السنة الرابعة والعشرون/ عدد خاص/تموز 2026
https://doi.org/10.31272/ijes.v24.1547

المجلة العراقية للعلوم الاقتصادية
Iraqi Journal For
Economic Sciences

PISSN : 1812-8742 EISSE : 2791-092X Arcif : 0.375

The role of intrusive auditing in enhancing cybersecurity risk governance: A field study on a sample of Iraqi banks

دور التدقيق التداخلي في تعزيز حوكمة مخاطر الأمن السيبراني: دراسة ميدانية على عينة من المصارف العراقية

م.د.عقيل كاطع جبار
Aqeel Gatea Jabbar
ajabbr@uowasit.edu.iq
مديرية تربية واسط

Abstract

This research aims to develop a theoretical framework for enhancing the role of internal auditors in strengthening cybersecurity risk governance in Iraqi banks. The most important conclusion is that internal auditing plays a crucial role in enhancing cybersecurity risk governance in the Iraqi banks included in the study sample. This is achieved through integrating cybersecurity into risk-based audit planning and enterprise risk management, and by assessing the adequacy of cybersecurity policies, incident response plans, and access controls. The study recommends that Iraqi banks enhance the training and professional development of internal auditors on the latest cybersecurity technologies and best practices, and that they regularly review and update their governance policies to align with international standards.

Keywords: Internal audit, cybersecurity, cybersecurity governance.

المستخلص

يهدف البحث إلى وضع إطار نظري لتحسين دراسة دور المدققين الداخليين في تعزيز حوكمة مخاطر الأمن السيبراني في المصارف العراقية، وتوصلت أهم الاستنتاجات، إلى أنّ للتدقيق الداخلي دورا هاما في تعزيز مخاطر حوكمة الأمن السيبراني في المصارف العراقية عينة البحث ، من خلال دمج الأمن السيبراني في تخطيط التدقيق القائم على المخاطر وإدارة مخاطر المؤسسة، وتقييم مدى كفاية سياسات الأمن السيبراني وخطط الاستجابة للحوادث وضوابط الوصول. وقد أوصت الدراسة المصارف العراقية بضرورة تعزيز التدريب والتطوير المهني للمدققين الداخليين حول أحدث تقنيات الأمن السيبراني وأفضل الممارسات. و مراجعة سياسات الحوكمة وتحديثها بانتظام لتتوافق مع المعايير العالمية.

الكلمات الرئيسية: التدقيق الداخلي، الامن السيبراني، حوكمة الامن السيبراني

المقدمة

استدعت التطورات العلمية والتكنولوجية، إلى جانب نمو عمليات الشركات وتنوعها، تطوير أنظمة رقابة لمساعدة الإدارة في ضمان الاستخدام الأمثل للموارد، وتحديد الانحرافات المحتملة

وتقييم كفاءة أنظمة الرقابة الداخلية. وأصبح الأمن السيبراني أحد أهم تحديات الحوكمة التي تواجه المؤسسات الحديثة مع تسارع التحول الرقمي وتزايد الاعتماد على أنظمة المعلومات. وقد كشفت اختراقات البيانات البارزة، وهجمات برامج الفدية، وتعطل الأنظمة، عن نقاط ضعف ليس فقط في الدفاعات التقنية، بل أيضًا في هياكل الحوكمة المسؤولة عن الإشراف على المخاطر. وتتحمل مجالس الإدارة ولجان التدقيق مسؤولية متزايدة عن إخفاقات الأمن السيبراني، مما يعزز الحاجة إلى آليات حوكمة قوية تتماشى مع إدارة مخاطر المؤسسة. وفي هذا السياق، اكتسب التدقيق الداخلي أهمية بالغة كوظيفة ضمان قادرة على تقييم وتعزيز حوكمة مخاطر الأمن السيبراني بشكل مستقل، وتقديم المشورة للإدارة بشأن فعالية الضوابط. وقد عززت حقبة ما بعد قانون ساربينز-أوكسلي على المساءلة والشفافية وموثوقية الرقابة الداخلية، مما أرسى الأساس لدور التدقيق الداخلي الموسع في مجالات المخاطر الناشئة. وقد تم توثيق تطور التدقيق الداخلي من وظيفة تركز على الامتثال إلى شريك حوكمة ذي قيمة مضافة بشكل جيد. وقد اكتسب مفهوم التدقيق الداخلي أهمية متزايدة مع مرور الوقت. فبعد أن كان يركز في البداية على فحص عمليات المنظمة وسجلاتها ووثائقها من قِبل قسم داخلي، تحوّل إلى وظيفة أوسع نطاقًا تُعرَّف بأنّها ضمان مستقل وموضوعي، ونشاط استشاري يركز على خلق القيمة وتحسين العمليات التنظيمية. ويُعنى التدقيق الداخلي بضمان الامتثال للقوانين المعمول بها، والمتطلبات التنظيمية، واللوائح الداخلية، والسياسات والخطط والإجراءات التي يضعها مجلس الإدارة وتُعد البنية التحتية للمؤسسات المالية هدفا حيويا للتهديدات السيبرانية. ولذلك، تضطلع وظائف التدقيق الداخلي بدور بالغ الأهمية في تحديد وتقييم وتعزيز تدابير حوكمة الأمن السيبراني لحماية البيانات الحساسة، والأنظمة التشغيلية، والامتثال التنظيمي داخل المؤسسات المالية.

1. منهجية البحث

اولاً: مشكلة البحث: مع مواجهة المؤسسات المالية لمخاطر سيبرانية متطورة، يُتوقع من التدقيق الداخلي بشكل متزايد تقييم ليس فقط تصميم الضوابط وفعاليتها التشغيلية، بل أيضًا مدى كفاية هياكل الحوكمة التي تُشرف على استراتيجية الأمن السيبراني. وعلى الرغم من تزايد هذه التوقعات، لا يزال هناك غموضٌ يكتنف النطاق الدقيق وفعالية مشاركة التدقيق الداخلي في حوكمة الأمن السيبراني. وتستمر التساؤلات حول ما إذا كان المدققون الداخليون يمتلكون الخبرة الفنية الكافية، ويحافظون على استقلاليتهم عن الإدارة، ويُوصلون بفعالية رؤى مخاطر الأمن السيبراني إلى مجالس الإدارة ولجان التدقيق. وتنسد مشكلة البحث إلى التساؤل الذي ينص (هل يوجد هناك دور للتدقيق الداخلي في تعزيز حوكمة مخاطر الامن السيبراني).

ثانياً: هدف البحث: يهدف هذا البحث إلى وضعِ إطارٍ نظريٍ لتحسين دراسة دور المدققين الداخليين في تعزيز حوكمة مخاطر الأمن السيبراني في المصارف العراقية، وتتفرع اهداف البحث:

1- التعرف على مفهوم حوكمة مخاطر الامن السيبراني وماهي اهميتها و اهدافها.

2- معرفة الاتجاهات الناشئة التي يجب مراعاتها من قبل التدقيق الداخلي عند تدقيق مخاطر الأمن السيبراني.

3- معرفة دور التدقيق الداخلي في تعزيز حوكمة مخاطر الامن السيبراني

ثالثاً: أهمية البحث: توفر عمليات التدقيق الداخلي إطارًا أساسيًا لإدارة مخاطر الأمن السيبراني والتخفيف من حدتها، مما يساعد المؤسسات المالية الحفاظ على مرونتها في بيئة رقمية سريعة

التطور. وتُمكّن هذه العمليات الجهات من إجراء تقييمات قائمة على المخاطر، وتحديد مخاطر تهديدات الأمن السيبراني، مثل الوصول غير المصرح به، واختراقات البيانات، وهجمات برامج الفدية. ويكشف المدققون عن نقاط الضعف في الأنظمة والشبكات والعمليات، مع إعطاء الأولوية لتلك التي تُشكل أعلى خطر على العمليات الحكومية الحساسة وبيانات المواطنين. بالإضافة إلى ذلك، يُقيّم المدققون سياسات وإجراءات الأمن السيبراني، ويضمنون تحديثها، وتنفيذها بشكل صحيح، والالتزام بها في جميع الإدارات، مع تحديد أي ثغرات تحتاج إلى معالجة. وبالتالي يكون للتدقيق الداخلي دورٌ مؤثرٌ في عملية تعزيز حوكمة مخاطر الأمن السيبراني، وتتحقق تلك الحوكمة من خلال تحديد المخاطر، وتقييم الضوابط، وضمان الالتزام بالمعايير التنظيمية. ومن خلال تعزيز أفضل ممارسات الأمن السيبراني، وتحسين جاهزية الاستجابة للحوادث، وترسيخ ثقافة اليقظة، وحماية البنية التحتية الحيوية، وضمان استمرارية العمليات، وتأمين المعلومات الحساسة.

