مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الاقتصادية والقانونية المجلد (10) العدد (8) 2026
Tartous University Journal for Research and Scientific Studies -Economic and Legal Sciences Series Vol. (10) No. (8) 2026

أثر الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) في الحد من المخاطر السيبرانية
دراسة ميدانية في المؤسسات المالية المدرجة في سوق دمشق للأوراق المالية

د. سوران محمود جوني*

(تاريخ الإيداع 5/19 /2026 – تاريخ النشر 8/7/ 2026)

□ ملخّص □

هدف البحث إلى تحديد أثر الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) بمجالاته الخمسة في الحد من المخاطر السيبرانية في المؤسسات المالية المدرجة في سوق دمشق للأوراق المالية، إلى جانب تحديد مستوى الالتزام بهذه المجالات، والوقوف على طبيعة التهديدات الرقمية التي قد تواجه البيئة التشغيلية للمصارف وشركات التأمين محل الدراسة. ولتحقيق هذه الأهداف، اعتمد البحث على المنهج الوصفي التحليلي، حيث وُزِّعت الاستبانة على عينة قصدية من الكوادر القيادية والتخصصية (مدراء تكنولوجيا المعلومات CIOs، مدراء الأمن السيبراني CISOs، المدراء التنفيذيين، والمدققين الداخليين) بلغت (80) مفردة، استُرِدَّ منها (74) استبانة كاملة وصالحة للتحليل الإحصائي، وبنسبة استجابة بلغت (92.5%).

أظهرت النتائج أنّ المستوى العام لالتزام المؤسسات المالية محل الدراسة بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) جاء بمستوى متوسط، تصدره مجال التقييم والتوجيه والمراقبة وتذيله مجال البناء والاستحواذ والتنفيذ، في حين جاءت كفاءتها في الحد المخاطر السيبرانية بمستوى مرتفع رغم وجود ضعف نسبي في سرعة التعافي عند التعرض لهجمات حجب الخدمة (DDoS). كما أظهرت النتائج رفض الفرضية الرئيسة وقبول الفرضية البديلة؛ حيث تبيّن وجود أثر طردي ذي دلالة إحصائية لمبادئ حوكمة تكنولوجيا المعلومات يفسر ما نسبته (69.8%) من الحد من المخاطر السيبرانية، وتصدر مجال المراقبة والتقييم والتقدير المرتبة الأولى كأقوى المتغيرات تأثيراً في حماية البيئة التشغيلية الرقمية، يليه مجال التسليم والخدمة والدعم، ثم التقييم والتوجيه والمراقبة، وحلّ مجال البناء والاستحواذ والتنفيذ كأقل المجالات تأثيراً في النموذج المتعدد.

كلمات مفتاحية: حوكمة تكنولوجيا المعلومات، إطار (COBIT 2019)، المخاطر السيبراني، المؤسسات المالية، سوق دمشق للأوراق المالية.

* مدرّس، كلية العلوم الإدارية والمالية، جامعة قرطبة الخاصة، سورية.

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الاقتصادية والقانونية المجلد (10) العدد (8) 2026
Tartous University Journal for Research and Scientific Studies -Economic and Legal Sciences Series Vol. (10) No. (8) 2026

The Impact of Compliance with IT Governance Principles according to the COBIT 2019 Framework on Mitigating Cyber Risks
A Field Study on Financial Institutions Listed on the Damascus Securities Exchange

Dr. Souran Mahmoud Jouni *

(Received 19/5/2026.Accepted 8/7/2026)

□ABSTRACT □

This research aimed to determine the impact of compliance with IT governance principles, according to the COBIT 2019 framework across its five domains, on mitigating cyber risks in financial institutions listed on the Damascus Securities Exchange. Additionally, it sought to assess the level of compliance with these domains and identify the nature of digital threats facing the operational environment of the studied banks and insurance companies. To achieve these objectives, the study adopted a descriptive-analytical approach. A questionnaire was distributed to a purposive sample of executive and specialized personnel—including Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), executive managers, and internal auditors—totaling 80 respondents. Out of these, 74 fully completed questionnaires suitable for statistical analysis were retrieved, yielding a response rate of 92.5%.

The results showed that the overall level of compliance among the investigated financial institutions with the COBIT 2019 IT governance principles was moderate; the "Evaluate, Direct, and Monitor" domain ranked first, while the "Build, Acquire, and Implement" domain ranked last. Conversely, their efficiency in mitigating cyber risks was high, despite a relative weakness in recovery speed when exposed to Distributed Denial of Service (DDoS) attacks. Furthermore, the findings led to the rejection of the main null hypothesis and the acceptance of the alternative hypothesis; a statistically significant positive impact of IT governance principles was proven, explaining 69.8% of the variance in cyber risk mitigation. In the multiple regression model, the "Monitor, Evaluate, and Assess" domain emerged as the most influential variable in protecting the digital operational environment, followed by "Deliver, Service, and Support", then "Evaluate, Direct, and Monitor", while the "Build, Acquire, and Implement" domain had the least impact.

Keywords: IT Governance, COBIT 2019 Framework, Cyber Risks, Financial Institutions, Damascus Securities Exchange.

* Lecturer, Faculty of Administrative and Financial Sciences, Cordoba Private University, Syria.

1- المقدمة:

تُعدّ تكنولوجيا المعلومات والاتصالات العصب النابض للمؤسسات المالية المعاصرة، حيث أسهمت الطفرة الرقمية الهائلة والاعتماد المتسارع على قنوات الدفع الإلكتروني والخدمات المصرفية عبر الإنترنت في إعادة تشكيل ملامح القطاع المالي والمصرفي؛ إلا أنّ هذا التحول الرقمي المتسارع والاعتماد الكلي على الأنظمة التقنية المعقدة في تسيير المعاملات اليومية، واكبه نمو موازٍ ومقلق في حجم ونوعية التهديدات والمخاطر السيبرانية التي باتت تستهدف سرية البيانات المالية وسلامتها وإتاحتها بشكل مستمر. وضمن هذه البيئة الرقمية شديدة الحساسية والمحفوفة بالمخاطر، لم تعد الأساليب الرقابية والأمنية التقليدية كافية لتحصين القطاع المالي، مما فرض ضرورة تبني أطر عمل شمولية تضمن حوكمة وإدارة تكنولوجيا المعلومات بكفاءة واقتدار، ويبرز في طليعة هذه الأطر الدولية إطار (COBIT 2019) الصادر عن جمعية تدقيق ومراقبة نظم المعلومات (ISACA)، والذي يقدم منهجية متكاملة لربط الأهداف التقنية بالأهداف الاستراتيجية للمؤسسات مع تفعيل الرقابة على الموارد والعمليات. وتكتسب حوكمة التكنولوجيا أهمية بالغة في قطاع المال السوري، وتحديداً في المؤسسات المالية المدرجة في سوق دمشق للأوراق المالية، حيث تعمل هذه المؤسسات في ظل بيئة تشغيلية فريدة وتحديات استثنائية ترتبط بنقص الكفاءات البشرية والقيود الخارجية التي تصعّب أحياناً استقطاب أحدث البرمجيات الأمنية العالمية؛ الأمر الذي يجعل الامتثال الصارم لتعاميم مصرف سورية المركزي والالتزام بمجالات الحوكمة المتمثلة في التقييم والتوجيه، والمواءمة والتخطيط، وبناء النظم وتشغيلها ومراقبتها، هو الأداة المنهجية الأهم للحد من فرص اختراق النظم أو توقف الخدمات المالية الحيوية. وانطلاقاً من هذا الواقع، يأتي هذا البحث كدراسة ميدانية تسعى إلى سد الفجوة المعرفية والتطبيقية من خلال تحليل آراء نخبة من الخبراء التقنيين والماليين والمدققين في البيئة المصرفية السورية، للوقوف على الأثر الفعلي الذي يربط بين مستويات الالتزام بمبادئ ومجالات إطار حوكمة تكنولوجيا المعلومات (COBIT 2019) كمتغير مستقل، وقدرة هذه المؤسسات على الحد من المخاطر السيبرانية كمتغير تابع.

1-1- الدراسات السابقة:

1- الدراسات العربية:

- دراسة علي (2024)، بعنوان: مدى الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفقاً لإطار COBIT 2019: دراسة حالة جهاز تنفيذ وإدارة مشروع النهر الصناعي فرع بنغازي.

هدفت الدراسة إلى تقييم مدى التزام جهاز تنفيذ وإدارة مشروع النهر الصناعي (بنغازي) بتطبيق حوكمة تكنولوجيا المعلومات وفقًا لإطار COBIT 2019 بمجالاته الخمسة الرئيسة. ولتحقيق ذلك، اعتمدت الدراسة على المنهج المختلط عبر أسلوب المسح الشامل لمجتمع الدراسة المكون من (53) متخصصاً من المحاسبين والمراجعين وخبراء التكنولوجيا، حيث جُمعت البيانات بواسطة الاستبانات والمقابلات المدعمة لها. وقد أظهرت النتائج موافقة المشاركين على التزام الجهاز بتطبيق أغلب مجالات الحوكمة؛ ففي حين برز التزام واضح في تحديد الخدمات والضوابط التقنية (رغم القصور في تبني المبادئ العامة للحوكمة)، أثبتت الدراسة نجاح الجهاز في المواءمة والتخطيط لتحقيق التناغم الاستراتيجي وضمان جودة الخدمات، كما بينت النتائج كفاءة الجهاز في إدارة الأصول والبرمجيات وتحديث النظم، إلى جانب تميزه في الاستجابة السريعة للمشكلات التقنية وحماية البنية التحتية وخطوط المياه من التلف. وأخيراً، أكدت الدراسة التزام الجهاز بالمراقبة والتقييم عبر تعزيز الشفافية وتحديد المعوقات التي تحول دون التبني الكامل للتكنولوجيا.

