيسة.	إجراءات العمل الاحتياطية، خطط التعافي من الكوارث واستمرار التجارة، التوثيق، اختبار إجراءات الاحتفاظ واستعادة النشاط.

إعداد الباحثين بتصرف عن (الجراح، 2011: 55)

12- منهجية وإجراءات الدراسة:

12-1- تصميم منهجية الدراسة:

اعتمدت الدراسة المنهج الوصفي التحليلي المناسب لطبيعتها التي يغلب عليها الجانب الميداني القائم على جمع البيانات الأولية من البنوك اليمنية.

12-2- مجتمع الدراسة:

أجريت الدراسة الميدانية لجمع البيانات الأولية من موظفي البنوك اليمنية التي تمثل مجتمع الدراسة.

12-3- عينة الدراسة:

تم إجراء الدراسة الميدانية على موظفي البنوك اليمنية التي مثلت مجتمع الدراسة، حيث تم توزيع الاستبانة على عينة قصدية من شاغلي الوظائف المالية في البنوك اليمنية. وقد بلغ عدد الاستمارات الموزعة(114) استمارة، استجاب منها(107) موظفاً. تم استبعاد (7) استمارات لعدم صلاحيتها للتحليل الإحصائي، ليصبح عدد الاستمارات الصالحة للتحليل (100) استمارة.

12-4- الأساليب الإحصائية:

تم استخدام الرزمة الإحصائية للعلوم الاجتماعية (SPSS) لإجراء التحليلات, والإحصاءات اللازمة لبيانات الاستبانة, وتم استخدام الأساليب الإحصائية الآتية:

- معامل ارتباط بيرسون للتحقق من صدق الاتساق الداخلي للاستبانة.
- معامل ألفا كرونباخ للتحقق من ثبات الاستبانة.
- المتوسطات الحسابية والانحرافات المعيارية: تم استخدامها في تحليل متغيرات الدراسة.
- اختبار شابيرو ويلك للتحقق من التوزيع الطبيعي للبيانات
- اختبار(T) لعينة واحدة لمعرفة دلالة الفروق الإحصائية بين متوسطات استجابات أفراد العينة، والمتوسط الفرضي لمجتمع الدراسة، حول مستوى تطبيق حوكمة مخاطر تكنولوجيا المعلومات، ومستوى موثوقية نظم المعلومات المحاسبية الإلكترونية في البنوك اليمنية.
- اختبار تحليل الانحدار البسيط لمعرفة دلالة فاعلية المتغير المستقل (تطبيق حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية) في المتغير التابع (موثوقية نظم المعلومات المحاسبية في البنوك اليمنية).

12-5- أداة الدراسة:

تم بناء الاستبانة -وفقاً لأسلوب ليكرت الخماسي- بعد الاطلاع، والاستفادة من الأدبيات والدراسات السابقة ذات العلاقة بموضوع الدراسة. وتكونت الاستبانة في صورتها النهائية من الآتي:

الجزء الأول: يختص بالبيانات الديمغرافية لعينة الدراسة(العمر، المؤهل العلمي، الوظيفة الحالية، سنوات الخبرة).

الجزء الثاني: تمثل بالمحور الأول أثر حوكمة مخاطر تكنولوجيا المعلومات وتضمن(8) فقرات.

الجزء الثالث: تمثل بالمحور الثاني (موثوقية نظم المعلومات المحاسبية الإلكترونية في البنوك اليمنية) وتكون من(15) فقرة.

12-5-1- صدق الأداة:

تم التأكد من صدق الاستبانة في الدراسة الحالية باستخدام أسلوبين هما: أسلوب الصدق الظاهري المسمى بصدق المحكمين، وأسلوب صدق الاتساق الداخلي.

- **الصدق الظاهري:**

بعد الانتهاء من إعداد الاستبانة وبناء فقراتها؛ تم عرضها على (9) من المحكمين المتخصصين في المحاسبة في عدد من الجامعات اليمنية؛ لإبداء آرائهم حول فقرات الاستبانة من حيث مدى ارتباط كل فقرة بالبعد الذي تنتمي إليه، ومدى وضوح كل فقرة وسلامة صياغتها اللغوية وملاءمتها لتحقيق الهدف الذي وضعت من أجله، والتعديلات المقترح إجراؤها سواءً بالإضافة أو الحذف، وبعد استعادة النسخ المحكمة؛ تم تعديل صياغة بعض فقرات الاستبانة في ضوء آراء ومقترحات المحكمين، ومن ثم أصبحت الاستبانة تتمتع بالصدق الظاهري.