رابعا: فرضية البحث: يستند البحث إلى الفرضيات التالية:

1- يساهم التدقيق الداخلي في تعزيز الأطر التنظيمية لحوكمة مخاطر الأمن السيبراني.
2- يؤدي التدقيق الداخلي دوراً فعالاً في الرقابة الاستباقية لمنع الخروقات السيبرانية.
3- يعزز التدقيق الداخلي من قدرة المصارف العراقية على التعافي من التهديدات السيبرانية.

خامسا : مجتمع وعينة البحث: مجتمع البحث المصارف العراق المدرجة في سوق العراق للأوراق المالية، وكانت عينة البحث خمسة مصارف وهي (المصرف العراقي الاسلامي ومصرف بغداد ومصرف المنصور ومصرف التنمية الدولي ومصرف جيهان).

سادسا : منهج البحث: اعتمد الباحث على المنهج الوصفي التحليلي، وذلك لملاءمته لطبيعة الدراسة التي تسعى لوضع نموذج مقترح لدور التدقيق الداخلي في حوكمة مخاطر الأمن السيبراني. وقد تم تطبيق هذا المنهج من خلال المسارين التاليين:

* المنهج الوصفي (الجانب النظري): تم من خلاله استعراض الأدبيات المحاسبية والتقنية، والمعايير الدولية (مثل NIST 2.0 و COBIT)، وذلك لوصف المتغيرات وبناء النموذج المقترح الذي يحدد أدوار المدقق الداخلي في البيئة المصرفية.
* المنهج التحليلي (الجانب الميداني): تم الاعتماد على "الدراسة الميدانية" من خلال إعداد قائمة استقصاء (Checklist) تم توجيهها لعينة من المصارف العراقية، وهي (المصرف العراقي الاسلامي ومصرف بغداد ومصرف المنصور ومصرف التنمية الدولي ومصرف جيهان) لغرض جمع البيانات الأولية وتحليلها لاختبار واثبات فرضيات الدراسة.

سابعا : الاطار الزماني والمكاني

*الحدود الزمانية: 2026
* الحدود المكانية : المصارف العراقية في داخل البلد عينة البحث (المصرف العراقي الاسلامي ومصرف بغداد ومصرف المنصور ومصرف التنمية الدولي ومصرف جيهان)

ثامنا : هيكلية البحث: يتكون البحث من المحور الاول الذي تناول الجانب النظري للبحث حيث تم تناول الإطار النظري للتدقيق الداخلي وحوكمة مخاطر الأمن السيبراني وأهميتها وأهدافها، والأطر والمعايير المعززة لحوكمة النظام السيبراني، ودور التدقيق الداخلي في تعزيز

حوكمة مخاطر الأمن السيبراني. كما تناول المحور الثاني نموذج مقترح يوضح الدور الذي يمكن أن يؤديه التدقيق الداخلي في تعزيز حوكمة مخاطر الأمن السيبراني في المصارف العراقية، من خلال الاستفادة من التكامل بين الأطر الدولية الرائدة المتمثلة في ISO/IEC 27001 و COBIT و NIST CSF. ويأتي هذا النموذج استجابة للتحديات المتزايدة التي تواجه القطاع المصرفي نتيجة التحول الرقمي وتنامي التهديدات السيبرانية، وكما تم عمل استمارة استقصاء لتعزيز الجانب التطبيقي واثبات فرضيات البحث. ومن ثم تناول البحث اهم الاستنتاجات والتوصيات.

المحور الاول : الجانب النظري

اولا: التـــــدقيق الـــــداخلي: يُعدّ التدقيق الداخلي ممارسةً متميزةً وموضوعيةً تُضيف قيمةً وتُقدّم استشاراتٍ بهدف تحسين عمليات المؤسسة. فهو يُساعد المؤسسة على تحقيق أهدافها من خلال تقديم منهجٍ مُنظّمٍ قائمٍ على الكفاءة لتقييم وتحسين كفاءة إدارة المخاطر والرقابة وعمليات الإدارة (معهد المدققين الداخليين). ويعتبر التدقيق الداخلي وظيفة تقييمٍ مستقلةٍ تُنشأ داخل المؤسسة لمراجعة وتقييم أنشطتها باعتباره خدمةٍ لها. ويُسهم في دعم قادة الشركة في تنفيذ التزاماتهم بنجاح. كما يُعدّ ميزة تقييمٍ مستقلةٍ تُطوّر داخل المؤسسة لتقييم فعالية نظام الرقابة الإدارية وإنتاجيته وكفاءته. والهدف هو إقناع الإدارة بأنّ آليات الرقابة الداخلية لديها كافيةٌ لتلبية احتياجات المؤسسة وتعمل بشكلٍ مُرضٍ. وهو جزءٌ من عملية الرقابة الداخلية لإدارة المؤسسة، والتي تُنشأ لتدقيق وتحليل ومراقبة العمليات المحاسبية وغيرها من عمليات الرقابة. من الناحية العملية، يُعدّ أداء وكفاءة إجراءات التدقيق الداخلي أمرًا بالغ الأهمية، نظرًا لأنّ المدققين الداخليين يؤدون نطاقًا واسعًا من المهام. وأنّ فعالية دور التدقيق الداخلي تعتمد جزئيًا على: الهيكل القانوني والتنظيمي، وموقع الوظيفة واستقلاليتها، ووجود لجان التدقيق، والموارد المخصصة لمهام موظفي التدقيق الداخلي، وكفاءتهم المهنية. وتُعدّ فعالية إجراءات التدقيق الداخلي مؤشرًا على قدرة البرنامج على تحقيق الأثر أو النتيجة المرجوة التي يمكن قياسها نوعيًا. وان وجود إجراءات تدقيق داخلي فعّالة تضمن موثوقية البيانات المالية والتقارير التشغيلية وحماية أصول الشركة وفعالية الضوابط التنظيمية.(Abiodun,2020:409) ومن الواضح أن دور التدقيق الداخلي هو دعم الإدارة خلال عملية الرقابة. وبالتالي، يمكن تلخيص تركيز التدقيق الداخلي على عملية الرقابة على النحو التالي: (Alhawtmeh,2025:319-320)

1. يساعد التدقيق الداخلي الوحدة على تحقيق رقابة داخلية فعالة، كما يشجع على التحسين المستمر لعملية الرقابة. حيث تُعتبر مخرجات التدقيق مدخلات لنظام الرقابة الداخلية.
2. تتضمن الوظيفة الإدارية عدة وظائف فرعية، منها التخطيط والتنظيم والتوجيه والإشراف والمراقبة، والتي تُشكل جوهر أنشطة الرقابة. ويلعب التدقيق الداخلي دورًا أساسيًا في دعم تنفيذ هذه الوظائف.
3. إنّ استقلالية التدقيق عن العمليات التشغيلية داخل الوحدة تُعزز قدرة التدقيق الداخلي على تقييم مستوى الثقة في الأداء. وهذا بدوره يسمح لنظام الرقابة بمواءمة الأداء الفعلي مع الأداء المخطط له، مما يضمن رقابة فعالة.
4. نظرًا لأنّ التدقيق الداخلي يُعتبر أحد الأنظمة داخل الوحدة، فإنّ قربه من الأنظمة المحاسبية يجعله على دراية بالمشكلات التي تواجه الوحدة. وهذا يدفعه إلى فهم العمليات التشغيلية التي تُنفذها هذه الأنظمة لتعزيز المعرفة واستكمال عملية الرقابة.

