Professional responsibility of the auditor for cyber security risks (proposed audit program

Mushtaq Ali Dheyab
Post-Graduate Institute for Accounting Financial studies-University of Baghdad
Mushtaq.Ali1101a@pgiafs.uobaghdad.edu.iq

Assist.Prof.Dr.Ali Mohammad Thijeel Al-mamouri
Post-Graduate Institute for Accounting Financial studies-University of Baghdad
asst.prof.ali@pgiafs.uobaghdad.edu.iq

Received:12/8/2024 Accepted:3/9/2024 Published:31/3/2025

Abstract:

The continuous digital and technical development has led to the transformation of transactions from their traditional reality to the digital and cyberspace. The research problem is that all businesses, transactions and operations are electronic, which exposes them to cyber attacks, and that the professional responsibility of the auditor will be affected by cyber security risks. The main research hypothesis was the existence of a direct relationship between responsibility The professionalism of the auditor and cyber security risks, as the research seeks to know the extent to which the public and private sectors have adopted a cyber-security plan through a program or framework emanating from the Iraqi cyber security strategy (2022-2025) and the conclusions it reached that there is a relationship between the professional responsibility of the auditor The most important of which are cyber security risks, the most important of which is that most financial and banking entities have not identified or disclosed cyber security risks and the absence of a law or binding legal framework, which affects the audit procedures and the opinion of the auditor. This affects the professional responsibility of the auditor, as well as the failure to disclose these risks, which exposes them to threats from by organizing a cyber-security law that is binding on everyone. Opening remarks auditor cyber security

Keywords: Auditor, Cybersecurity.

المسؤولية المهنية لمراقب الحسابات عن مخاطر الامن السيبراني (برنامج تدقيق مقترح)

مشتاق علي ذياب حسين
جامعة بغداد – المعهد العالي للدراسات المحاسبية والمالية

ا.م.د .علي محمد ثجيل المعموري
جامعة بغداد – المعهد العالي للدراسات المحاسبية والمالية

المستخلص

التطور الرقمي والتقني المستمر الى تحويل التعاملات من واقعها التقليدي الى الفضاء الرقمي والسيبراني، والمشكلة البحث ان جميع الاعمال والتعاملات و العمليات الكترونية مما يعرضها لهجمات سيبرانية وان المسؤولية المهنية لمراقب الحسابات سوف تتاثر بمخاطر الامن السيبراني وكانت فرضية البحث الرئيسية وجود علاقة مباشرة بين المسؤولية المهنية لمراقب الحسابات و مخاطر الامن السيبرانية اذ يسعى البحث الى معرفة مدى تبني القطاع العام والخاص لخطة الامن السيبرانية من خلال برنامج او اطار منبثقة من استراتيجية الامن السيبرانية العراقي (2022–2025) و ما توصل اليه من استنتاجات ان هناك علاقه ما بين المسؤولية المهنية لمراقب الحسابات ومخاطر الامن السيبرانية واهمها ان اغلب الجهات المالية والمصرفية لم تقوم بتحديد مخاطر الامن السيبرانية او الإفصاح عنها وعدم وجود قانون او اطار قانوني ملزم مما يؤثر على إجراءات التدقيق وراي مراقب الحسابات وهذا يؤثر على المسؤولية المهنية لمراقب الحسابات وكذلك عدم الإفصاح عن هذه المخاطر مما يعرضها للتهديدات من خلال تنظيم قانون للأمن السيبراني ملزم للجميع .

الكلمات الافتتاحية :مراقب الحسابات؛ الامن السيبراني.

المقدمة: introduction:- أن الأمن السيبراني نظام معقد ومهم على المستويات والأنظمة جميعها ان كانت عامة أو خاصة وان كل شيء متصل قابل للاختراق ولايوجد نظام امن ومطلق والامن السيبرانية نظام صعب ومعقد ولكن سلامتك وسلامة معلوماتك و أموالك الرقمية تستحق العناء والتواصل وتطوير كافة الأنظمة للحماية كون ان الهجمات ليست ضمن لائحة الاحتمالات بل هي حقيقة ومثبتة ينبغي التصدي لها والتعامل معها بصورة دائمة ومثلما نغلق ابوابنا لحماية منازلنا يقف الامن السيبرانية كأساس لحماية عالمنا الرقمي وبالنظر للتحول الرقمي في العراق وإصدار استراتيجيته للأمن السيبرانية وسوف يتطرق بحثنا من أربعة مباحث الأول منهجية البحث والثاني الاطارالنظري لمسؤولية مراقب الحسابات والثالث للجانب العملي حيث سوف يتم اقتراح برنامج تدقيق مقرح وأخيرا بحثنا الرابع الاستنتاجات والتوصيات لغرض حمايه وحداتنا الاقتصادية والمؤسسات من مخاطر الامن السيبراني وان تكون تقارير مراقب الحسابات ذات ثقة عالية وتحمي أصحاب المصالح من أي تهديدات وتكون مسؤولية المدقق الخارجي بعيده عن كل الإشكالات القانونية والمهنية.

المبحث الاول:

اولاً-منهجية البحث The methodology of Research:- يقدم هذا المبحث عرضاً لمنهجية البحث التي تضمنت مشكلة البحث وأهميته وأغراضه ومجال تطبيقه وحدود البحث، المنهج المعتمد، مصادر جمع البيانات، وطرائق تحليل بيانات البحث.

1-1مشكلة البحث: Research problem:- مشكلة البحث في تزايد التهديدات السيبرانية التي تواجه الشركات والمؤسسات، مثل الاختراقات والتهديدات الإلكترونية التي تم تحول عملها الى النظام الالكتروني وان عمليات التدقيق والمسؤولية المهنية لمراقب الحسابات الخارجي تتأثر بمخاطر الامن السيبرانية، كون التقارير لم تتطرق الى مخاطر الامن السيبرانية وعدم وجود برنامج تدقيق موحد لتحديد المخاطر السيبرانية للقطاع المالي.

1-2 أهمية البحث: Research importance:-تظهر أهمية البحث بأهمية تقنية المعلومات وتحديد المخاطر السيبرانية ودورها في النهوض بالعمل الموارد المطلوبة لمواصلة التشغيل لكل نشاط بالغ الأهمية وتأثير مخاطر الأمن السيبرانية في البيانات المالية الذي يمكن أن يكون كارثيًا وعندما يتم اختراق منظومة الأمان السيبرانية للشركات المالية، اذ يمكن للمهاجمين الوصول إلى معلومات مالية حساسة مثل معلومات الزبائن وهذا يمكن أن يؤدي إلى انتهاك المؤسسات الماليه وبالتالي تاثر المسؤولية المهنية لمراقب الحسابات الخارجي و يحمل أهمية كبيرى نظرًا للتطورات السريعة في مجال التقنيات والتحول الرقمي الذي يشهده العالم وتاثير مخاطر الامن السيبراني من الناحية القانونية والمهنيه لمراقب الحسابات.

1-3 أهداف البحث: Research Objectives:-أن الغرض الرئيسي من البحث يمكن أن يكون كثير الأبعاد ويشمل عدة جوانب ومن بين الأغراض الرئيسية يمكن تضمين:

1. تقييم تأثير المخاطر على المسؤولية: من خلال فهم كيفية تأثير المسؤولية المهنية لمراقب الحسابات الخارجي من الناحية القانونية والمالية على مخاطر الأمن السيبرانية
2. تحليل الاستجابة والاستعداد للتحديات السيبرانية: من خلال تقييم مدى استعداد المراقبين الخارجيين لمواجهة التحديات السيبرانية والاستجابة لها بفعالية.

1-4- **فرضية البحث** :ينطلق البحث من فرضية رئيسية مفادها (وجود علاقه مباشر مابين المسؤولية المهنية لمراقب الحسابات ومخاطر الامن السيبرانية في المؤسسات المالية العاملة المطبقة للتحول الرقمي) .

1-5 منهج البحث: Research method:- اعتمد الباحث في بحثه هذا على المنهج الوصفي في الإطار النظري لتحقيق أهداف البحث، وأعتمد على المنهج التحليلي في الإطار العملي من خلال اعداد برنامج تدقيق مقترح من قبل الباحث والحصول على النتائج.

1-6 وسائل جمع البيانات والمعلومات: Means of collecting data and information

1 –6–1 الجانب النظري: تم الاعتماد على مصادر محلية وعربية واجنبية من الكتب والاطاريح والرسائل والبحوث المنشورة في المجلات العربية والاجنبية او متوفرة في مختلف المكتبات او على شبكات الانترنت.

1–6–2 الجانب العملي: التقارير السنوية (للمؤسسة المبحوثة) خلال فترة البحث تم اعتماد البرنامج.

ثانيا –الدراسات السابقة :

الباحث//(الشريف. مصطفى كامل :2024) عنوان الدراسة//موسوعة الامن السيبرانية (حماية الفضاء الرقمي بين النظرية والتطبيق) مشكلة الدراسة//استكشاف الامن السيبرانية في العالم الرقمي اهداف الدراسة//حماية الفضاء الرقمي بين النظرية والتطبيق اهم الاستنتاجات//دليل مفيد وموثق لفهم وتطبيق الامن السيبرانية توصيات الدراسة//اعداد دليل رسمي لوضع خطط وتقوية الدفاعات للأمن السيبرانية
الباحث//(سلمان. 2023) عنوان الدراسة//جرائم الامن السيبرانية وأثر الجهود الدولية في مكافحتها مشكلة الدراسة //عدم كفاية الحماية القانونية الدولية لمكافحة الجرائم السيبرانية اهداف الدراسة//تكوين صورة واضحة عن الصعوبات التي تواجهه المنظمة والدول في مجال الامن السيبرانية (العلاقات – الخصوصية –التعزيز لامني) اهم الاستنتاجات//اجراء المزيد من البحوث حول تأثير الامن السيبرانية على الشركات والمنظمات والدول وصيات الدراسة//إيجاد صيغ قانون دولي للحد من التهديدات السيبراني
الباحث//(صالح واخرون :2022) عنوان الدراسة//التحول الرقمي من الأرض الى الفضاء (فرص للنمو الاقتصادي ام تهديد للأمن القومي) مشكلة الدراسة//تسارع وتقدم تقنية الاتصالات في حياة الانسان الحديثة اهداف الدراسة//الاستفادة من التقدم الالكتروني والاتصالات الحديثة وتجارب الدول والعمل على الحفاظ عليها من خلال تحديد مخاطر الامن السيبرانية ومن العمل التحول الرقمي في العراق اهم الاستنتاجات//ان تقنية المعلومات لها تأثير كبير في النمو الاقتصادي في حال استخدام التقانيات المحدثة توصيات الدراسة//دخول العراق لهذه التقانيات وحمايتها من الهجمات السيبرانية يساعد في النمو الاقتصادي وحماية الامن القومي اسم الباحث (Caustic, 2021) عنوان الدراسةThe Impact of Cyber security on Competitive Advantage//تأثير الامن السيبرانية على الميزة التنافسية مشكلة الدراسة– هل يوجد تأثير للميزة في المؤسسة على الامن السيبرانية اهداف الدراسة//تهدف هذه الأطروحة إلى استكشاف العناصر اللازمة لتنفيذ الأمن السيبرانية وإدارته في المنظمة، وكذلك استكشاف كيف يمكن للأمن السيبرانية أن يسهم في الميزة التنافسية للمنظمة. أهم الاستنتاجات//الأمن السيبرانية (القدرات التشغيلية، القدرات الديناميكية). توصيات الدراسة//هناك حاجة إلى نهج شامل لإدارة الأمن السيبرانية من خلال نظام اجتماعي تقني يوازن بين الجوانب الاستراتيجية والتنظيمية والمخاطر والتكنولوجيا.