- **صدق الاتساق الداخلي:**

تم التحقق من صدق الاستبانة أيضاً باستخدام صدق الاتساق الداخلي، وهو يعطي صورة عن مدى التناسق الموجود بين الفقرات الموجودة داخل البعد، ومدى اتساق هذه الفقرات مع البعد الذي تنتمي إليه، وتم التأكد من توافر صدق الاتساق الداخلي باستخدام معامل ارتباط بيرسون، عن طريق حساب معامل الارتباط بين درجة كل فقرة مع الدرجة الكلية للبعد الذي تنتمي إليه؛ وذلك بعد تطبيق الأداة على عينة استطلاعية مكونة من(27) موظفاً من شاغلي الوظائف المالية في البنوك اليمنية، غير عينة الدراسة الأصلية. وكانت النتائج كما هو موضح في الجدول(6) الآتي.

جدول(6): معاملات ارتباط الفقرات بالدرجة الكلية للبعد الذي تنتمي إليه

الفقرة	درجة الارتباط	مستوى الدلالة	الفقرة	درجة الارتباط	مستوى الدلالة
أولا": حوكمة مخاطر تكنولوجيا المعلومات.					
1	**0.595	0.001	5	**0.699	0.000
2	**0.614	0.000	6	**0.727	0.000
3	**0.620	0.000	7	**0.599	0.000
4	*0.457	0.011	8	*0.435	0.015
ثانيًا: موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية.					
1	**0.525	0.003	9	**0.651	0.000
2	**0.590	0.001	10	**0.558	0.001
3	**0.583	0.001	11	**0.580	0.000
4	*0.455	0.011	12	**0.575	0.001
5	**0.489	0.006	13	**0.571	0.001
6	**0.533	0.002	14	**0.485	0.007
7	**0.542	0.002	15	*0.449	0.013
8	**0.496	0.005	-	-	-

****علاقة الارتباط دالة عند مستوى 0.01، *علاقة الارتباط دالة عند مستوى 0.05.**

يتضح من الجدول(6): أن قيم معاملات ارتباط الفقرات بالدرجة الكلية للبعد الذي تنتمي إليه ذات دلالة إحصائية عند مستوى الدلالة (0.01) و(0.05)، وتشير إلى الاتساق الداخلي بين درجة كل فقرة ودرجة البعد الذي تنتمي إليه؛ وهو ما يثبت صدق تلك الفقرات وتمتعها بدرجة عالية من الصدق.

12-5-2- ثبات الأداة: تم التأكد من ثبات الاستبانة في الدراسة الحالية, وتم استخدام أسلوب ألفا كرونباخ (Cronbach Alpha) من خلال تطبيق الاستبانة على عينة استطلاعية المكونة من(27) موظفاً من شاغلي الوظائف المالية في البنوك اليمنية، غير عينة الدراسة الأصلية. وكانت النتائج كما هو موضح في الجدول (7).

جدول(7): معاملات ألفا كرونباخ للتحقق من ثبات أداة الدراسة

البعد	عدد الفقرات	معامل ألفا كرونباخ
جميع فقرات المحور الأول	8	0.75
جميع فقرات المحور الثاني	15	0.83

يبين الجدول(7): أن قيم معامل ألفا كرونباخ لأبعاد المحور الأول كانت (0.75)، وبلغت قيم معامل ألفا كرونباخ لأبعاد المحور الثاني (0.83)، وهذا يعني أن جميع قيم معامل ألفا

كرونباخ للثبات مرتفعة ومقبولة؛ وتشير إلى أن الأداة تتمتع بدرجة عالية من الثبات.

12-5-3 التوزيع الطبيعي للبيانات: قبل إجراء التحليل الإحصائي؛ تم التحقق من اعتدالية التوزيع الطبيعي للبيانات، باستخدام اختبار شابيرو ويلك، (Shapiro-Wilk), والجدول (8) يوضح نتيجة اختبار (شابيرو ويلك) للتحقق من اعتدالية التوزيع الطبيعي لبيانات المتغير المستقل (حوكمة مخاطر تكنولوجيا المعلومات) والمتغير التابع (موثوقية نظم المعلومات المحاسبية الإلكترونية).