٥. يوفر التدقيق الداخلي مراجعة وتقييمًا مستمرين للأنظمة والإجراءات التي وضعتها الإدارة، بهدف تمكين الرقابة الداخلية من مراقبة أنشطة الوحدة بفعالية.
٦. يمكن تعزيز عمليات إدارة المخاطر من خلال الأدوار الرئيسية للتدقيق الداخلي، نظرًا لوجود علاقة وثيقة بين إدارة المخاطر والتدقيق الداخلي.

ثانيا: حوكمة مخاطر الامن السيبراني: يمكن تعريف حوكمة الأمن السيبراني بأنّها إدارة عمليات صنع القرار بطريقة تزيد من المشاركة والشفافية والمساءلة في اتخاذ التدابير المتعلقة بالفضاء السيبراني، وذلك بالتنسيق مع آليات الاتفاقيات والاستراتيجيات والقوانين والتدابير واللوائح والمعايير الدولية التي تتكامل على النحو الأمثل. وتُعدّ حوكمة الأمن السيبراني في العلاقات الدولية من أبرز القضايا في السنوات الأخيرة، وقد سعت المنظمات الدولية إلى إيجاد حلولٍ لتحدياتها. وفي هذا الصدد، اتُخذت الخطوات الأولى بتوقيع "اتفاقية الجرائم الإلكترونية" من قِبل مجلس أوروبا (أونوك، 2013). إضافةً إلى ذلك، تم اعتماد معايير دولية في هذا المجال. فعلى سبيل المثال، يوفر معيار ISO/IEC 38500:2015 مبادئ توجيهية لأعضاء الهيئات الإدارية في المنظمات بشأن الاستخدام الفعال والكفء والمقبول لتكنولوجيا المعلومات داخل منظماتهم. وينطبق هذا المعيار على حوكمة استخدام المنظمة الحالي والمستقبلي لتكنولوجيا المعلومات، ويشمل أيضًا عمليات الإدارة والقرارات المتعلقة باستخدامها. علاوة على ذلك يُعرّف معيار ISO/IEC38500:2015 حوكمة تكنولوجيا المعلومات كجزء من حوكمة المؤسسات والشركات. ويمكن التحكم في هذه العمليات من قِبل متخصصي تكنولوجيا المعلومات داخل المؤسسة، أو مزودي الخدمات الخارجيين، أو وحدات الأعمال داخل المؤسسة (ISO 2015). وكما ذُكر، على الرغم من وجود بعض الخطوات لتوحيد معايير حوكمة الأمن السيبراني ومعايير أمن المعلومات، مثل ISO 22301 وISO 27001 وISO/IEC 27002 و27031 و27032 و27701، إلا أنه لا يوجد حتى الآن معيار إطاري يجمع بين حوكمة الأمن السيبراني وأمن المعلومات كموضوعين منفصلين. (Sava&Karata,2022:11-12) ووفقًا للمعيار الدولي للمنظمات(ISO)(38500)، تُعدّ حوكمة الأمن السيبراني آليةً تُمكّن المنظمة من توجيه أمن نظم المعلومات والتحكم فيه ومراقبته وتقييمه لدعم عملياتها التجارية. وتُشكّل حوكمة الأمن السيبراني جزءًا لا يتجزأ من أنظمة حوكمة الشركات وتقنية المعلومات. ويتم توجيه الأمن السيبراني في المنظمة من خلال وضع مجموعة مناسبة من سياسات الأمن ومعاييره وإجراءاته وتوجيهاته، بدءًا من التوجهات الاستراتيجية مرورًا بالتكتيكية وصولًا إلى التشغيلية. علاوة على ذلك، تتم إدارة الأمن السيبراني في المنظمة والتحكم فيه بشكل أساسي من خلال تقييم الامتثال ومراقبته وقياسه والإبلاغ عنه، بدءًا من المستوى التشغيلي مرورًا بالتكتيكي وصولًا إلى المستوى الاستراتيجي. في الوقت الراهن، ونظرًا لطبيعة التهديدات السيبرانية والمشهد التكنولوجي المتغيرة والمتطورة باستمرار، تحتاج كل منظمة إلى مجموعة كاملة ومناسبة من أطر حوكمة الأمن السيبراني لتلبية جميع احتياجاتها الأمنية بشكل كامل. وفقًا لمعهد حوكمة تكنولوجيا المعلومات، يضمن تطبيق حوكمة أمنية فعّالة توافق استراتيجيات الأمن السيبراني مع استراتيجية تكنولوجيا المعلومات والاستراتيجية التنظيمية الشاملة، ودعم تحقيق الأهداف التنظيمية، وتوفير قيمة تجارية مُعظّمة لجميع أصحاب المصلحة، وإدارة المخاطر والموارد السيبرانية بشكل استباقي، وقياس الأداء التنظيمي باستخدام مؤشرات الأداء الرئيسية لتحقيق الأهداف التنظيمية. ينبغي أن يركز إطار حوكمة الأمن السيبراني بشكل أساسي على المسؤوليات والممارسات التي يجب أن تمارسها الإدارة العليا للمؤسسات(مجلس الإدارة والإدارة التنفيذية)(Melaku,2023:327)

ثالثا: الاطر والمعايير المعززة لحوكمة الأمن السيبراني: تقدم أطر عمل مثل ISO/IEC27001، وإطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا(NIST CSF)و2019 COBIT، مناهج راسخة لإدارة المخاطر، ومواءمة الامتثال وتقييم الأداء. من خلال تقديم أفضل الممارسات المُقننة ومبادئ الحوكمة المُهيكلة، تُساعد هذه الأُطر المؤسسات على دمج الأمن السيبراني في عملية صنع القرار الاستراتيجي، مما يُتيح الامتثال والمرونة على حدٍ سواء. ورغم أنّ لكل إطار نقاط قوة فريدة، إلّا أنّ تطبيقها المُتكامل يُوفر وسيلة فعّالة لتحسين حوكمة مخاطر الأمن السيبراني. يُوفر معيار ISO/IEC 27001 نظامًا مُحددًا وقابلًا للاعتماد لإدارة أمن المعلومات (ISMS) يُضفي الطابع الرسمي على السياسات والضوابط وعمليات التحسين المُستمر. في المقابل، يُعد إطار NIST CSF إطارًا مرنًا قائمًا على المخاطر، مبنيًا حول الوظائف الأساسية الخمس: التحديد، والحماية، والكشف، والاستجابة، والتعافي، مما يسمح للمؤسسات بتخصيص التنفيذ بناءً على مستوى تقبّل المخاطر والسياق التشغيلي. ويُضيف إطار COBIT 2019 بُعدًا آخر من خلال التركيز على الحوكمة وتقديم القيمة، وربط نتائج الأمن السيبراني بمؤشرات أداء المؤسسة وأهدافها الاستراتيجية. ويُسهم توحيد هذه الأطر الثلاثة في إنشاء بنية حوكمة موحدة تستفيد من نقاط قوتها التكاملية. يضمن معيار ISO/IEC27001، بدقته في التوثيق وتطبيق الضوابط بينما تُمكّن مرونة إطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا(NISTCSF) من الاستجابة السريعة لتطورات بيئات التهديدات. وتضمن مبادئ حوكمة COBIT بقاء مبادرات الأمن السيبراني متوافقة استراتيجياً مع أهداف المؤسسة وتوقعات الأداء. وتُشكل هذه الأطر مجتمعةً دفاعاً متعدد الطبقات يدمج الضوابط التكتيكية، والمرونة التشغيلية، والإشراف الاستراتيجي. ويُعدّ الأساس المنطقي لهذا التوحيد تشغيلياً واستراتيجياً على حد سواء. فمن الناحية التشغيلية، يُقلل توحيد الأطر من ازدواجية الجهود في عمليات التدقيق والتقييم وإعداد تقارير الامتثال، مما يُتيح موارد لإدارة المخاطر الاستباقية. كما يُتيح رسم خرائط ضوابط متسقة عبر أنظمة تنظيمية متعددة، مما يُقلل من مخاطر وجود ثغرات في الامتثال. من الناحية الاستراتيجية، يُرسّخ نهج الإطار المتكامل الأمن السيبراني كعامل تمكين للقيمة، مما يعزز الثقة بين أصحاب المصلحة، ويُحسّن القدرة التنافسية، ويعزز قدرة المؤسسة على العمل بأمان عبر الحدود والقطاعات. (Essien at el,2022:618)

رابعا: التحديات الاساسية في حوكمة الامن السيبراني: تواجه العديد من المنظمات خمسة تحدياتٍ أساسية في حوكمة الأمن السيبراني، وهي: (Oliver&Foscarini, 2014:31)
(1) استراتيجية الأمن السيبراني. (2) العمليات الموحدة. (3) الإنفاذ والتنفيذ. (4) المساءلة. (5) إشراف القيادة العليا. (6) الموارد.