2- دراسة صالح وآخرون (2024)، بعنوان: أثر استخدام تقنية حوكمة تكنولوجيا المعلومات COBIT 5 في تحسين جودة التقارير المالية في الشركات الناشئة: دراسة تطبيقية.

هدفت الدراسة إلى التعرف على أثر تطبيق إطار حوكمة تكنولوجيا المعلومات (COBIT 5) في تحسين جودة التقارير المالية بالشركات الناشئة. ولتحقيق هذا الهدف، تم تحليل أثر مجالات الإطار الأربعة المتمثلة في: (التخطيط والتنظيم، الامتلاك والتنفيذ، الدعم والتوصيل، بالإضافة إلى المتابعة والتقييم) على الخصائص النوعية للمعلومات المحاسبية (الموثوقية والملاءمة). ولغرض جمع البيانات الأولية، تمّ تصمم استبانة، حيث بلغت العينة الفعلية التي اعتمدت عليها الباحثة لتمثيل مجتمع الدراسة تمثيلاً صادقاً (391) مشاهدة، شملت الاستبيانات المستردة والصالحة للتحليل الإحصائي. خلصت النتائج إلى وجود أثر إيجابي ذي دلالة معنوية لمجالات حوكمة تكنولوجيا المعلومات وفقاً لإطار (COBIT 5) على خاصية الموثوقية كإحدى الخصائص النوعية للمعلومات المحاسبية، فضلاً عن وجود أثر إيجابي ومعنوي مماثل لتلك المجالات على خاصية الملاءمة.

3- دراسة الفار (2024)، بعنوان: أثر حوكمة تكنولوجيا المعلومات وفقاً لأبعاد إطار COBIT 2019 على جودة الإفصاح عن معلومات تقارير نظام إدارة المعلومات المالية الحكومية.

استهدفت الدراسة بيان أثر حوكمة تكنولوجيا المعلومات وفقاً لإطار (COBIT 2019) على جودة الإفصاح في تقارير نظام إدارة المعلومات المالية الحكومية (GFMIS). وباعتماد المنهج الوصفي التحليلي، جُمعت البيانات ميدانياً عبر استبانة وُزعت على (195) فرداً من ممثلي وزارة المالية، ومراجعي الجهاز المركزي للمحاسبات، وأكاديميّين. وقد أظهرت النتائج أن نظام (GFMIS) يحقق مزايا استراتيجية هامة تدعم التحول الرقمي ورؤية مصر 2030، مثل رفع كفاءة الموارد وإحكام الرقابة؛ ورغم اتفاق المشاركين على وجود تحديات تواجه تطبيقه كضعف البنية التحتية وقصور التأهيل ونظم الرقابة الداخلية؛ إلا أن النتائج أكدت أن تطبيق مجالات إطار (COBIT 2019) الخمسة يمثل حلاً جوهرياً للتغلب عليها، ويسهم مباشرة في تحسين جودة التقارير المالية من خلال ضمان الخصائص النوعية للمعلومات المحاسبية، مما يدعم اتخاذ القرارات بصورة سليمة.

4- دراسة راجح وسلام (2025)، بعنوان: دور حوكمة تكنولوجيا المعلومات وفق إطار COBIT 5 في الحد من مخاطر المحاسبة السحابية: دراسة ميدانية على مجموعة هائل سعيد أنعم وشركاه.

هدفت الدراسة إلى بيان دور حوكمة تكنولوجيا المعلومات وفق إطار (COBIT) بأبعادها (التخطيط والتنظيم، الاكتساب والتنفيذ، الدعم والتوصيل، التوجيه والرقابة، المتابعة والتقييم) في الحد من مخاطر المحاسبة السحابية في شركات مجموعة هائل سعيد أنعم وشركاه، واعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبانة لجمع البيانات، ووزعت (161) استمارة على العاملين في شركات المجموعة. وتوصلت الدراسة إلى عدد من النتائج أهمها: أنّ مستوى ممارسة حوكمة تكنولوجيا المعلومات بأبعاده في شركات المجموعة كان عالٍ، وأن هذا المستوى المرتفع كان له دور في الحد من مخاطر المحاسبة السحابية التي تمارسها.

2- الدراسات الأجنبية:

1- دراسة (Haouam,, 2020) بعنوان.

IT governance impact on financial reporting quality using COBIT framework.

تأثير حوكمة تكنولوجيا المعلومات على جودة التقارير المالية باستخدام إطار عمل COBIT.

هدفت الدراسة إلى توضيح أثر تطبيق حوكمة تكنولوجيا المعلومات وفقاً لأبعاد إطار (COBIT) الأربعة الرئيسة المتمثلة في: (التخطيط والتنظيم، الامتلاك والتنفيذ، الدعم والتوصيل، بالإضافة إلى المتابعة والتقييم). كما سعت الدراسة إلى قياس هذا الأثر على جودة التقارير المالية المقدمة للعملاء من خلال مدى توافر الخصائص

النوعية الرئيسة والفرعية للمعلومات اللازمة لإعدادها، بما يضمن تقديم تقارير تتميز بالدقة والنزاهة والموثوقية. وقد توصلت الدراسة في نتائجها إلى وجود علاقة ارتباطية إيجابية وذات دلالة بين أبعاد إطار عمل (COBIT) الأربعة وبين خصائص الجودة في التقارير المالية.

2- دراسة (Sherly & Fianty, 2024) بعنوان.

Enhancing Financial Technology Operations: A Comprehensive Evaluation Using COBIT 2019 Framework.

تعزيز عمليات التكنولوجيا المالية: تقييم شامل باستخدام إطار عمل COBIT 2019.

هدفت الدراسة إلى تعزيز حوكمة تكنولوجيا المعلومات في شركة التكنولوجيا المالية Fintech بإندونيسيا، وذلك في ظل التحديات الرئيسية التي تواجهها الشركة وغياب الشفافية فيها، حيث سعت الدراسة إلى مواجهة هذه التحديات والحد منها من خلال الاعتماد على إطار العمل العالمي COBIT 2019 وللوصول إلى هذا الهدف وتحقيقه، اعتمدت الدراسة ميدانياً على إجراء مقابلات مكثفة مع المختصين في مجال التكنولوجيا بالشركة. وقد تمثلت أهم نتائج الدراسة في إظهار احتياج الشركة الفعلي إلى مزيد من التحسينات الاستراتيجية في مجال تكنولوجيا المعلومات، وخاصة في الجوانب المتعلقة بتصميم النظام، وتعزيز القدرات والامكانيات من خلال التقييم الاستباقي، بالإضافة إلى تحسين خطط الأمان، وتطوير استراتيجيات فعالة للحصول على حلول وتقنيات تكون أكثر تكيفاً مع التكنولوجيا المطبقة حالياً وصولاً إلى تشكيل بيئة تشغيلية متكاملة تتميز بكونها أكثر فعالية وشفافية في شركات التكنولوجيا المالية.

1-2 تعقيب على الدراسات السابقة:

تتشابه الدراسة الحالية مع الدراسات السابقة في استخدام إطار الحوكمة (COBIT) مع دراسة علي (2024)، والفار (2024)، و(Sherly & Fianty, 2024) في تطبيق الإصدار الحديث (COBIT 2019) بمجالاته الخمسة، بينما تختلف مع دراسة صالح وآخرون (2024)، وراجح وسلام (2025)، و(Haouam, 2020) في تبنيها للإصدار الأقدم (COBIT 5) القائم على أربعة مجالات. وتبرز نقطة الاختلاف الأخرى في طبيعة المتغير التابع؛ إذ ركزت دراسات كل من صالح وآخرون (2024)، والفار (2024)، و(Haouam, 2020) على جودة التقارير المالية والإفصاح المحاسبي، وتناولت دراسة علي (2024) حوكمة قطاع المياه، وتطرقت دراسة راجح وسلام (2025) لمخاطر المحاسبة السحابية، في حين اهتمت دراسة (Sherly & Fianty, 2024) بالشفافية؛ لتتميز الدراسة الحالية بإسقاط إطار (COBIT 2019) على الحد من المخاطر السيبرانية في المؤسسات المالية (المصارف وشركات التأمين) المدرجة في سوق دمشق للأوراق المالية.