جدول(8): نتيجة اختبار شابيرو ويلك للتحقق من التوزيع الطبيعي للبيانات

المتغير	قيمة الاختبار	درجة الحرية	مستوى الدلالة
حوكمة مخاطر تكنولوجيا المعلومات	0.979	100	0.111
موثوقية نظم المعلومات المحاسبية الإلكترونية	30.97	100	360.0

يتضح من الجدول (8):

- أن قيمة اختبار شابيرو لاعتدالية بيانات المتغير المستقل (حوكمة مخاطر تكنولوجيا المعلومات) غير دالة إحصائياً؛ إذ أن قيمة مستوى الدلالة بلغت (0.111)، وهي أكبر من (0.05)؛ وهو ما يعني أن بيانات المتغير المستقل موزعة توزيعاً طبيعياً.
- أن قيمة اختبار شابيرو لاعتدالية بيانات المتغير التابع (موثوقية نظم المعلومات المحاسبية الإلكترونية) غير دالة إحصائياً؛ إذ أن قيمة مستوى الدلالة بلغت (0.036)، وهي أكبر من (0.01)؛ وهو ما يعني أن بيانات المتغير التابع موزعة توزيعاً طبيعيا.

13- تحليل بيانات محاور الدراسة:

13-1- تحليل المتغيرات الديموغرافية:

اشتملت المتغيرات الديموغرافية على الجنس، العمر، المؤهل العلمي، الوظيفة الحالية، سنوات الخبرة، والجدول(9) الآتي: يوضح المتغيرات الديموغرافية لأفراد عينة الدراسة.

جدول (9): توزيع أفراد العينة وفقاً لمتغيرات الديموغرافية

المتغير		العدد	النسبة المئوية
الجنس	ذكر	86	86.0
	أنثى	14	14.0
العمر	25-35 سنة	29	29.0
	36-45 سنة	52	52.0
	أكبر من 45 سنة	19	19.0
المؤهل العلمي	بكالوريوس	58	58.0
	ماجستير ودكتوراه	42	42.0
الوظيفة الحالية	محاسب	56	56.0
	مدير حسابات	30	30.0
	مراجع داخلي	14	14.0

المتغير		العدد	النسبة المئوية
سنوات الخبرة	أقل من 5 سنوات	24	24.0
	5 – 15 سنة	49	49.0
	أكثر من 15 سنة	27	27.0
	المجموع	**100**	**%100**

11-2- تحليل بيانات المحور الأول: حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية: تم استخراج المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة حول حوكمة مخاطر تكنولوجيا في البنوك اليمنية، والجدول (10) الآتي: يوضح ذلك.

جدول (10): المتوسطات والانحرافات المعيارية لاستجابات أفراد العينة حول حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	المستوى
1	تحديد وتصويب المخاطر حسب قابلية تحمل الخطر.	4.29	0.71	2	عال جداً
2	تبني وجود خريطة للمخاطر المحتملة المقبولة وغير المقبولة.	4.21	0.62	7	عال جداً
3	تعزيز خطط التعامل مع المخاطر واختبار فاعلية الاستجابة.	4.21	0.55	6	عال جداً
4	تصنيف المعلومات حسب حساسيتها لضمان حماية الخصوصية.	4.21	0.72	8	عال جداً
5	تقييم المخاطر بشكل دوري لتحديد نقاط الضعف والتهديدات المحتملة.	4.23	0.64	5	عال جداً
6	توفير آليات لتخفيف المخاطر تشمل خطط الطوارئ والإجراءات الوقائية.	4.26	0.66	4	عال جداً
7	دعم تدريب الموظفين على كيفية التعامل مع المخاطر المحتملة.	4.27	0.67	3	عال جداً
8	تنفيذ اختبارات دورية لتقييم فعالية تدابير إدارة المخاطر.	4.34	0.59	1	عال جداً
	المتوسط العام للبعد الرابع	4.25	0.41	-	عال جداً

يبين الجدول(10) ما يأتي:

- حصلت جميع الفقرات على مستوى عال جداً.
- تراوح المتوسط الحسابي لفقرات البعد الأول **(حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية)** بين (4.21) و(4.34)، ويُلاحظ أن الفقرتين (8، 1): "تنفيذ اختبارات دورية لتقييم فعالية تدابير إدارة المخاطر"، و"تحديد وتصويب المخاطر حسب قابلية تحمل الخطر" قد حصلتا على التوالي على الترتيب الأول والثاني بمستوى عالٍ جدًا للفقرتين، في حين الفقرتان (2، 4)، "تبني وجود خريطة للمخاطر المحتملة المقبولة وغير المقبولة" و "تصنيف المعلومات حسب حساسيتها لضمان حماية الخصوصية" حصلتا على التوالي على الترتيب قبل الأخير والأخير

بمستوى عالٍ جداً للفقرتين.

13-3- تحليل بيانات المحور الثاني: مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية:

تم استخراج المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة حول مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية، والجدول(11) الآتي: يوضح ذلك.