خامسا: أهداف حوكمة الأمن السيبراني: تهدف حوكمة الأمن السيبراني إلى توفير التوجيه الاستراتيجي لتأمين نظام تكنولوجيا المعلومات الذي يدعم العمليات التجارية؛ وضمان تحديد أهداف الأمن وتحقيقها بشكل واضح؛ والتأكد من تحليل المخاطر الأمنية وإدارتها بشكل مناسب؛ والتحقق من الاستخدام الأمثل لموارد الشركة وإنفاقها على تأمين أصولها. ويلعب إطار حوكمة الأمن السيبراني دورًا حيويًا في تحقيق الأهداف الأمنية للمؤسسة، سواءً للمشاكل الحالية أو التحديات المستقبلية . ومعالجة المشكلات الأمنية الراهنة، وينبغي لإطار حوكمة الأمن أن يدرس ويأخذ في الاعتبار في حال وجود سياسة واستراتيجية أمنية، فإنها تحتاج إلى مراجعة وتحديث دوريين لمعالجة الثغرات الأمنية الحالية ومظاهر التهديدات. أما في حال عدم وجود سياسة أمنية، فيُوصى بشدة بتطبيق مجموعة مناسبة من الضوابط الأمنية لتدقيق وتقييم

الوضع الأمني للمؤسسة بشكل دوري. وتصميم وتنفيذ برامج للتوعية والتدريب الأمني بين الموظفين والمستخدمين النهائيين، وغيرهم. علاوة على ذلك، لمواجهة تحديات الأمن السيبراني المستقبلية، ينبغي لإطار حوكمة الأمن يراعي عوامل ومظاهر التهديدات الناشئة والمتغيرة باستمرار. ومراعاة ومعالجة الثورة التكنولوجية المتسارعة. والعمل المستمر على تغيير مواقف الأفراد تجاه الأمن لخلق قوة عاملة واعية بالأمن السيبراني. و التركيز على تحويل ثقافة العمل. (Melaku,2023:328)

سادسا: فوائد عمل نموذج موحد لحوكمة مخاطر الأمن السيبراني: يوفر دمج معايير ISO/IEC 27001 وNIST CSF وCOBIT 2019 في نموذج حوكمة موحد لمخاطر الأمن السيبراني ميزة استراتيجية وتشغيلية تتجاوز مجموع فوائد كل جزء على حدة. فمن خلال مواءمة الضوابط التوجيهية، وعمليات إدارة المخاطر المرنة، والإشراف على الحوكمة على مستوى المؤسسة، تستطيع المؤسسات الانتقال من الجهود المجزأة التي تركز على الامتثال إلى نهج شامل يركز على المرونة. ويُمكّن هذا النموذج المؤسسات ليس فقط من تلبية المتطلبات التنظيمية، بل أيضًا من التكيف مع التهديدات المتطورة، مع ضمان دعم مبادرات الأمن السيبراني لأهداف العمل بشكل مباشر. و يستفيد نموذج الحوكمة الموحد من نهج إدارة المخاطر المنظم لمعيار ISO/IEC 27001، وقابلية التكيف في تحديد أولويات المخاطر ضمن إطار عمل NIST CSF، والإشراف على الحوكمة ضمن إطار عمل COBIT، لإنتاج تقييمات مخاطر أكثر دقة وقابلية للتنفيذ. تضمن منهجية المنظمة الدولية للمعايير (ISO) تحديد الأصول والتهديدات ونقاط الضعف والضوابط وتقييمها بشكل منهجي، مما يُرسي أساسًا متينًا للتوعية بالمخاطر. يُثري المعهد الوطني للمعايير والتكنولوجيا (NIST) هذه العملية من خلال تمكين المؤسسة من وضع المخاطر في سياق بيئتها التشغيلية، وبيئة التهديدات الخاصة بقطاعها، وأساليب الهجوم المتطورة. بدوره، يدمج إطار عمل COBIT هذه الرؤى في عمليات إدارة مخاطر المؤسسة (ERM)، مما يضمن توافق قرارات معالجة المخاطر مع أهداف العمل، واستراتيجيات تخصيص الموارد، وتوقعات الأداء. ينتج عن هذا التآزر بين الأطر المتعددة خطط لمعالجة المخاطر تتسم بالمتانة التقنية والملاءمة الاستراتيجية، مما يقلل من المخاطر المتبقية ويعظم العائد على الاستثمارات الأمنية. (Essien at el,2022:621)

سابعا: التدقيق الداخلي ومخاطر الأمن السيبراني: يُعرَّف دور التدقيق الداخلي بأنّه مساعدة الإدارة في تطبيق ضوابط كافية وفعّالة. وفي سعيها لتحقيق أهداف المنظمة بشكل أكثر فعالية، من الضروري وجود نظام تدقيق داخلي قوي، مُكلَّف بإضافة قيمة وتحسين عمليات المنظمة، ليساهم في منع الهجمات السيبرانية وحوكمتها. ويؤكد كلٌّ من جاميسون وآخرون (2018) ونيوزواير (2018) على ضرورة تكيُّف التدقيق الداخلي مع المخاطر الحرجة المرتبطة بالأمن السيبراني ومعالجتها. ويتمثل دور التدقيق الداخلي في ظل التغيرات التكنولوجية الحالية في مواكبة أحدث اتجاهات الأمن السيبراني، والمراقبة والتقييم المستمر لسياسات وإجراءات الأمن السيبراني في المنظمة، لتحديد أوجه القصور في الضوابط التي قد تُعرِّض المنظمة للخطر. ولضمان تحقيق قيمة مضافة في جميع المؤسسات، ينص الدليل العالمي لتدقيق التكنولوجيا (2016)(GTAG) على ضرورة أن يتبنى المدققون الداخليون نهجًا محدثًا لتقديم ضمانات بشأن مخاطر الأمن السيبراني، والتي تتأثر بشكل كبير بالعديد من العوامل الناشئة التي تؤثر على المؤسسات. وتعتمد العديد من المؤسسات بشكل متزايد على استخدام التكنولوجيا والشبكات والتطبيقات والبيانات في عملياتها اليومية، مما قد يؤدي إلى ثغرات أمنية ومخاطر الهجمات السيبرانية. ويعود ضعف المؤسسات الحكومية والخاصة أمام التهديدات السيبرانية إلى الاعتماد

المتزايد على تكنولوجيا المعلومات، الأمر الذي يتطلب مراجعة داخلية شاملة لمخاطر الأمن السيبراني لتحسين بيئة الرقابة في المؤسسة. من خلال مراجعة شاملة لتقييم الأمن السيبراني في الدوائر الحكومية والهيئات العامة، يُمكن للتدقيق الداخلي تقديم ضمان وتقييم مستقلين للإدارة بطريقة منظمة، مما يُساعد في تحديد الثغرات الأمنية السيبرانية في الضوابط الرقابية. (Dikokoe,2021:1) ويُمكن لوظيفة التدقيق الداخلي أن تعزز من إدارة الأمن السيبراني من خلال:(Whitehouse, 2015)& (Newswire, 2018)

1- إجراء تقييم للمخاطر المتعلقة بعمليات الأمن السيبراني، وتقديم توصيات لتحسينها.
2- تحسين تدابير الأمن السيبراني في المؤسسة.
3- إجراء اختبارات اختراق لأصول تكنولوجيا المعلومات المختارة.
4- مراجعة العمليات القائمة، وتقييم ما إذا كانت الإدارة قد أخذت في الاعتبار المخاطر السيبرانية الرئيسية التي يُشكلها تغير بيئة تكنولوجيا المعلومات.
5- تقييم تطبيق ضوابط الأمن السيبراني وآليات الدفاع لمعالجة المخاطر السيبرانية الناشئة بشكل كافٍ.