1-3 مشكلة البحث:

تتمثل مشكلة البحث من خلال الدراسة الاستطلاعية التي قامت بها الباحثة، والتي شملت ثلاثاً من المؤسسات المالية المدرجة في سوق دمشق للأوراق المالية (بنك بيمو السعودي الفرنسي، بنك البركة سورية، وشركة العقيلة للتأمين التكافلي)؛ حيث أجرت الباحثة مجموعة من المقابلات مع (15) خبيراً من الكوادر العليا المتخصصة الموزعين بين مدراء تكنولوجيا المعلومات (CIOs)، ومدراء الأمن السيبراني (CISOs)، ومدققي النظم والمراقبين الداخليين. وقد تمّ توجيه مجموعة من الأسئلة حول تطبيق مجالات إطار (COBIT 2019) ومدى انعكاسها على الحد من المخاطر السيبرانية في ظل الظروف الحالية؛ وحيث سُئل الخبراء في التساؤل الأول عن مدى خضوع نظم المعلومات بالمؤسسة لعمليات تدقيق تقني مستمر يضمن التوافق مع ضوابط حوكمة التكنولوجيا والتعاميم الصادرة عن مصرف سورية المركزي، أبدى (86.67%) من المستجوبين موافقة مرتفعة، مؤكدين أنّ الرقابة والامتثال للتشريعات المحلية هما المحرك الأساسي

والأقوى لضبط النظم التقنية وتجنب المخالفات القانونية والتنظيمية. وفي السياق ذاته، وعند سؤالهم عما إذا كانت المؤسسة تمتلك سياسات صارمة لإدارة صلاحيات الوصول وحفظ النسخ الاحتياطية للبيانات المالية بشكل يحميها من التهديدات السيبرانية اليومية، أكد (80%) من الخبراء وجود التزام مؤسسي مصرفي صارم جداً بآليات منح الصلاحيات وحفظ النسخ الاحتياطية، باعتبارها خط الدفاع الفوري الأول لحماية أموال المودعين وسجلات المعاملات المالية. وعلى النقيض من هذا الالتزام الرقابي والتشغيلي المرتفع، كشفت المقابلات عن فجوات تطبيقية حقيقية فرضتها البيئة المحلية؛ فعند سؤال المشاركين حول مدى توفر الميزانيات والاعتمادات المالية الكافية والمستمرة لتغطية متطلبات حوكمة الأنظمة وتطوير البنية الأمنية، أفاد (60%) منهم بوجود تحفظ تجاه كفاية التمويل، معللين ذلك بالضغوط الاقتصادية الحالية وتقلبات تكاليف التشغيل التي تؤثر سلباً على رصد ميزانيات كافية للمشاريع التقنية طويلة الأجل. كما امتدت هذه التحديات لتشمل الجانب البشري والمعرفي، حيث أشار (73.33%) من المستجوبين (بإجابات تراوحت بين المحايدة والسلبية) إلى وجود تحدٍ حقيقي يتعلق بنقص الكوادر التخصصية الناتجة عن تسرب وهجرة الكفاءات التقنية، فضلاً عن ضعف برامج نشر الوعي الأمني المستمر بين الموظفين الإداريين غير التقنيين. وفي تساؤلٍ آخر حول مدى توفر القدرة التكنولوجية الكاملة لاستقطاب برمجيات أصلية حديثة تضمن الرصد المبكر والتعافي السريع من الهجمات السيبرانية المتقدمة (مثل هجمات حجب الخدمة DDoS)، تبين أن (66.67%) من الإجابات جاءت في نطاق المحايد، حيث أجمع الخبراء على أن القيود الخارجية والعقوبات المفروضة تفرض عقبات لوجستية بالغة الصعوبة أمام الاستحواذ على أحدث أنظمة الحماية والتحديثات الأمنية العالمية، مما يحد من الأثر الفعلي لمرحلة التخطيط والبناء المستقل ويجعل التركيز منصباً على آليات الرقابة الخلفية والدعم اليومي المتاح. وبناءً على هذه الفجوة التي كشفت عنها الدراسة الاستطلاعية بين التزام المؤسسات المالية الدفتري والرقابي بالتشريعات، وبين التحديات التشغيلية واللوجستية التي تواجهها في بيئتها التكنولوجية والبشرية للحد من التهديدات، يمكن تحديد مشكلة البحث في التساؤل الرئيس الآتي: **ما أثر الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) في الحد من المخاطر السيبرانية في المؤسسات المالية المدرجة في سوق دمشق للأوراق المالية؟**

1-4 أهداف البحث:

هدف البحث إلى تحديد أثر الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة، ويتفرع عن هذا الهدف الأهداف الفرعية الآتية:

1- تحديد مستوى التزام المؤسسات المالية محل الدراسة بتطبيق مجالات حوكمة تكنولوجيا المعلومات الخمسة المعتمدة في إطار COBIT 2019 من وجهة نظر العينة المستهدفة.

2- تحديد حجم المخاطر السيبرانية والتهديدات الرقمية التي قد تواجه البيئة التشغيلية للمصارف والشركات المالية المدرجة في سوق دمشق للأوراق المالية.

3- دراسة أثر الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) في الحد من التهديدات السيبرانية في المؤسسات المالية محل الدراسة.

1-5 أهمية البحث:

تكمن الأهمية النظرية لهذا البحث في إثراء الأدبيات الأكاديمية والمكتبة العربية بمضمون علمي حديث يربط بين إطار حوكمة تكنولوجيا المعلومات (COBIT 2019) وإدارة المخاطر السيبرانية في القطاع المالي السوري. أما الأهمية العملية فتتمثل في تقديم مؤشرات عملية لمدراء التكنولوجيا والأمن السيبراني والمراقبين في سوق دمشق للأوراق المالية تبيّن مواطن القوة والضعف في بيئاتهم الرقمية، إلى جانب رفد الجهات الإشرافية والتنظيمية كمصرف سورية المركزي بتوصيات قد تسهم في صياغة سياسات حمائية ترفع كفاءة الحوكمة الفعلية وتدعم استقرار النظام المالي وتحصينه ضد الهجمات الرقمية المتجددة.

1-6فرضيات البحث:

الفرضية الرئيسة للبحث: لا يوجد أثر ذو دلالة إحصائية للالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

ويتفرع عن هذه الفرضية الفرضيات الفرعية الآتية:

1- لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال التقييم والتوجيه والمراقبة في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

2- لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال المواءمة والتخطيط والتنظيم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

3- لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال البناء والاستحواذ والتنفيذ في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

4- لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال التسليم والخدمة والدعم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

5- لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال المراقبة والتقييم والتقدير في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

1-7 منهجية البحث:

لتحقيق أهداف البحث اعتمدت الباحثة على المنهج الوصفي التحليلي، وشمل مجتمع البحث جميع المؤسسات المالية المدرجة في سوق دمشق للأوراق المالية (المصارف الخاصة الإسلامية والتقليدية، بالإضافة إلى شركات التأمين)، ونظراً لأن مجتمع الدراسة صغير تمّ استخدام أسلوب الحصر الشامل للمؤسسات المالية وتمّ استهداف عينة قصدية شملت (مدراء تكنولوجيا المعلومات CIO، مدراء الأمن السيبراني/أمن المعلومات CISO، المدراء التنفيذيين، والمراقبين الداخليين/المدققين)، وقد بلغت (80) مفردة تمّ توزيع الاستبانة أداة البحث عليهم، وتمّ استرجاع (74) استبانة كاملة وصالحة للتحليل الإحصائي وبنسبة استجابة بلغت (92.5%).

لتحقيق أهداف البحث اعتمدت الباحثة الاستبانة كأداة لجمع المعلومات، حيث تمّ تصميمها من قبل الباحثة، وقد تضمنت الاستبانة جزأين: الجزء الأول: مبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019): التقييم والتوجيه والمراقبة، المواءمة والتخطيط والتنظيم، البناء والاستحواذ والتنفيذ، التسليم والخدمة والدعم، المراقبة والتقييم والتقدير. أما الجزء الثاني فيتمثل بالمخاطر السيبرانية والتهديدات الرقمية التي قد تواجه البيئة التشغيلية في المؤسسات المالية محل الدراسة. وقد توزعت عبارات الاستبانة على (48) عبارة. تمّ تحكيم هذه الاستبانة من قبل عدد من السادة أعضاء الهيئة التدريسية في كلية الاقتصاد، وذلك من أجل التأكد من صدقها، حيث أجمع السادة المحكمين على كفاية

بنود الاستبانة وصلاحيتها لقياس ما وضعت لقياسه، بينما كان لديهم ملحوظات تتعلق بصياغة بعض البنود، حيث أجري التعديل المناسب في ضوء هذه الملاحظات. تمّ التأكد من ثبات الاستبانة باستخدام معادلة كرونباخ ألفا، حيث بلغت قيمة معامل الثبات الكلي للاستبانة (0.884)، أما بالنسبة لكل محور من محاور الاستبانة فكانت قيمة معامل ثبات ألفا كرونباخ وفق الآتي: (مجال التقييم والتوجيه والمراقبة 0.808، مجال المواءمة والتخطيط والتنظيم 0.811، مجال البناء والاستحواذ والتنفيذ 0.787، مجال التسليم والخدمة والدعم 0.823، مجال المراقبة والتقييم والتقدير 0.769، محور المخاطر السيبرانية 0.857)، وتدل هذه القيم على ثبات الاستبانة وصلاحياتها للقياس. تمّ الاعتماد على مقياس ليكرت الخماسي في الإجابة عن بنود الاستبانة، وتمّ استخدام برنامج الرزمة الإحصائية للعلوم الاجتماعية SPSS.25 في تفريغ البيانات، كما تمّ استخدام مجموعة من الأساليب الإحصائية تمثلت بـ: المتوسط الحسابي، الانحراف المعياري، الأهمية النسبية، معامل الاختلاف، اختبار (t) لعينة واحدة، الانحدار الخطي البسيط والمتعدد.

2-الإطار النظري للبحث:

1- مفهوم حوكمة تكنولوجيا المعلومات: إن توفير الحماية الشاملة لنظم تكنولوجيا المعلومات، وتحصين مخرجاتها من البيانات والمعلومات، يستدعي بالضرورة البحث عن الآليات والإجراءات الكفيلة بتحقيق الإدارة الفعالة لهذه الأنظمة؛ وهو ما ألزم الباحثين بالعمل المستمر لإيجاد ضوابط رقابية تضمن تعظيم المنافع المتوخاة من التقنيات الحديثة. وفي هذا الصدد، قدّم الباحثون العديد من التعريفات لحوكمة تكنولوجيا المعلومات؛ حيث عُرّفت بأنها: مجموعة من الاستراتيجيات، والسياسات، والأهداف، والإجراءات، والمسؤوليات التي تُناط بصناع القرار والمديرين في الشركات، لإدارة تكنولوجيا المعلومات والرقابة عليها، بغية تحقيق المنفعة القصوى من المعلومات والتكنولوجيا المتعلقة بها (نصور، 2015، ص56). كما عُرّفت الحوكمة أيضاً بأنها: تطور أفقي لحوكمة الشركات في ظل تكنولوجيا المعلومات، يعمل على توضيح الإجراءات والسياسات، وتحديد مسؤولية ورقابة الاستخدامات الحالية والمستقبلية للتقنية، من أجل رصد نواحي القصور -إن وُجدت- وتحديد الطرق الكفيلة بمعالجتها؛ مما يضيف قيمة حقيقية للمنشأة عبر موازنة المخاطر بعوائد التكنولوجيا، وربطها بالأهداف الاستراتيجية لضمان أمن وجودة المعلومات المحاسبية على نحو ملائم (العازمي، 2022، ص1127).