جدول(11): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة حول مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	المستوى
1	تعتمد تقنية حماية متقدمة في المكافحة والكشف والاستجابة لمخاطر الأمن.	4.35	0.62	1	عال جدًا
2	تدعم تقنيات التشفير وآلية الإشعار للحماية الأمنية من التلاعب المحتمل.	4.14	0.68	12	عال
3	يعزز التدريب مهارات وأخلاقيات ومتطلبات تحقيق أمن النظم المحاسبية.	4.14	0.79	13	عال
4	تدعم خيارات متعددة في الإفصاح عن سياسات وإجراءات حماية السرية.	4.16	0.67	10	عال
5	توفر تقنيات آلية في المصادقة الفورية لضمان حماية سرية المعلومات.	4.16	0.65	9	عال
6	تدعم البرمجيات التوثيق الآلي لمراقبة سرية استخدام المعلومات وفق الصلاحيات.	4.21	0.60	6	عال جدًا
7	تبني تقنيات متعددة في إدارة الوصول للكشف عن استخدام البيانات الخاصة.	4.17	0.68	8	عال
8	تطبيق إجراءات رقابية صارمة في حماية الخصوصية من الوصول غير المصرح.	4.23	0.67	4	عال جدًا
9	تصنيف المعلومات حسب حساسيتها لضمان حماية الخصوصية.	4.23	0.65	3	عال جدًا
10	تحقيق متطلبات ضمان سلامة معالجة البيانات ومطابقتها للمعايير المحاسبية.	4.22	0.67	5	عال جدًا
11	تدعم أساليب وتقنيات الالتقاط والتشغيل والتبادل سلامة المعالجة المحاسبية.	4.10	0.61	15	عال

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الرتبة	المستوى
12	يحقق تصميم الضوابط الرقابية الآلية صحة وسلامة المعالجة المحاسبية.	4.19	0.59	7	عال
13	توفر آلية النسخ الاحتياطي التلقائي وآليات الاستعادة ضمان للاستمرارية والجهوزية.	4.34	0.63	2	عال جدًا
14	تطبيق بدائل متعددة وخطة استجابة للطوارئ المحتملة لانتظام واستمرار الأداء.	4.15	0.68	11	عال
15	يعمل النظام بضوابط رقابية متعددة لضمان استمرارية إتاحة النظم.	4.12	0.71	14	عال
المتوسط العام للمحور الثاني		4.27	0.41	-	عال جداً

يبين الجدول (11) ما يأتي:

- بلغ المتوسط الحسابي للمحور الثاني (موثوقية النظم المحاسبية الإلكترونية) (4.16) وانحراف معياري بلغ (0.42) وبمستوى عالٍ جداً.
- حصلت (9) عبارات على مستوى عال، في حين حصلت (6) عبارات على مستوى عال جدًا.
- تراوح المتوسط الحسابي للمحور الثاني (موثوقية النظم المحاسبية الإلكترونية) بين (4.10) و(4.35), ويُلاحظ أن الفقرتين (1، 13): "تعتمد تقنية حماية متقدمة في المكافحة والكشف والاستجابة لمخاطر الأمن"، و"توفر آلية النسخ الاحتياطي التلقائي وآليات الاستعادة ضمان للاستمرارية والجهوزية" قد حصلتا على التوالي على الترتيب الأول والثاني بمستوى عالٍ جدًا للفقرتين، في حين الفقرتان (15، 11): "يعمل النظام بضوابط رقابية متعددة لضمان استمرارية إتاحة النظم، وتدعم اساليب وتقنيات الالتقاط والتشغيل والتبادل سلامة المعالجة المحاسبية" حصلتا على التوالي على الترتيب قبل الأخير والأخير بمستوى عالٍ للفقرتين.

14- اختبار الفرضيات:

14-1- اختبار الفرضية الأولى:

للتأكد من صحة الفرضية الأولى التي تنص على: "لا توجد فروق دال إحصائياًعند مستوى دلالة أقل من أو يساوي(0.05) حول حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية، تم استخدام اختبار(T) لعينة واحدة لمعرفة دلالة الفرق بين متوسط استجابات أفراد العينة (الواقعي) والمتوسط الفرضي لمجتمع الدراسة والجدول(12) الآتي: يوضح نتيجة اختبار(T) لعينة واحدة.

جدول(12): نتيجة اختبار(T) لعينة واحدة لمعرفة دلالة الفرق بين متوسط استجابات العينة والمتوسط الفرضي حول حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية.