الامتثال للمتطلبات المختلفة، يمكن للمنافسين محاكاة الامتثال بسهولة لأنه يعتمد على القدرات التشغيلية، من خلال تطوير قدرات ديناميكية محددة للأمن السيبرانية، يمكن للشركات تحقيق قيمة استراتيجية يصعب تقليدها، لتحقيق ميزة تنافسية مستدامة.

المبحث الثاني –الإطار المفاهيم لمفهوم مراقب الحسابات وتعريفه وتقييم ادائه على مخاطر الامن السيبرانية

2-1مفهوم مراقب الحسابات:- **أن** مراقب الحسابات "جهة رقابية شرعه القانون للرقابة الوحدة والتدقيق في حساباتها ، لغرض حماية هيكلية الوحدة ومساهميها والغير من خلال تعيين مراقب واحد أو مراقبين للحسابات، وهي مسالة ملزمة وفقاً للقانون الذي ينظم عمل الشركات، لذا يستوجب ان يعيين شخصاً يعهد لهم بمهمة رقابة وتدقيق عمل الوحدة من خلال تدقيق حساباتها " ، كما" يمكن ان يكون الشخص طبيعياً أو معنوياً في إطار حوكمة الشركات إلا أنه يشترط فيه ان يكون من المقيدين في الجدول، ومكلفاً من طرف المساهمين بمراقبة بصفة دائمة للحسابات المنجزة من قبل الشركة، وانه يمارس هذا العمل لغرض تقديم التقارير المؤكدة لشتى مجالات عمل الشركة "(جيرارد كومو، 1994 :ص 155)، " يقوم برقابة دائمة وفعالة في الشركة لحساب المساهمين، ويتم ابلاغهم عن أي سلوك يشكل انحراف في عمل الادارة أو مخالف لأحكام التشريع، ويتم تعيينهم من الجمعية العمومية ولمدة سنة ويلتزموا بتقديم لائحة التقرير الختامي قبل خمسين يوماً على الاقل من تاريخ الانعقاد السنوي للجمعية العمومية"(ناصيف؛ الياس ، ٢٠٠٨ : ص ٧٧) ، " وعلى الرغم من ذلك فإن القوانين لم تضع تعريفاً له، وإنما نظمت عملية ممارسة مهنة الرقابة والتدقيق وبيان الشروط الواجب توافرها فيه، والصلاحيات التي يتمتع بها، وهذا مسار للمشرع لأنه عملية وضع التعاريف ستقيد من الاشخاص في ظل ظروف تتسم بالسرعة في التغيير والتطور، وهو ما جعل مجالاً رحباً للفقه لتعريف مراقب الحسابات، ولذلك فقد عرفه جانب من الفقه بانه خبير معين من لدن الجمعية العامة للشركة يناط به مهمة الرقابة على اعمال مجلس الادارة في مدة محددة عادة ما تكون سنة"(محرز ؛احمد محمد ، ٢٠٠٩ : ص ٥٦٨)، "وقدعرفه بعض التشريعات بأسم مفوض المراقبة " وهو الخبير المتخصص الذي ويلاحظ ان تحديد تاريخ التعيين بمدة سنة هو امر نراه غير صائب لأنه عمليات المراقبة وان قام بها متخصص إلَّا أن تحديد اعمال الشركة وارباحها وخسارتها امر يحتاج إلى مدة اطول نسبياً من سنة، ولأجل الاحاطة بذلك يمكن ان تكون مدة عمل مراجع الحسابات مدة اطول من السنة حتى يكون ضمانة حقيقة للمساهمين ومراجع فعال على سلوك الشركة، وتجنباً للانتقاد فقد خرج قانون المصارف العراقي رقم (٩٤) لسنة ٢٠٠٤ عن ذلك في المادة (٦٤)، ليمدد المدة وجعلها تصل إلى خمس سنوات على أن لا تتجاوز ذلك الا بموافقة البنك المركزي العراقي، وقد عرفها جانب آخر بكونها خبرة فنية يختص بتقديرها الخبير ليقرر مدى انتظام الدفاتر والسجلات، ودقة ما تحتويه من بيانات لغرض تحديد المركز المالي للشركة" (عيسى ابو الطبل، وعبد المنعم محمود، ١٩٦٧ : ص ٤٠) مشار اليه ، ويلاحظ على هذه التعريفات انها لم تضع تعريفاً جامعاً له كما انها لم تتفق على تسمية له، فقد اطلق عليه اسم "مفوض الرقابة " في التشريع اللبناني، انظر (الياس ناصيف ، مصدر سابق، ص 41) ، أو" مراجع الحسابات" يلاحظ ان (قانون الشركات الاردني رقم ٤٦ لعام ٢٠٠٦)، أو "مدقق الحسابات" (يلاحظ ان لفظ مراقب الحسابات قد ورد في المواد ٥٩ ، و ٨٧ و ١١٧ ، ١٠٢ في قانون الشركات العراقي رقم ٢١ لسنة ١٩٩٧ المعدل النافذ) ، أو" مفتش الحسابات، كما سمي بمراقب الحسابات الخارجي "(نهلة ؛طعمة خلف؛ ٢٠٠٦ : ص ١٥ .) ، وفي العراق حيث تم ذكره في القانون العراقي رقم ٤٩ لسنة ٢٠٠٤ حيث نصت المادة (٢٤) منه على ١ / ب – التوصية والموافقة على مراقب الحسابات لكي يعين كمراقب حسابات خارجي للمصرف استناداً للمادة ٤٦". (وقد استخدم لفظ المدقق المالي المستقل في المادة (ثامناً ١١٧) " أ –اختيار مدققين ماليين مستقلين ..." من قانون الشركات العراقي المعدل النافذ) ينظر المادة ٦٦/٤ من قانون الشركات الاردني رقم ٢٢ لسنة ١٩٩٧ المعدل النافذ التي نصت على (انتخاب مدقق حسابات الشركة وتحديد اتعابه)، وكذلك سار القانون الشركات الإماراتي على ذلك بموجب القانون رقم (٢) لسنة ٢٠١٥ الذي خصص فيه المواد (٢٤٣-٢٥٤) لبيان الأحكام المتعلقة بمدققي حسابات الشركة.

2-2-المسؤولية المهنية لمراقب الحسابات: -يعد مراقب الحسابات الخارجي ذات اهمية بعد اتساع المهام المناطة بالوحدات الاقتصادية في ضوء العولمة وما انطوى عليها في ضوء الاقتصاد الحر، ولذا فإن دور مراقب الخارجي قد ازداد في اهمية في ظل الاقتصاد المنفتح وامتد ذلك على النطاق الداخلي،والدولي (خلف؛نهلة طعمه ؛2006:ص 45) وعن التأكيد المعقول والتمثيل الصحيح والعادل حيث إن المساهمون يتوقعون إن يكون المراقب ضامنا لاستثماراتهم ورغم إن ذلك يبدوا غريب إلا انه أمر واقع و لذا يتعين على مدقق الحسابات بالتقرير عن مصداقية المعلومات النوعية وتكنولوجيا معلومات قاعدة البيانات المعقدة فضلا عن التقارير لعمليات وأداء الشركات في ضوء ما ينجم عن ذلك من خطر لعملية التدقيق.(عبد الوهاب ؛شحاته؛2006 :ص19) كما في عام 2008التي رافقها انهيار بعض القطاعات" (سندس؛ ماجد رضا ؛ ٢٠١١: ص 12) "فعند قيام مراقب الحسابات بمهامه عليه أن يلتزم بتطبيق إجراءات وأساليب مُتعارف عليها في مجال المهنة"، "وقد يحدث أن لا يلتزم بهذه الإجراءات أما عمداً أو سهواً"،" وفي الحالتين يجب مساءلته عما ارتكبهُ من أخطاء أو إهمال أو تقصير"(المجالي، 2016:ص 17).

إن تحديد المسؤولية القانونية وكذلك المسؤولية المهنية للمدقق الخارجي يرتبط بشكل كبير بمعيار الواجب للمهنة، بمعنى إن القانون يُركز أساساً على التقصير في بذل العمل المهني الملائم كأساس لمساءلة مدقق الحسابات، وعادةً ما تمثل المسؤولية القانونية لمراقب الخارجي الحد الأدنى لما يتحمله من مسؤوليات، إذ تفرض المنظمات والنقابات المهنية مسؤوليات أكبر عليه بهدف رفع مستوى العناية المهنية عن الحد الأدنى الذي يفرضه القانون (دحدوح والقاضي، 2009:ص 190). وإن المفهوم الذي يفسر مسؤولية المراقب الخارجي هو مفهوم الوظيفة الاجتماعية ، إذ إن أبعاد هذا الدور هي التي تحدد مجال مراقب الحسابات والتبعية القانونية و ليس لإتجاه المساهمين فقط بل إتجاه الأطراف الأخرى والمستخدم الخارجي والتي لها جميعها مصالح متباينة في المعلومات الاقتصادية التي يقدمها المشروع ويقررها مراقب الحسابات وقد تضافرت عوامل عدة أدت إلى تحمل مراقب الحسابات المسؤولية اتجاه الأطراف المُختلفة