وترى الباحثة أنّ حوكمة تكنولوجيا المعلومات لا تقتصر على كونها مجرد حزمة من الإجراءات والضوابط التقنية الجامدة، بل هي فلسفة إدارية ورقابية متكاملة تهدف إلى صياغة بيئة رقمية آمنة توازن بين الفرص والمخاطر؛ وهي تكتسب أهمية بالغة في بيئة الأعمال المعاصرة لضمان المواءمة الاستراتيجية بين البنية التكنولوجية والأهداف التنظيمية، مما يحصّن أصول المنشأة ويدعم موثوقية تقاريرها المالية.

2- مفهوم إطار (COBIT): يُعد إطار عمل الأهداف الرقابية للمعلومات والتكنولوجيا المصاحبة لها (COBIT) من التطورات الجوهرية الهامة في مجال حوكمة تكنولوجيا المعلومات؛ إذ يهدف هذا الإطار إلى تحديد أفضل ممارسات الحوكمة والإدارة للأنظمة الإلكترونية، مع التأكيد على المواءمة الاستراتيجية بين أهداف تكنولوجيا المعلومات المطبقة في المنظمات والأهداف العامة لتلك المنظمات (الحسناوي والموسوي، 2017، ص6). وقد عُرّف إطار (COBIT) بأنه: إطار عمل ووسيلة قياسية تُستخدم للسيطرة والرقابة على تكنولوجيا المعلومات، ويساعد المدققين والمديرين والمستخدمين على فهم الأنظمة التقنية المطبقة في منظماتهم، كما يرشدهم نحو اختيار أفضل مستويات الأمان، وتطوير نموذج الحوكمة، واتباع أساليب الرقابة الفعالة لحماية موجودات

منظماتهم بكفاءة واقتدار" (نصور، 2015، ص70). أما من حيث النشأة والتطور التاريخي، فقد طُوِّر هذا الإطار في الولايات المتحدة الأمريكية من قِبل جمعية تدقيق ومراقبة نظم المعلومات (ISACA)، ويُمثّل المصطلح اختصاراً لـ (Control Objectives for Information and Related Technologies). ويحدد الإطار في بنيته التقليدية أربعة وثلاثين هدفاً عالي المستوى للرقابة على العمليات التقنية، فضلاً عن توفيره معياراً قياسياً قابلاً للتطبيق لضمان أمن التكنولوجيا، ودعم احتياجات الإدارة في متابعة وتحديد المستويات المطلوبة لتأمين البيانات ونظم المعلومات. وقد ظهر إطار (COBIT) لأول مرة في حقبة التسعينات من القرن الماضي، حيث صدرت النسخة الأولى منه عام 1996، تلتها النسخة الثانية عام 1998، ثم النسخة الثالثة عام 2002. واستمرت حركة التطوير والتحديث لمواكبة طفرة الحوكمة الرقمية، وصولاً إلى إطلاق الإصدار الخامس من هذا الإطار (COBIT 5) في عام 2012 (عوض، 2016، ص25).

وترى الباحثة أن إطار (COBIT) يُمثّل لغة القياس والمعيارية الأنجح عالمياً لتحويل المفاهيم النظرية للحوكمة الرقمية إلى ممارسات تشغيلية قابلة للتطبيق والتقييم؛ حيث تجاوزت أهميته مجرد كونه أداة لتدقيق تكنولوجيا المعلومات، ليصبح مظلة استراتيجية متكاملة تمنح الإدارات العليا والمدققين القدرة على الفهم الشامل للمخاطر التقنية، وضمان السيطرة الفعالة عليها بما يتوافق مع متطلبات الأمان والمواءمة المؤسسية.

3- دور إطار COBIT 2019 في حوكمة وإدارة المخاطر السيبرانية: يُمثّل إطار عمل (COBIT 2019) أداة استراتيجية تمكّن المؤسسات من إدارة التهديدات السيبرانية بكفاءة؛ حيث لا تقتصر فاعليته على الضوابط التقنية الإجرائية، بل يمتد ليوفر نموذجاً متكاملاً يدمج الأمن الرقمي في صياغة القرارات التنظيمية والخطط بعيدة المدى للمؤسسة (Smith & Jones, 2021, P345-367). وتنبع كفاءة هذا الإطار من مبادئه الأساسية التي تركز على تعظيم قيمة المؤسسة ومصالح أصحاب المصلحة، من خلال تأمين الأصول المعلوماتية ضد الاختراقات التي قد تسفر عن خسائر مالية أو أضرار بالسمعة المؤسسية (ISACA, 2018). ومن أجل معالجة الفجوات الهيكلية، يتبنى الإطار مدخلاً شمولياً يحوّل الأمن السيبراني من وظيفة محصورة في قسم تكنولوجيا المعلومات إلى مسؤولية تضامنية تشمل جميع المستويات الإدارية؛ بدءاً من الموظفين التنفيذيين وحتى مجلس الإدارة. ويعتمد هذا المدخل على نظام حوكمة ديناميكي يتسم بالمرونة والقدرة على الاستجابة للتهديدات المتطورة والتقنيات الناشئة (ISACA, 2020). وتحقيقاً لفاعلية المساءلة، يضع الإطار فصلاً تنظيماً واضحاً بين الحوكمة المعنية برسم السياسات العامة وتحديد مستوى المخاطر المقبول، والإدارة المنوط بها تنفيذ تلك السياسات وتشغيلها (ISACA, 2018). ومن الناحية التطبيقية، يُترجم الإطار هذه المبادئ إلى أهداف تشغيلية محددة تضمن بناء بيئة أمنية متماسكة؛ حيث يركز الهدف (EDM03) على موازنة المخاطر وضمان إبقائها ضمن الحدود المعتمدة، بينما يتولى الهدف (APO12) الفحص الدوري والتقييم المستمر للمخاطر التقنية لضمان استمرارية الأعمال. ولضمان عدم نشوء ثغرات أمنية ناتجة عن التحديثات العشوائية، يتدخل الهدف (BAI06) لإدارة التغييرات في الأنظمة البرمجية بأسلوب مقنن وآمن (ISACA, 2018). وفي جانب الحماية المباشرة، يبرز الهدف (DSS05) ليتولى إدارة الهويات الرقمية، وتشفير البيانات الحساسة، وحماية أمن الشبكات، بالتكامل مع الهدف (MEA02) الذي يعمل كأداة رقابية لقياس مستوى الأداء الأمني ومدى الامتثال للمعايير وتحديد مجالات التحسين المستمر (ISACA, 2020). ولضمان تلبية المتطلبات الخاصة لكل منشأة، يوفر الإطار ميزة تنظيمية تُعرف بعوامل التصميم، والتي تسمح بتخصيص نظام الحوكمة ليلائم طبيعة عمل المؤسسة؛ فالمؤسسات ذات الحساسية العالية كالمصارف يمكنها الاستناد إلى ملف المخاطر الخاص بها لتطبيق بروتوكولات حماية صارمة تتناسب مع حجم التهديدات التي تواجهها (World Economic Forum, 2022). وتساعد هذه المرونة في توجيه الموارد المالية والدفاعية لصد هجمات نوعية محددة مثل برمجيات

الفدية وسرقة البيانات، فضلاً عن تمكين المؤسسة من التوافق التام مع التشريعات القانونية الصارمة وقوانين حماية البيانات العالمية، مما يجنبها الغرامات المالية والمساءلات القضائية، ويضمن لها استقراراً تشغيلياً مستداماً (Smith & Jones, 2021, P345-367). وترى الباحثة أن القيمة الحقيقية لإطار (COBIT 2019) تكمن في قدرته على تحويل الأمن السيبراني من مجرد عبء تقني مالي إلى ميزّة تنافسية واستراتيجية؛ فمن خلال مرونة عوامل التصميم والفصل الحازم بين الأدوار الرقابية والتنفيذية، يمنح الإطار المؤسسات المالية مظلة وقائية ديناميكية تمكنها من التنبؤ الذكي بالمخاطر وتخصيص مواردها الدفاعية بكفاءة، مما يضمن استمرارية أعمالها التشغيلية والامتثال الصارم للتشريعات المنظمة في بيئة رقمية شديدة التعقيد.

