السنة الرابعة والعشرون/ عدد خاص/ تموز 2026
https://doi.org/10.31272/ijes.v24.1537

المجلة العراقية للعلوم الاقتصادية
Iraqi Journal For
Economic Sciences

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

The Role of External Auditing in Supporting Cybersecurity Requirements under the COBIT 2019 Framework

دوره التدقيق الخارجي في دعم متطلبات الأمن السيبراني وفق اطار COBIT- 2019

ا. د سلوان حافظ حميد كايد
SALOWAN HAFADH HAMED
Drsalowan_altaey@uomustansiriyah.edu.iq

ا م دسنان سالم قاسم الشيخ
Sinan Salem Qasim
dr.s.al-aikh@uomustansiriyah.edu.iq

كلية الادارة والاقتصاد / جامعة المستنصرية

Abstract

The research aimed to study cyber requirements according to the COBIT-2019 framework, while highlighting the role of external auditing in supporting regulatory controls to limit cyber violations and attacks. To achieve the research objectives, the researchers adopted the method of interviewing and an analysis study of financial reports for a sample of banks registered in the Iraq Stock Exchange, as well as auditing reports of an auditing company that issued for the financial year 2025. The interview questions included three axes. The first axis focused on studying external auditing for cybersecurity (consisted of ten questions). The second axis has adopted the COBIT-2019 framework in auditing cyber requirements and consists of seven questions. The last axis was the relationship between cybersecurity auditing and COBIT-2019 requirements and included seven questions. One of the most important conclusions reached by the research is the disparity between the auditing company and the sampled banks regarding the research that the knowledge of cyber requirements or the areas of the COBIT-2019 framework, which can see this gap, fundamentally reflects the assessment of governance requirements, information security and cyber risk management requirements.

Keywords: External audit, COBIT-2019, Information security, Cybersecurity requirements.

المستخلص

يهدف البحث إلى دراسة المتطلبات السيبرانية وفق اطار COBIT -2019 مع بيان دور التدقيق الخارجي في دعم الضوابط الرقابية للحد من الانتهاكات والهجمات السيبرانية ولغرض تحقيق أهداف البحث اعتمد الباحثان أسلوب المقابلة والدراسة التحليلية لمحتوى التقارير المالية لعينة من المصارف المسجلة في سوق العراق للأوراق المالية وتقارير شركات التدقيق الصادرة بموجب النشرة للسنة المالية 2025 وتضمنت أسئلة المقابلة على ثلاثة محاور ركّز الأول على دراسة التدقيق الخارجي للأمن السيبراني ويتكون من عشرة اسئلة أما المحور الثاني فاعتمد اطارا COBIT-2019 في تدقيق المتطلبات السيبرانية ويتكون من سبعة أسئلة والمحور الأخير العلاقة بين تدقيق

الأمن السيبراني ومتطلبات COBIT-2019 ويشمل سبعة اسئلة وأشارت أهم الاستنتاجات التي توصل اليها البحث إلى تفاوت شركات التدقيق والمصارف عينة البحث في معرفة المتطلبات السيبرانية او مجالات اطار COBIT-2019 الذي ينعكس بشكل جوهري في تقييم الالتزام بمتطلبات الحوكمة وأمن المعلومات وإدارة المخاطر السيبرانية .

الكلمات الرئيسية: التدقيق الخارجي , COBIT-2019 ,امن المعلومات , المتطلبات السيبرانية

المقدمة

في ظل المتغيرات التكنلوجية والتطورات التقنية الأمر الذي انعكس على كافة مجالات الأعمال ومنها القطاع المصرفي ذلك لما لها من دورٍ جوهريٍ في إدارة أمن المعلومات وإدارة المخاطر ,وضمن هذا التسارع الرقمي هناك انتهاكاتٍ وهجماتٍ سيبرانية او تعطيل في الأنظمة الالكترونية او اختراق البيانات الالكترونية التي تؤثر على موثوقية التقارير المالية وثقة اصحاب المصلحة. لذا فأنّ مسؤولية إدارة أمن المعلومات او المخاطر السيبرانية مسؤولية تكاملية بين المصارف والجهات الرقابية القطاعية في أمن حماية المعلومات وضمان توفير ضوابط رقابية الكترونية ,وهناك دور مهم لشركات التدقيق في تقييم تلك الضوابط ومدى التزام المصارف بها ,وان اطار COBIT-2019 من الأطر ذات العلاقة في مجال حوكمة أمن المعلومات والتكنلوجيا حيث يوفر مجالاتٍ تربط بين تحقيق الأهداف على المستوى الاستراتيجي للمصارف وبين الحوكمة التقنية ويتضمن الإطار مجموعة أهداف ومبادئ تساعد على تحديد وقياس مستوى النضج في ضوابط السيبرانية من حيث قوة او ضعف تلك الضوابط .

المبحث الأول : منهجية البحث وتشكيل المنهجية الأساس للبحث وتتضمن :

اولا: مشـــكله البحـــث: في ظل التغيرات المتسارعة في قطاعات الأعمال ذات الطابع الالكتروني والتهديـدات الـتي تتعـرض لهـا الأنظمـة الالكترونيـة مـن اختراقـات أمنيـة وتسريب للمعلومـات وانتهاكات وتعرضها إلى المخاطر السيبرانية التي تؤثر بشكل مباشر على جوده التقارير بالرغم من اعتماد المصارف أطرَ حوكمةٍ تقنية إلّا أنّ هناك قصور وعدم وضوح في دور التدقيق الخارجي في تقييم متطلبات الأمن السيبراني وفق اطار COBID 2019. بالشكل الذي يعزز الحوكمة ويحد من المخاطر السيبرانية هذا من جهة ويمكن النظر إلى المشكلة بالتعمق أكثر في دور شركات التدقيق في الحد من الهجمات السيبرانية باعتماد اطرٍ عالمية أحدها اطار COBIT- اذ يمكن صياغة المشكلة من خلال التساؤلات الاتية:

1. هل تدعم اجراءات التدقيق الحالية متطلبات الأمن السيبراني وفق إطار COBID 2019.
2. هل تمتلك شركات التدقيق الخبرات التقنية بشكل يعزز فاعلية الضوابط السيبرانية والاستعانة بالخبراء إذا تطلب الأمر.
3. هل تكشف تقارير شركات التدقيق بشكل كافي عن توتر متطلبات الأمن السيبراني ومخاطره .

ثانيا: أهداف البحث: يسعى البحث إلى تحقيق الأهداف الاتية:

1. تحديد مفهوم ومتطلبات الأمن السيبراني وفق إطار COBID 2019
2. بيان دور شركات التدقيق في دعم الضوابط الرقابية السيبرانية .
3. إجراء دراسة تحليليه توضح العلاقة بين التدقيق الخارجي ومتطلبات الأمن السيبراني وفق إطار COBID 2019

ثالثا: أهمية البحث: تنبع أهمية البحث من أهمية موضوع الأمن السيبراني والانتهاكات والمخاطر التي تتعرض لها الوحدات الاقتصادية ودعمها في تحسين جاهزيتها السيبرانية فضلا عن محاولة بعض من الباحثين في تحديد نواحي القصور او القوة التي تدعم التدقيق الخارجي في دعم متطلبات الضوابط السيبرانية والحد من المخاطر من خلال توضيح البعد الرقابي لإطار COBID 2019

رابعا :فرضيات البحث: يستند البحث إلى الفرضيات الاتية

1. تدعم اجراءات التدقيق الحالية متطلبات الأمن السيبراني وفق إطار COBID 2019
2. تمتلك شركات التدقيق الخبرات التقنية بشكل يعزز فاعليه الضوابط السيبرانية والاستعانة بالخبراء إذا تطلب الأمر توضح تقارير التدقيق الخارجي متطلبات الأمن السيبراني ومخاطره

خامسا: مجتمع وعينه البحث: يتمثل مجتمع البحث في دراسة التقارير المالية للمصارف المسجلة في سوق العراق للأوراق المالية للسنة المالية 2024 وشركات التدقيق بموجب النشرة الصادرة للسنة المالية2025أما عينة البحث فقد شملت المصرف الأهلي العراقي ,المصرف التجاري العراقي مصرف الائتمان العراقي ,مصرف المشرق العربي الاسلامي للاستثمار والتمويل أما شركات التدقيق شركة عادل الحسون وشركاؤه وشركة فرقد السمان وشركاؤه, شركة مصطفى عباس وشركاؤه وعدد من المحاسبين القانونيين ومراقبي الحسابات العامليين في تلك الشركات وتم اختيار المصارف وشركات التدقيق لسهولة الحصول على المعلومات وتعاون تلك الشركات مع الباحثين.