2-3شروط مراقب الحسابات:- ان مهمة التدقيق ومراقبة العمل الصادرة عن الوحدة التي قد تكون صحيحه وقد يعتريها بعض الاخطاء ، ولذلك فإن وجود المراقب يعني وجود نظام لمراقبة العمل فإن عليه ان يقوم بتدقيق كاملة للدفاتر والسجلات، وهذه المهمة لا يمكن ان يمارسها اي شخص عادي، ولذلك فقد نظم التشريع العراقي،" شروطاً المزاولة مهمة مراجعة الحسابات؛ والتي يمكن أن يكون تدقيق الحسابات من ذوي الكفاءة تعزز الشركات الاقتصاد الوطني وتعمل على تنميته وازدهاره ؛ولذلك كان لابد من وضع الية عامة لحكومة الشركات وضمان حقوق المساهمين فيها"، بما يضمن من تحقيق انضباط مؤسسي في ادارة الشركة واتباعاً للأساليب العالمية في ذلك (ينظر نص المادة (٨) من قانون المعهد العالي للدراسات المحاسبية والمالية العراقي) ، "وحيث ان تحقيق هذا الانضباط يقتضي ان تناط مهمة الرقابة بشخصية كفؤة قادرة على أن تلزم الادارة باتباع نسق منتظم في عملياتها بما يتناغم والتشريع في البلد"، ولذلك فقد نص المشرع العراقي في المادة (١٣٣) من قانون الشركات العراقي رقم (٢١) لسنة ١٩٩٧ "على ... حسابات الشركة الخاصة فتخضع للرقابة والتدقيق من قبل مراقبي الحسابات تعينهم الجمعية العمومية للشركة" ... والملاحظ ان هذا النص لم يتطرق إلى شرط الكفاءة وإنما حاول ان يكفل الاستقلالية للمراجع، وعلى ذلك سار تشريع الشركات التجارية الذي عهد للجمعية العمومية صلاحية تعيين مراجع الحسابات دون ان ينظم شروط كفاءته (نصت المادة السابعة من نظام ممارسة مهنة مراقب وتدقيق الحسابات العراقي)، "والملاحظ ان التشريع العراقي اناط مهمة ترشيح مراقب الحسابات بمجلس الادارة وهو ما قد ينقص من استقلاليته"، "ولذلك فقد عالج القرار الوزاري المرقم (٥١٨) لسنة ٢٠٠٩ على أن يكون ترشيح مراقب الحسابات من لدن مجلس الادارة و قيد هذا الحق بوجود توصية من لجنة التدقيق"، ويمكن ملاحظة ان نص القرار الوزاري هو اسبق من القانون، وهو ما يدفع البعض للتساؤل ان تشريع الشركات هو لاحق على أحكام القرار وبالتالي فإن قوته تعلو عليه، كما انه في ذات الوقت لم يسلب صلاحية مجلس الادارة من الترشيح، في ضرورة سحب صلاحية ترشيح أو تعيين مراقب الحسابات من مجلس الادارة، "لأن المدقق يمارس عملية الرقابة على اعمال مجلس الادارة، ولذلك لابد من ضمان استقلاله ان المتبع لقانون الشركات يرى انها لم تنص على شرط الكفاءة المهنية ولذلك فلابد من البحث عن اساس هذا الشرط"،

(ولدى الرجوع إلى نظام ممارسة مهنة مراقبة وتدقيق الحسابات العراقي رقم (٣) لسنة ١٩٩٧ المعدل النافذ)، نجد انها قد احتويا على شرط الكفاءة من خلال النصوص الواردة فيهما، التي يمكن من خلالها استنباط شرط الكفاءة .

4-2مفهوم الأمن السيبراني: Cyber security :-والأمن السيبراني هو عملية حماية الأنظمة والبيانات والاتصالات والشبكات الموجودة والمتصلة بالإنترنت ضد الهجمات الرقمية؛ فهذه الهجمات، التي يشار إليها عادة باسم "الهجمات السيبرانية"، ما هي إلا محاولة اختراق، أو تعديل أو تعطيل أو دخول أو استخدام غير مشروع؛ و يمكن أن تتراوح الهجمات السيبرانية من تثبيت رموز برمجية ضارة على جهاز حاسوب شخصي وصولا إلى محاولة تدمير البنية التحتية لدول بأكملها.وبإيجاز، يشير المصطلح نطاق افتراضي تم إنشاؤها بواسطة أجهزة الحاسب الآلي المترابطة وشبكات الحاسب الآلي على الشبكة ، وهو الوسط الذي تتواجد فيه جميع شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني؛ القدرة على الحماية أو الدفاع عند استخدام الفضاء السيبراني من الهجمات السيبرانية (Rodriguez, 2019:P21)[3]. ببساطة، يهتم الأمن السيبرانية بالتهديدات بما الجهات سواء كانت داخلية أم خارجية، أو اقتصاره على نقاط ضعف الجهاز الذي يستخدمه الفرد ومن ثم، حماية الأجهزة والشبكات والخوادم والتطبيقات المتصلة بشبكة المعلومات أو الموجودة عليها والتي تتعرض للقرصنة أو الهجمات المستهدفة أو الوصول غير القانوني.يرتبط "ضمان وأمن المعلومات" بعملية إدارة المخاطر المتعلقة ؛ باستخدام البيانات وأنظمة ؛ وتخزينها؛ ونقلها؛ وسيشمل ذلك خططًا أو سياسات ذات تركيز أوسع لضمان وظائف البيانات أو الأنظمة .(Rawass, 2019:13) ،وحمايةأصول المعلومات الرقمية وغير الرقمية، مثل سجلات النسخ الورقية. اذ يقدم المعهد الوطني للمعايير والتقنية (NIST) "في سرد مصطلحات أمن المعلومات الرئيسية تعريفات لكل من "ضمان المعلومات" و "أمن المعلومات".[4]التدابير التي تقوم على الحماية والأنظمة والدفاع عنها لضمان توافرها وسلامتها والمصادقة والسرية وعدم الانتهاك وتشمل هذه التدابير على استعادة الأنظمة من خلال دمج قدرات الحماية والكشف وقدرتها على التفاعل (صالح، **واخرون :2022 ص 38**). أن الأمن السيبراني "على النحو الذي عرفّه المعهد الوطني للمعايير والتقنية ؛حماية المعلومات وأنظمة تقنية المعلومات من أي اختراق، أو تعطيل، أو تعديل أو دخول غير مصرح به أو استخدام أو استغلال غير مشروع لتوفير أساسيات او عناصر والبنية التحتية الوطنية الحساسة " Critical National Infrastructure "هي العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم والشبكات والعمليات والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها التي قد يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرض سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات مع مراعاة الآثار الاقتصادية و/أو الاجتماعية على المستوى الوطني و تأثير كبير على الأمن الوطني و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية .

2-5 المسؤولية عن مخاطر الامن السيبراني : أن مسوؤلية الإدارة هي مهمة جدا فهي تتضمن التخطيط والتنظيم والتوجية والرقابة واتخاذ القرار فهي وظيفة للإدارة العمل والخطر السيبرانية التي قد تواجه الإدارة او قد تستعين بخبراء داخلين او خارجين وينبغي أن يقترن الاستخدام المتزايد لتقانة بتعزيز الرقابة الادارة على الأنشطة المالية لحماية الاستقرار المالي، أذ قد تظهر مخاطر جديدة تزيد اتجاهات الرقمية المالية من الحاجة إلى الأمن السيبراني لحماية المستهلكين والمنتجين الماليين؛ ومن ثم، إلى تنفيذ اللوائح ذات الصلة المالية والأنظمة المالية للتخفيف من مخاطر الأمن السيبرانية المحتملة، حيث فرضت العديد من الدول قيوداً على حواجز التجارة الإلكترونية بهدف تصنيفها في الفئات الأتية، التوطين، ويتكون أول تقيد للتجارة من متطلبات التوطين، بما في ذلك البيانات أو توطين النظام ذي الصلة، على سبيل المثال، تتطلب الهند أن يتم وضع جميع البيانات الدفع التي تحتفظ بها الشركات الدفع في المنشاءات المحلية داخل الدولة ولا يسمح بتصديرها خارج البلاد، ولا حتى المعالجة، إلى جانب متطلبات البيانات(Murphy, F., &13-2 Materne, S. (2022) Cyber risk and cyber security)وان أحد المنتجات التي تم إنشاؤها من نموذج Fintech هو منصة الإقراض من شخص إلى شخص (P2P)، على الرغم من أن إقراض P2P يقدم خدمات أفضل بتكاليف منخفضة، إلا أنه زاد أيضا من الخطورة الائتمانية وبالتالي ظهور المخاطر النظامية ومما لا شك فيه أن الوسائط الرقمية قد زادت من مستوى الشمول المالي عالمياً من 51 بالمائة عام 2011 إلى 85 بالمائة في 2022 والتحدي الذي يواجه

المصارف هو تحديد أنسب نموذج للاتصال للتفاعل مع شرائح مختلفة من الزبائن من أجل إقناعهم بتبني قنوات مصرفية رقمية علما بان العراق قد وصل الى ما يقارب خمسة مليون محفظة الكترونية نهاية عام 2023.وعلى الرغم من أن Fintech تخلق فوائد للاستقرار المالي، إلا أنه من المحتمل أن يكون لها تأثير نظامي سلبي على الأخير ويمكن أن تنتج اثارا سلبية خطيره ويمكن أن تعرض الاقتصاد الحقيقي للمخاطر المتعددة، وتعتبر التقانات الحديثة إحدى التقنيات الهامة التي يمكن أن تقوض الاستقرار المالي من خلال قنوات التمويل الأصغر والقنوات الكبرى المالية؛ لذلك يمكن أن تخلق تقنيات مالية مخاطر مالية صغيرة وكبيرة على الاستقرار المالي؛ و بينما يعمل رأس المال والسيولة من جانب على تعزيز المرونة المالية من ناحية أخرى، وتدعم الحوكمة والضوابط القوية المرونة التشغيلية؛ وتتبع مصادر المخاطر التشغيلية من الحوكمة ومراقبة العمليات والمخاطر الإلكترونية والاعتماد على الأطراف الثالثة والمخاطر القانونية ومخاطر الأعمال المتعلقة بالبنية التحتية الحيوية للأسواق المالية (D'Arcy, J., & Basoglu, A. (2022) p39؛) ويشير الشمول المالي إلى عدد المستفيدين الذين يمكنهم الوصول إلى الخدمات المصرفية أو المالية، حيث أن الخطوة الأولى نمو الشمول المالي في امتلاك حساب على نحو متزايد، يتم استخدام المدفوعات الرقمية في المعاملات المالية. كما يعد إجراء المدفوعات الرقمية أو استدامه مع أحد الاستخدامات المهمة لحساب الادخار. مع ذلك، أفاد عدد قليل من الأشخاص باستخدام حساباتهم للادخار ولكن ليس للإجراء مدفوعات رقمية أو استخدمها في العام الماضي، كما ساعدت التكنولوجيا في تحقيق التكافؤ بين الجنسين وقللت الفجوة بين البالغين الأكثر ثراء والفقراء (منشورات البنك الدولي (WB) عن الأمن السيبراني)ونظراً للاضطرابات غير نقديه لا تستطيع المؤسسات المالية التحكم في تجربة الزبائن في المعاملات بسبب التكامل وتفقد الوحدات الاقتصادية الرؤية وسيتعين عليها أن تهدف الى تامين مكان البطاقة الافتراضية في السوق و أن التطورات السريعة في تقانيات المالية على الأسواق المالية ونماذج الأعمال للوحدات المالية التقليدية من أجل متابعة الاتجاهات المالية والمنافسة في منافستها سريعة النمو، للوصول إلى الشمول المالي حيث تتبنى المؤسسات المالية التقليدية التغييرات من أجل تلبية احتياجات السوق. ويمكن أن تكون عوامل جانب العرض والطلب بمثابة محركات للابتكارات المالية وتبحث للأجيال الجديدة بشكل خاص عن خدمة مالية سريعة وسهلة الوصول يمكن الوصول إليها في أي وقت وفي أي مكان وفيما يتعلق بذلك من المرجح أن يستخدموا المعلومات الإلكترونية أو الخدمات المالية عبر الهاتف المحمول أو الضمانات Fintech أو غيرها من المنتجات بدلاً من استخدام أساليب الخدمات المالية التقليدية والشاغل الرئيسي هو التأثير الرقمي على استقرار وسلامة أسواق والأنظمة المالية الأوسع.(منشورات البنك الدولي (WB) عن الأمن السيبراني.)وقد عرف مخاطر الأمن السيبرانية على أنه تشغيل خطر لأصول المعلومات والتقانية التي تؤثر في سرية؛ أو توافر؛ أو سلامة المعلومات؛ أو أنظمة المعلومات (منشورات مركز التميز التعاوني للدفاع السيبراني التابع لمنظمة حلف شمال الاطلسي.NATO CCD COE ، 2018)وان سرقة بيانات ومعلومات الزبون وكذلك التلاعب بها بكونها تهديدات الكترونية رئيسية تؤثر على أموال المصارف والتهديدات التي تتعرض لها البنية التحتية المالية والمخاطر التي تمثلها البرامج الضارة للأنظمة (الفتلاوي ؛أحمد عبيس نعمة؛ 2018:ص5) ، وإن تحديد المخاطر السيبرانية والاسس الكامنة وراءها يمكن أن يؤدي إلى وجود تعريف وفهم مشترك عبر المصارف بما في ذلك من قبل السلطات والمشاركين من القطاع الخاص، والى زيادة تسهيل تبادل البيانات والتعاون المناسب في السيطرة على المخاطر الإلكترونية وحسب نوع مخاطر الامن السيبرانية