3- النتائج والمناقشة:

1- تحديد مستوى التزام المؤسسات المالية محل الدراسة بمبادئ حوكمة تكنولوجيا المعلومات الخمسة المعتمدة في إطار COBIT 2019 من وجهة نظر العينة المستهدفة:

الجدول (1) الإحصاءات الوصفية لمستوى التزام المؤسسات المالية بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار COBIT 2019

الرقم	العبارات	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية%	معامل الاختلاف%	Test Value = 3		
						مؤشر tالاختبار	احتمال الدلالة	القرار
1	يحرص مجلس الإدارة على مواءمة استراتيجية تكنولوجيا المعلومات مع الأهداف الاستراتيجية العامة للمؤسسة المالية.	3.82	0.615	76.4	16.1	11.469	.000	دال
2	توجد سياسات واضحة ومعتمدة من الإدارة العليا تحدد المسؤوليات والصلاحيات المتعلقة بالأنظمة التقنية.	3.75	0.640	75	17.1	10.080	.000	دال
3	يشارك مجلس الإدارة بانتظام في تقييم العوائد والمخاطر الناتجة عن الاستثمارات التكنولوجية للمؤسسة.	3.20	0.742	64	23.2	2.319	.000	دال
4	توفر الإدارة العليا التمويل والموارد الكافية لتطبيق متطلبات الحوكمة الرقمية.	2.75	0.785	55	28.5	-2.739	.000	دال
5	توجد آليات واضحة لمراقبة أداء تكنولوجيا المعلومات ورفع التقارير الدورية للإدارة العليا.	3.42	0.690	68.4	20.2	5.236	.000	دال
6	تلتزم الإدارة العليا بالتعليمات والضوابط الصادرة عن مصرف سورية المركزي وهيئة الأوراق المالية السورية بخصوص حوكمة التكنولوجيا.	3.90	0.580	78	14.9	13.348	.000	دال

7	يتم دمج متطلبات الأمن السيبراني في التوجهات الاستراتيجية الكبرى للمؤسسة المالية.	3.48	0.672	69.6	19.3	6.144	.000	دال
8	تقوم الإدارة العليا بمراجعة دورية لمدى كفاءة نظام حوكمة التكنولوجيا المطبق وتوجيه مسارات تعديله.	3.25	0.730	65	22.5	2.946	.000	دال
مجال التقييم والتوجيه والمراقبة		3.45	0.682	68.9	19.8	5.631	.000	دال
9	تمتلك المؤسسة المالية هيكلاً تنظيمياً واضحاً ومحدد الأدوار لإدارة تكنولوجيا المعلومات.	3.85	0.610	77	15.8	11.986	.000	دال
10	يتم تحديث استراتيجية تكنولوجيا المعلومات بشكل مستمر لتواكب التغيرات المتسارعة في بيئة الأعمال المصرفية.	3.18	0.755	63.6	23.7	2.051	.000	دال
11	توجد عمليات رسمية ومستمرة لتحديد وتقييم المخاطر المرتبطة بتكنولوجيا المعلومات.	3.35	0.712	67	21.3	4.229	.000	دال
12	تولي المؤسسة اهتماماً كافياً لنشر ثقافة الوعي الأمني والتكنولوجي بين جميع الموظفين.	2.77	0.792	55.4	28.6	-2.498	.000	دال
13	توجد معايير واضحة لاختيار الكفاءات البشرية وتأهيلها في قسم تكنولوجيا المعلومات والأمن السيبراني.	2.78	0.780	55.6	28.1	-2.426	.000	دال
14	يتم إدارة جودة البيانات والأنظمة وفق سياسات وإجراءات موثقة ومعلنة.	3.38	0.685	67.6	20.3	4.772	.000	دال
15	تؤخذ متطلبات الابتكار والتحول الرقمي (كالدفع الإلكتروني) بعين الاعتبار عند تخطيط البنية التكنولوجية.	3.22	0.720	64.4	22.4	2.628	.000	دال
16	يوجد تنسيق وتواصل فعال بين إدارة المخاطر العامة وإدارة تكنولوجيا المعلومات في المؤسسة.	3.55	0.650	71	18.3	7.279	.000	دال
مجال المواءمة والتخطيط والتنظيم		3.26	0.713	65.2	21.9	3.137	.000	دال
17	تتبع المؤسسة منهجية معتمدة ورصينة عند شراء أو تطوير الأنظمة البرمجية والتطبيقات المالية.	3.48	0.660	69.6	19.0	6.256	.000	دال

18	يتم فحص واختبار الأنظمة والبرمجيات الجديدة للتأكد من خلوها من الثغرات قبل تشغيلها الفعلي.	3.27	0.764	65.4	23.4	3.040	.000	دال
19	توجد إجراءات صارمة لإدارة التغييرات على الأنظمة لتجنب أي ثغرات طارئة.	3.25	0.738	65	22.7	2.914	.000	دال
20	يتم توثيق كافة العمليات والبرمجيات والأنظمة وتحديث أدلة التشغيل الخاصة بها بشكل مستمر.	3.60	0.642	72	17.8	8.039	.000	دال
21	تراعي المؤسسة دمج ضوابط الأمان والتشفير ضمن مواصفات الأنظمة التقنية المستحوذ عليها.	3.30	0.710	66	21.5	3.635	.000	دال
22	تلتزم المؤسسة بجدول زمني وميزانيات محددة عند تنفيذ المشروعات التقنية الجديدة.	2.71	0.796	54.2	29.4	-3.134	.000	دال
23	يتم تقديم التدريب الكافي للموظفين والمستخدمين على أي نظام تقني جديد قبل اعتماده.	3.22	0.744	64.4	23.1	2.544	.000	دال
24	يتم مراجعة وتقييم كفاءة الأنظمة والحلول التقنية بعد فترة وجيزة من تنفيذها الفعلي.	3.18	0.725	63.6	22.8	2.136	.000	دال
	مجال البناء والاستحواذ والتنفيذ	3.25	0.722	65.0	22.2	2.992	.000	دال
25	تقدم إدارة التكنولوجيا خدمات الدعم الفني للمستخدمين والعملاء بمستويات جودة وموثوقية عالية.	3.32	0.695	66.4	20.9	3.961	.000	دال
26	يتم التعامل مع الأعطال والمشكلات التقنية وحلها بناءً على نظام أولويات وإجراءات موثقة.	3.28	0.710	65.6	21.6	3.392	.000	دال
27	تطبق المؤسسة سياسات صارمة لإدارة صلاحيات الوصول إلى البيانات والأنظمة الحساسة.	3.78	0.612	75.6	16.2	10.963	.000	دال
28	توجد خطط طوارئ مفعّلة وبدائل تقنية لضمان استمرارية الأعمال في حال الكوارث.	3.24	0.760	64.8	23.5	2.716	.000	دال
29	يتم الاحتفاظ بنسخ احتياطية من البيانات المالية والمصرفية بشكل دوري واختبار استرجاعها بانتظام.	3.88	0.590	77.6	15.2	12.830	.000	دال

30	يتم تشغيل وإدارة العمليات اليومية لتكنولوجيا المعلومات بما يمنع التداخل أو إساءة استخدام الصلاحيات.	3.45	0.664	69	19.2	5.830	.000	دال
31	تخضع الأجهزة الشخصية وشبكات الاتصال الداخلية في المؤسسة لرقابة وحماية مستمرة.	3.24	0.722	64.8	22.3	2.859	.000	دال
32	يتم تدريب موظفي الدعم الفني على كيفية رصد المؤشرات الأولية للهجمات أو الاختراقات السيبرانية.	3.28	0.750	65.6	22.9	3.211	.000	دال
	مجال التسليم والخدمة والدعم	3.43	0.688	68.7	20.0	5.424	.000	دال
33	يخضع قسم تكنولوجيا المعلومات لعمليات تدقيق داخلي دورية ومستقلة.	3.72	0.628	74.4	16.9	9.862	.000	دال
34	يتم قياس أداء تكنولوجيا المعلومات باستمرار باستخدام مؤشرات أداء رئيسية (KPIs) واضحة.	3.30	0.715	66	21.7	3.609	.000	دال
35	يتم تقييم مستوى امتثال تكنولوجيا المعلومات بشكل مستمر مع القوانين والتشريعات المحلية والنافذة.	3.80	0.602	76	15.8	11.431	.000	دال
36	تقوم المؤسسة بتقييم دوري لمدى كفاءة نظام الرقابة الداخلية المفروض على الأنظمة والبيانات.	3.52	0.648	70.4	18.4	6.903	.000	دال
37	يتم رفع تقارير دورية وموضوعية للإدارة العليا عن أي انحرافات أو نقاط ضعف في الأداء التقني.	3.65	0.630	73	17.3	8.875	.000	دال
38	تحرص المؤسسة على مقارنة كفاءة حوكمتها التكنولوجية مع أفضل الممارسات والمعايير الدولية.	2.78	0.788	55.6	28.3	-2.402	.000	دال
39	يتم تقييم كفاءة وموثوقية الجهات الخارجية المزودة للخدمات التكنولوجية أو السحابية للمؤسسة.	3.21	0.740	64.2	23.1	2.441	.000	دال
40	تساهم عمليات المراقبة والتقييم في تقديم توصيات فعلية تطبق لتطوير البنية التقنية.	3.41	0.670	68.2	19.6	5.264	.000	دال
	مجال المراقبة والتقييم والتقدير	3.42	0.678	68.5	19.8	5.379	.000	دال
	جميع مجالات إطار COBIT 2019	3.36	0.697	67.2	20.7	4.443	.000	دال

تُظهر الإحصاءات الوصفية في الجدول (1) أنّ الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) لجميع المجالات جاء بمتوسط حسابي إجمالي قدره (3.36) وبأهمية نسبية بلغت (67.2%)، وهو ما يُصنّف وفقاً لسلم ليكرت الخماسي عند مستوى التزام متوسط؛ ما يشير إلى وجود أرضية تنظيمية مقبولة للحوكمة في المؤسسات المالية محل الدراسة. وبتحليل المجالات الفرعية وترتيبها تنازلياً حسب مستوى الالتزام الفعلي (المتوسطات الحسابية)، نجد أن مجال التقييم والتوجيه والمراقبة احتل المرتبة الأولى بمتوسط (3.45) وبمستوى مرتفع، مترافقاً بالالتزام الصارم بالتشريعات الصادرة عن مصرف سورية المركزي (العبارة 6 بمتوسط 3.90)، يليه مباشرة في المرتبة الثانية مجال التسليم والخدمة والدعم بمتوسط (3.43) ومستوى مرتفع أيضاً نظراً لكفاءة عمليات الحفظ الاحتياطي الدوري للبيانات المالية الحساسة (العبارة 29 بمتوسط 3.88). وفي المقابل، استقر مجال المراقبة والتقييم والتقدير في المرتبة الثالثة بمتوسط (3.42) ومستوى التزام مرتفع أيضاً يقترب من الحد الأعلى للمستوى المتوسط، يليه في المرتبة الرابعة مجال المواءمة والتخطيط والتنظيم بمتوسط (3.26) ومستوى متوسط أيضاً، في حين تذيل مجال البناء والاستحواذ والتنفيذ المرتبة الخامسة والأخيرة بمتوسط (3.25) ومستوى التزام متوسط. ويُفسر هذا التباين إلى وجود فجوات تشغيلية حادة تتمثل في قلة التمويل المالي اللازم للبنية التكنولوجية، وضيق الميزانيات المخصصة للمشروعات التقنية الجديدة، وعجز المؤسسات عن مقارنة حوكمتها مع أفضل الممارسات الدولية، علاوة على ضعف آليات استقطاب الكفاءات البشرية المؤهلة وتدريبها ونشر الوعي الأمني بين الموظفين.