العينة	المتوسط الحسابي	الانحراف المعياري	المتوسط الفرضي	درجة الحرية	قيمة ت	مستوى الدلالة	الدلالة اللفظية
100	4.25	0.41	3	99	29.87	0.000	دالة إحصائياً

يبين الجدول (12): أن قيمة ت تساوي (29.87)، وهي قيمة دالة إحصائياً عند مستوى (0.05)؛ لأن قيمة مستوى الدلالة بلغت (0.000) وهي أصغر من (0.05)؛ وهو ما يعني وجود فرق دال إحصائياً عند مستوى دلالة (0.05) بين متوسط استجابات أفراد العينة (4.25)، وبين المتوسط الفرضي لمجتمع الدراسة (3)، حول حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية، لصالح متوسط استجابات أفراد العينة؛ وهو ما أدى إلى رفض الفرضية الصفرية السابقة، وقبول الفرضية البديلة التي تنص: يوجد فرق دال إحصائيًا عند مستوى دلالة أقل من أو يساوي (0.05) بين متوسط استجابات أفراد العينة، والمتوسط الفرضي لمجتمع الدراسة حول حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية، لصالح متوسط استجابات أفراد العينة؛ وهذا يدل أن حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية ظهر بمستوى عالٍ جداً.

14-2- اختبار الفرضية الثانية:

للتأكد من صحة الفرضية الرئيسة الثانية التي تنص على: لا يوجد فرق دال إحصائيًا عند مستوى دلالة أقل من أو يساوي (0.05) حول مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية، وذلك باستخدام اختبار (T) لعينة واحدة. والجدول (13) يوضح نتيجة اختبار (T) لعينة واحدة.

جدول(13): نتيجة اختبار(T) لعينة واحدة لمعرفة دلالة الفرق بين متوسط استجابات العينة والمتوسط الفرضي حول مستوى موثوقية النظم المحاسبية الإلكترونية

العينة	المتوسط الحسابي	الانحراف المعياري	المتوسط الفرضي	درجة الحرية	قيمة ت	قيمة مستوى الدلالة	الدلالة اللفظية
100	4.27	0.41	3	99	30.47	0.000	دالة إحصائياً

يبين الجدول(13): أن قيمة T تساوي (30.47)، وهي قيمة دالة إحصائياً عند مستوى (0.05)؛ وذلك لأن قيمة مستوى الدلالة بلغت (0.000) وهي أصغر من (0.05)؛ وهو ما يعني وجود فرق دال إحصائياً عند مستوى دلالة (0.05) بين متوسط استجابات أفراد العينة (4.27)، وبين المتوسط الفرضي لمجتمع الدراسة (3) حول مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية لصالح متوسط استجابات أفراد العينة؛ وهو ما أدى إلى رفض الفرضية الصفرية السابقة، وقبول الفرضية البديلة التي تنص على: يوجد فرق دال إحصائيًا عند

مستوى دلالة أقل من أو يساوي (0.05) بين متوسط استجابات أفراد العينة والمتوسط الفرضي لمجتمع الدراسة حول مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية لصالح متوسط استجابات أفراد العينة؛ وهذا يدل على أن موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية تحققت بمستوى عالٍ جداً.

14-3- اختبار الفرضية الثالثة:

للتأكد من صحة الفرضية الرئيسة الثالثة التي تنص على: "لا توجد فروق ذو دلالة إحصائية عند مستوى دلالة أقل من أو يساوي (0.05) حول تأثير حوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية نظم المعلومات المحاسبية الإلكترونية في البنوك اليمنية"، تم استخدام اختبار تحليل الانحدار البسيط لمعرفة الدور التأثيري لحوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية، ويوضح الجدول (14) الآتي نتيجة اختبار تحليل الانحدار البسيط.

جدول (14): نتيجة اختبار تحليل الانحدار البسيط لمعرفة تأثير حوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية

الارتباط R	معامل التحديد R^2	قيمة F	مستوى الدلالة	الثابت	معامل الانحدار ß	قيمة ت	مستوى الدلالة
0.71	0.49	97.1	0.000	0.52	0.88	9.8	0.000

يوضح الجدول(14): أن هناك علاقة طردية دالة إحصائياً عند مستوى دلالة (0.05) بين حوكمة مخاطر تكنولوجيا المعلومات وموثوقية النظم المحاسبية الإلكترونية؛ إذ بلغ معامل الارتباط (0.71)، وهو معامل ارتباط قوي؛ كما يتضح من الجدول (14) أن قيمة معامل التحديد (مربع معامل الارتباط) بلغت (0.49)؛ ويعني ذلك أن مستوى تطبيق حوكمة مخاطر تكنولوجيا المعلومات يفسر ما نسبته (0.49) من التباين/التغيرات الحاصلة في موثوقية النظم المحاسبية الإلكترونية؛ أي أن (49%) من مستوى موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية ناتج عن دور حوكمة مخاطر تكنولوجيا المعلومات، والباقي (51%) يعزى إلى عوامل أخرى لم تتطرق إليها الدراسة الحالية.