المبحث الثالث: ملامح لبرنامج تدقيق(عراقي) مُقترح بشأن مخاطر الامن السيبرانية للمؤسسات المالية

Features for Iraqi Proposed Audit Guide about Representations Cyber security

لدى قيام الباحث بالبحث عن دليل أو برنامج محلي في الكتب والبحوث او لدى المنظمات ذات الصلة في العراق لم نجد دليل أو برنامج او اطار تدقيق(عراقي) يُعنى بتدقيق مخاطر الامن السيبرانية كدليل إثبات في التدقيق، ولوجود حاجة مُلحة ومتزايدة لمثل هكذا دليل ، و لما له من أثر بالغ في دعم رأي مراقب الحسابات أولاً، وفي محاولة لدرء أو تخفيض مسؤوليته غير المحدودة ثانياً، اجتهد الباحث في وضع ملامح لدليل تدقيق(عراقي) مُقترح يُعنى بهذه المخاطر ومحتوياته، وأخذ بنظر الاعتبار المقارنات

التي وردت ليتم العمل بها من قبل الجهات الرقابية والتشريعات المنظمة في جمهورية العراق وقد الاستفادة من تجارب الدول الأخرى مثل" المملكة العربية السعودية" (دليل الامن السيبرانية) وكذلك "المملكة الأردنية الهاشمية "(دليل الامن السيبرانية في القطاع المالي)وبما يسهم في تعزيز ما يُمثله من مخاطر الامن السيبرانية كونه دليل إثبات يُعين مراقب الحسابات على أداء مهمته،حيث لم نجد من خلال البحث عن خبراء ضمن مهنة مراقبي الحسابات يختصون بهذا الموضوع فتعذر على الباحث عرض برنامجه التدقيق واعتمد على تجارب الدول ذات الخبره بهذه المخاطر حتى وإن لم يكن لهذه المخاطر دورٌ أساسيٌ بل داعمٌ لأدلة الإثبات الأخرى ويتمثل دليل التدقيق المُقترح بالآتي:

أولاً–الغرض والنطاق Goal and Scope

1–يسعى هذا الدليل او البرنامج إلى وضع معايير وتوافر إرشادات في الحصول على إقرارات خطية (تحريرية) عن تدقيق خطر الامن السيبرانية من إدارة الشركة او الجهة موضوع العمل، ويشتمل هذا الدليل على العناصر الآتية:

أ– الإجراءات التي ينبغي تطبيقها عند تقييم المخاطرالسيبرانية وتوثيقها.

ب– الإجراء المُتخذ في حالة رفض الإدارة تقديم الإقرارات المناسبة حول تقيم مخاطر السيبرانية.

ج–ينبغي على المدقق الخارجي أن يحصل على إقرارات مناسبة من الإدارة بتدقيق المخاطر السيبرانية.

د– يتضمن هذا الدليل الإطار العام لما ينبغي إقراره من معلومات عن البيانات المالية التي تعدها: –

أولاً–"شركات القطاع العام".

ثانياً–"شركات القطاع المختلط".

ثالثاً–"الشركات المساهمة العامة؛ والخاصة".

رابعاً–"فروع الشركات؛ والمؤسسات الاقتصادية الأجنبية العاملة في العراق".

ثانيا: البرنامج التدقيقي الخارجي لمخاطر الامن السيبرانية (cyber internal audit):

التسلسل	إجراءات التدقيق	اسم المدقق وتوقيعه	نسبة التدقيق	رقم ورقة العمل	رقم ورقة الاستفسار وتاريخها
1–	(الخطة) ينبغي التخطيط للعمل للأمن السيبرانية والاغراض والانشطة والمشاريع داخل الوحدة الخاضعة للتدقيق في تحقيق المتطلبات القانونية والادارية .				
1–1	ينبغي العمل بخطة للحد من مخاطر الامن السيبرانية ودعمها من قبل رئيس الوحدة أو من ينوب عنه؛ وبموجب الصلاحيات وأن تتماشى وغرض خطة لأمن السيبرانية				
2–1	ينبغي العمل على خطة عمل لتنفيذ استراتيجية الامن السيبرانية من قبل الوحدة.				
3–1	ينبغي متابعة خطة الامن السيبرانية على اوقات زمنية مخطط لها (أو في حالة تغييرات في المتطلبات التشريعية والتنظيمية).				
2	(الإدارة) ضمان التزام ودعم مسؤول الصلاحية للوحدة فيما يتعلق بإدارة وتطبيق برامج الامن السيبرانية وفق المتطلبات التشريعية والتنظيمية .				

1-2	ينبغيتنظيم إدارة معنية بخطرالأمن السيبرانية في الجهة مستقلة عن إدارة تقانيه المعلومات وفق خطة العراق للأمن السيبرانية ويفضل ارتباطها مباشرة برئيس التنفيذي الاعلى للوحدة أو من ينوب عنه، مع الاخذ بالاعتبار عدم تعارض المسوؤليات.				
2-2	ينبغي أن يشغل منصب مسؤول بالأمن السيبرانية المشرفة والحساسة بها موظفون متفرغون وذوخبرة و كفاءة عالية في مجال الامن السيبرانية.				
3-2	ينبغي إنشاء لجنة المتابعة على لأمن السيبرانية بتوجيه من مسوؤل الوحدة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الامن السيبرانية، ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الدائرة المعنية بالأمن السيبرانية أحد أعضائها؛ ويفضل ارتباطها مباشرة برئيس الجهة أو معاونه، مع الاخذ بالاعتبار عدم تعارض المصالح والمسؤلية .				
3	(السياسة والإجراءات)اعداد إجراءات تتناسب مع مخاطر الامن السيبرانية والتزام الوحدة بها، وذلك وفقاً لمتطلبات العمل الاداريةو التنظيمية .				
1-3	ينبغي على الدائرة الاهتمام بمخاطر بالأمن السيبرانية في الوحدة و تحديد الضوابط و وإجراءات وما تشمله من متطلبات الامن السيبرانية، وتوثيقها واعتمادها من قبل الدائرة، كما يجب اعلام ذوي العلاقة من العاملين والاطراف الاخرى.				
2-3	ينبغي على الدائرة الاهتمام بالأمن السيبرانية وضمان تطبيق سياسة الامن السيبرانية في الوحدة وما تشمله من ضوابط ومتطلبات.				
3-3	ينبغي أن تكون إجراءات الامن السيبرانية بمعايير تقنية أمنية من خلال المعايير التقانية الامنية لجدار الحماية؛ وقواعد البيانات، وأنظمة التشغيل، وغيرها.				
4-3	ينبغي تدقيق معايير الامن السيبرانية وتحديثها على فترات زمنية مخطط لها أو حدوث خرق او تغير في المتطلبات الإدارية والقانونية، كما يجب توثيق التغييرات واعتمادها.				
4	(المسؤولية) ينبغي تعين وتحديد واضح لجميع الاطراف جميعها في تطبيق اجراءات الامن السيبرانية في الوحدة الخاضعة للتدقيق.				
1-4	ينبغي على المسوؤل عن تحديد وتوثيق واعتماد الهيكل التنظيمي للحوكمة والادوار الخاصة بالأمن السيبرانية للوحدة، وتكليف الاشخاص الاختصاص، و ينبغي تقديم الدعم اللازم لتنفيذ ذلك، مع الاخذ بالاعتبار عدم تعارض الاعمال.				
2-4	ينبغي تدقيق الدرجات الوظيفية بالامن السيبرانية في الوحدة				

	وتحديثها على فترات زمنية مخطط لها أو في حالة حدوث تغييرات في العمل				
5	(إدارة المخاطر) تدقيق خطر الامن السيبرانية على نحو ممنهج يهدف إلى حماية القواعد المعلوماتية والتقنية وذلك وفقاً للضوابط والاجراءات				
1-5	ينبغي على الوحدة المعنية بالأمن السيبرانية تحديد وتوثيق واعتماد خطة وإجراءات إدارة مخاطر الامن السيبرانية وذلك وفقاً العناصر السرية وتوافر وسلامة الاصول المعلوماتية والتقانية.				
2-5	ينبغي على الوحدة المعنية بالأمن السيبرانية تطبيق إجراءات إدارة مخاطر الامن السيبراني فيها				
3-5	ينبغي التقيد بإجراءات تقييم مخاطر الامن السيبراني بحد أدنى وكما يلي 1-عند البدء المبكر من المشاريع التقنية. 2 -عند إجراء تغيير جوهري في البنية التقانية. 3-عند التخطيط للاستفادةمن خدمات خارجيه. 4-عند التخطيط وقبل تنفيذ خدمات تقنية اول مرة				
4-5	ينبغي تدقيق خطة وإجراءات إدارة مخاطر الامن السيبرانية وتحديثها على فترات زمنية مخطط لها عند تبديل او تغير او قانون محدث				
6	(الامن السيبراني ضمن إدارة المشاريع التقنيه)ينبغي تنفيذ متطلبات الامن السيبرانية مضمنة في خطة إدارة مشاريع الوحدة لحفاظ على السرية وسلامة الاصول المعلوماتية والتقانية للجهة ودقتها وتوافرها،				
1-6	ينبغي توفير اساسيات الامن السيبراني في خطة وإجراءات إدارة المشاريع وفي إدارة التغيير على الاصول المعلوماتية والتقنية في حياة المشروع التقني، وأن تكون اساسيات الأمن السيبرانية جزء أساسي من متطلبات المشاريع التقنية.				
2-6	ينبغي أن تغطي احتياجات الامن السيبرانية إدارة المشاريع والتغييرات على الاصول المعلوماتية والتقنية للوحدة وبما يلي: 1-تقيم الثغرات ومعالجات والتحصين للإعدادات تدقيق شامل 2-ينبغي التحديث قبل إطلاق المشاريع والتغييرات.				
3-6	ينبغي أن تغطي اساسيات الامن السيبرانية لمشاريع التطوير للتطبيقات والبرمجيات للوحدة بحد أدنى وبما يلي:تنفيذ معايير التطوير الأمن للتطبيقات.Secure Coding Standards توفير مصادر مرخصة وموثوقة الأدوات لتطوير التطبيقات والمكتبات (Librarie)اجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة الخاضعة للتدقيق.				