2- تحديد حجم المخاطر السيبرانية والتهديدات الرقمية التي تواجه البيئة التشغيلية للمصارف والشركات المالية المدرجة في سوق دمشق للأوراق المالية:

الجدول (2) الإحصاءات الوصفية لطبيعة وحجم المخاطر السيبرانية والتهديدات الرقمية التي تواجه المؤسسات المالية محل الدراسة

الرقم	العبارات	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية%	معامل الاختلاف%	Test Value = 3		
						مؤشر tالاختبار	احتمال الدلالة	القرار
1	تمتلك المؤسسة القدرة على الرصد المبكر للهجمات السيبرانية المحتملة والتصدي لها قبل وقوع الضرر.	3.27	0.725	65.4	22.2	3.204	.000	دال
2	تنخفض معدلات نجاح محاولات الاختراق أو الوصول غير المصرح به لبيانات العملاء في المؤسسة إلى أدنى حد.	3.58	0.660	71.6	18.4	7.559	.000	دال
3	تتميز الأنظمة البرمجية وقواعد البيانات المصرفية بالحصانة العالية ضد التعديل أو التلاعب غير المشروع بالبيانات.	3.52	0.642	70.4	18.2	6.967	.000	دال
4	تنجح المؤسسة في الحفاظ على استمرارية تقديم خدماتها (كالصرافات الآلية والتطبيقات) دون انقطاع نتيجة الهجمات	3.25	0.752	65	23.1	2.860	.000	دال

	السيبرانية (مثل هجمات حجب الخدمة DDoS).							
5	تسجل المؤسسة انخفاضاً واضحاً في حجم الخسائر المالية أو القانونية الناتجة عن الحوادث والتهديدات السيبرانية.	3.45	0.680	69	19.7	5.693	.000	دال
6	يتميز نظام الحماية السيبرانية بالمرونة والسرعة الفائقة في التعافي والاستجابة بعد أي حادث أمني.	3.23	0.746	64.6	23.1	2.652	.000	دال
7	تنخفض احتمالية حدوث تسريب للبيانات الحساسة أو السرية الخاصة بالمؤسسة أو عملائها نتيجة الالتزام بالضوابط الأمنية.	3.63	0.618	72.6	17.0	8.769	.000	دال
8	تسهم البنية الأمنية للمؤسسة في تجنب العقوبات أو المخالفات التنظيمية الصادرة عن الجهات الإشرافية (كمصرف سورية المركزي).	3.77	0.595	75.4	15.8	11.132	.000	دال
	المتوسط الحسابي العام	3.46	0.677	69.3	19.6	5.874	.000	دال

تُظهر معطيات الجدول (2) أن التقييم الإجمالي العام لحجم المخاطر السيبرانية جاء بمتوسط حسابي (3.46) وأهمية نسبية (69.3%)، وهو ما يصنف عند مستوى مرتفع وفقاً لمجالات ليكرت، مما يعكس نجاحاً ملموساً للمؤسسات المالية في التقليل من التهديدات الرقمية، ويتضح من خلال تحليل العبارات أن البنية الدفاعية نجحت بقوة في تجنب المخالفات التنظيمية الصادرة عن الجهات الإشرافية كمصرف سورية المركزي وحماية سلامة البيانات من التسريب (العبارة 8 بمتوسط 3.77 والعبارة 7 بمتوسط 3.63). وفي المقابل، تراجعت مؤشرات استمرارية الخدمات المصرفية دون انقطاع والقدرة على التعافي السريع إثر الهجمات السيبرانية (العبارات 4 و6) إلى أدنى متوسطات الجدول عند (3.25) و(3.23) على التوالي وبمستوى متوسط. ويُفسر ذلك بامتلاك المصارف السورية أنظمة حماية وموثوقية تقنية جيدة للبيانات المخزنة، إلا أنها تعاني ضعفاً نسبياً في مهارات الاستجابة الديناميكية وصد هجمات حجب الخدمة (DDoS)، نتيجة النقص في أدوات الرصد الاستباقي الحديثة ومحدودية كفاءة خطط التعافي الفوري في ظل العقوبات التقنية المفروضة على البيئة البرمجية المحلية.

3- اختبار فرضيات البحث:

1- الفرضية الفرعية الأولى: لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال التقييم والتوجيه والمراقبة في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

لاختبار الفرضية تمّ الاعتماد على الانحدار البسيط:

الجدول (3) معاملا الارتباط والتحديد لأثر الالتزام بمجال التقييم والتوجيه والمراقبة في الحد من المخاطر السيبرانية

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.750	.562	.556	.35506

الجدول (4) تحليل تباين الانحدار لأثر الالتزام بمجال التقييم والتوجيه والمراقبة في الحد من المخاطر السيبرانية

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.641	1	11.641	92.338	.000
	Residual	9.077	72	.126		
	Total	20.718	73			

الجدول (5) معاملات الانحدار لأثر الالتزام بمجال التقييم والتوجيه والمراقبة في الحد من المخاطر السيبرانية

Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.611	.251		2.434	.017
	التقييم والتوجيه والمراقبة	.800	.083	.750	9.609	.000

تُظهر نتائج التحليل الإحصائي لنموذج الانحدار البسيط وجود أثر طردي قوي ذي دلالة إحصائية للالتزام بمجال التقييم والتوجيه والمراقبة في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة؛ حيث بلغت قيمة معامل الارتباط $R = 0.75$، وسجل معامل التحديد قيمة (0.562)، مما يعني أنّ هذا المجال يفسر ما نسبته (56.2%) من التغيرات الحاصلة في مستوى الأمن الرقمي للمؤسسات المالية محل الدراسة. وتأكدت صلاحية النموذج وجودته التفسيرية من خلال اختبار التباين ANOVA، حيث بلغت قيمة F المحسوبة (92.338) عند احتمال دلالة (.000). كما أثبت معامل الانحدار الأثر الإيجابي للمتغير المستقل عبر قيمة t البالغة (9.609) وبمعامل ميل قدره (0.75)، مما يشير إلى أن زيادة التزام مجالس الإدارات بالتوجيه والمراقبة الاستراتيجية للتقنية تؤدي مباشرة إلى تحصين البيئة المالية؛ وبناءً على هذه المعطيات، يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تؤكد وجود أثر ذي دلالة إحصائية للالتزام بمجال التقييم والتوجيه والمراقبة في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

9- الفرضية الفرعية الثانية: لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال المواءمة والتخطيط والتنظيم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

لاختبار الفرضية تمّ الاعتماد على الانحدار البسيط:

الجدول (6) معاملا الارتباط والتحديد لأثر الالتزام بمجال المواءمة والتخطيط والتنظيم في الحد من المخاطر السيبرانية

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.702	.493	.486	.38204

الجدول (7) تحليل تباين الانحدار لأثر الالتزام بمجال المواءمة والتخطيط والتنظيم في الحد من المخاطر السيبرانية

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.209	1	10.209	69.946	.000
	Residual	10.509	72	.146		
	Total	20.718	73			

الجدول (8) معاملات الانحدار لأثر الالتزام بمجال المواءمة والتخطيط والتنظيم في الحد من المخاطر السيبرانية

Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.519	.181		8.383	.000
	المواءمة والتخطيط والتنظيم	.489	.058	.702	8.363	.000

تُظهر نتائج التحليل الإحصائي لنموذج الانحدار البسيط وجود أثر طردي قوي ذي دلالة إحصائية للالتزام بمجال المواءمة والتخطيط والتنظيم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة؛ حيث بلغت قيمة معامل الارتباط $R = 0.702$، وسجل معامل التحديد قيمة (0.493)، مما يعني أنّ هذا المجال يفسر ما نسبته (49.3%) من التغيرات الحاصلة في مستوى الأمن الرقمي للمؤسسات المالية محل الدراسة. وتأكدت صلاحية النموذج وجودته التفسيرية من خلال اختبار التباين ANOVA، حيث بلغت قيمة F المحسوبة (69.946) عند احتمال دلالة (.000). كما أثبت معامل الانحدار الأثر الإيجابي للمتغير المستقل عبر قيمة t البالغة (8.363) وبمعامل ميل قدره (0.702)، مما يشير إلى أن صياغة هيكل تنظيمي واضح وتنسيق التواصل بين إدارة المخاطر العامة وإدارة التكنولوجيا يساهمان مباشرة في تحصين البيئة المالية وعملياتها، وبناءً على هذه المعطيات، يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تؤكد وجود أثر ذي دلالة إحصائية للالتزام بمجال المواءمة والتخطيط والتنظيم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

3- الفرضية الفرعية الثالثة: لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال البناء والاستحواذ والتنفيذ في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