ثامنا : الاتجاهات الناشئة التي يجب مراعاتها من قبل التدقيق الداخلي عند تدقيق مخاطر الأمن السيبراني: إنّ الاتجاهات الناشئة في تدقيق الأمن السيبراني التي وُجد أنها تُؤثر بشكل كبير على قدرة المؤسسة هي: (Siyaya at al,2025:18-20)

1- **طبيعة عمليات التدقيق الداخلي:** تقليديًا، كانت المؤسسات تُعطي الأولوية لعمليات تدقيق الأعمال وتُولي اهتمامًا أقل لعمليات تدقيق تكنولوجيا المعلومات. يُحوّل التحول الرقمي الحالي للعمليات التنظيمية تركيز برامج عمل التدقيق نحو إعطاء الأولوية لعمليات تدقيق تكنولوجيا المعلومات ويعتقد أن عمليات تدقيق الأمن السيبراني باتت الآن تتمتع بفرصة متساوية لإدراجها في برنامج عمل التدقيق.

2- **نقص المهارات:** باتت هناك حاجة إلى مجموعة مهارات جديدة لكل من متخصصي تكنولوجيا المعلومات والمدققين الداخليين بسبب الحاجة إلى إدارة مخاطر الأمن السيبراني ، وأنّ غالبية الموظفين يفتقرون إلى المهارات التقنية في إدارة مخاطر الأمن السيبراني، ويجب اتخاذ تدابير لمعالجة هذا النقص.

3- **عمليات التدقيق من جهات خارجية:** ازداد الاعتماد على ضوابط وعمليات الجهات الخارجية في السنوات الأخيرة. وتقيم المؤسسات علاقات مع جهات خارجية لتبادل مخاطر الأمن السيبراني والموارد اللازمة لإدارتها. وقد تحدث مخاطر الأمن السيبراني مثل فقدان البيانات وسرقة الهوية وإساءة استخدام الأنظمة، وتتضمن برامج عمل التدقيق الحديثة تقييم عمليات الجهات الخارجية لضمان أمن عمليات الأمن السيبراني لمجلس الإدارة والإدارة التنفيذية.

4- **التدقيق المستمر:** على عكس المخاطر التقليدية، تتسم مخاطر الأمن السيبراني بالديناميكية والتغير المستمر. ولم يعد إجراء تقييم المخاطر عبر عمليات المؤسسة مهمة تُنفذ لمرة واحدة. حيث قد أدى أتمتة عمليات الأعمال إلى تغيير طبيعة المخاطر وسلوكها. يُلزم التشغيل الآلي المدققين بتقييم سلوك المخاطر المحددة باستمرار، واحتمالية ظهور مخاطر أخرى ، ويشهد التشغيل الآلي وتحليلات البيانات نموًا متزايدًا في مجالي التدقيق والأمن السيبراني. تُدمج أساليب التشغيل الآلي والتحليلات في برامج عمل التدقيق لتعزيز البيانات داخل جميع المؤسسات. ويتزايد اختبار ممارسات التشغيل الآلي نظرًا لاعتماد المؤسسات المتزايد عليه . تُطبّق وظائف التدقيق عمليات تدقيق مستمرة لرصد الأنشطة غير المرغوب فيها في بيئة تكنولوجيا المعلومات، ولتشجيع الالتزام بالإجراءات المعتمدة.

5- **حوكمة الأمن السيبراني:** يتزايد الضغط على فرق الحوكمة لإدارة العمليات التنظيمية بكفاءة. ويتطلب مجلس الإدارة ولجنة التدقيق تقديم ضمانات بأنّ عمليات الحوكمة تستجيب لإدارة مخاطر الأمن السيبراني. وإن تقييم آليات تعزيز حوكمة الأمن السيبراني، مثل التعليم السيبراني والسياسات والإجراءات، يكتسب اهتمامًا متزايدًا استجابةً للتهديد الحالي الذي يواجه مشهد الأمن السيبراني للأعمال.

تاسعا: دور التدقيق الداخلي في تعزيز حوكمة مخاطر الأمن السيبراني: شهدت السنوات الأخيرة تغيراً في أساليب عمل الشركات، مواكبةً للتغيرات المستمرة على المستويات الاقتصادية والتكنولوجية وغيرها، مما يجعل تطبيق عمليات التدقيق الداخلي أمراً بالغ الأهمية. وتدفع مستويات التنافسية المتزايدة في السوق الشركات إلى استكشاف أساليب جديدة لتحقيق ميزة تنافسية وضمان استمراريتها. وفي ظل بيئة غير مستقرة، يتعين على الشركات الاستجابة للمخاطر التي تواجهها، حيث يُعدّ دور التدقيق الداخلي حاسماً. ويُعدّ ضمان الأمن السيبراني أحد المخاطر الجسيمة والمعاصرة، وهو نابع من التحول الرقمي الذي شهده العالم في السنوات الأخيرة من خلال تطبيق أنظمة المعلومات. مع ذلك، قد يُؤدي استخدام هذه الأنظمة إلى عواقب وخيمة في حالات الاختراق السيبراني. علاوة على ذلك، تتزايد وتيرة هذه الاختراقات مُسببةً خسائر فادحة. مما يجعل من الضروري للمؤسسات التصدي لهذه المشكلة، وذلك من خلال الاستفادة الفعّالة من استراتيجيات الابتكار الوظيفية المتنوعة لتخطيط العمليات وتنفيذها. وفي هذا السياق، يجب على التدقيق الداخلي، الذي توسّع دوره نتيجةً للتغيرات الحديثة، أن يُسهم بفعالية في حماية أمن الخدمات والعمليات الإلكترونية. أدت تزايد حوادث اختراق أنظمة معلومات الأعمال إلى لفت انتباه الشركات إلى الأساليب اللازمة للحد من هذه الحوادث وآثارها. ومع ذلك، فإنّ الأساليب التي يقترحها خبراء تكنولوجيا المعلومات غير كافية. ولضمان أمن أنظمة المعلومات التي تحتوي على معلومات حساسة، من الضروري أن تُسهم عمليات التدقيق الداخلي في تحقيق أهداف الحماية نفسها. (Lois at el,2021:27-28) ويعد التدقيق الداخلي ركيزة أساسية لحوكمة فعّالة لمخاطر الأمن السيبراني، إلّا أنّ فعاليته مرهونة بتوافق الحوكمة والكفاءة الوظيفية. وبالاستناد إلى دراسة Cohen وآخرون (2010) يُسلّط النقاش الضوء على كيف أن استقلالية التدقيق الداخلي وإمكانية وصوله إلى مجالس الإدارة تُمكّنه من الإشراف بشكل فريد على مخاطر الأمن السيبراني التي تتجاوز حدود الأقسام التشغيلية. ومن خلال تقديم ضمانات بشأن فعالية الضوابط وتقديم المشورة بشأن تحسينات الحوكمة، يدعم التدقيق الداخلي المساءلة والشفافية في إدارة المخاطر الرقمية. وأنه بدون التطوير المستمر للمهارات والتوجه الاستراتيجي، يُخاطر التدقيق الداخلي بالتهميش في مجالات المخاطر المعقدة كالأمن السيبراني. وأن إصلاح التدقيق الداخلي ضرورة لتزويد المدققين الداخليين بالكفاءات اللازمة لتقييم التهديدات السيبرانية المتطورة. ويشمل هذا الإصلاح الاستثمار في التدريب التقني، وتعزيز التعاون مع وظائف أمن المعلومات، وتحديد صلاحيات حوكمة أكثر وضوحًا. وأنّ الأطر التنظيمية وحدها غير كافية لإدارة المخاطر السيبرانية المتغيرة باستمرار، ويجب أن يتجاوز دور التدقيق الداخلي مجرد الامتثال ليشمل إدارة المخاطر الاستباقية، بما يتماشى مع توقعات ما بعد قانون ساربينز-أوكسلي فيما يتعلق بوظائف ضمان الجودة. ومن خلال دمج الأمن السيبراني في تخطيط التدقيق القائم على المخاطر وإدارة مخاطر المؤسسة، يُمكن للتدقيق الداخلي تعزيز مرونة المؤسسة وفعالية حوكمتها. وأن التدقيق الداخلي يلعب دورًا حيويًا ومتناميًا في حوكمة مخاطر الأمن السيبراني، حيث يعمل كمزود مستقل لضمان الجودة ومستشار استراتيجي لمجالس الإدارة والإدارة التنفيذية. وبالاستناد إلى أدبيات