	امن التكامل بين التطبيقات (Integration) (Secure Configuration and Hardening) وتدقيق الإعدادات وتحصينها والتحديث قبل إطلاق التطبيقات.				
4-6	ينبغي تدقيق مخاطر الامن السيبرانية في إدارة المشاريع في الوحدة دورياً.				
7	(الالتزام بالتشريعات وتنظيمات ومعايير الامن السيبرانية) ينبغي تدقيق برنامج الامن السيبرانية لدى الوحدة يتلائم والاجراءات				
1-7	ينبغي للوحدة الالتزام بالقوانين الادارية المحلية بالأمن السيبرانية.				
2-7	ينبغي التعرف على الاتفاقيات أو الالتزامات دولية معتمدة محلياً تتضمن تدقيق مخاطر الأمن السيبرانية، فيجب على الوحدة الالتزام والعمل بها.				
8	(تدقيق الدوري لمخاطر الامن السيبراني) تدقيق و التأكيد على مخاطر الامن السيبرانية والمعمول وفقاً للتعليمات، والاجراءات ، محليا و الدولية وتنظيمياً				
1-8	ينبغي على الوحدة المعنية بالأمن السيبرانية بتدقيق تطبيق اجراءات الامن السيبرانية دورياً.				
2-8	ينبغي تدقيق اجراءات الأمن السيبرانية في الوحدة، من قبل أطراف خارجية مستقلة عن الدائرة المعنية بالأمن السيبراني على أن تتم المراجعة والتدقيق من قبل خبير بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح، وذلك وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات .				
3-8	ينبغي توثيق نتائج تدقيق مخاطر الامن السيبرانية، وعرضها على اللجنة الاشرافية لأمن السيبراني و كما يجب أن تشتمل النتائج على نطاق المراجعة ، والملاحظات المكتشفة، والتوصيات والاجراءات التصحيحية، وخطة معالجة الملاحظات لغرض العمل بها.				
9	(مخاطر الامن السيبراني والموارد البشرية) ينبغي التأكد من أن مخاطر ومتطلبات الامن السيبرانية المتعلقة بالموظفين الدائمين والمتعاقدين في الوحدة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والاجراءات التنظيمية للوحدة.				
1-9	ينبغي تحديد وتوثيق واعتماد متطلبات الامن السيبرانية المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في الجهة.				
2-9	ينبغي تنفيذ اجراءات الامن السيبرانية المتعلقة بالموظفين في الوحدة للتدقيق				
3-9	ينبغي توفر الإجراءات الامن السيبرانية قبل بدء علاقة العاملين				

	المهنية بالوحدة وبما يلي: توفير ضمانات لمسؤوليات الامن السيبرانية للحفاظ على سرية المعلومات (Clauses Disclosure–Non) وكذلك العقود للعاملين في الوحدة لتشمل قبل وبعد العمل و إجراء المسح الامني (Vetting or Screening) للعاملين في الامن السيبرانية و التقانية ذات الصلاحيات المهمة والحساسة.				
4-9	ينبغي ان توفرمخاطر الامن السيبرانية خلال علاقة العاملين المهنية بالوحدة بحد أدنى بما يلي: التوعية بخطرالأمن السيبرانية عند بداية المهنة العمل وخلالها. توفير متطلبات الامن السيبرانية والالتزام بها وفقاً لإجراءات وعمليات الامن السيبرانية				
5-9	ينبغي تدقيق وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء الخدمة المهنية لهم بالوحدة.				
6-9	ينبغي تدقيق متطلبات الامن السيبرانية المتعلقة بالعاملين في الوحدة دورياً				
10	(التدريب والتوعية لمخاطر الأمن السيبرانية)ينبغي تدقيق الموظفين العاملين بالوحدة بان لديهم التوعية الازمة الامنية ومعرفة بمسؤوليات في مجال الامن السيبرانية؛ والتأكد من ان تم تزويدهم بالمهارات والمؤهلات والدورات التدريبية في مجال الامن السيبرانية لحماية الاصول المعلوماتية والتقانية ؛ والقيام بمسؤولياته تجاه خطرالامن السيبرانية.				
1-10	ينبغي تدقيق و تطوير ولاعتماد على برنامج بالأمن السيبرانية للتوعية في الوحدة من خلال العديد من القنوات دورياً، لزيادة الوعي بخطرالأمن السيبرانية وتهديداته ومخاطرة، واعطاء ثقافة إيجابية لأمن السيبرانية.				
2-10	ينبغي تنفيذ البرنامج المعتمد للتوعية بالأمن السيبراني في الوحدة.				
3-10	ينبغي أن يغطي البرنامج التوعية بالأمن السيبرانية وطريقة حمايتها من أهم المخاطر والتهديدات السيبرانية وبما بلي: تعامل الامن مع الخدمات البريدية الكترونية و خصوصاً مع الرسائل التصيد الكتروني. الحماية مع الأجهزة المحمولة والوسائط التخزينة. التعامل الامن مع الخدمات للتصفح داخل الشبكة التعامل الامن مع الوسائل الخاصة بالشبكة الاجتماعية.(التواصل)				
4-10	ينبغي توفير المهارات المتخصصة والتدريب الإلزامية للموظفين في المجالات العمل ذات العلاقة بالأمن السيبرانية في الوحدة،				

	والتصنيف بما يتلائم مع مسؤولياته للعمل فيما يتعلق بالأمن السيبرانية، وبما يلي:-العاملين بالدائرة المعنية بالأمن السيبرانية. العاملون في التطوير للبرامج والتطبيقات و المشغلون لأصول المعلوماتية والتقانية للوحدة وللاشراف عليها تنفيذيا				
5-10	ينبغي تدقيق تطبيق البرنامج التوعي بالأمن السيبرانية في الوحدة الخاضعة دوريا.				
11	(إدارة البنية التحتية) التأكد من أن الوحدة لديها قائمة جرد دقيقة وحديثة للأملاك والموجودات تشمل التفاصيل ذات العلاقة والمعلوماتية والتقانية المتاحة للوحدة، لغرض الدعم للعمليات الصناعية ومتطلبات الامن السيبرانية، لتحقيق السرية والسلامة الموجودات المعلوماتية والتقانية ودقتها وتوفيرها.				
1-11	ينبغي تحديد وتوثيق واعتماد متطلبات الامن السيبرانية لإدارة الاصول المعلوماتية والتقانية .				
2-11	ينبغي تنفيذ المتطلبات الأمن السيبرانية للإدارة الموجودات المعلوماتية والتقانية للوحدة.				
3-11	ينبغي توثيق وتحديد والاعتماد والنشر لسياسة الاستخدام المقبول للموجودات المعلوماتية والتقانية للوحدة.				
4-11	ينبغي تنفيذ السياسة الاستخدام للموجودات المقبولة المعلوماتية والتقانية للوحدة.				
5-11	ينبغي تبويب الموجودات المعلوماتية والتقانية للوحدة وترميزها (Labeling) والتعامل معها وفقاً للمتطلبات والتنظيمية والقانونية المشتركة				
6-11	ينبغي تدقيق المتطلبات الامنه السيبرانية لحوكمة الموجودات التقنية و المعلوماتية دوريا للوحدة.				
12	(إدارة الهويات للدخول والصلاحيات) ضمان حماية الامنة السيبرانية للتنفيذ المنطقي (Access Logical) للموجودات المعلوماتية والتقانية للوحدة من أجل منع الدخول الغير المصرح والتقييد الدخول للمطلوب إنجازه الاعمال المتعلقة بالوحدة الخاضعة للتدقيق				
1-12	ينبغي توفير واعتماد والتوثيق المتطلبات الامنة السيبرانية للإدارة للهويات والدخول والصلاحيات في الوحدة.				
2-12	ينبغي تطبيق متطلبات الامن السيبرانية لإدارة هويات الدخول والصلاحيات في الجهة.				
3-12	ينبغي أن توفر المتطلبات الامن السيبرانية المتعلقة بإدارة الهويات الدخول والصلاحيات في الوحدة وبما يلي: تدقيق هوية المستخدمين (User Authentication) استنادا لكلمة				

	المرور .تدقيق الهوية المتعدد العناصر(Authentication Factor–Multi) للعمليات الدخول إدارة الصلاحيات والتصاريح المستخدمين) Authorization) بناء على مبدا التحكم بالدخول والصلاحيات مبدا الحاجة للمعرفة ، " Need–to–know and "Need–to–use" ومبدأ للحدالادنى من الامتيازات والصلاحيات "Privilege Least،"ومبدأ الفصل للمهام و للصلاحيات والحساسية المهمة والتدقيق لهويات الدخول والصلاحيات دوريا				
4–12	ينبغي تدقيق والتطبيق للمتطلبات الامنه السيبرانية للإدارة من خلال الهويات والصلاحية للدخول في الوحدة دورياً				
13	(حماية الأنظمة وأجهزة تقنية معالجة المعلومات) لضمان الحماية الامنة لانظمة والأجهزة لمعالجة المعلومات بما في ذلك لأجهزة للمستخدمين والبنى التحتية للوحدة من الخطر السيبرانية.				
1–13	ينبغي التحديد والتوثيق والاعتماد على المتطلبات الامنة السيبرانية للحماية الانظمة والأجهزة للمعالجة المعلومات للوحدة				
2–13	ينبغي التنفيذ الامن للمتطلبات السيبرانية للحماية النظم والأجهزة وللمعالجة معلومات للوحدة الخاضعة للتدقيق.				
3–13	ينبغي أن توفر الامان للمتطلبات السيبرانية للحماية الانظمة والأجهز و لمعالجة معلومات للوحدة باقل مما يمكن وبما ياتي: توفيرالحماية من الفيروسات والبرامج الضارة والانشطة المشبوهة (Malware) على لأجهزة المستخدم والخوادم باستخدام التقانيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن. الالتزام الحازم للاستخدام الأجهزة ووسائط التخزين الخارجية والامنة المتعلقه بها.الإدارة الحازمة للتحديثات التطبيقات والاجهزة والإصلاحات للأنظمة Patch (Management.) للمزامنة خلال التوقيت (Synchronization Clock) ومركزياً ومن المصدر الدقيق والموثوق، وان من هذه المصادر ما تم توفيرة للجهات ذات العلاقة بالموضوع وللمواصفات والجودة والمقاييس .				
4–13	ينبغي تدقيق الامان للمتطلبات السيبرانية للحماية الانظمة والأجهزة الخاصة لمعالجة معلومات دورياً للوحدة.				
14	(حماية البريد الالكتروني) ينبغي الحماية للبريد الخاص الكترونيا للوحدة من خطر السيبرانية.				
1–14	ينبغي توثيق و تحديد والاعتماد للمتطلبات الامان السيبرانية لحماية الخاصة للبريد الإلكتروني للوحدة.				
2–14	ينبغي توفير المتطلبات الامان السيبرانية للحماية الكتروني للبريد للوحدة.				