لاختبار الفرضية تمّ الاعتماد على الانحدار البسيط:

الجدول (9) معاملا الارتباط والتحديد لأثر الالتزام بمجال البناء والاستحواذ والتنفيذ في الحد من المخاطر السيبرانية

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.698	.487	.480	.38425

الجدول (10) تحليل تباين الانحدار لأثر الالتزام بمجال البناء والاستحواذ والتنفيذ في الحد من المخاطر السيبرانية

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.087	1	10.087	68.319	.000
	Residual	10.631	72	.148		
	Total	20.718	73			

الجدول (11) معاملات الانحدار لأثر الالتزام بمجال البناء والاستحواذ والتنفيذ في الحد من المخاطر السيبرانية

Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.619	.559		2.895	.005
	البناء والاستحواذ والتنفيذ	1.439	.174	.698	8.266	.000

تُظهر نتائج التحليل الإحصائي لنموذج الانحدار البسيط وجود أثر طردي قوي ذي دلالة إحصائية للالتزام بمجال البناء والاستحواذ والتنفيذ في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة؛ حيث بلغت قيمة معامل الارتباط $R = 0.698$، وسجل معامل التحديد قيمة (0.487)، مما يعني أنّ هذا المجال يفسر ما نسبته (48.7%) من

التغيرات الحاصلة في مستوى الأمن الرقمي للمؤسسات المالية محل الدراسة. وتأكدت صلاحية النموذج وجودته التفسيرية من خلال اختبار التباين ANOVA، حيث بلغت قيمة F المحسوبة (68.319) عند احتمال دلالة (.000). كما أثبت معامل الانحدار الأثر الإيجابي للمتغير المستقل عبر قيمة t البالغة (8.266) وبمعامل ميل قدره (0.698)، مما يشير إلى أن اتباع منهجيات رصينة عند شراء أو تطوير الأنظمة المالية، وفحصها ضد الثغرات قبل التشغيل الفعلي، يساهم مباشرة في حماية البيئة المصرفية، وبناءً على هذه المعطيات، يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تؤكد وجود أثر ذي دلالة إحصائية للالتزام بمجال البناء والاستحواذ والتنفيذ في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

4- الفرضية الفرعية الرابعة: لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال التسليم والخدمة والدعم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

لاختبار الفرضية تمّ الاعتماد على الانحدار البسيط:

الجدول (12) معاملا الارتباط والتحديد لأثر الالتزام بمجال التسليم والخدمة والدعم في الحد من المخاطر السيبرانية

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.775	.601	.595	.33897

الجدول (13) تحليل تباين الانحدار لأثر الالتزام بمجال التسليم والخدمة والدعم في الحد من المخاطر السيبرانية

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.445	1	12.445	108.311	.000
	Residual	8.273	72	.115		
	Total	20.718	73			

الجدول (14) معاملات الانحدار لأثر الالتزام بمجال التسليم والخدمة والدعم في الحد من المخاطر السيبرانية

Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.010	.194		5.203	.000
	التسليم والخدمة والدعم	.797	.077	.775	10.407	.000

تُظهر نتائج التحليل الإحصائي لنموذج الانحدار البسيط وجود أثر طردي قوي ذي دلالة إحصائية للالتزام بمجال التسليم والخدمة والدعم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة؛ حيث بلغت قيمة معامل الارتباط $R = 0.775$، وسجل معامل التحديد قيمة (0.601)، مما يعني أنّ هذا المجال يفسر ما نسبته (60.1%) من التغيرات الحاصلة في مستوى الأمن الرقمي للمؤسسات المالية محل الدراسة. وتأكدت صلاحية النموذج وجودته التفسيرية من خلال اختبار التباين ANOVA، حيث بلغت قيمة F المحسوبة (108.311) عند احتمال دلالة (.000). كما أثبت معامل الانحدار الأثر الإيجابي للمتغير المستقل عبر قيمة t البالغة (10.407) وبمعامل ميل قدره (0.775)، مما يشير إلى أن التطبيق الصارم لسياسات إدارة الصلاحيات والنسخ الاحتياطي الدوري وإجراءات التشغيل اليومية يساهم مباشرة في تحصين البيئة المالية، وبناءً على هذه المعطيات، يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تؤكد وجود أثر ذي دلالة إحصائية للالتزام بمجال التسليم والخدمة والدعم في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

5- الفرضية الفرعية الخامسة: لا يوجد أثر ذو دلالة إحصائية للالتزام بمجال المراقبة والتقييم والتقدير في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

لاختبار الفرضية تمّ الاعتماد على الانحدار البسيط:

الجدول (15) معاملا الارتباط والتحديد لأثر الالتزام بمجال المراقبة والتقييم والتقدير في الحد من المخاطر السيبرانية

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.810	.656	.651	.31473

الجدول (16) تحليل تباين الانحدار لأثر الالتزام بمجال المراقبة والتقييم والتقدير في الحد من المخاطر السيبرانية

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	13.586	1	13.586	137.152	.000
	Residual	7.132	72	.099		
	Total	20.718	73			

الجدول (17) معاملات الانحدار لأثر الالتزام بمجال المراقبة والتقييم والتقدير في الحد من المخاطر السيبرانية

Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.343	.145		9.244	.000
	المراقبة والتقييم والتقدير	.544	.046	.810	11.711	.000

تُظهر نتائج التحليل الإحصائي لنموذج الانحدار البسيط وجود أثر طردي قوي ذي دلالة إحصائية للالتزام بمجال المراقبة والتقييم والتقدير في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة؛ حيث بلغت قيمة معامل الارتباط $R = 0.81$، وسجل معامل التحديد قيمة (0.656)، مما يعني أنّ هذا المجال يفسر ما نسبته (656%) من التغيرات الحاصلة في مستوى الأمن الرقمي للمؤسسات المالية محل الدراسة. وتأكدت صلاحية النموذج وجودته التفسيرية من خلال اختبار التباين ANOVA، حيث بلغت قيمة F المحسوبة (137.152) عند احتمال دلالة (.000). كما أثبت معامل الانحدار الأثر الإيجابي للمتغير المستقل عبر قيمة t البالغة (11.711) وبمعامل ميل قدره (0.81)، مما يشير إلى أن إخضاع الأنظمة لعمليات تدقيق داخلي دورية مستقلة، والتقييم المستمر للامتثال للقوانين، ورفع تقارير الانحرافات للإدارة العليا، يُمثّل حجر الأساس والدفاع الأقوى في صد التهديدات الرقمية، وبناءً على هذه المعطيات، يتم رفض الفرضية الصفرية وقبول الفرضية البديلة التي تؤكد وجود أثر ذي دلالة إحصائية للالتزام بمجال المراقبة والتقييم والتقدير في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

6- الفرضية الرئيسة للبحث: لا يوجد أثر ذو دلالة إحصائية للالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) في الحد من المخاطر السيبرانية في المؤسسات المالية محل الدراسة.

لاختبار الفرضية تمّ الاعتماد على الانحدار المتعدد:

الجدول (18) تحليل الانحدار المتعدد لأثر الالتزام بمبادئ حوكمة التكنولوجيا المعلومات وفق (COBIT 2019) في الحد من المخاطر السيبرانية

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.836	.698	.676	.14702	.698	31.459	5	68	.000

الجدول (19) تباين الانحدار المتعدد لأثر الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق (COBIT 2019) في الحد من المخاطر السيبرانية

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.400	5	.680	31.459	.000
	Residual	1.470	68	.022		
	Total	4.870	73			

الجدول (20) معاملات الانحدار المتعدد لأثر الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق (COBIT 2019) في الحد من المخاطر السيبرانية

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.808	.528		7.213	.000
	مجال التقييم والتوجيه والمراقبة	.057	.025	.204	2.286	.025
	مجال المواءمة والتخطيط والتنظيم	.228	.106	.201	2.141	.036
	مجال البناء والاستحواذ والتنفيذ	.123	.046	.073	2.684	.009
	مجال التسليم والخدمة والدعم	.164	.013	.314	12.324	.000
	مجال المراقبة والتقييم والتقدير	.258	.091	.437	2.836	.006

أظهرت نتائج تحليل الانحدار المتعدد وجود أثر طردي قوي وذي دلالة إحصائية للالتزام بمبادئ حوكمة تكنولوجيا المعلومات كمنظومة متكاملة في الحد من المخاطر السيبرانية؛ حيث تبيّن من الجدول (18) أن قيمة معامل التحديد بلغت (0.698)، مما يعني أنّ إطار (COBIT 2019) بمجالاته الخمسة يفسر مجتمعاً ما نسبته (69.8%) من التغيرات الحاصلة في الحد المخاطر السيبرانية وحماية البيئة الرقمية للمؤسسات المالية محل الدراسة، وهي علاقة معنوية بالكامل نظراً لأن قيمة احتمال الدلالة في جدول تحليل التباين (ANOVA) بلغت (.000) وهي أقل من مستوى الدلالة (0.05).