كما يبين الجدول (14): أن قيمة (ف) التي بلغت (97.1) دالة إحصائياً؛ إذ أن قيمة مستوى الدلالة (0.000) أصغر من (0.05)؛ وهذا يؤكد وجود تأثير دال إحصائياً لحوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية. ويتضح ذلك جلياً من قيمة معامل الانحدار أو درجة التأثير التي بلغت (0.88) - بافتراض تحييد بقية المتغيرات- الأمر الذي يعني أن كل زيادة في تطبيق حوكمة مخاطر تكنولوجيا المعلومات بمقدار درجة واحدة سيؤدي إلى تعزيز موثوقية النظم المحاسبية الإلكترونية بمقدار (0.88) من الدرجة. كما نلاحظ أن قيمة (T) دالة إحصائياً؛ إذ أن قيمة

مستوى الدلالة بلغت (0.000)، وهي أصغر من (0.05)؛ الأمر الذي يعني أن تطبيق حوكمة مخاطر تكنولوجيا المعلومات دال، وهو ما يؤكد دلالة تحليل الانحدار؛ بمعنى أن تطبيق حوكمة مخاطر تكنولوجيا المعلومات له تأثير دال إحصائيًا في موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية. في ضوء النتيجة السابقة تم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على: "يوجد دور تأثيري ذو دلالة إحصائية عند مستوى دلالة أقل من أو يساوي (0.05) لحوكمة مخاطر تكنولوجيا المعلومات في تعزيز موثوقية النظم المحاسبية الإلكترونية في البنوك اليمنية.

15- النتائج:

1. أظهرت الدراسة الميدانية، أن البنوك تبدي التزاماً ملحوظاً بتطبيق مبادئ حوكمة مخاطر تكنولوجيا المعلومات. فقد بلغ المتوسط العام لمستوى التطبيق حوالي 4.25، مما يشير إلى أن الإجراءات والسياسات المتبعة في هذا المجال تُنفّذ بمستوى عالٍ جداً.

2. بلغ متوسط مستوى موثوقية نظم المعلومات المحاسبية الإلكترونية حوالي 4.27، مما يؤكد أن الأنظمة الإلكترونية المستخدمة قادرة على توفير معلومات دقيقة وكاملة وفي الوقت المناسب. ويمتاز النظام الإلكتروني باتخاذ إجراءات أمان مشددة، مثل استخدام تقنيات التشفير وتوثيق البيانات وإجراءات النسخ الاحتياطي والاستعادة، مما يسهم في الحفاظ على سلامة البيانات ومصداقيتها.

3. أظهرت التحليلات الإحصائية وجود علاقة إيجابية قوية بين تطبيق حوكمة مخاطر تكنولوجيا المعلومات وموثوقية النظم؛ حيث بلغ معامل الارتباط 0.71 ومعامل التحديد 0.49، مما يعني أن 49% من التباين في موثوقية الأنظمة يُفسّر بتطبيق مبادئ الحوكمة. علاوة على ذلك، بيّن تحليل الانحدار البسيط أن كل زيادة بمقدار درجة واحدة في تطبيق حوكمة مخاطر تكنولوجيا المعلومات ترتب زيادة بمعدل 0.88 في مستوى موثوقية نظم المعلومات المحاسبية الإلكترونية. وهذا يشير بوضوح إلى الفاعلية الكبيرة لهذه الممارسات في رفع جودة المعلومات.

16- التوصيات:

1. ضرورة الاستمرار في تطوير ممارسات إجراءات حوكمة مخاطر تكنولوجيا المعلومات في البنوك اليمنية من خلال الآتي:

أ) العمل على توفير برامج تدريبية متخصصة لموظفي المحاسبة وتقنية المعلومات حول أحدث الممارسات في إدارة مخاطر تكنولوجيا المعلومات.

ب) اعتماد آليات تحديد وتصنيف المخاطر بشكل دوري مع تطبيق خطط الطوارئ والاستجابة.

ج) استخدام تقنيات متقدمة لرصد التهديدات؛ مثل أنظمة الكشف عن التسلل والتشفير المتطور لضمان حماية البيانات.

2. ضرورة العمل على تعزيز المتطلبات الرقابية لموثوقية النظم المحاسبية الإلكترونية.