سادسا: الاطار المكاني والزماني للبحث: تمثلت الحدود المكانية في دراسة التقارير المالية وتقارير شركات التدقيق في بغداد أما الحدود الزمانية فقد شملت دراسة التقارير المالية للمصارف - للسنة المالية2024 ودراسة تقارير شركات التدقيق بموجب النشرة الصادرة للسنة المالية 2025

سابعا: مصادر جمع البيانات والمعلومات: شملت مصادر الجانب النظري والمقالات المنشورة ضمن المجلات المحكمة والمعايير الدولية الخاصة بمتطلبات الأمن السيبراني في اطار COBID 2019 فضلا عن المعايير الدولية للتدقيق الصادرة من IFAC. أما الجانب العملي فيتمثل بإجراء المقابلات وتحليل المحتوى للتقارير المالية وتقارير شركات التدقيق عند تنفيذ اجراءات التدقيق وبيان المتطلبات اللازم توفرها للأمن السيبراني فضلا عن تحديد التقنيات المعتمدة في المصارف عينة البحث للحد من المخاطر السيبرانية التي تعرضت لها المصارف عينة البحث .

ثامنا: منهج البحث: اعتمد الباحثان المنهج الاستنباطي في تحديد المفاهيم النظرية ذات العلاقة بمتطلبات الأمن السيبراني وفق اطار COBID 2019 فضلا عن ذلك دراسة المعايير الدولية للتدقيق ذات العلاقة بموضوع البحث أما ما يخص تحليل المحتوى للتقارير لغرض الحصول على المؤشرات التي تدعم البحث وتحديد نقاط القوة والضعف في مدى توفر المتطلبات التي تدعم المتطلبات السيبرانية التي تدعم عملية التدقيق.

تاسعا : نموذج البحث:

المتغير المستقل	المتغير التابع
التدقيق الخارجي	المتطلبات السيبرانيه وفق اطار COBID 2019

يشمل هذا المحور دراسات سابقة والاطار النظري للبحث

اولا: الدراسات السابقة: تمت مناقشة دراسات سابقة ذات العلاقة بمتغيرات البحث:

1- **دراسة Slapnicar etal.،[2022]:** هدفت الدراسة إلى تحليل العلاقة بين متطلبات الأمن السيبراني وفعالية التدقيق الداخلي حيث عمد الباحثون إلى دراسة آليه تدقيق الأمن السيبراني من ثلاثة ابعاد اولها التخطيط وثانيها الأداء وثالثها الابلاغ وقد توصل الباحثون إلى أنّ فعالية تدقيق الأمن السيبراني ترتبط ايجابيا بنضج إدارة المخاطر السيبرانية وسلبيا باحتمالية نجاح الهجوم السيبراني وقد توصل الباحثون إلى وجود ارتباط قوي وايجابي بين بعدي التخطيط والأداء بينما الابلاغ عن المخاطر السيبرانية إلى الإدارة العليا ومجلس الإدارة أقل من البعد الأول والثاني .

2- **دراسة عثمان 2023:** هدفت إلى دراسة واختبار أثر توكيد مراقب الحسابات في الإفصاح عن عمليات إدارة المخاطر السيبرانية على رغبة وقدرات المستثمرين في الأسهم فضلا عن اختيار

مستوى الخبرة و التأهيل العلمي للمستثمر و توصلت الدراسة إلى وجود علاقة معنوية إيجابية بين التوكيد المهني لمراقب الحسابات والافصاح عن المخاطر السيبرانية التي تواجهها الشركات لما لها من أثر على المدى البعيد على القدرة التنافسية للشركة على أسعار الأسهم وإنّ الافصاح عن تلك المخاطر يعمل على تعزيز سلامة وموثوقية التقارير المالية وزيادة الثقة والرغبة في الاستثمار بأسهم تلك الشركات إلى جانب ذلك توصلت الدراسة إلى وجود تأثير معنوي للعلاقة بين الخبرة وتأهيل المستثمر والافصاح عن تلك المخاطر من قبل مراقب الحسابات.

3- **دراسة Fadial ,etal.2023 :** و تهدف إلى دراسة تأثير الارتفاع الكبير في استخدام التكنولوجيا والمعلومات في زياده المخاطر والتهديدات التي تواجه أمن تلك المعلومات من قبل دائرة الاتصالات والمعلومات في مدينه pontianak ومن جهة حكومية تعتمد على التقنيات وتكنولوجيا المعلومات بشكل كبير ولمعرفه مدى قدره تلك الدائرة على إدارة المخاطر الاستراتيجية التي تتطلب إجراء تدقيق عليها من خلال دمج إطار center for internet security (cIs) مع critical security controls (csc) وذلك لتحديد مجالات التركيز في أمن الأصول التقنية مع استخدام COBIT- 2019 أهداف الرقابة على تكنلوجيا المعلومات لغرض اكتساب capaillty level باعتماد مصفوفه الأوليات Action priorty Madrit ومن خلال هذه المصفوفة ثم تحديد الأنشطة التي لم تنفذ والأنشطة الواجب تنفيذها لغرض رفع مستوى قابلية الأمن السيبراني .

4- **دراسة Metin etal. 2025:** هدفت الدراسة إلى تقديم دليلا عمليا لتطوير استراتيجيه الأمن السيبراني يستند إلى دمج اطار COBIT- 2019 مع مجموعه معايير ISO/EC2700 ذلك لأنّ اطار COBITيوفر مدخل إلى استراتيجيه وحوكمة تقنية المعلومات واعتمدت الدراسة معايير ISO لبناء استراتيجية قابلة للتكيف مع الوحدات الاقتصادية بمختلف أنواعها ومجالاتها فضلا عن ملائمة المتطلبات التقنية. وركزت الدراسة على تقديم تكامل بين COBID 2019 ومعاييرISO/EC وقد اقترحت منهجية لتطبيق التكامل من خلال المواءمة بين الأهداف المطلوب وتحقيقها ونطاق الاستراتيجية وتحويل تلك الأهداف إلى قرارات استراتيجيه لتكنولوجيا المعلومات باعتماد الحوكمة لنظم المعلومات وفقCOBID 2019 وأخيرا اعتمد ISO/EC 2700 أساس لغرض او اعتماد استراتيجيه الأمن السيبراني .

5- **دراسة الحسين و المعموري 2025:** هدفت الدراسة إلى معرفة العلاقة بين المسؤولية المهنية لمراقب الحسابات عن المخاطر السيبرانية و إنّ غالبية الجهات المالية والمصرفية لم تقوم بتحديد المخاطر السيبرانية او الافصاح عنها وغياب الاطار القانوني الذي يؤثر على إجراءات التدقيق ورأي مراقب الحسابات و الذي بدوره ينعكس على المسؤولية المهنية للمراقب وإنّ عدم الإفصاح عن المخاطر يعرضها إلى التهديدات السيبرانية ويتطلب وجود قانون للأمن السيبراني ملزم للجميع.

6- **دراسة الصير في2025:** هدفت الدراسة إلى اختبار أثر افصاح الشركات عن تفعيل إدارة مخاطر الأمن السيبراني على تقدير مراقب الحسابات لمستوى مخاطر التدقيق الخارجي واعتمد الباحث على اختبار أثر متغيرين معدلين moderators على العلاقة في البحث والمتمثلان بخبرة مراقب الحسابات وحجم المكتب وقد اسفرت نتائج الدراسة عن وجود علامة ذات أثرٍ معنويٍ بين الافصاح وتقدير مخاطر التدقيق فضلا عن وجود علامة ذات تأثير معنوي بين خبره مراقب الحسابات ومخاطر الاكتشاف ولا يوجد تأثير بالخطر المتلازم والخطر الطبيعي مع وجود علاقة ذات تأثير معنوي بين حجم الكتب ومخاطر التدقيق. وتشير الدراسات السابقة إلى دور اطار

COBID2019في دعم الحكومة بعينة المعلومات وإدارة المخاطر السيبرانية إذ أنّ بعض الدراسات ركزت على تكامل الاطار مع مجموعه معاييرISO/EC لبناء استراتيجيه الأمن السيبراني قابل التكيف بشكل يناسب الوحدات الاقتصادية في حين أنّ بعض تلك الدراسات ركز على كيفية تأثير المخاطر السيبرانية والعلاقة بالمسؤولية والمهنية لمراقب الحسابات وكيف تؤثر تلك المخاطر على مخاطر التدقيق ,بينما في دراسة أخرى ركزت على اليات التدقيق للأمن السيبراني من خلال أبعاد التخطيط والأداء والابلاغ حيث وجدت علاقة قوية من البعد الأول والثاني بينما البعد الاخير المتمثل بالإبلاغ عن تلك المخاطر إلى الإدارة اقل منها .لذا جاء البحث لغرض دراسة كيف يكون هناك دورٌ للتدقيق الخارجي في دعم المتطلبات الخاصة بالأمن السيبراني باعتماد2019-COBIT.