حوكمة الشركات وإصلاح التدقيق الداخلي، يتضح أنّ فعالية التدقيق الداخلي في الإشراف على الأمن السيبراني تعتمد على قدرته على التكيف مع التعقيد التكنولوجي وتوقعات الحوكمة. وتؤكد النتائج أنّ التدقيق الداخلي قادر على سد الفجوات الحرجة بين العمليات التقنية للأمن السيبراني والإشراف على مستوى مجلس الإدارة، مما يُعزز الشفافية والمساءلة. مع ذلك، فإنّ تحقيق هذا الإمكان يتطلب إصلاحًا مستمرًا للتدقيق الداخلي، كما أنّ الاستثمار في المهارات والموارد وتكامل الحوكمة ضروري لضمان استمرار أهمية التدقيق الداخلي في مواجهة المخاطر السيبرانية المتطورة. وبالتالي، يُعد تعزيز دور التدقيق الداخلي في حوكمة مخاطر الأمن السيبراني أمرًا جوهريًا للحفاظ على ثقة المؤسسات وقدرتها على الصمود في العصر الرقمي. (Reynolds,2019:3) وأنّ المدققين الداخليين يحتاجون إلى مهارات حوكمة قوية لضمان توافق سياسات الأمن السيبراني مع أهداف المؤسسة الأوسع. وأن المدققين الملمين بحوكمة تكنولوجيا المعلومات قادرون على تعزيز حوكمة مخاطر الأمن السيبراني بشكل أفضل، مما يساعد المؤسسات على تبني نهج استباقي لإدارة المخاطر السيبرانية. ويضمن هذا المنظور الأوسع للحوكمة دمج الأمن السيبراني في إطار إدارة المخاطر الشامل، بدلًا من التعامل معه كقضية تقنية منفصلة. (Alzeban,2025: 5) يرى الباحث أنّ للمدققين الداخليين دورا كبيرا في الكشف عن التهديدات السيبرانية ومنعها, لذلك، من الضروري أن يدمج المدققون في جميع قطاعات الأمن السيبراني خطط التدقيق الخاصة بهم، وأن يتم تقييم باستمرار فعالية أدوات الأمن السيبراني، وأن يبلغوا مجلس الإدارة بجميع المخاطر المتعلقة بالأمن السيبراني لاتخاذ الإجراءات المناسبة. وأن للتدقيق الداخلي دورا اساسيا في تعزيز حوكمة مخاطر الأمن السيبراني من خلال التقييم الفعال لضوابط الرقابة الداخلية الخاصة بمخاطر الامن السيبراني وتحصين البنية التحتية للمعلومات ضد التهديدات المتطورة، وهو ما يثمر عن تطوير مرونة المؤسسات في مواجهة الاختراقات السيبرانية المحتملة. و تقوية فعالية الاستجابة للحوادث وتثبيت معايير الامتثال للوائح الدولية، مما يعزز من حوكمة مخاطر الأمن السيبراني، ويحول الأمن السيبراني من مجرد تحدٍ تقني إلى أولوية قيادية تضمن استدامة العمليات وحماية الأصول المعنوية والمادية.

المحور الثاني : الجانب التطبيقي

أولا: النموذج المقترح لدور التدقيق الداخلي في تعزيز حوكمة مخاطر الأمن السيبراني:

السيبراني: يعرض هذا المحور إلى بناء نموذج مقترح يوضح الدور الذي يمكن أن يؤديه التدقيق الداخلي في تعزيز حوكمة مخاطر الأمن السيبراني في المصارف العراقية، من خلال الاستفادة من التكامل بين الأطر الدولية الرائدة المتمثلة في ISO/IEC 27001 و COBITو NIST CSFويأتي هذا النموذج استجابة للتحديات المتزايدة التي تواجه القطاع المصرفي نتيجة التحول الرقمي وتنامي التهديدات السيبرانية، الأمر الذي يتطلب وجود إطار حوكمي متكامل يضمن حماية الأصول المعلوماتية واستمرارية العمل.

- **مبررات اختيار أبعاد النموذج:** جاء اختيار أبعاد النموذج المقترح انسجاماً مع ما ورد في إطارNISTCSF، وبما يتكامل مع متطلباتISO/IEC27001في إدارة أمن المعلومات وأهدافCOBITفي حوكمة وإدارة تكنولوجيا المعلومات. وتمثلت هذه الأبعاد في: الحوكمة والتخطيط، تحديد المخاطر، الحماية، الاكتشاف، الاستجابة والتعافي، حيث تمثل هذه الأبعاد دورة متكاملة لتعزيز حوكمة مخاطر الأمن السيبراني داخل المصارف.

الحوكمة والتخطيط: يركز هذا البعد على الدور الاستراتيجي للتدقيق الداخلي في تقييم مدى التزام مجلس الإدارة والإدارة العليا بحوكمة الأمن السيبراني، ومدى تكامل السياسات

والاستراتيجيات المعتمدة مع أهداف المصرف وإدارة المخاطر المؤسسية.

تحديد المخاطر: يهتم هذا البعد بتقييم آليات التعرف على المخاطر السيبرانية وتحليلها وضمان شمولية سجلات المخاطر وتصنيف الأصول المعلوماتية بما يعكس مستوى الأهمية والخطورة.

الحماية: يعالج هذا البعد دور التدقيق الداخلي في تقييم كفاية الضوابط الوقائية، سواء كانت تقنية أو إدارية، بهدف تقليل احتمالية وقوع الاختراقات والهجمات السيبرانية.

الاكتشاف: يركز هذا البعد على قدرة المصرف على الاكتشاف المبكر للحوادث السيبرانية، من خلال تقييم أنظمة المراقبة والإنذار وإجراءات الإبلاغ والتحليل.

الاستجابة والتعافي: يتناول دور التدقيق الداخلي في تقييم خطط الاستجابة للحوادث وخطط استمرارية الأعمال والتعافي من الكوارث بضمن الحد من آثار الحوادث واستدامة العمل المصرفي.

الحوكمة والتخطيط (Governance & Planning)

البعد	الإطار المعتمد	دور التدقيق الداخلي
الحوكمة والتخطيط(Governance & Planning)	ISO 27001 / COBIT EDM	تقييم التزام مجلس الإدارة بحوكمة الأمن السيبراني
الحوكمة والتخطيط(Governance & Planning)	ISO 27001 / COBIT EDM	فحص وجود سياسة أمن معلومات معتمدة
الحوكمة والتخطيط(Governance & Planning)	ISO 27001 / COBIT EDM	مراجعة مواءمة أهداف الأمن السيبراني مع الأهداف الاستراتيجية
الحوكمة والتخطيط(Governance & Planning)	ISO 27001 / COBIT EDM	تقييم دمج مخاطر الأمن السيبراني ضمن إدارة المخاطر المؤسسية

تحديد المخاطر(Identify)

البعد	الإطار المعتمد	دور التدقيق الداخلي
تحديد المخاطر(Identify)	ISO 27001 / NIST Identify	مراجعة منهجية تحديد مخاطر الأمن السيبراني
تحديد المخاطر(Identify)	ISO 27001 / NIST Identify	تقييم سجل المخاطر السيبرانية
تحديد المخاطر(Identify)	ISO 27001 / NIST Identify	تصنيف الأصول المعلوماتية الحساسة
تحديد المخاطر(Identify)	ISO 27001 / NIST Identify	تحليل التهديدات والثغرات المحتملة

الحماية(Protect)