3. ضرورة العمل على تبني المعايير الدولية لضمان فاعلية حوكمة مخاطر تكنولوجيا المعلومات في مختلف الجوانب والتي ستكون لها دور فاعل في تعزيز ضوابط وإجراءات الرقابة في البنوك اليمنية بما يتطلب على تعزيز موثوقية النظم المحاسبية الإلكترونية.

4. دمج النتائج في استراتيجيات التحول الرقمي من خلال:

- تكثيف الجهود لتوحيد الاستراتيجيات التقنية مع استراتيجيات العمل لتحقيق تكامل أفضل بين الأقسام.
- استخدام نتائج الدراسة لتوجيه السياسات المستقبلية ودعم اتخاذ قرارات استراتيجية قائمة على البيانات.

تساهم هذه التوصيات في تحسين مستوى الموثوقية والاستفادة المثلى من تقنيات تكنولوجيا المعلومات في البنوك، مما يدعم مشاركة المعرفة واتخاذ القرارات المستندة إلى معلومات دقيقة ومتاحة بشكل دائم.

17- المراجع والمصادر:

المراجع العربية:

1.أبو الهيجاء، عدنان (2017). أثر موثوقية نظم المعلومات المحاسبية في ظل تطبيق حوكمة تكنولوجيا المعلومات على ربحية البنوك الأردنية. في بورصة عمان، أطروحة دكتوراه. *العلوم الإسلامية العالمية، عمان.*

2.التكريتي، رؤى؛ والزواري، غازي (2024). دور حوكمة تكنولوجيا المعلومات في تعزيز أداء نظم المعلومات المحاسبية. المجلة العلمية لإدارة الأعمال والتكنولوجيا. ISSN: 1737-619 - 19(3) .P 1-20

3.الجابري، سعيد (2020). دور تكنولوجيا المعلومات في تحسين الرقابة الداخلية والحد من المخاطر الأمنية. *المجلة العربية للمحاسبة، 10(1)، 120-140.*

4. الجراح، محمد خير (2011). مدى موثوقية نظم المعلومات المحاسبية وأثرها في تحسين كفاءة الرقابة الداخلية لدى البنوك التجارية الأردنية. *رسالة ماجستير غير منشورة. جامعة آل البيت.*

5.السريحي، سلطان؛ والربيدي، محمد؛ والحميري، نبيل (2025). الوسيط للضوابط الأمنية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية: دراسة ميدانية في شركات الاتصالات العاملة في الجمهورية اليمنية. *المجلة الأردنية في إدارة الأعمال، المجلد21، العدد1.*

6.العازمي، عبدالله (2022). دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات المحاسبية من المخاطر الإلكترونية في ظل عصر الرقمنة. *المجلة العلمية للدراسات والبحوث المالية والإدارية، مصر، 13 (2)، ص 1115-1155* .

7.العلي، صالح (2016). إدارة المخاطر القانونية في النظم المحاسبية الإلكترونية. *دار الفكر العربي.*

*8.*الربيعي، محمد (2021). حوكمة المخاطر في النظم المحاسبية الرقمية. *دار الثقافة للنشر*.

9. المرزوقي، خالد. (2021). حماية البيانات الشخصية في ظل التحول الرقمي: دراسة تحليلية. *مجلة الاقتصاد الرقمي، 6(4)، 200-220.*

10.المطيري، خالد (2017). دور تكنولوجيا المعلومات في تحسين الأداء المالي للشركات. *مجلة الاقتصاد الإسلامي، 91.*

11.النسور، أسامة؛ والحياري، هديل (2018). مبادئ موثوقية نظم المعلومات المحاسبية المحوسبة وأثرها في إدارة الأزمات – دراسة ميدانية في الشركات الصناعية المساهمة العامة الأردنية–بيروت. مجلة المحاسبة والتدقيق والحوكمة 1,(3).

12.حجر، عبدالملك (2024). *نظم المعلومات المحاسبية المحوسبة*. الأمين للنشر والتوزيع.

13.حسن، علي (2021). حوكمة تكنولوجيا المعلومات كمدخل لتفعيل إدارة المخاطر: دراسة تحليلية. *مجلة العلوم الإدارية، 23(3)،ص 75-90.*

14.خليفة، أحمد؛ وزين،عبدالملك؛ وضيف الله، محمد (2021). أثر حوكمة تكنولوجيا المعلومات على الحد من مخاطر نظام المعلومات المحاسبي.دراسة ميدانية. مجلة الدراسات المالية و المحاسبية و الإدارية، المجلد 8،العدد1.