المبحث الثاني : الجانب النظري : التدقيق الخارجي للأمن السيبراني

قبل الدخول في تعريف التدقيق الخارجي للأمن السيبراني لابد من تعريف الأمن السيبراني حيث عرّف المعهد الوطني للمعايير التقنية الأمن السيبراني بأنّه حماية المعلومات والأنظمة من الهجمات الإلكترونية من خلال استخدام تقنيات وإجراءات وأدوات محددة لضمان السرية والتكامل والتوافر للمعلومات والأنظمة. أما ISO/IEC 27001 فقد عرفه بأنّه الجهود المتعمدة لحماية استخدام الإنترنت والبنية التحتية المتصلة بالإنترنت، بما في ذلك البرامج والأجهزة والبيانات من الهجمات والتدخلات الإلكترونية. بينما المعهد الأمريكي للمحاسبين القانونيين (AICPA) عرّفه بأنّه مجموعة من الأنشطة المتعددة التي تشمل حماية الأنظمة والشبكات والبرمجيات والبيانات من الهجمات السيبرانية، وكذلك استعادة الأنظمة بعد حدوث الهجمات. في حين أنّ المنتدى الاقتصادي العالمي .World Economic Forum يُعرّف الأمن السيبراني بأنه مجموعة من التقنيات والعمليات والممارسات المصممة لحماية الشبكات والأجهزة والبرمجيات والبيانات من الهجمات أو التلف أو الوصول غير المصرح به.ويعرف ISACA الأمن السيبراني بأنّه حماية الاصول المعلوماتية عن طريق التصدي للتهديدات التي تواجه المعلومات المعالجة والمخزنة والمنقولة عبر الأنظمة المعلوماتية المتصلة بالشبكة(ISACA,2019:13). وبذلك فإنّ الأمن السيبراني يتمثل بمجموعه من الآليات والإجراءات والوسائل التي تهدف إلى حماية البرمجيات وأجهزه الكمبيوتر من مختلف التهديدات والهجمات والاختراقات ولضمان الالتزام بمتطلبات الأمن السيبراني التي تهدف إلى تحقيق سرية المعلومات وسلامة المعلومات وتوافرها وإنّ التدقيق يساعد على تحقيق تلك الأهداف. ومن خلال المعيار الدولي للتدقيق 200 ISAيعرف بأنّه عملية منتظمة للتجميع والتقويم الموضوعي للأدلة المرتبطة بإقرارات الأحداث واقرارات اقتصاديه بهدف تحديد مدى التوافق بين هذه الاقرارات ومعيار المستخدم للحكم على صحة تلك القرارات ثم توصيل النتائج إلى المستخدمين المعنيين (هاينز واخرون ,2016:35) , وبذلك يحقق التدقيق قيمة اقتصاديه من خلال جعل المعلومات أكثر موضوعية للمستخدمين (والحد من مخاطر المعلومات الخاطئة او المحذوفة) وبذلك توسعت الخدمات التي يقدمها المدقق الخارجي حيث لا تشتمل فقط على الجوانب المالية إنما اتخذت مجالات أخرى تمثلت بالجوانب غير ماليه ومنها توكيدات تكنولوجيا المعلومات وبإمكان المدقق تقديم الخدمات الاستشارية او توكيدات في المتطلبات اللازمة لدعم الأمن السيبراني. ويوضح Tysiac (2020) وفقا لمعايير التصديق الصادرة من AICPA أنّه بإمكان المدقق تقديم تقرير مستقل حول ما إذا كان وصف الإدارة لبرنامج إدارة المخاطر للأمن السيبراني يفي بمواصفات اطار عمل تقارير الشركة اولا . وإن تدقيق الأمن السيبراني عملية حيوية تمكن المنظمات بمختلف أحجامها من تحديد وتقابل مخاطر الأمن السيبراني التي تواجهها، ويتمثل هذا التنسيق في فحص منهجي ودقيق للضوابط أمان المعلومات داخل. المنظمة، بهدف التحقق من كفاءتها في حماية البيانات والأنظمة الحساسة

بشكل فعال (Azab. 2024 : 2). يعد تدقيق الأمن السيبراني وفقا لإطار NIST عملية تقييم تهدف إلى ضمان أنّ المنظمات تطبق ضوابط أمنية فعالة وفقا للمعايير الواردة في الإطار وتشمل خمس وظائف التحديد Identify الحماية Protect والاكتشاف Detect والاستجابةrespond وأخيرا التعافي Recover لتعزيز قدرتها على مواجهة التهديدات السيبرانية وإدارة المخاطر الأمنية بفعالية (احمد ,2024 :574), والتعريف وفقا لمنظمة الأيزو: (ISO) تعريف تحقيق الأمن السيبراني من منظمة الأيزو (ISO) يعكس منهجاً شاملاً وموحداً لتقييم وإدارة الأمن السيبراني ضمن المنظمات تقدم الأيزو مجموعة من المعايير مثل ISO/IEC 27001 ، التي توفر إطارا لإدارة أمن المعلومات يشمل جميع أنواع المخاطر الأمنية (ISO,2022:4).يشتمل تدقيق الأمن السيبراني وفقاً لمعايير الأيزو على تقييم منهجي للسياسات الأمنية، الإجراءات والضوابط التي تحمي المعلومات من التهديدات أو الخروقات. كما إن عمليات إجراء تدقيق الأمن السيبراني تتم بشكل معمق لمعرفة التدابير التي تعتمدها الوحدة الاقتصادية وهي جزء من استراتيجيه إدارة المخاطر وذلك لأنه اذا كانت الإجراءات المعتمدة في عمليه التدقيق صحيحه وفق أسس سليمة فإنه يتم الكشف عن المخاطر السيبرانية التي تواجه الوحدة ,ويمكن تشخيص السياسات والاجراءات وضوابط الإدارة لهذه المخاطر بتشكل فعال وبذلك يساعد التدقيق في الافصاح عن المعلومات التاليه https://www.csentity.com/Compliancecurity

1. ممارسات أمن البيانات
2. أداء البرامج والأجهزة
3. الامتثال التنظيمي والقانوني
4. نقاط الضعف التي تؤثر على النظام
5. فعاليات السياسات والإجراءات الأمنية الحالية
6. وجود تهديدات داخلية وخارجية

إنّ عملية التدقيق تتطلب أن تستند إلى معايير يعتمدها المدقق فضلا عن الالتزام بالمعايير الدولية للتدقيق التي تؤكد على أداء تدقيق عالي الجودة وبكفاءة ونزاهة وموضوعية واستقلالية بهدف دعم التحسين المستمر وتحقيق أعلى معايير الجودة والمساءلة في عمليات التدقيق ولا يقتصر الأمر على ذلك بل يعتمد على دور المدقق حيث يشير إلى مركز جودة التدقيق Thecenter for Audit Quality يشتمل دور مراقبي الحسابات على جانبين مهمين تدقيق ومراجعة القوائم المالية ونظم الرقابة الداخلية على التقارير المالية Control Over Financial Reporting(ICFR) ، والإفصاحات. ويحتاج مراقبو الحسابات إلى تقييم مخاطر التحريف الجوهري الناتج عن القضايا المتعلقة بالأمن وتأثيرها على القوائم المالية وعلى نظم الرقابة الداخلية على التقارير المالية (ICFR) ، كما يحتاج مراقبو الحسابات أيضا إلى تنفيذ الإجراءات المتعلقة بمعلومات الأمن السيبراني التي تم الإفصاح عنها في القوائم المالية وفي أي مكان آخر. وتعتمد مسؤوليات مراقب الحسابات على ما إذا كان الإفصاح مدرجا في القوائم المالية المدققة أو في أي مكان آخر. فإذا كان الإفصاح في القوائم المالية المدققة ، يحتاج إلى مراقب الحسابات لإجراء تدقيق محدد لتقييم ما إذا كانت القوائم المالية ككل معروضة بشكل عادل من جميع الجوانب الجوهرية. أما إذا تم الإفصاح عن معلومات الأمن السيبراني في مكان آخر، يحتاج مراقب الحسابات إلى قراءة الإفصاح والنظر فيما إذا كانت المعلومات التي تم الإفصاح عنها أو طريقة عرضها غير متوافقة جوهريا مع الإفصاح الظاهر في القوائم المالية (Calderon & Gao ,2021). أمّا مجلس (PCAOB) ، فأشار إلى أنّه يجب على المراقبين ألّا يقوموا فقط بتقييم تأثير الحادث والتحريفات الجوهرية على القوائم المالية للشركة، ولكن أيضا تقييم مخاطر أحداث الأمن