البعد	الإطار المعتمد	دور التدقيق الداخلي
الحماية(Protect)	ISO 27001 Annex A / COBIT DSS	تقييم ضوابط التحكم في الوصول
الحماية(Protect)	ISO 27001 Annex A / COBIT DSS	مراجعة سياسات كلمات المرور والصلاحيات
الحماية(Protect)	ISO 27001 Annex A / COBIT DSS	فحص حماية بيانات العملاء
الحماية(Protect)	ISO 27001 Annex A / COBIT DSS	تقييم برامج التوعية والتدريب

الاكتشاف(Detect)

البعد	الإطار المعتمد	دور التدقيق الداخلي
الاكتشاف(Detect)	NIST Detect / COBIT MEA	تقييم أنظمة المراقبة والإنذار
الاكتشاف(Detect)	NIST Detect / COBIT MEA	مراجعة آليات تسجيل الحوادث
الاكتشاف(Detect)	NIST Detect / COBIT MEA	تقييم إجراءات الإبلاغ عن الحوادث

الاستجابة والتعافي(Respond & Recover)

البعد	الإطار المعتمد	دور التدقيق الداخلي
الاستجابة والتعافي(Respond & Recover)	NIST Respond & Recover / ISO 27001	تقييم خطط الاستجابة للحوادث
الاستجابة والتعافي(Respond & Recover)	NIST Respond & Recover / ISO 27001	مراجعة خطط استمرارية الأعمال
الاستجابة والتعافي(Respond & Recover)	NIST Respond & Recover / ISO 27001	تقييم الدروس المستفادة وتحسين الضوابط

ثانيا: استمارة استقصاء:(Checklist) اعتمدت هذه الدراسة على قائمة استقصاء (Checklist)صفها أداةً تدقيقية تحليلية، تهدف إلى تقييم الدور الفعلي للتدقيق الداخلي في تعزيز حوكمة مخاطر الأمن السيبراني في المصارف العراقية من خلال الفحص المهني المباشر للسياسات والأنظمة والإجراءات المعتمدة. وكانت عينة الدراسة كل من المصرف العراقي الاسلامي ومصرف بغداد ومصرف المنصور ومصرف التنمية الدولي ومصرف جيهان.

المحور الأول :حوكمة مخاطر الأمن السيبراني: اثبات الفرضية الأولى: يساهم التدقيق الداخلي في تعزيز الأطر التنظيمية لحوكمة مخاطر الأمن السيبراني

ت	معايير الاستقصاء	نعم	لا	النسبة المئوية	مستوى التطبيق
1	هل يوجد ميثاق معتمد للتدقيق الداخلي يحدد صراحة صلاحياته في فحص أنظمة وتقنيات المعلومات والأمن السيبراني؟	4	1	80%	مرتفع
2	هل يقوم التدقيق الداخلي بمراجعة وتقييم هيكلية حوكمة تكنولوجيا المعلومات لضمان وضوح الصلاحيات واستقلالية وظيفة أمن المعلومات؟	4	1	80%	مرتفع
3	هل يتحقق التدقيق الداخلي من وجود سياسة مكتوبة ومحدثة للأمن السيبراني ومتوافقة مع تعليمات البنك المركزي العراقي؟	5	0	100%	مرتفع جداً
4	هل يرفع التدقيق الداخلي تقارير مستقلة عن مخاطر الأمن السيبراني إلى لجنة التدقيق أو مجلس الإدارة؟	3	2	60%	متوسط

5	هل يقيم التدقيق الداخلي مدى التزام الإدارة العليا بتطبيق أطر حوكمة الأمن السيبراني المعتمدة داخل المصرف؟	4	1	80%	مرتفع

المحور الثاني :إدارة المخاطر والضوابط الوقائية للأمن السيبراني: اثبات الفرضية الثانية: يؤدي التدقيق الداخلي دوراً فعالاً في الرقابة الاستباقية لمنع الخروقات السيبرانية.

ت	معايير الاستقصاء	نعم	لا	النسبة المئوية	مستوى التطبيق
6	هل يقوم التدقيق الداخلي بتدقيق عملية حصر وتصنيف الأصول الرقمية والمعلوماتية وفقاً لأهميتها وحساسيتها؟	4	1	80%	مرتفع
7	هل يفحص التدقيق الداخلي ضوابط التحكم في الوصول إلى الأنظمة والبيانات الحساسة بما يضمن مبدأ الحاجة إلى المعرفة؟	5	0	100%	مرتفع جداً
8	هل يراجع التدقيق الداخلي مخاطر الأمن السيبراني الناجمة عن التعامل مع الجهات الخارجية ومقدمي الخدمات؟	3	2	60%	متوسط
9	هل يتحقق التدقيق الداخلي من تطبيق ضوابط حماية (البيانات والمعلومات الحساسة) التشفير، الصلاحيات، الفصل الوظيفي؟	4	1	80%	مرتفع
10	هل يراجع التدقيق الداخلي فاعلية برامج التوعية والتدريب الخاصة بالأمن السيبراني لموظفي المصرف؟	3	2	60%	متوسط

المحور الثالث :الكشف والاستجابة والتعافي من الحوادث السيبرانية: اثبات الفرضية الثالثة: يعزز التدقيق الداخلي من قدرة المصارف العراقية على التعافي من التهديدات السيبرانية

ت	معايير الاستقصاء	نعم	لا	النسبة المئوية	مستوى التطبيق
11	هل يقوم التدقيق الداخلي بمراجعة كفاءة أنظمة كشف ومراقبة الأحداث الأمنية السيبرانية داخل المصرف؟	3	2	60%	متوسط
12	هل يدقق التدقيق الداخلي خطط الاستجابة للحوادث السيبرانية وسيناريوهات الاختراق المحتملة؟	4	1	80%	مرتفع
13	هل يفحص التدقيق الداخلي جاهزية فرق الاستجابة للحوادث السيبرانية من حيث الهيكل والمهام والمسؤوليات؟	3	2	60%	متوسط
14	هل يتحقق التدقيق الداخلي من فاعلية أنظمة النسخ الاحتياطي وسرعة استعادة البيانات في حالات الطوارئ؟	5	0	100%	مرتفع جداً
15	هل يتابع التدقيق الداخلي تنفيذ التوصيات الواردة في تقارير الحوادث والاختراقات السيبرانية السابقة؟	4	1	80%	مرتفع

ملخص نتائج استمارة الاستقصاء حسب محاور البحث

المحور	عدد الفقرات	نعم	لا	النسبة المئوية	مستوى التطبيق
حوكمة مخاطر الأمن السيبراني	5	20	5	84%	مرتفع
إدارة المخاطر والضوابط الوقائية	5	19	6	76%	جيد
الكشف والاستجابة والتعافي	5	19	6	80%	مرتفع

اختبار فرضيات البحث

الفرضية	المحور	النسبة	النتيجة
الفرضية الأولى	حوكمة مخاطر الأمن السيبراني	84%	قبول الفرضية
الفرضية الثانية	إدارة المخاطر والضوابط الوقائية	76%	قبول الفرضية
الفرضية الثالثة	الكشف والاستجابة والتعافي	80%	قبول الفرضية

بناءً على الجداول أعلاه، يتضح أنّ التدقيق الداخلي في المصارف العراقية يمارس دوراً جوهرياً في تعزيز حوكمة الأمن السيبراني بنسبة إجمالية بلغت (80. %)، وهي نسبة مرتفعة تؤكد إدراك المصارف لأهمية الرقابة التقنية في حماية أموال المودعين واستمرارية العمل المصرفي.

الاستنتاجات والتوصيات

اولاً : الاستنتاجات

1- إنّ مواءمة معايير ISO/IEC 27001 وNISTCSF وCOBIT2019 ليست مجرد إجراء امتثال، بل هي ضرورة استراتيجية لبناء نموذج حوكمة قوي ومرن وقائم على القيمة للأمن السيبراني. من خلال الاستفادة من القدرات التكميلية لهذه الأطر، يُمكن للمصارف إنشاء بيئة حوكمة لا تقتصر على كونها قابلة للدفاع عنها أمام الجهات التنظيمية فحسب، بل تتميز أيضاً بالمرونة الكافية لمعالجة التهديدات الناشئة في الوقت المناسب.