3-14	ينبغي توفيرالامان للمتطلبات السيبرانية للحماية البريد الكترونية للوحدة باقل مما يمكن وبما يلي:-التصفية والتحليل (Filtering) للرسائل البريدية الكترونية وفيما يخص الرسائل التصدي الكترونية «Emails Phishing » والرسائل الاقتحامين» Emails Spam)» باستخدام التقانيات والآليات للحماية الحديثة و للبريد الإلكتروني المتقدمة. تدقيق الهوية المتعددة المصادر -Authentication Factor (Multi وللدخول عن بعد وللدخول عن طريق الصفحة للموقع البريد الإلكتروني (Webmail.) النسخ الاحتياطي والارشفة للبريد الإلكترونية-للحماية من التهديدات المتقدمة المستمرة Protection APT،) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً) Malware Day-Zero،) وإدارتها بشكل آمن.التوثيق للمجال الالكتروني للبريد للوحدة بالطرق التقانية، مثال الطريقة الإطار لسياسة المرسل. (Sender Policy Framework)				
4-14	ينبغي تدقيق وتوفير المتطلبات الامان السيبرانية الخاصة بالحماية البريدية الالكترونية دورياً للوحدة				
15	(ادارة حماية الشبكة من مخاطر الامن السيبرانية) ضمان حماية الوحدة للشبكة من المخاطر السيبرانية.				
1-15	ينبغي توثيق و توفير والاعتماد الامان متطلبات السيبرانية للإدارة أمنة للوحدة من خلال الشبكات .				
2-15	ينبغي توفير الامان للمتطلبات السيبرانية للإدارة أمان الوحدة من خلال الشبكة الخاضعة للتدقيق.				
3-15	ينبغي توفير امان للمتطلبات السيبرانية الإدارة أمان الوحدة للشبكة من خلال مايلي وباقل مايمكن : التدقيق المنطقي للأجزاء والشبكات و العزل والتقسيم المادي أو بشكل آمن، واللازمة للسيطرة على المخاطر الامان السيبرانية ذات العلاقة، بالاستخدام لجدار الحماية) Firewall) ومبدأ للدفاع الامنية المتعددة المراحل Defense-in-Depth				
4-15	العزل البيئة الانتاجية عن بيئات الشبكة التطويرية والاختبارية.				
5-15	أمان التواصل والتصفح بالأنترنت، و الذي يشمل التقييد الحازم للمواقع الكترونية المشبوهة، و المشاركة والتخزين للملفات، والمواقع الدخول والسيطرة عن بعد.				
6-15	توفيرامان للشبكة لاسلكي ولحمايتها باستخدام الوسائل الآمنة للتدقيق من التشفيرو الهوية ، وعدم الربط الشبكي اللاسلكي والشبكة للوحدة				

	الداخلية إلا بناء اعلى دراستها المتكاملة للمخاطر المترتبة مستقبلا والتعامل بما يوفر الحماية التقانية للموجدود للوحدة.				
7-15	التدقق للقيود وإدارة المنافذ والبروتوكولات ولخدمات الشبكة للامان				
8-15	توفير امن لأنظمته المتقدمة و للاكتشاف والمنع الاختراقات Intrusion Prevention Systems				
9-15	امن أسماء النطاقات (DNS)				
10-15	الحماية لقناة التصفح لانترنت من التهديدات المتقدمة والمستمرة(Protection APT،) والتي يتم الاستخدم لعدة فيروسات وبرمجيات ضارة الغير معروفة سابقا) Malware Day-Zero وإدارتها امنيا				
11-15	ينبغي تدقيق الامان لتطبيق المتطلبات السيبرانية لحوكمة الأمن دوريا للشبكة.				
16	(امن الأجهزة المحمولة) لضمان توفيرالامان للاجهزة (للوحدة المحمولة) وأجهزة الحاسب المحمولة والهواتف الذكية والاجهزة الذكية اللوحية (من المخاطر السيبرانية ولضمان التعامل بشكل آمن مع المعلومات الحساسة و الخاصة بالاعمال للوحدة ولحمايتها أثناء التخزين والنقل عنده الاستخدام للاجهزة الشخصية (BYOD.) للعاملين في الوحدة				
1-16	ينبغي توثيق تحديد الأمان باعتماد على المتطلبات السيبرانية الخاصة بأمان الاجهزة المحمولة و الشخصية للعاملين(BYOD) عند ارتباطها بشبكة للوحدة.				
2-16	ينبغي توفير امان لمتطلبات السيبرانية الخاصة بأمن الأجهزة المحمولة وأجهزتها(BYOD) للوحدة و يجب أن يوفر الأمان للمتطلبات السيبرانية الخاصة بأمن الأجهزة المحمولة وأجهزة(BYOD) للوحدةبما يلي: الفصل والتشفير لقاعدة المعلومات الخاصة بالوحدة والتي تم تخزينها على الأجهزة المحمولة وأجهزة الاستخدام المحددة والمقيدة بناءا على ما يتطلبه المصلحة الأعمال للوحدة.الغاء مصادر المعلومات الخاصة بالوحدة ("المخزنة على الأجهزة المحمولة وأجهزة") (BYOD) عند ضياع الاجهزة أو بعد انتهاء/إنهاء علاقتة بالوظيفية مع الوحدة والعمل والتوعية الأمنية للمستخدم.				
3-16	ينبغي تدقيق الامان لتطبيق المتطلبات السيبرانية الخاصة بالأمان لاجهزة المحمولة وأجهزتها) (BYOD دوريا للوحدة				
17	(حماية البيانات والمعلومات) توفير الحماية سرية والسالمة للبيانات والمعلومات للوحدة مع دقتها وتوفيرها، ويكون ذلك وفقاً للادارةالتنظيمية للسياسات والاجراءات ، والمتطلبات القانونية				

	المتعلقة بها.				
1-17	ينبغي توفير الامان والتوثيق والاعتماد لمتطلبات السيبرانية لحماية البيانات والمعلومات للوحدة، بما يوجب الالتزم بالاطر القانونيه والتنظيمية				
2-17	ينبغي توفير وتطبيق الامان لمتطلبات السيبرانية للحماية الوحدة وبياناتها ومعلوماتها الخاضعة للتدقيق والرقابة.				
3-17	ينبغي توفيرالامان لمتطلبات السيبرانية للحماية القواعد و بياناتها ومعلوماتها بما يلي: 1- امتلاك البيانات والمعلومات المهمة 2- تحديد وتعين والية ترميزها للبيانات 3- تخصيص أسس لسرية المعلومة او توفيرها				
4-17	(التشفير) الاستخدام الضامن الفعال والسليم للتشفير لقواعد المعلوماتية الالكترونية للوحدة للبيانات، ومن خلال الالتزام بالاطر القانونية والادارية				
5-17	ينبغي توفير الامان والتوثيق والاعتماد للمتطلبات السيبرانية للتشفير للوحدة.				
6-17	ينبغي توفير امان موثق للمتطلبات السيبرانية للوحد لغرض التشفير الخاضعة للتدقيقها.				
7-17	ينبغي أن تلبي الامان لمتطلبات السيبرانية للتشفير باقل مما يمكن وبما يلي: 1- المعايير للحلول الخاصة بالتشفير المعتمدة قانونا وللقيود المطبقةفيها (فنياوتنظيميا وتقنياً). 2- امان الادارة للمفاتيح المهمة للتشفيرمن خلال العمليات لدورة حياتها. 3- التشفير للبيانات أثناء التخزين والنقل بناء على التصنيف ولحسب المتطلبات الإدارية والقانونية للوحدة المتعلق بها العمل				
8-17	ينبغي تطبيق الامان والتدقيق لمتطلبات السيبرانية في الوحدة الخاضعة للتدقيق من خلال لتشفير دوريا				
18	(إدارة النسخ الاحتياطي) توفير الحماية لبيانات والمعلومات للوحدة والاعدادات التقانية للأنظمة والتطبيقات بالوحدة من الاضرار والاجراءات الناجمة عن التهديدات السيبرانية، من خلال الالتزم بالقانون والضوابط المتعلقه بالعمل				
1-18	ينبغي توفيرامان لتوثيق والاعتماد لمتطلبات السيبرانية للإدارة الوحدة من خلال النسخ الاحتياطي.				
2-18	ينبغي تنفيذ الامان والتدقيق لمتطلبات السيبرانية للإدارة النسخ البديلة				

	والاحتياطية وتوثيقها				
3-18	ينبغي تغطية الامان للمتطلبات السيبرانية اي إدارة النسخ الاحتياطية وكما يلي: 1- النطاق للنسخ الاحتياطي ولشموليتها للموجودات المعلوماتية والتقانية المهمة. 2- الاستعادة السريعة للبيانات والنظم عند تعرضها للحوادث ومخاطرها السيبرانية. 3-توفير الفحص الدوري لمدى الفعالية لاستعادة النسخ المحفوظةوالنسخ الاحتياطية.				
4-18	ينبغي تدقيق الامان لتطبيق المتطلبات السيبرانية للإدارة النسخ الثانية و الاحتياطية للوحدة الخاضعة للتدقيق والمتابعة				
19	(إدارة الثغرات) توفير امان إضافي لضمان ولاكتشاف الثغرات المهة التقنية في الزمن المناسب ولمعالجتها بالشكل الفعال ولذلك لتقليل و لمنع أو احتمالية لاستغلال لهذه الثغرات من قبل الهجمات السيبرانية؛ ولتقليل الاثار المترتبة على أعمال الوحدة				
1-19	ينبغيتوفير الامان والتوثيق والاعتماد على المتطلبات السيبرانية لإدارة الثغرات التقانية للوحدة				
2-19	ينبغي التطبيق الأمان لمتطلبات السيبرانية للإدارة الثغرات التقانية الخاضعة للرقابة فيما يخص الوحدة				
3-19	ينبغي أن توفرالامان لمتطلبات السيبرانية للإدارة الثغرات ومما يلي: 1- التدقيق والفحص والاكتشاف دوريا للثغرات 2- تحديد خطورة الثغرة وحسب تصنيفها 3- المعالجة للثغرات بناءا على التصنيفات والمخاطر السيبرانية المحدد لها. 4- الإدارة لحزم الإصلاحات والتحديثات لمعالجة الثغرات امنيا. 5- الاشتراك والتواصل مع الثقة من المصادر التي يتعلق بالتنبيهات بالثغرات والمحدثة والجديدة.				
4-19	ينبغي تدقيق الأمان لتطبيق المتطلبات السيبرانية دوريا من قبل لإدارة الثغرات تقنيا				
20	(اختبار الاختراق) لتقييم والاختبار لمدى الفعالية لقدرات التعزيز الامان السيبرانية في الوحدة، لعمل محاكاة لتقانيات والأساليب الهجومية السيبرانية الفعلية؛ والاكتشاف لنقاط الأمنية الضعيفة والغير المعروفة وتؤدي إلى الاختراقات السيبرانية للوحدة وحسب معايير الالتزام بالقانون والتنظيمات.				
1-20	ينبغي توفير الامان ولتوثيق والاعتماد لمتطلبات السيبرانية للعمليات				