السيبراني حتى لو لم تحدث مثل هذه الأحداث بعد , وفي نفس السياق، أصدر مجلس AICPA إطارا لإعداد تقارير الأمن السيبراني على مستوى الشركة ,يتكون الاطار من ثلاثة مكونات وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني للوحدة الاقتصادية وتأكيد الإدارة وتقرير المراقب. المكون الاول وصف سردي لبرنامج إدارة المخاطر للأمن السيبراني للوحدة الاقتصادية والذي يوفر أساسا لفهم الطريقة التي تدير بها الوحدة مخاطرها السيبرانية وضوابطها الرقابية استجابةً لتلك المخاطر. المكون الثاني هو تأكيد من الإدارة حول ما إذا كان وصف الإدارة مقدما بما يتماشى مع معايير الوصف المحددة من قبل AICPA وما إذا كانت الضوابط المنفذة جزءً من البرنامج فعالة في تحقيق أهداف .المكون الأخير هو رأي مراقب الحسابات حول العرض العادل لوصف الإدارة ومدى ملاءمة تصميم ضوابط الرقابة وفعاليتها في تحقيق أهداف الأمن السيبراني(2021).Lietal. Cyber SECURITY PROG RAM Audit GUIDE (2023 وحدد خطوات تدقيق الأمن السيبراني والتي تضمنت بالتخطيط ثلاث خطوات رئيسية على التدقيق اعتمادها اولا التخطيط والتصميمPlanning and designing والثانية الأداء والتنفيذ Preforming والأخيرة إعداد التقريرReporting وقد تضمنت الخطوة الأولى على البحث التمهيدي والحصول على المعلومات حيث تشكل هذه الخطوة نقطة انطلاق والخطوة الثانية تحديد أهداف التدقيق السيبراني دعما تقييميا للضوابط السيبرانية بموجب متطلبات إدارة أمن المعلومات واستكمال تدقيق الأداء من خلال تقييم فعالية الأمن السيبراني ضمن سياق التدقيق والمراجعة بشكل أوسع للأنظمة , حماية سرية البيانات وموثوقية المعلومات وتحديد المخاطر السيبرانية من خلال تدقيق الضوابط وفحص عمليات واجراءات تطوير الأنظمة والخطوة الاخرى ضمن ذلك تتمثل بتحديد مجال او نطاق التدقيق ويقصد بها شمولية التدقيق بمعنى شامل لجميع أنظمة الوحدة الاقتصادية او محدد بتدقيق تقنية معينه على سبيل المثال الشبكات الكلاسيكية المحاسبية السحابية البلوك تشين والذكاء الاصطناعي .والخطوة الثانية قيام المدقق بعقد اجتماع من الجهة الخاضعة إلى التدقيق بغرض تحديد هدف التدقيق والنطاق والاطر الزمنية مع الطلب بتزويد فريق التدقيق بالوثائق المطلوبة عن العمليات التشغلية والهيكل التنظيمي لتقنية المعلومات والإدارة ووظائفها والوثائق الفعلية من النفقات التقنية والمعلومات عن الموظفين المتعاقدين والموقع والعقود ومسؤوليات الجهة والمتعاقدين ومعلومات عن هيكلة الشبكات والأنظمة وضوابط الأمن والخصوصية ومخططات الشبكات والحصول من وثائق ذات علاقة بالأحداث المهمة الأخيرة كالحوادث التقنية الخاصة بالمعلومات والأمن السيبراني ذات الأثر الكبير والجوهري. وبعد ذلك يعمل المدقق على تحديد المعايير اللازمة لإجراء عملية تدقيق وفق متطلبات القانون و إدارة المعلومات الفيدرالية او اطار إدارة المخاطر الصادرة للمعهد الوطني للمعايير التقنية او اطار COBIT-2019 او 53-800 – NISTSP او غير ذلك أما في مرحله التصميم وهي توثيق إجراءات التدقيق لضمان الوصول الكاف للمعلومات وإجراء الاختبارات والحصول على الأدلة المادية ومن أمثله ذلك جرد أنظمة المعلومات ,التقارير التدقيق ذات العلاقة وتقييمات الأمن والخصوصية مخططات الشبكات والاتفاقيات وحوادث الأمن السيبراني خلال فترة زمنية. في هذه المرحلة يعتمد المدقق على تقسيم موثوقية البيانات والأدلة التي تم الحصول عليها ويشير الدليل بالرجوع إلى GAO الفقرة الخاصةAssessing Data Reliability(المهتدي ,2021: 20-21):

تقرير نتائج التدقيق: بعد تنفيذ عمل التدقيق، يجب على الفريق الرقابي .

1. مراجعة النتائج مع المنظمة المدققة.
2. إعداد مسودة التقرير.
3. الحصول على أراء المنظمة المنافقة على مسودة التقرير.

4. إتمام التقرير

مراجعة نتائج الوحدة المدققة: عند إتمام عمل التدقيق، يجب على فريق التدقيق تقديم بيان بالحقائق للهيئة الخاضعة يصف نتائج التدقيق. يمكن للهيئة الخاضعة التعليق على هذا البيان ومناقشته وتقديم ملاحظات ووثائق داعمة قد تؤثر على النتائج والتوصيات خلال هذه الفترة، ويتم مناقشة أية مسائل حساسة قد تكون لدى العينة الخاضعة وتحديث. مسودة التقرير وفقا لذلك يجب التواصل مع هذه الأخيرة بشأن أية نتائج تتطلب إصلاحا فوريا طوال فترة التدقيق حسب الحاجة.

إعداد مسودة التقرير: يجب أن تقدم تقارير التدقيق النتائج بطريقة واضحة ومفهومة. كما يجب أن يتضمن التقرير أهداف التدقيق. النطاق المنهجية النتائج الاستنتاجات والتوصيات يجب دمج المعلومات المقدمة من الهيئة الخاضعة استنادا إلى بيان الحقائق بشكل مناسب في التقرير، يفضل استخدام الرسوم البيانية والجداول لتعزيز وضوح التقرير وقراءته.

الحصول على آراء الوحدة المدققة على مسودة التقرير: تقديم مسودة التقرير مع النتائج المراجعة والتعليق من قبل المسؤولين في الهيئة الخاضعة ما يساعد في تطوير تقرير عادل، شامل، وموضوعي تفضل التعليقات المكتوبة من الوحدة، ولكن التعليقات الشفهية مقبولة أيضا.

إنهاء التقرير: بعد أن يتم حصول الهيئة الخاضعة على الوقت الكافي لمراجعة مسودة التقرير وتقديم تعليقاتها، يمكن لفريق التدقيق إنهاء تقرير التدقيق، يتضمن إنهاء تقرير التدقيق معالجة تعليقات الهيئة الخاضعة أو رسالة استجابة الإدارة الموقعة، إذا تم تقديم تعليقات شفهية بدلاً من ذلك، يجب تحديد مصدرٍ في تقرير التدقيق. بعد إتمام هذه الخطوات، يمكن لفريق التدقيق المضي قدما في عملية نشر وتوزيع التقرير. التعليقات

تحديد حساسية التقارير: عند إعداد تقارير الشقيق في الأمن السيبراني، غالبا ما تقوم المنظمات بإعداد تقريرين: تقرير عام وتقرير حساس يحتوي على محتوى لا يمكن نشره الجمهور، يتميز التقرير الحساس بتقديم تفاصيل إضافية حول. المنظمة ونتائج التدقيق، ولكن عيبه هو خطر الكشف، خاصة إذا تم إصدار المنظمة تشاركه مع عدد كبير من الموظفين لتسهيل التصحيح فيتمتع التقرير العام بجمهور أوسع وشفافية أكبر ولكنه لا يمكن أن يحتوي على معلومات حساسة. لتجنب الكشف العلني للمعلومات الحساسة، يجب تقديم مسودات تقارير الأمن السيبراني إلى الهيئة. الخاضعة لمراجعة الحساسية بعد تلقي نتائج مراجعة الحساسية، يتم إجراء التعديلات المناسبة على اعتمادا على التدقيق، يمكن إصدار تقرير عام أو حساس أو كليهما (GAO,2024-15-14)وتشير الفقرة سادسا من دليل ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات في الاتصالات بالقطاع المصرفي الصادر البنك المركزي لسنه 2019 عراقي ان هناك معايير تدقيق تقنية المعلومات والاتصالات وحسب المعايير الدوليةInformationTechnology Assurance Framework الصادر عن جمعية التدقيق والرقابة على نظم المعلومات ISACAC تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الشأن نأخذ بالحسبان الأهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير في أهداف ومصالح المؤسسة, توفير والالتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد الالتزام بمعايير الاستقلالية المهنية والإدارية وضمان عدم تضارب المصالح الحالية والمستقلية والالتزام بمعايير الموضوعية ونقل العناية المهنية والحفاظ المستمر على مستوى التنافسية والمهنية من المعارف والمهارات الواجب التمتع بها، ومعرفة معمقة في اليات وعمليات المؤسسة المختلفة المرتكزة على تقنية المعلومات والاتصالات وتقارير التدقيق (المالية

والتشغيلية والقانونية)، والقدرة على تقييم المتناسب مع الحالة و الوضع العام في كشف الممارسات غير المقبولة و المخالفة لأحكام القوانين والأنظمة والضوابط. (البنك المركزي العراقي ، 2019 : 10 - 11) وقد أصدر ISACA الإصدار الرابع وتضمن إرشادات ومعايير مهنية أشارت إلى دور ومسؤولية إجراءات تدقيق تقنية المعلومات والاخلاقيات المهنية والمعرفة والخبرة اللازمة لمن ينفذ هذا النوع من التدقيق ، فضلا عما تم طرحه أعلاه من ارشادات يعتمدها المدقق تتوافق مع مراحل عملية التدقيق والتي تؤكد على الجوانب السيبرانية و المتطلبات الواجب توفرها وتقييم المخاطر وموضوعية مراقب الحسابات عند تنفيذ المهام التدقيقية. (Mani, 2-1 -2020). وضمن هذا الاتجاه يشير المبدأ الثالث الكفاءة المهنية والعناية اللازمة بالدليل قواعد السلوك الاخلاقي للمحاسبين المهنيين الصادرة عن IFAC : (IFAC,2024:26)

(1) أن يحافظ على المعرفة والمهارات المهنية بالمستوى المطلوب لضمان أن يستلم العميل أو صاحب العمل خدمات مهنية تتسم بالكفاءة مبنية على التطورات الحالية في المعايير التقنية والمهنية والتشريعات ذات العلاقة.