2- يؤدي التدقيق الداخلي دورًا متعدد الأوجه في إدارة مخاطر الأمن السيبراني، يشمل وظائف التأكيد والاستشارة والتنسيق، ويُسهم التدقيق الداخلي في رقابة مجلس الإدارة من خلال التقييم المستقل لضوابط الأمن السيبراني وعمليات إدارة المخاطر.

3- يعمل التدقيق الداخلي كوسيط حاسم بين فرق الأمن السيبراني التقنية وهيئات الحوكمة.

ومن خلال ترجمة النتائج التقنية المعقدة إلى رؤى ذات صلة بالحوكمة، يُعزز المدققون الداخليون فهم مجلس الإدارة لمخاطر الأمن السيبراني وفعالية الضوابط. وبالتالي فان التدقيق الداخلي يعزز من حوكمة مخاطر الامن السيبراني.

4- أنّ مشاركة التدقيق الداخلي في حوكمة الأمن السيبراني تختلف اختلافًا كبيرًا بين المؤسسات، متأثرةً بنضج الحوكمة ودعم القيادة. و وجود التحديات التي تتعلق بالخبرة الفنية وقيود الموارد، التي تُحد من قدرة التدقيق الداخلي على توفير ضمانات شاملة للأمن السيبراني.

5- للتدقيق الداخلي دورا هاما في تعزيز مخاطر حوكمة الأمن السيبراني في المصارف العراقية عينة البحث، من خلال دمج الأمن السيبراني في تخطيط التدقيق القائم على المخاطر وإدارة مخاطر المؤسسة، وتقييم مدى كفاية سياسات الأمن السيبراني وخطط الاستجابة للحوادث وضوابط الوصول، حيث يعمل كمزود تأكيد مستقل ومستشار استراتيجي لمجالس الإدارة والإدارة التنفيذية، وبهذا يمكن للتدقيق الداخلي تحسين مرونة المؤسسة وتعزيز حوكمة مخاطر الأمن السيبراني.

ثانياً: التوصيات

1- أهمية تبني أطر عمل موحدة توفر لغة مشتركة، وعمليات منظمة، وضوابط قابلة للقياس لإدارة المخاطر السيبرانية ، نظرا لتشتت السياسات، واختلاف اللوائح التنظيمية في مختلف القطاعات، وعدم اتساق ممارسات الأمن بين وحدات الأعمال والمناطق الجغرافية، وذلك لضمان إدارة المخاطر السيبرانية كمسؤولية شاملة على مستوى المؤسسة، لا كمشكلة تقنية بحتة.

2- العمل على توفر كفاءات رقمية قوية، تشمل الأمن السيبراني، والحوسبة السحابية، وإدارة البيانات، وأتمتة العمليات الروبوتية. وتُعد هذه المهارات التقنية بالغة الأهمية لضمان مرونة المؤسسة في مواجهة التهديدات السيبرانية. ويجب ان يدعمها التدقيق الداخلي بكفاءات شخصية، مثل التواصل، والقدرة على التكيف، وحل المشكلات، مما يمكّن الموظفين والقادة من التعرف على تحديات الأمن السيبراني والاستجابة لها بشكل استباقي.

3- ضرورة قيام المدققين الداخليين في المصارف العراقية بتحسين بيئة الرقابة الداخلية والحوكمة وعمليات إدارة المخاطر، وذلك بالتركيز على مجالات التقنية أو الرقمية عالية المخاطر، مثل الأمن السيبراني، وكيفية إدارته بشكل أفضل أثناء التدقيق.

4- ضرورة تبني التدقيق الداخلي في المصارف العراقية نهجًا استشرافيًا يركز على المخاطر للحفاظ على أهميته في بيئات تنظيمية معقدة. ويُعدّ خطر الأمن السيبراني مثالًا على هذا التعقيد، إذ يتجاوز الضوابط المالية التقليدية ويتطلب تنسيقًا بين تكنولوجيا المعلومات وإدارة المخاطر والقيادة التنفيذية. وضرورة إصلاح التدقيق الداخلي لمعالجة ثغرات الحوكمة التي خلّفتها أطر الامتثال
التنظيمي التي لم تُصمّم لمواجهة التهديدات التكنولوجية سريعة التطور.

5- على المصارف العراقية العمل على تعزيز التدريب والتطوير المهني للمدققين الداخليين حول أحدث تقنيات الأمن السيبراني وأفضل الممارسات. و مراجعة سياسات الحوكمة وتحديثها بانتظام لتتوافق مع المعايير العالمية، بما في ذلك مؤشرات أداء واضحة وإجراءات تقييم المخاطر. واستخدام تحليلات البيانات المتقدمة لرصد الأنشطة غير المعتادة وتحديد المخاطر المحتملة بشكل استباقي. وتحسين التعاون بين فرق التدقيق الداخلي، وإدارات الأمن السيبراني، والإدارة العليا لتعزيز استراتيجيات الأمن وتخصيص الموارد وحوكمة مخاطر الامن السيبراني.

REFERENCES المصادر

1.Abiodun,E,A,. 2020. Internal Control Procedures And Firm's Performance. International Journal Of Scientific & Technology Research. Vol 9, No 02,.

2.Alhawtmeh,O,M,. 2025. The Role Of Internal Audit As A Tool For Enhancing Cybersecurity Effectiveness In Jordanian Government Agencies. Heritage And Sustainable Development. Vol. 7, No. 1,. Pp.317-328.

3.Alzeban,A,. 2025. The Quality Of Cybersecurity Audits: Do Synergies Among The Chief Audit Executive, It Governance, And Internal Audit Functions Matter. Laboratory For Studies And Research In Management, Economics, Social Sciences, Administration And Law (L-Ermessad), Cadi Ayyad University - Marrakech, Morocco.

4.Dikokoe,T,. 2021. Role Of Internal Audit In Managing Cyber Security Risks. Limited Scope Dissertation,Submitted In Fulfilment Of The Requirements For The Degree ,Magister Commercii In Computer Auditing. In The College Of Business And Economics At The University Of Johannesburg. South Africa.

5.Essien,L,. Cadet,E,. Ajayi,J,. Erigh,E,. Obuse,E,. Ayanbode,N,& Babatunde,L. 2022. Optimizing Cyber Risk Governance Using Global Frameworks: Iso, Nist, And Cobit Alignment. Journal Of Frontiers In Multidisciplinary Research. Vol.03. No 01. Http://Www.Multidisciplinaryfrontiers.Com/ .

6.Lois.P,. Drogalas,G,& Karagiorgos,A,. Thrassou ,A,& Vrontis,D,. 2021. Internal Auditing And Cyber Security: Audit Role And Procedural Contribution Int. J. Managerial And Financial Accounting, Vol. 13, No. 1,.

7.Melaku,H,M. 2023. A Dynamic And Adaptive Cybersecurity Governance Framework. J.Cybersecur. Priv. , 3.Pp 327–350. Https://Www.Mdpi.Com/Journal/Jcp

8.Newswire, P.R. (2018). Internal Audit's Growing Engagement In Cyber Management. Pr Newswire. Us.

9.Oliver, G., & Foscarini, F. (2014). Information Culture: An Essential Concept For Next Generation Records Management. In Dlm Forum-7th Triennial Conference P. 31.

10. Reynolds,M,J,. 2019. Assessing Audit's Role In Cybersecurity Risk Governance. Https://Www.Researchgate.Net/Publication/399713890_Assessing_Internal_Audit's_Role_In_Cybersecurity_Risk_Governance .

11. Sava¸S, & Karata¸S. 2022. Cyber Governance Studies In Ensuring Cybersecurity: An Overview Of Cybersecurity Governance. Int. Cybersecur. Law Rev. Vol, 3.No7. Https://Creativecommons.Org/Licenses/By/4.0/ .

12. Siyaya,M,C. Dubihlela ,J, & Sibanda,M,. 2025. A Literature Review Of Internal Auditing Involvement In Cybersecurity Risk Management Of The Organization. Journal Of Contemporary Management. Vol 22. No 1.

13. Whitehouse, T. (2015). Where Internal Audit Can Help In Cyber-Security. Compliance Week, 12(135):1-3.

14. Yusif,S& Hafeez-,A,. 2021. A Conceptual Model For Governance. Journal Of Applied Security Research. Doi: Https://Doi.Org/10.1080/19361610.2021.1918995