وعند تحليل جدول المعاملات (20) لترتيب درجة التأثير تنازلياً وفقاً لقيمة معامل الانحدار المعياري (Beta)، نجد أن مجال المراقبة والتقييم والتقدير قد تصدر المرتبة الأولى كأقوى المتغيرات أثراً في النموذج بقيمة (Beta = 0.437) وبدلالة إحصائية بلغت (0.006)، تلاه في المرتبة الثانية مجال التسليم والخدمة والدعم بقيمة (Beta = 0.314) وبدلالة عالية قدرها (.000)، وحلّ مجال التقييم والتوجيه والمراقبة في المرتبة الثالثة بقيمة (Beta = 0.204) ودلالة (0.025) ليؤكد الأهمية البالغة للدور الاستراتيجي والرقابي للإدارة العليا، ليأتي بعده مجال المواءمة والتخطيط والتنظيم في المرتبة الرابعة بقيمة (Beta = 0.201) ودلالة (0.036)، في حين تذيل مجال البناء والاستحواذ والتنفيذ المرتبة الخامسة والأخيرة بالأثر الأقل نسبياً بقيمة (Beta = 0.073) وباحتمال دلالة (0.009). ووفقاً لهذه المعطيات المتكاملة وثبوت معنوية النموذج إحصائياً، يتم رفض الفرضية الرئيسة

الصفرية وقبول الفرضية البديلة، مما يؤكد وجود أثر ذي دلالة إحصائية عند مستوى دلالة (0.05) للالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفق إطار (COBIT 2019) في الحد من المخاطر السيبرانية في المؤسسات المالية المدرجة في سوق دمشق للأوراق المالية.

4- الاستنتاجات والتوصيات:

1- الاستنتاجات:

1- مستوى الالتزام بإطار (COBIT 2019): أظهرت النتائج أن المستوى الإجمالي لالتزام المؤسسات المالية جاء متوسطاً، حيث تصدر الترتيب تنازلياً لالتزام المجالات التقييم والتوجيه والمراقبة أولاً، يليه التسليم والخدمة والدعم، ثم المراقبة والتقييم والتقدير، وحلّ رابعاً المواءمة والتخطيط والتنظيم، بينما جاء البناء والاستحواذ والتنفيذ في المرتبة الأخيرة.

2- حجم المخاطر والتهديدات السيبرانية: بينت النتائج أن كفاءة البنية الدفاعية للمصارف وشركات التأمين في كبح المخاطر السيبرانية وحماية سلامة البيانات جاءت بمستوى مرتفع، بالرغم من وجود مستوى متوسط في قدرة الأنظمة على التعافي السريع الفوري عند التعرض لهجمات حجب الخدمة.

3- أثر مجال التقييم والتوجيه والمراقبة: أثبت التحليل الإحصائي وجود أثر طردي دال إحصائياً لهذا المجال، حيث يفسر وحده (56.2%) من جهود الحد من المخاطر السيبرانية، مما يؤكد أهمية الرقابة الاستراتيجية المباشرة من قِبل مجالس الإدارات.

4- أثر مجال المواءمة والتخطيط والتنظيم: تبين وجود أثر إيجابي ذي دلالة إحصائية للمجال في تعزيز الأمن الرقمي وبنسبة تفسيرية بلغت (49.3%)، مما يعكس دور التنسيق الهيكلي وربط خطط التكنولوجيا بالأهداف العامة للمؤسسة.

5- أثر مجال البناء والاستحواذ والتنفيذ: أكدت النتائج وجود أثر طردي دال إحصائياً للمجال بنسبة تفسير قدرها (48.7%)، مما يؤكد على أن فحص الأنظمة المالية الجديدة وتوثيق إجراءات تغييرها يمنعان نشوء الثغرات البرمجية الطارئة.

6- أثر مجال التسليم والخدمة والدعم: أظهرت النتائج وجود أثر طردي دال إحصائياً لهذا المجال في تحصين البيئة المالية يفسر (60.1%) من التغيرات، مما يجعله المجال الأهم لإدارة الصلاحيات الصارمة وحفظ النسخ الاحتياطية دورياً.

7- أثر مجال المراقبة والتقييم والتقدير: سجل هذا المجال أعلى قدرة تفسيرية في الانحدار البسيط بلغت (65.6%) بأثر طردي معنوي، مما يثبت أن التدقيق الداخلي الدوري والامتثال للتشريعات يمثلان حجر الزاوية للدفاع السيبراني.

8- أثر النموذج المتكامل لحوكمة التكنولوجيا (الفرضية الرئيسة): خلص تحليل الانحدار المتعدد إلى رفض الفرضية الصفرية؛ حيث تبين أن مجالات (COBIT 2019) مجتمعةً تمتلك أثراً طردياً قوياً يفسر (69.8%) من الحد من المخاطر السيبرانية، وتصدرها مجال المراقبة والتقييم والتقدير كأقوى المتغيرات تأثيراً.

2- التوصيات:

1- دعم التمويل وجداول المشروعات الرقمية: يُوصى بأن تقوم الإدارات العليا برصد ميزانيات مستقلة ومستدامة لتمويل البنية التكنولوجية، مع تفعيل رقابة صارمة تضمن تنفيذ المشروعات والتحولات الرقمية (كالدفع الإلكتروني) وفق جداولها الزمنية والمالية المحددة لتجنب الثغرات الطارئة.

2- تأهيل الكفاءات ونشر ثقافة الوعي الأمني: يجب وضع معايير دقيقة لاستقطاب الكفاءات البشرية المتخصصة في الأمن السيبراني وتأهيلها، بالتوازي مع إطلاق برامج تدريبية مستمرة لرفع وعي جميع موظفي المؤسسة بالمؤشرات الأولية للاختراقات والتهديدات الرقمية.

3- تعزيز الجاهزية الاستباقية واستمرارية الخدمات: يُقترح تبني حلول تقنية متقدمة للرصد المبكر ضد التهديدات وتحديث خطط الطوارئ البديلة، لضمان استمرارية عمل الصرافات الآلية والتطبيقات المصرفية دون انقطاع، ورفع كفاءة التعافي السريع خاصة عند التعرض لهجمات حجب الخدمة (DDoS).

4- تفعيل آليات الرقابة التشغيلية والتدقيق الشامل: يوصى بتعميق ممارسات إدارة الصلاحيات والنسخ الاحتياطي الدوري (باعتباره خط الدفاع الأول)، مع بناء قنوات تنسيق دائم بين إدارتي المخاطر والتكنولوجيا، وإخضاع المنظومة لتدقيق داخلي مستقل لضمان الامتثال المستمر للتشريعات الصادرة عن مصرف سورية المركزي.

5- المراجع:

1- المراجع العربية:

1- الحسناوي، عقيل حمزة حبيب؛ والموسوي، إنعام محسن غدير. *دور حوكمة تكنولوجيا المعلومات في تقليل مخاطر تدقيق نظم المعلومات المحاسبية الإلكترونية في ظل إطار عمل (COBIT) للرقابة الداخلية*. مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية، المجلد (9)، العدد (3)، 2017، 1-25.

2- راجح، ميثاق أحمد؛ وسلام، مروان عبد الملك عبد الله. *دور حوكمة تكنولوجيا المعلومات وفق إطار COBIT 5 في الحد من مخاطر المحاسبة السحابية: دراسة ميدانية على مجموعة هائل سعيد أنعم وشركاه*. مجلة العلوم التربوية والدراسات الإنسانية، العدد (49)، 2025، 315-357.

3- صالح، سمير أبو الفتوح؛ والفقي، مصطفى إبراهيم؛ وداود؛ وميريت علاء الدين حسني. *أثر استخدام تقنية حوكمة تكنولوجيا المعلومات COBIT 5 في تحسين جودة التقارير المالية في الشركات الناشئة: دراسة تطبيقية*. مجلة راية الدولية للعلوم التجارية، المجلد (3)، العدد (10)، 2024، 1032-1080.

4- العازمي، عبد الله فالح خليفة عقيل. *دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات المحاسبية من المخاطر الالكترونية في ظل عصر الرقمنة: دراسة تطبيقية على البنوك التجارية الكويتية*. المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد (13)، العدد (3)، الجزء (2)، 2022، 1115-1155.

5- علي، ريم سعد. *مدى الالتزام بمبادئ حوكمة تكنولوجيا المعلومات وفقاً لإطار COBIT 2019: دراسة حالة جهاز تنفيذ وإدارة مشروع النهر الصناعي فرع بنغازي*. مجلة دراسات محاسبية، العدد السابع، 2024، 13-46.

6- عوض، آية عادل محمود. *أثر حوكمة تكنولوجيا المعلومات في تدعيم القرارات الاستثمارية في نظم المعلومات المحاسبية*. رسالة ماجستير، كلية التجارة، جامعة القاهرة، مصر، 2016.

7- الفار، محمد محمد سليمان. *أثر حوكمة تكنولوجيا المعلومات وفقاً لأبعاد إطار COBIT 2019 على جودة الإفصاح عن معلومات تقارير نظام إدارة المعلومات المالية الحكومية*. المجلة العلمية للدراسات التجارية والبيئية، المجلد (15)، العدد (1)، 2024، 628-702.

8- نصور، ريم محمد. *أثر حوكمة تكنولوجيا المعلومات على جودة التقارير المالية: دراسة ميدانية*. أطروحة دكتوراه، كلية الاقتصاد، جامعة تشرين، اللاذقية، سورية.

2- المراجع الأجنبية:

9- HAOUAM, D .IT IT *governance impact on financial reporting quality using COBIT framework.* Global Journal of Computer Sciences: Theory and Research, 10(1), 2020,1-10.

10- ISACA .COBIT 2019. *Design Guide: Designing an Information and Technology Governance Solution* .Schaumburg, IL: ISACA, (2018), 1-150.

11- ISACA .COBIT 2019. *Focus Area: Cybersecurity .Schaumburg*, IL: ISACA, 2020, 1-85.

12- SHERLY, S & ,.FIANTY, M. I .*Enhancing Financial Technology Operations: A Comprehensive Evaluation Using COBIT 2019 Framework*. Jurnal Riset Informatika, 6(2), 2024, 57-66.

13- SMITH, J & ,.JONES, R .*The impact of IT governance on cybersecurity resilience*. Journal of Information Security,12(4),2021,345-367.

14- WORLD ECONOMIC FORUM .*The Global Risks Report 2022* .Geneva: WEF, 2022, 1-116.