(٢) وأن يؤدي مهامه بكل اجتهاد وعناية وفقا للمعايير الفنية والمهنية المعمول بها.

يؤكد كلا من Alford, etal.(2022) على أنّ الأمن السيبراني أصبح بالغا الأهمية في العالم الرقمي لذا على المراقب الالتزام بمبادئ دليل قواعد السلوك لأنّ متطلبات العالم الرقمية تؤكد الحاجه إلى زيادة المعلومات ونظرا لأهمية السرية والنزاهة التي لابد من توفيرها والالتزام بها , لذا على المراقب عند القيام بهذا النوع من نشاط التدقيق الى فهم ذلك, هذا الأمر يتطلب تحليل العوامل التي تؤثر على أداء التدقيق في ظل التقنيات المتسارعة من خلال توسيع دور المراقب بشكل يساهم في تحقيق الإسهام الفعال في هذا المجال (Alford,2022:10). ويوضح (2018) Raguseoأنّ لامتلاك مراقب الحسابات قدرة فنية تقنية على تطبيق التكنولوجيا من أعمال التدقيق ويساعد ذلك على نجاح استراتيجيات التدقيق في التنبؤ بالمخاطر ومعالجتها ومن ثم المعالجة والمتابعة إلى النتائج التدقيقية. في حين أشارت دراسة Alles (2015) أنّ المعهد الامريكي للمحاسبين القانوني أكد على ضرورة تحويل التدقيق من منهج التدقيق التقليدي إلى اعتماد مناهج حديثه مبنية على استخدام التقنيات في أداء مهام التدقيق , على نحو دراسة Bizarro, etal. (2019) التي استندت على معايير التدقيق الصادرة من مجلس الرقابة والاشراف على محاسبة الشركات العامة ، وارشاداتISACAC حيث أكدت الدراسة على مراقب الحسابات ضرورة وأهمية القدرة على فهم أثر استخدام التكنولوجيا من قبل الوحدات الاقتصادية موضوع التدقيق عند تقييم الخدمات التدقيقية, أما Munoko,etal (2020) فقد أشار إلى دار مجلس معايير التدقيق والتأكيد الدوليةIAASB في انشاء مجموعه عمل متخصصه بالتكنولوجيا بهدف الحصول على مصدر البيانات من مختلف أصحاب المصلحة في ضوء ذلك تشير المجموعة دليلUsing the work of an External Expert إلى الحاجه في الاعتماد على الخبراء في هذا المجال وبذلك فإنّ معيار التدقيق الدولي260 IAS يوضح تحمل المدقق المسؤولية المهنية عند الاعتماد على الخبرة والمهارات والمعرفة والتجربة في مجال التقنيات مع مراعاة الشروط التي وردت في المعيار في حالة الاستعانة بالخبير (SCOCPA,2024:778) ،أما بخصوص الدليل الصادر عن المجموعة التابعة إلى IFAC فإنّ ما ورد سيتم تطبيقه في نهاية عام 2026 ومن أهم ما ركز عليه الدليل هو أنّ عمل الخبير الخارجي يساعد في توفير معلومات إلى الجهات ذات المصلحة وأنّ تزايد الحاجة إلى الخبراء الخارجيين في مجال الأمن السيبراني او التكنولوجيا في ظل تقنيات الأعمال ذات التطور والابتكار المتسارع, ولكن في نفس الوقت اكد الدليل على ضرورة الالتزام بمبادئ الاخلاقيات التي وردت في دليل قواعد السلوك الصادرة IFAC (IFAC,2025,2).

ثالثا: متطلبات الأمن السيبراني وفق إطار COBIT- 2019: قبل تحديد متطلبات الأمن السيبراني وفق اطار COBIT وهو باختصار Control Objective For Information Related Technologies يمثل اطار عمل إدارة تكنلوجيا المعلومات تم تطويره بواسطة ISACA لمساعدة الشركات على تطوير وتنظيم استراتيجيات حول إدارة المعلومات والحوكمة ويمثل الإطار المحدث إطار عمل للمؤسسات من خلال معالجة الاتجاهات والتقنيات والاحتياجات الأمنية الجديدة . ويساعد الإطار في المواءمة بين أهداف العمل مع أهداف تكنلوجيا المعلومات من خلال انشاء روابط بين الاثنين وانشاء عملية يمكن أن تساعد في سد الفجوة بين تكنلوجيا المعلومات او صوامع تكنلوجيا المعلومات والإدارات الخارجية .(الموسوعة العربية -htpps//wwwarab ency.com,2022)ويستند الاطار الى المبادئ الاتية :

1- تلبية اصحاب المصلحة تمكن الوحدة الاقتصادية تكيف الاطار بما يناسب سياق عملها الخاص وتوضيح تتابع الاهداف والاولويات وترجمة الغايات الوحدة الاقتصادية العالية المستوى إلى أهداف محددة متعلقة بتقنية المعلومات والإدارة بمعنى مواءمة تكنلوجيا المعلومات مع أهداف العمل وتوقعات أصحاب المصلحة.

2- تغطية الوحدة الاقتصادية من البداية إلى النهاية : يتضمن الاطار ضمن هذا المبدأ شمولية الحوكمة وإدارة تكنلوجيا المعلومات إلى الوحدة الاقتصادية ,حيث لا يركز الاطار على وظيفة تقنية المعلومات فقط ,انما يتعامل مع المعلومات والتقنيات باعتبارها أصولا ويجب على كل فرد في الوحدة الاقتصادية التعامل معها تماما مثل اية اصول اخرى.

3- تطبيق اطار عمل واحد متكامل يركز هذا المبدأ على الوحدة ودمج المعايير مع افضل الممارسات ضمن مظلة واحدة لتوحيد وتظافر الجهود .

4- تمكين اسلوب كلي ضمن هذا المبدأ يعرف الاطار سبع فئات على عناصر التمكين اولها المبادئ والسياسات واطر العمل وثانيهما الاجراءات والثالث الهياكل التنظيمة اما الرابع الثقافة والاخلاق والسلوكيات والخامس المعلومات والسادس الخدمات والبنية التحتية والتطبيقات والأخير الافراد والمهارات والكفاءات .

5- فصل الحوكمة عن الإدارة :يميز الاطار بالوضوح بين الحوكمة والإدارة وهذان المجالان يتضمنان أنواعا مختلفة من الأنشطة ويتطلب هياكل تنظيمية مختلفة حيث يحدد بشكل واضح مسؤوليات الحوكمة في التقييم والتوجيه والمراقبة اما مسؤولية الادارة في التخطيط والبناء والتشغيل والمراقبة.

وعلى المحاسب ان يلاحظ المجالات ذات العلاقة بالأمن السيبراني وفق الاطار والتي تتمثل بالحوكمة والادارة وفق النموذج المرجعي المعتمد حيث تتضمن الحوكمة خمس عمليات وفي كل عملية يتم تعريف ممارسات التقييم Evaluate والتوجيه Direct والمراقبة Monitor والمعروفة اختصارا EDM وتشمل هذ المجموعة (EDM01 تأكد من وضع يانة اطار الحوكمة ,EDMO2 تأكد من تحقيق المنافع ,EDM03 تأكد من تحسين المخاطر ,EDM04 تأكد من تحسين الموارد EDMO5 تأكد من شفافية اصحاب المصلحة)اما مايخص الادارة كما ذكرنا سابقا يركز الإطار على اربعة مجالات متماشية مع مناطق ومسؤوليات التخطيط Plan والبناء Build والتشغيل Operate والمراقبةMonitor والمعروفة اختصارا PBRM وتوفر هذه النطاقات تغطية شاملة لمسائل تقنية المعلومات وهي مطوره عن الاطار السابق الى COBIT وتتضمن الاتي:

1- المواءمة Allige والتخطيط Plan والتنظيم Organize واختصارا APO
2- البناء Build والاستحواذ Acquire والتنفيذ ImplementواختصارBAI
3- تقديم الخدمة Deliver وصيانتها Service ودعمها Suport واختصارDSS

4- المراقبة Monitor والتقييم Evaluate والتقريرAssess واختصارا MEA
ويحتوي كل نطاق على مجموعة من العمليات وان معظم العمليات تتطلب انشطة التخطيط والتطبيق والتنفيذ والمراقبة وتشير دراسة Handayani ,etal.(2023) التي ركزت على تحليل مجموعة من الدراسات السابقة ذات العلاقة بتدقيق عمليات ادارة المخاطر التكنلوجية وفق اطارCOBIT للأبحاث والدراسات المنشورة للفترة 2019-2023 وتوصل الباحثون ان نطاق ادارة المخاطر وتاكد من تحسين ادارة المخاطر يعدان الاساس في حوكمة وادارة المخاطر الخاصة بتكنلوجيا المعلومات لما يتميز به الاطار من الشمولية في تحديد المخاطر وقياسها وينعكس ذلك على تحسين الاداء , في حين توضح دراسة AlMusawi(2021) ان على مراقب الحسابات عند تنفيذ عملية التدقيق للأنظمة المحاسبية الالكترونية ان يركز على مدى الالتزام المصارف العراقية بمتطلبات الحوكمة الالكترونية وان الاعتماد على الاطار لتعزيز ضوابط الرقابة الداخلية وينعكس بذلك على امن المعلومات وموثوقية البيانات المحاسبية وبذلك يقلل من المخاطر الجوهرية التي تواجه مراقب الحسابات. اما دراسة Toyner and Sfenrianto (2023) ركزت الدراسة على تقييم امن المعلومات في شركة PT xyz كونه عنصر اساسي في جميع الانشطة التجارية الخاصة بها ذلك لوجود تهديدات تعرض امن المعلومات الى خطر وتعد بذلك اصل assets للشركة وانه من الضروري اجراء تقييم او قياس فعالية الانشطة الرقابية وضوابطها لحماية المعلومات ,ومن خلال الاطار وبالأخص التركيز على ادارة خدمات الامن Manage Security Service(DSS05) يهدف الى قياس مدى كفاءة الضوابط المطبقة على امن المعلومات داخل الشركة. يعد ماتم عرضه في الجانب النظري من دراسات سابقة والتدقيق الخارجي في المتطلبات السيبرانية ومبادئ ومرتكزات اطار COBITسيعتمد ذلك في بناء وانجاز الجانب العملي.