	الاختبارو الاختراق في الوحدة				
2-20	ينبغي تدقيق وتنفيذ العمليات واجراء الاختبار للوحدة من خلال الاختراق				
3-20	ينبغي توفير الأمان لمتطلبات السيبرانية الاختبار الاختراق وكمايلي: 1- العمل اختبار الوحدة من خلال الاختراق، ليشمل الجميع من الخدمات خارجياً عن طريق شبكة الانترنيت ولمكوناتها التقانية، والبني التحتية،و المواقع الكترونية، والتطبيقات الويب،و التطبيقات الهواتف الذكية واللوحية، والبريد الالكتروني والدخول اون لاين عن بعد. 2- اختبارالوحدة عمليا من خلال الاختراق للشبكة دورياً.				
21	(إدارة سجلات الاحداث ومراقبة الامن السيبرانية) لضمان و تجميع والتحليل والمراقبة للسجلات و الأحداث الامان السيبرانية في الوقت المحدد من أجل الاستباقية لحدوث التهديدات السيبرانية وإدارتها لمخاطرها بفعالية وكفاءة لمنع أو لتقليل الاثار المترتبة على الوحدة و أعمالها.				
1-21	ينبغي توفيرالامان والتوثيق والاعتماد لمتطلبات إدارتها لسجلات الاحداث والمراقبة الامان السيبرانية للوحدة.				
2-21	ينبغي تدقيق و تطبيق الأمان لمتطلبات إدارتها للسجلات والاحداث ولمراقبة الامان السيبرانية.				
3-21	ينبغي توفير لمتطلبات إدارتها لسجلات الاحداث ولمراقبة الامان السيبرانية باقل مما يكن وكما يلي : 1- العمل لتفعيل السجلات الاحداث(logs Event) الخاصة بالأمان السيبرانية على المعلوماتية وموجوداتها لدى الوحدة 2- التفعيل لسجلات الاحداث الخاصة بالحسابات ذات الصلاحيه الهامة على الموجودات المعلوماتية والأحداث لعمليات الدخول عن اون لاين عن بعد 3- التحديد للتقانيات اللازمة (SIEM) للجميع السجلات و الاحداث الخاصة بالأمان السيبرانية. 4- التدقيق المستمرة للسجلات و الاحداث الخاصة بالأمان السيبرانية. 5- المدة الخاصة بالاحتفاظ بالسجلات والاحداث الخاصة بالأمان السيبرانية (سنة كاملة).				
4-21	ينبغي توفيرو تطبيق المتطلبات إلادارة السجلات والاحداث والمراقبة الامان السيبرانية دورياً.				

5-21	(ادارة حوادث والتهديدات للأمن السيبرانية) لضمان التحديد والاكتشاف لحوادث الامان السيبرانية في الوقتالمحدد وإدارتها بشكل كفوء والتعامل مع التهديدات الامان السيبرانية استباقياً من أجل منع أو التقليل من الاثار المترتبة على أعمال الوحدة مع ما يتلاءم مع القانون والتعليمات				
6-21	ينبغي توفير الامان والتوثيق والاعتماد لمتطلبات إدارتها للحوادث والتهديدات السيبرانية				
7-21	ينبغي تدقيق والتطبيق للمتطلبات الأمان لإدارة الحوادث والتهديدات الامان السيبرانية في المؤسسة.				
8-21	ينبغي أنتوفيرالامان لمتطلبات الإدارة للحوادث والتهديدات الامان السيبرانية باقل مما يلي : 1- ايجاد الخطط والاستجابة للحوادث الامنية وتصعيد الياتها 2- التصنيف والتحديدلحوادث الامان السيبرانية. 3- يتم تبليغ الهيئة المسؤولة عند الحوادث الأمن سيبرأنيه. 4- المشاركة للتنبيهات والمعلومات الاستباقية وصور الاختراق والتقارير للحوادث الامن السيبرانية مع الجهات ذات العلاقة والمسوؤلة 5- ينبغي التوصل على البيانات الاستباقية Intelligence (Threat) والتعامل معهاونوع التهديد وحسب المعالجة				
9-21	ينبغي تدقيق و تطبيق للمتطلبات إدارتها للحوادث وتهديدات الامان السيبرانية دورياً للوحدة				
22	(الامن المادي) ضمان حماية الموجودات المعلوماتية والتقانية للوحدة من الحصول على الامان المادي الغير المصرح به والضياع والسرقات و والعبث والتخريب.				
1-22	ينبغي توفيرالامان والتوثيق والاعتماد للمتطلبات الامان السيبرانية للحماية الموجودات والتقانية للوحدة من التواصل المادي الغير المصرح به والضياع				
2-22	ينبغي توفير الأمان المادي لمتطلبات الامان السيبرانية للحماية الاصول والتقانية للوحدة من للحصول على العلومة والغير المصرح به والتخريب باقل مما يلي: 1- دخول مصرح به للاماكن المهمة في الوحدة ("مثل: مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الامداد الخاصة بالأجهزة والعتاد التقنية، وغيرها") 2- السجلات الدخول والخروج والتدقيق.CCT				

	3- الحماية للمعلومات والسجلات والدخول والتدقيق عليها 4-(أمن الإتلاف ولإعادة الاستخدام للموجود المادية التي تحتوي على المعلومات المصنفة) وتشمل: الوثائق الورقية ووسائط الحفظ والتخزين) 5- أمان الاجهزة والمعدات داخل مباني الوحدة وخارجها				
3-22	ينبغي تدقيق الامان لمتطلبات الامن السيبرانية للحماية قاعدة المعلوماتية والتقانية للوحدة من الولوج المادي الغير المصرح به والفقدان وغيرها دورياً.				
23	(حماية تطبيقات الويبWeb Application Security) الضمان للحماية للتطبيقات الويب الخارجية المخاطر السيبرانية للوحدة.				
1-23	ينبغي توافر الامان والتوثيق والاعتماد للمتطلبات الامان السيبرانية للحماية التطبيقات الويب للوحدة الخارجية للمخاطر السيبرانية.				
2-23	ينبغيتوفير وتدقيق المتطلبات الامان السيبرانية لحماية التطبيقات من الخرق (الويب الخارجية)				
3-23	ينبغي توفير الأمان لمتطلبات الامن السيبرانية للحماية ون ضمنها التطبيقات الويب الخارجية للوحدة باقل مما يكن وكما يلي: 1- (Web Application Firewall) الاستخدام لجدار الحماية تطبيقات الويب والتواصل) 2- Multi-tier Architecture الاستخدام لمبدا المعمارية لمستويات متعددة 3- الاستخدام للبروتوكولات الآمنة ("مثل بروتوكول HTTPS") 4- التوضيح للسياسة الاستخدام الامان للمستخدمين الداخلي والخارجي 5- تدقيق الهوية المتعدد للإجراءات و للعناصر Authentication (Factor-Multi) دخول المستخدمين.				
4-23	ينبغي تدقيق الأمان وتوفيره للمتطلبات الامان السيبرانية للحماية التطبيقات (التواصل الويب) من المخاطر السيبرانية دورياً للوحدة				
24	(صمود الامن السيبرانية في إدارة استمرارية الاعمال) الضمان المتوافر للمتطلبات الصمود الامان السيبرانية في إدارتها لاستمرارية للوحدة ولضمان المعالجة والتقليل الاثار المترتبة على الاضطرابات في الخدمات المؤتمته الحرجة للوحدة وأنظمتها وأجهزتها لمعالجة المعلوماتها جراء الكوارث الناتجة عن المخاطروالتهديدات السيبرانية.				
1-24	ينبغي توافر الأمان والتوثيق واعتماد للمتطلبات الامان السيبرانية لضمان إدارتها واستمراريتها لأعمال الوحدة				
2-24	ينبغي توفير المتطلبات الامان السيبرانية لضمان إدارتها و				

	استمراريتها لأعمال الوحدة دوريا				
3-24	ينبغي توافر إدارتها لاستمرارية الاعمال في الوحدة باقل مما يجب ومما يلي : 1- الفحص والتأكد من استمرارية والاجراءات والأنظمة المتعلقة بالأمان السيبرانية. 2- تحديد الخطط اللاستجابة للحوادث والهجمات الامان السيبرانية التي قد يكون لها تاثير على استمرارية لأعمال الوحدة 3- تحديد خطط التعافي من الكوارث Disaster Recovery Plan				
4-24	ينبغي تدقيق المتطلبات الامان السيبرانية ضمن إدارتها لاستمرارية أعمالها دوريا للوحدةال				
25	(مخاطر الامن السيبرانية المتعلقة بالأطراف الخارجية) (الضمان لحماية الموجودات الوحدة من مخاطر الامان السيبرانية المتعلقة بالأطراف الخارجية) بما في ذلك خدماتها المساندة لتقانية "المعلومات" "Outsourcing "والخدمات المدارة "" Services Managed.) "وفقاً للسياسات والاليتزام				
1-25	ينبغي تحديد وتوثيق واعتماد متطلبات الامن السيبرانية ضمن العقود والاتفاقيات مع الاطراف الخارجية للجهة الخاضعة للتدقيق				
26	ينبغي أن تغطي متطلبات الامن السيبرانية ضمن العقود والاتفاقيات) (اتفاقية مستوى الخدمة SLA) مع الاطراف الخارجية التي قد تؤثر بإصابتها بيانات للوحدة أو الخدمات المقدمة لها باقل مما يكن وكما يلي: 1- البنود المحافظة على السرية للمعلومات) Clauses (Disclosure-Non) والحذف الامان من قبل الطرف الخارجي لبياناتها عند انتهاء الخدمة للوحدة 2- الإجراءات المتواصلة في الحال لحدوث الحادثة أمان سيبرأنية. 3- التزام الطرف الخارجي بالتطبيق للمتطلبات والسياسات الامان السيبرانية وضوابط الوحدة				
1-26	توفير المتطلبات الامان السيبرانية مع الاطراف الخارجية التي يتم تقدم خدماتها لإسناد لتاقنية المعلومات، أو خدمات مدارة باقل مما يكن وكما يلي : 1- التقييم للمخاطر الامان السيبرانية، والتدقيق من وجود ماتضمن السيطرة على خذه المخاطر، قبل التوقيع للعقود والاتفاقيات أو عند التغيير للمتطلبات القانونيه ذات العلاقة. 2-ينبغي لمراكز العمليات لخدمات الامان السيبرانية التعاون				