DOI: https://doi.org/10.35516/jjb.v21i1.270

15.عبد الله، ناصر. (2023). حماية البيانات المحاسبية من التلاعب باستخدام تقنيات التشفير والأمان الإلكتروني. مجلة الاقتصاد الرقمي، 6(4)، 200-225

16.عبد الحميد، ياسر (2019). إدارة مخاطر تكنولوجيا المعلومات في المحاسبة المالية. *دار النهضة العربية،ص 22-72.*

17.عبد القادر، محمود (2019). أثر نظام الحماية الإلكتروني في الحد من مخاطر تكنولوجيا المعلومات والاتصال. *دراسة مقارنة لعينة من المؤسسات. مجلة الدراسات التقنية، 15(2)، 105-120.*

18.غالي، زينة؛ وحسين، عمر؛ ومحمد، علي (2024). تأثير حوكمة تكنولوجيا المعلومات في تقليل مخاطر نظم المعلومات المحاسبية السحابية. مجلة دراسات محاسبية و مالية) (JAFS، المؤتمر العلمي الدولي الثالث و الوطني الخامس، عدد خاص.
P-ISSN:1818-9431,E-ISSN:2617-984

19.كراز، شادي ايليا. (2021). دور حوكمة تكنولوجيا المعلومات في تعزيز أمن المعلومات. مجلة جامعة تشرين للبحوث والدراسات العلمية – سلسلة العلوم الاقتصادية والقانونية، المجلد43, العدد1.

19.مسعود، أحمد (2020). أمن المعلومات في نظم المحاسبة الإلكترونية. *دار النهضة العربية.*

20.مشتهي، صبري؛ وحمدان، علام؛ وشكر، طلال (2001). مدى موثوقية نظم المعلومات المحاسبية وأثرها في تحسين مؤشرات الأداء المصرف : دراسة مقارنة على المصارف الأردنية والفلسطينية المدرجة ببورصتي عمان والقدس. *مجلة دراسات العلوم الإدارية، 38(1)* .

ثانيا المراجع الاجنبية:

1.Abu Mahdi, S. T. (2017). The impact of the reliability of electronic accounting information systems on banking performance indicators, applied to public local banks in Palestine. *a master's thesis published at the Faculty of Commerce at the Islamic University, Gaza, Palestine.*

2.AICPA/CICA. (2002). Trust Services Principles and Criteria, Incorporating Systrust and Webtrust. American Institute of Certified Public Accountants, Retrived: 16 Oct 2016, from: (www.aicpa.org).

3.Al-Salahi, E. (2018). The Effectiveness of Electronic Audit in Assuring Confidence in Automated Accounting Information Systems. *Master Thesis, Al-Andalus University of Science and Technology, Republic of Yemen.*

4.Aven,T (2016) .risk and governance: Best practices for business continuity . *PricewaterhouseCoopers* ،P77.

5.Elshorbagy, Rana E.& Abu-Musa, Ahmad A.& El-Shishini, Hatem M.& Aladwey, Laila (2025). The Relationship between Information Technology Governance and Cloud Accounting Information Systems' Risks. Journal of Accounting Research. Volume 12, Issue 1. 2025 https://com.tanta.edu.eg/abj-journals.aspx. DOI:10.21608/abj.2025.418330

6.Hall, J. (2018). Accounting information systems. Cengage Learning.

7.Kshetri, N. (2017). Cybercrime and cyber-security issues. *Journal of Global Information Technology Management, 20(1), 105.*

8.Laudon,K.&Laudon,L .(2020). Management information systems: Managing the digital firm .*Pearson* ،, P35.

9.Mahdi, Zahraa (2021). IT Governance and Information Security of Accounting Information Systems: A Case Study. *Akkad Journal of Contemporary Accounting Studies, Vol. 1, No. 2, 2021, 75-93.*

10.NIST (2014) .Framework for Improving Critical Infrastructure Cybersecurity.,

11.NIST .(2020) .Artificial Intelligence Risk Management Framework.

12.Otim, M & O'Brien, J Campbell (2016) . Legal and regulatory risks in accounting information systems: A comparative study .*Journal of Accounting and Technology, 22(3), 132-145.*

13.Romney, M. & Steinbart, P. (2015). Accounting Information Systems, New Pearson Education, U.S.A.

14.Romney, M & Steinbart, P (2018). Accounting Information Systems (14th ed) ،Pearson ،Inc. ،UK. Sun ،P. (2020) ، "Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications ،Vol. 160 ،pp. 102642. doi:10.1016/j.jnca.2020.102642.*

15.Turban, E. Pollard, C. & Wood, G. (2018). Information technology for management: On-demand strategies for

performance, growth, and sustainability (11th ed.). Wiley.

16. Whitman & Mattord (2020). Principles of information security. Cengage Learning.

17. Weber,R17 (2019) . Information systems control and audit. Pearson.