المبحث الثالث : الجانب التطبيقي

بعد عرض الجانب النظري سيعتمد الباحثان على المقابلات الشخصية الى عينة من مراقبي الحسابات العاملين في شركات التدقيق المجازة لسنة المالية 2025 , فضلا الى الزيارة الميدانية الى عينة ن المصارف العراقية المسجلة في سوق العراق للأوراق المالية ,وتم اختيار العينة لمساعدتهم في الحصول على المعلومات وتنفيذ متطلبات الجانب العملي من البحث وتضمن اسئلة المقابلة على ثلاثة محاور يتضمن المحور الاول عشرة اسئلة اما المحور الثاني والثالث يتضمن سبعة اسئلة ,فضلا الى ذلك تحليل محتوى البيانات المالية وتقرير مراقب الحسابات ,واعتمد الباحثان من خلال الزيارة الميدانية اسلوب الملاحظة والمشاهدة بهدف تعزيز المعلومات التي تم الحصول عليها من خلال المقابلات .

المحور الاول: التدقيق الخارجي للأمن السيبراني يتضمن هذا المحور عشر اسئلة:

1- هل يتم الاستعانة بخبراء وفق معايير التدقيق الدولية عند الحاجة لتنفيذ متطلبات التدقيق للأمن السيبراني؟ من خلال اجابة عينة البحث لديهم لمعرفة الجوانب السيبرانية والتقنية وهناك حاجة الى الاستعانة بالخبراء لتنفيذ عمليات التدقيق ,بالرغم ان الجهات الرقابية المتمثلة بالبنك المركزي العراقي اصدر العدد من الضوابط كضوابط الصمود السيبراني للقطاع الملي والمصرفي وتهدف الى توفير تفاصيل اضافية تتعلق بتدابير على المصارف اتخاذها لتعزيز القدرات الصمود السيبراني والتنبؤ بالهجمات السيبرانية ومقاومتها والتعافي منها بسرعة ,هذا من جانب اما الجانب الاخر اكد مراقبي الحسابات الى تزايد الاهتمام من قبل المصارف بمتطلبات الامن السيبراني ولكن هذا الاهتمام يركز بالأخص على الجوانب التشغيلية بشكل اوسع .ومن خلال تحليل محتوى تقارير الإدارة للمصارف عينة البحث افصحت العديد من المصارف ضمن أهدافها الاستراتيجية استثمرت في انشاء البنية التحتية والتشغيلية والتكنلوجية التي تمكن المصارف من الاستفادة من

فرص الأعمال وتوفير افضل خدمة الى الزبائن.

2- ماهي ابرز المخاطر السيبرانية ؟ من ابرز المخاطر السيبرانية تتمثل بالاختراقات الالكترونية والهجمات السيبرانية على أنظمةCoreBanking والمخاطر التي تؤدي بالتلاعب بالبيانات المالية.

3- هل ان الهجمات السيبرانية تؤثر على موثوقية القوائم المالية؟ تشير اجابات عينة البحث ان الهجمات السيبرانية بشكل عام تؤثر على القوائم المالية من خلال التلاعب او فقدان المعلومات ومن خلال تحليل القوائم المالية للمصارف تؤكد على تطبيق متطلبات الحوكمة الالكترونية للحد من الاختراقات التي تؤثر على الزبائن وعلى المصرف على اعتباره أحد الاهداف التي تسعى الى تحقيقها في ظل التحولات الرقمية وان بعض المصارف عينة البحث فعلت نظام اكتشاف الثغرات Tenable للاكتشاف الثغرات وفعلت برنامج Siem لمراقبة البنى التحتية من الهجمات السيبرانية واقامة العديد من الدورات التدريبية لموظفين في مجال الامن السيبراني.

4- شركات التدقيق تأخذ المخاطر السيبرانية عند وضع خطة التدقيق وتنفيذها؟ تشير اجابة مراقبي الحسابات انه يتم الاخذ بالمخاطر السيبرانية ولكن بدرجات متفاوتة حيث البعض منها يعطي الأولوية لها والبعض الاخر يركز بشكل بسيط على تقييم المخاطر السيبرانية ضمن مخاطر تكنلوجيا المعلومات.

5- تقييم الضوابط الرقابية الخاصة بتكنلوجيا المعلومات؟ ان اجابات مراقبي الحسابات الخاصة بتقييم الضوابط الرقابية العامة على تكنلوجيا المعلومات ذات الصلة بموثوقية التقارير المالية والتأكد على مدى التزام المصارف بالضوابط والإعمامات الصادرة من البنك المركزي وتنفيذها فضلا عن الضوابط الرقابة العامة ذات العلاقة بأمن الملفات لنظم المعلومات المحاسبية وحمايتها التي تؤثر على موثوقية التقارير المالية ,ومن خلال دراسة وتحليل محتوى التقارير افصحت ادارة بعض المصارف قد فعلت نظام AM Lock لمكافحة غسيل الاموال ونظام ISE لحماية البيانات فضلا الى ذلك تحديث اجهزة FortiGate لتأمين الشبكة من الهجمات مع تطبيق COBIT و PCI/DSS لضمان الامتثال الى متطلبات البنك المركزي.

6- تأثير العلاقة بين جودة الضوابط الرقابية ومخاطر التدقيق؟ هناك علاقة بين جودة الضوابط من حيث الضعف والمتانة والمخاطر التدقيق حيث ان ضعف الضوابط له علاقة بزيادة حجم الاجراءات الجوهرية .ومن خلال تحليل محتوى تقرير شركات التدقيق عينة البحث تم الافصاح عن تحديد وتقييم المخاطر الجوهرية سواء ناتجة تلك المخاطر عن الاحتيال بأنواعه او الخطأ ويتم تصميم إجراءات التدقيق بشكل يستجيب إلى المخاطر بهدف الحصول على الادلة الكافية والملاءمة التي توفر الاساس لإبداء الرأي.

7- هناك معايير محلية صادرة عن مجلس معايير المحاسبية والرقابية خاصة بالأمن السيبراني؟ كانت اجابة مراقبي الحسابات ان هناك دليل صادر عن ديوان الرقابة المالية الاتحادي ادارة تكنلوجيا المعلومات والاتصالات وتخضع المصارف إلى رقابة البنك المركزي باعتباره الجهة القطاعية واكد مراقبو الحسابات ملاحظتهم على التزام المصارف بالضوابط الجهة القطاعية فضلا عن ذلك فإنّ شركات التدقيق مستقلة في تنفيذ التدقيق وفق قواعد السلوك المهني للمحاسبين القانونيين والالتزام بمعايير التدقيق الدولية الصادرة عن IFAC.

8- التحديات التي تواجه شركات التدقيق عند الانظمة المصرفية الالكترونية Core Banking systems؟ من التحديات التي تواجه شركات التدقيق عدم وضوح وتعقيد بعض الانظمة المصرفية فضلا عن حاجة شركات التدقيق إلى الاستعانة بالخبراء وهذا يتطلب اجور اضافية وتحمل تكاليف تدقيق اخرى.

9- مساهمة ادوات التدقيق الالكتروني في اكتشاف المخاطر السيبرانية؟ من خلال تواجد الباحثين

في عينة البحث تعتمد المصارف على ادوات وتقنيات تعتمد على اجراء تحليل والاستجابة التلقائية وان استخدام ليس بشكل موسع ومن هذه الادوات ادارة برمجيات حماية اسماء النطاقات (DNS Security) حماية منصات البريد الالكتروني وخدمات شبكات مايكروسوفت السحابية Microsofit office 365 وفضلا الى ذلك متابعة وتطبيق تقنيات التشفير لحماية البيانات اثناء النقل والتخزين وادارة وحدات الامان المادي Hardware Security Module وتطبيق وادارة التحكم بالوصول الشيبكيNAS/ Network Access Control .

10- المتطلبات السيبرانية والتطورات التقنية وماهي المقترحات لتطويرات مهارات مراقبي الحسابات؟ اجاب مراقبي الحسابات على المدقق الالمام بكافة مقومات مهنة التدقيق وتقنية المعلومات كاستخدام البرامج الجاهزة والتدقيق عن بعد ذلك من خلال التدريب المستمر لإنجاز المهام التدقيقية بدرجة عالية من الكفاءة والفاعلية والاطلاع على الارشادات الصادرة من المنظمات المهنية ذات العلاقة بالتدقيق التقني ومن ابرز التقنيات التعلم الالي Learning Machine الخاصة هذه التقنية بالتعرف على الانماط والتمثيل المرئي للبيانات وتقنية التنقيب Mining Data حيث يمكن تطبيقها قي عملية التدقيق من خلال استخدام الشبكات العصبية وشجرة القرارات في الكشف عن البيانات المضللة في القوائم المالية وتقنية سلاسل الكتل Computing Cloud حيث تعد وسيلة حيوية تقوم بتوفير مساحات تخزين للبيانات الكبيرة يمكن الاستفادة منها كبنية تحتية في عملية التدقيق .فضلا الى ذلك يتطلب ادخال منهاج حديثة خاصة بالتقنيات المتطورة على مستوى التدريس في المعهد العربي للمحاسبين القانونيين او الدراسات العليا.

المحور الثاني : اعتماد اطار COBIT-2019 في تدقيق متطلبات السيبرانية

تضمن هذا المحور سبعة اسئلة ذات العلاقة بالاطار :

1- المام مراقب الحسابات بمجالات الاطار عند تدقيق المصارف عينة البحث: من خلال تواجد الباحثين واللقاء بمراقبي الحسابات يوجد الالمام بمجالات الاطار من الجانب النظري من قبل اغلبية عينة البحث في حين هناك تفاوت في معرفة اليات التطبيق العملي لهذا الاطار ومن خلال تحليل محتوى التقارير حيث افصحت المصارف ضمن تقرير الادارة قد انجزت مجموعة من المشاريع منها ترحيل جميع مستخدمي CBIQ الى Microsoft Cloud Azure AD مع ترحيل جميع صناديق البريد CBI 216 من ON-Prime الى Exchange عبر الانترنيت Microsoft Cloud مع تمكين جميع حسابات CBIQ 216 الى Microsoft office APPS وتطبيق One Drive, Share Point, Teams مع تمكين رفع الحسابات الخاملة الى منصة البنك المركزي فضلا الى ذلك خلق بيئة DR لانظمة Cashier و SigCap فضلا الى ذلك فأن تقرير الادارة للمصارف تؤكد على تنفيذ وتحديث اطار لحوكمة الخاصة بادارة امن المعلومات بما يتواكب مع اطار COBIT-2019 فضلا الى ذلك كما ذكرنا سابقا فان مراقب الحسابات يستعين بالخبراء وفق المعايير الدولية للتدقيق.

2- يدعم اطار COBIT متطلبات تدقيق الامن السيبراني؟ يساعد الاطار في تقييم الضوابط السيبرانية من خلال الربط مع اهداف الحوكمة وادارة المخاطر حيث تشير التقارير الى تحديث نظام المراقبة الاحداث الامنية لمواكبة افضل الاصدارات العالمية فضلا الى ذلك مراجعة فعاليات ضوابط الحماية المعتمدة في سياسة الامن السيبراني لدى المصرف وبشكل مستمر

3- المجالات الخمسة الاكثر ارتباطا في عمل المصرف APO, EDM ,BIA,DSS,MEA: من اكثر المجالات ارتباطا EDM التقييم والتوجيه والمراقبة EDM البناء والاستحواذ والتنفيذ BAI , تقديم الخدمة والدعم DSS والمراقبة والتقييم والتقرير MEA ومن خلال تحليل محتوى

التقارير فأن المصارف عينة البحث قد انجزت مشاريع ذات العلاقة بالمجالات الخمسة اعلاه وهناك مشاريع قيد الانجاز مثل اعتماد PCI-DSS ل CBIQ وتطبيق نظام GOAML مع CBI تحسين ركز البيانات ومن المشاريع المقترحة نظام E-Statements ونظام ITSM تفعيل منصة CBI (Extral) لتحويل العملات الاجنبية وتحسين واجهة RTGS مع النظام المصرفي.

4- يسهم اطار COBIT في دعم عملية التدقيق: من خلال الرد على هذا السؤال من قبل عينة البحث يساعد الاطار في دعم عملية التخطيط والتنفيذ والاختبارات حيث يشير ISACA إلى أنّ استخدام الاطار اساسي في التخطيط لعملية التدقيق وتقييم المخاطر كباعتباره أداة فعالة في تقييم الرقابة الداخلية وبعض الاجابات ركزت تقييم الانظمة الالية في معالجة البيانات المالية ,وعند ثبوت فعالية ضوابط الرقابية فأن ذلك له علاقة عكسية لحجم الاختبارات الجوهرية ومتطلبات امن المعلومات وادارة العمليات بما يعزز موثوقية الادلة الالكترونية .

5- ماهي المؤشرات المعتمدة لتقييم الضوابط السيبرانية؟ يتم تقييم الضوابط السيبرانية من خلال الالتزام المصارف عينة البحث بمتطلبات البنك المركزي فضلا الى ذلك دراسة تحليلية الى الملاحظات المثبتة في تقارير البنك المرزي بخصوص المصارف فيما يخص قواعد البيانات ,الانظمة الرئيسة ,تحديد متطلبات المطبقة للمعايير الدولية الخاصة بأمن المعلومات والتعليمات المحلية الصادرة من الهيئة الوطنية للأمن السيبراني ويتضمن ذلك فحص الضوابط التشغيلية والتقنية مثال ذلك برنامج مكافحة الفيروسات تأمين انظمة الدفع الالكتروني حماية البيانات الحساسة للعملاء.

6- التحديات التي تواجه المصارف في الالتزام بتطبيق متطلبات الاطار؟ تتمثل المعوقات ومن خلال تواجد الباحثين في عينة البحث ,المصارف تتمثل في ان بعض المصارف تعاني من اكتمال البنى التحتية ,تدريب العاملين ,عدم الاقناع من قبل ادارات بعض المصارف بالتبني الكامل لمتطلبات الاطار الذي ينعكس على توفر الموارد المالية اللازمة لهذا التبني.

7- يساهم الالتزام بمتطلبات الاطار في تحقيق من المخاطر التدقيق؟ من دراسة محتوى التقارير للمصارف عينة البحث يساهم الاطار في تقليل المخاطر السيبرانية من خلال التزام المصارف بتقنيات واستخدام برامج وانظمة حديثة.

المحور الثالث: العلاقة بين تدقيق الأمن السيبراني واطار COBIT-2019

يتكون هذا المحور من سبعة اسئلة تم طرحها على مراقبي الحسابات :

1- طبيعة العلاقة بين تدقيق الأمن السيبراني ومتطلبات COBIT-2019؟ إنّ اعتماد الأطار يساعد في تحقيق التكامل ويعد أساسا منهجيا لغرض ارساء ودعم التخطيط ووضع اجراءات التدقيق.

2- الالتزام بمتطلبات الإطار يعزز موثوقية التقارير المالية؟ من خلال تحليل محتوى التقارير حيث أشارت إلى وجود الأنظمة والتقنيات واعتماد الإطار يساعد في الحد من الهجمات الالكترونية ويعزز جودة المعلومات المحاسبية.

3- تطبيق الإطار يساعد على ايجاد منهجية موحدة في تقييم المخاطر السيبرانية من قبل مراقبي الحسابات؟ من خلال دراسة التقارير تعتمد عينة البحث مجموعة من التقنيات في اساسها واحد ولكن البعض قد تختلف عن الاخر في تقنية معينة ومن خلال الاستفسار من مراقبي الحسابات ان الاجراءات موحدة في عملية التقييم

4- الالتزام بالاطار يؤثر على جودة ادلة التدقيق ؟ كانت اجابات مراقب الحسابات تركيزهم على الادلة الالكترونية من حيث جودة الدليل وان المصارف تملك تقنيات حديثة وتسعى الى ادخال تقنيات متطورة تنعكس على أداء الخدمة المصرفية وخاصةً أنّ غالبية المصارف عينة البحث

أطلقت العديد من الخدمات المصرفية عبر الانترنيت او الموبايل و الأتمتة الى العمولات والرسوم وغيرها .

5- الاطار يساعد مراقب الحسابات في ابداء الملاحظات والتوصيات ؟ كانت اجابة مراقبي الحسابات من خلال دراسة الضوابط الداخلية وتقييم قوة ومتانة والخروقات والهجمات السيبرانية مع ربط هذه الملاحظات بإمكانيات الإدارة في تحسين تلك الخروقات وهو ما يعرف بمستويات النضج

6- تمارس الادارة ضغوطاتٍ على مراقب الحسابات عند تدقيق الأمن السيبراني ؟ كانت اجابات مراقبي الحسابات أنّ مراقب الحسابات يتمتع بالاستقلالية المهنية والالتزام بآداب وسلوك المهنة ومن خلال دراسة تحليل المحتوى التقارير لم نجد اشارة الى التحفظات وان التدقيق يشمل تنفيذ الاجراءات التي تم تحديدها .

7- التكامل بين المتطلبات الاطار واستدامة الاداء المصرفي ؟ يساعد الالتزام بمتطلبات الإطار في كافة مجالاته فضلا عن الارشادات والتوجيهات الصادرة من البنك المركزي في تحقيق استدامة الاداء وتقديم الخدمات المصرفية.

المبحث الرابع : الاستنتاجات والتوصيات

اولا: الاستنتاجات:

1- تفاوت شركات التدقيق في معرفة المتطلبات السيبرانية او مجالات إطار COBIT- 2019 الذي ينعكس بشكل جوهري في تقييم الالتزام بمتطلبات الحوكمة والرقابة الخاصة بأمن المعلومات وإدارة المخاطر السيبرانية .

2- تفاوت المصارف في وجود البنى التحتية او تطبيق الانظمة الالكترونية التي تدعم مجالات اطار COBIT-2019 للحد من الهجمات والاختراقات السيبرانية.

3- توجد فقط ادلة وضوابط صادرة من البنك المركزي العراقي ذات العلاقة بتحديد المتطلبات السيبرانية ولا توجد معايير محلية معتمدة صادرة من مجلس مهنة رقابة وتدقيق الحسابات ذات العلاقة بالتدقيق.

4- تسهم شركات التدقيق في تحديد امتثال المصارف للضوابط بشكل عام ومنها الضوابط التقنية الصادرة من البن المركزي لأن ذلك يؤثر على موثوقية الأنظمة الالكترونية ويعزز من ثقة اصحاب المصلحة.

ثانيا: التوصيات

1- على الجهات المهنية والرقابية الخاصة بتنظيم مهنة الرقابة والتدقيق بتوحيد المعرفة بالمتطلبات السيبرانية من خلال التأهيل والتدريب بالأطر الدولية ومنها اطار COBIT-2019 بشكل تضمن تقليل التفاوت في تقييم الالتزام بحوكمة امن المعلومات وادارة المخاطر السيبرانية.

2- على البنك المركزي العراقي باعتباره جهة رقابية في الزام المصارف بتوفير البنى التحتية والانظمة الالكترونية الداعمة الى تطبيق مجالات اطار COBIT-2019 فضلا الى ذلك اصدار الضوابط والتعليمات الملزمة الى المصارف لغرض اجراء تقييم بشكل دوري لمستوى النضج السيبراني وفق الاطار.

3- على مجلس مهنة رقابة وتدقيق الحسابات بالتنسيق مع المركز الوطني للأمن السيبراني والبنك المركزي والجهات ذات العلاقة في اصدار معايير مهنية محلية معتمدة للتدقيق السيبراني وفق اطار COBIT-2019 مع الرجوع الى المعايير المحلية والدولية ISAللتدقيق وبشكل يساعد على توحيد الممارسات والإجراءات بين الشركات .

4- تعزيز ور شركات التدقيق في فحص وتقييم امتثال المصارف بالضوابط الالكترونية الصادرة من البنك المركزي من خلال ادراج فقرة ضمن برنامج التدقيق والافصاح عنها ضمن تقرير التدقيق لما لها من أثر جوهري وبشكل يساعد على تعزيز شفافية الافصاح لأصحاب المصلحة.

المصادر Reference

1-عثمان, محمد أحمد عبد العزيز ، أثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين بالأسهم: دراسة تجريبية، مجلة الإسكندرية للبحوث المحاسبية، مج. 7، ع. 2، ص ص 167–238 (مايو 2023)، https://doi.org/10.21608/aljalexu.2023.308564

2-SCOCPA , 2023, المعايير الدولية للمراجعة والفحص ,ترجمة السعودية , الهيئة السعودية للمراجعيين والمحاسبين القانونيين.

3-. الموسوعة العربية (htpps//wwwarab-ency.com,2022

4- حسين، مشتاق علي ذياب, المعموري، علي محمد ثجيل. (2025). المسؤولية المهنية للمدقق تجاه مخاطر الأمن السيبراني: برنامج تدقيق مقترح. مجلة الدراسات المالية والمحاسبية (JAFS)، 20(70)، 336 -361. https://jpgiafs.uobaghdad.edu.iq/index.php/JAFS/article/view/2073?utm_source=chatgpt.com

5- الصيرفي، أسماء احمد, (2025). أثر إفصاح الشركات عن تفعيل إدارة مخاطر الأمن السيبراني على تقدير مراقب الحسابات لمستوى مخاطر المراجعة الخارجية. مجلة البحوث المحاسبية, 12(1), 106-150. https://doi.org/10.21608/abj.2025.411403

6- المنظمة الدولية للمعايير – ISO/IEC 27032:2023 .(2023) .إرشادات الأمن السيبراني .المنظمة الدولية للمعايير https://www.csentity.com/Compliancecurity .

7- المهتدي , رعد محمد عبد الله . (2021). أثر تطبيق نظم المعلومات COBIT-2019 في تحسين الأداء المؤسسي للبنوك التجارية الأردنية (رسالة ماجستير، كلية الأعمال، [جامعة الاسراء]).

8- البنك المركزي العراقي .(2019) , ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي

9- هاينز، وآخرون .(2016) .مبادئ المراجعة.ترجمة الهيئة السعودية للمحاسبين القانونيين

10-United States Government Accountability Office. (2024). Cybersecurity: Efforts initiated to harmonize regulations, but significant work remains (Report No. GAO-24-107602). U.S. Government Accountability Office. https://www.gao.gov/products/gao-24-107602

11-Mani, V. (2021, May 19). Demystifying the implementation of cyberresilience programs. ISACA Journal, Volume 3. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/demystifying-the-implementation-of-cyberresilience-program

12-Iinternational Ethics Standards Board for Accountants. (2024). Handbook of the International Code of Ethics for Professional Accountants (including International Independence Standards). International Federation of Accountants. Retrieved from https://www.ethicsboard.org/publications/2025-handbook-international-code-ethic…

13-Alford, R., Lawrence, D., & Kouremetis, M. (2022). CALDERA: A red-blue cyber operations automation platform. In Proceedings of the International Conference on Automated Planning and Scheduling (ICAPS 2022). The MITRE Corporation. Retrieved from https://icaps22.icaps-conference.org/demos/ICAPS_2022_paper_375.pdf

14-Raguseo, E. (2018). Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. International Journal of Information Management, 38(1), 187–195. https://doi.org/10.1016/j.ijinfomgt.2017.07.008

15-Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of Big Data by the audit profession. Accounting Horizons, 29(2), 439–449. https://doi.org/10.2308/acch-51054
16-Bizarro, P. A., Garcia, A., & Moore, Z. (2019). Blockchain explained and implications for accountancy. ISACA Journal – Volume 1, 2019. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/blockchain-explained-and-implications-for-accountancy
17-Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. Journal of Business Ethics, 167(2), 209-234. https://doi.org/10.1007/s10551-019-04407-1
18-Handayani, R., Utami, E., & Luthfi, E. T. (2023). Systematic literature review on auditing information technology risk management using the COBIT framework. Prisma Sains : Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram, 11(4), 1028–1036. https://doi.org/10.33394/j-ps.v11i4.8871
19-Almusawi, E. G. (2022). Using COBIT framework for reducing the audit risks of accounting information systems. Akkad Journal of Contemporary Accounting Studies, 1(1), 52–74. https://doi.org/10.55202/ajcas.v1i1.18
20-Toyner, L. G., & Sfenrianto, S. (2023). Information system security evaluation using COBIT 5 framework. Journal of Information System Management (JOISM), 4(2), 147-157. https://doi.org/10.24076/joism.2023v4i2.992
21-Slapničar, S., Rejc Buhovac, A., Aneja, A., & Vovko, P. (2022). Neural -1correlates of ethical decision-making in accounting. Journal of Business Ethics, 177(4), 857-876. doi.org
22-Fadila, V., Mutiah, N., & Sari, R. P. (2023). Cyber security audit using CIS CSC, NIST CSF and COBIT 2019 framework. CESS (Journal of Computer Engineering, System and Science), 8(2), 271–283. https://doi.org/10.24114/cess.v8i2.43257
23-Metin, B., Sevim, S. B., & Wynn, M. (2025). Cybersecurity strategy development: Towards an integrated approach based on COBIT 2019 and ISO/IEC 27000 series standards. Standards, 5(4), Article 33. https://doi.org/10.3390/standards5040033
ISACA. (2019). COBIT 2019 Framework: Introduction and methodology. ISACA.
24-Azab, O. (2024, October 22). How the emerging technology landscape is impacting cybersecurity audits. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/how-the-emerging-technology-landscape-is-impacting-cybersecurity-audits
25-International Organization for Standardization. (2023). ISO/IEC 27032:2023 – Guidelines for cybersecurity. ISO. https://www.iso.org/standard/44375.html
Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. International Journal of Auditing, 25(1), 24–39. https://doi.org/10.1111/ijau.12209
26-Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126
27-United States Government Accountability Office. (2023). Cybersecurity program audit guide (Publication No. GAO-23-104705). U.S. Government Accountability Office. https://www.gao.gov/products/gao-23-104705