	للتدقيق ، والتي يتم ان تستخدم لطريقتها للتوصل عن بعد				
2-26	ينبغي تدقيق الامان للمتطلبات الامان السيبرانية دوريا من قبل الوحدة مع الاطراف الخارجية				
27	(الامن السيبرانية المتعلق بالحوسبة السحابية والاستضافة) لضمان المعالجة للامان السيبرانية والتنفيذ للمتطلبات الامان السيبرانية (للحوسبة السحابية)والاستضافة بالشكل الملائم والفعال، وذلك وفقاً ولضمان الحماية قاعدةالمعلوماتية والتقانيةللوحدة على الخدمات (الحوسبة السحابية) التي تتم استضافتها أوالتي يتم معالجتها أو إدارتها بواسطة أطراف خارجية وحسب الضوابط والقانون				
1-27	ينبغي توافرالامان والتوثيق والاعتماد للمتطلبات الامان السيبرانية باستخدام الخدمات (الحوسبة السحابية والاستضافة)				
2-27	ينبغي تدقيق الامان للمتطلبات السيبرانية بالخدمات (الحوسبة السحابية والاستضافة للوحدة وحمايتها من الهجمات).				
3-27	ينبغي تدقيق الأمان للمتطلبات السيبرانية باستخدام خدمات (الحوسبة السحابية والاستضافة)باقل ما يمكن ومما يلي: 1-"التصنيف للبيانات قبل استضافتها" لدى مقدمي خدمات (الحوسبة السحابية والاستضافة)، وإعادتها للجهة و بالصيغة قابلة للاستخدام (عند انتهاء الخدمة). 2- الفصل البيئ للوحدة وخصوصاً الخوادم الافتراضية وعن غيرها من توابع البيئات لأخرى في (الخدمات الحوسبة السحابية) 3- الموقع الاستضافة والتخزين والمعلومات يجب أن يكون داخل العراق بالنسبة للوحدات .				
4-27	ينبغي تدقيق ومتابعة الأمان للمتطلبات الامان السيبرانية التي تخص (الخدمات الحوسبة السحابية والاستضافة) للوحدةدورياً.				
28	(الامن السيبرانية للأنظمة التحكم الصناعي) لضمان إدارة الامان السيبرانية بالشكل السليم والفعال للحماية وتوافر والسلامة والسرية للموجود الوحدة المتعلقة بأجهزتها وأنظمتها للتحكم الصناعي(ICS/OT) ضد (الهجوم السيبرانية) مثل" الوصول غير المصرح به والتخريب والتجسس والتلاعب" (بما يتماشى مع خطة الامن السيبرانية للجهة،) وإدارتها لمخاطر الامان السيبرانية، والالتزان بالقانون الإداري والضوابط الفعاله للوحدة .				
1-28	ينبغي وافر الامان والتوثيق والاعتماد للمتطلبات الامان السيبرانية للحماية لأجهزة وأنظمتها للتحكم الصناعي (OT/ICS للجهة الخاضعة للتدقيق				
2-28	ينبغي توافر المتطلبات الامان السيبرانية للحماية الأجهزة وأنظمتها				

	للتحكم الصناعي (ICS/OT) للوحدة.				
3-28	توافر المتطلبات الامان السيبرانية للحماية الأجهزة وأنظمتها للتحكم الصناعي(ICS/OT) يجب أن تغطي باقل ما يمكن وكما يلي: (الالتزام الحازم والمنطقي والتقسيم المادي عند الربط لشبكة التشغيلICS/OT) مع الجهات الأخرى للوحدة، مثال: "شبكة الأعمال الداخلية للجهة" "Corporate Network" وكذلك (الانترنت أو الدخول عن بعد أو اتصال اللاسلكي و التفعيل للسجلات الاحداثlogs Event) (الخاصة بالأمن السيبرانية للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك، والمراقبة المستمرة لها)SIS" (Safety Instrumented System "عزل أنظمة معدات السلامة") (تدقيق الإعدادات والتحصين الانظمة الصناعية، وأنظمتها الدعم والاجهزة الالية الصناعية دوريا) (Secure Configuration .and Hardening) (OT/ICS Vulnerability Management(إدارة ثغرات الأنظمة الصناعية)"إدارة حزم التحديثات والإصلاحات الامنية للأنظمة الصناعية") OT/ICS Patch Management (ادارة البرامج الخاصة بالأمن السيبرانية الصناعي للحماية من الفيروسات والبرمجيات المشبوهة والضارة)."				
4-28	ينبغي تدقيق الامان للمتطلبات الامان السيبرانية للحماية أجهزتها وأنظمتها (التحكم الصناعي ICS/OT للجهة الخاضعة للتدقيق دورياً)				

من خلال ماتقدم أعلاه من برنامج التدقيق الخاص بمخاطر الامن السيبراني وجود علاقه مابين مخاطر الامن السيبراني والمسؤولية المهنية لمراقب الحسابات .

المبحث الرابع: الاستنتاجات والتوصيات: -

أولا: الاستنتاجات /

يعرض هذا المبحث اهم الاستنتاجات النظرية التي تم التوصل اليها عن نتائج تقييم اداء المحافظ الاستثمارية، التي تمثلت بالاتي

1- إن تقرير تحديد مخاطر الامن السيبرانية والمرفق (البيانات المالية وتقرير الإدارة السنوي)، مما يحمل مراقب الحسابات (المراقب الخارجي) مسؤولية كبيرة أمام الأطراف الخارجية في حدوث خروقات او تهديدات سيبرانيه لم يتم الاعتراف بها من لدن الجهة الخاضعة لتدقيقه.

2- على الرغم من إن الأمانة العامة لمجلس الوزراء أصدرت استراتيجية الامن السيبرانية(2022-2025)؛ واستمرت بالتأكيد على الجهات كافة بالالتزام بمتطلبات الامن السيبرانية الان لم يصدر أي نظام او قانون يلزم بموجبه.

3-إن مراقب الحسابات لم يولي الاهتمام الكافي لمخاطر الامن السيبرانية لوجود شكوك في إعداده، الأمر الذي حال دون الاعتماد على هذا الخطاب بشكل جدّي، لذا تطلبت عملية التدقيق بذله جهداً كبيراً بسبب عدم وجود خبره كافيه في هذا المجال.

4–قلة إدراك بعض مراقبي الحسابات لصدق الإقرارات الخاصة بمخاطر الامن السيبرانية التي يُفترض أن تُقدم لهم كدليل إثبات، مما يؤثر سلباً في الرأي الفني المُحايد الذي سيتم إبداؤه حول إجراءات التدقيق لتلك المخاطر.

5–من خلال ما ورد أعلاه تم اثبات فرضية البحث الأساسية (وجود علاقة مباشر ما بين المسؤولية المهنية لمراقب الحسابات ومخاطر الامن السيبرانية في المؤسسات المالية العاملة المطبقة للتحول الرقمي).

ثانياً: التوصيات

1- على مراقب الحسابات أن يبذل العناية المهنية اللازمة عند حصوله على تقارير الإدارة لدعم أدلة الإثبات الأخرى التي تخص مخاطر الامن السيبرانية التي اجتهد في الحصول عليها، من خلال تدقيق محتوياته والتحقق من صحته، علاوةً على قيام مراقب الحسابات بمناقشة هذا الخطاب والاجراءات مع الإدارة لتخفيض مسؤوليته بهذا الشأن من خلال تنظيم قانون بالامن السيبراني ملزم للجهات الرسميه والغير رسميه لتحديد هذه المخاطر .

2- على مراقب الحسابات أن يصدر تقريراً متحفظاً أو أن يمتنع عن إبداء الرأي في حالة رفض الإدارة تقديم الإقرار بشأن الإجراءات التي تخص مخاطر الامن السيبرانية الذي يعتقد مراقب الحسابات أنه ضروري لأن ذلك سيشكل تحديداً لنطاق عملية التدقيق مخاطر الامن السيبرانية.

3- إن عدم اعتذار أو تقييد مراقب الحسابات لرأيه بشأن عدالة وسلامة البيانات المالية (في حال عدم تقديم الشركات الخاضعة للتدقيق خطاب الإقرارات للأمور الهامة في البيانات فيما يخص حماية البيانات من مخاطر السيبرانية والتي يتعذر فيها وجود أدلة إثبات كافية)، سيُحمله مسؤولية كبرى في المستقبل عند اكتشافه أخطاء جوهرية لم يتم الإفصاح عنها في البيانات المالية المُقدمة لغرض التدقيق.

المصادر

اولاً – العربية:

- **القوانين والأنظمة والوثائق الرسمية:**

1. استراتيجية الامن السيبرانية في العراق
2. إطار الامن السيبرانية للهيئات المالية في المملكة الأردنية ال هاشمية2021
3. قانون الشركات رقم (21) لسنة (1997م) المعدل العراقي.
4. قانون العقوبات العراقي رقم (111) لسنة (1969م) المعدل.
5. منشورات الاتحاد الدولي للاتصالات (ITU).
6. منشورات البنك الدولي (WB) عن الأمن السيبرانية.

- **المواقع الإلكترونية:**

https://www.rmg-sa.com/الامتثال–لمعايير –الأمن–السيبراني
https://mawdoo3.com/أنواع_الأمن_السيبراني
An business framework from ISACA of www.isaca.org/cobit.

- **الكتب:**

1. أحمد عبيس نعمة التلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، الطبعة الأولى، منشورات زين الحقوقية للنشر والتوزيع، بيروت، لبنان 2018.

2. حسين محمد الغول جرائم شبكة الانترنيت والمسؤولية الجزائية الناشئة عنها، الطبعة الأولى، مكتبة بدران الحقوقية، لبنان، 2015.
3. علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية الطبعة الأولى منشورات شركة المؤسسة الحديثة للكتاب، بيروت،2019
4. كاميرا عزيز حسن الجهود الدولية في مواجهة الجرائم السيبرانية، ط1 منشورات الحلبي الحقوقية، لبنان، 2067. منير البعلبكي، المورد قاموس عربي إنكليزي، دار العلم للمل ايين2004، بيروت
5. براق واخرون؛ العوامل المؤثرة على استقلال مراجع الحسابات؛ طبعة أولى سنة 2017
6. ماري ايكن؛ التأثير السيبرانية، ط1، الدار العربية للعلوم، لبنان، 2017.
7. سلمان.عبد الستار شاكر "جرائم الامن السيبراني واثر الجهود الدولية في مكافحتها "هاتريك للتوزيع والنشر الطبعة الأولى 2023.
8. احمد .سراب ثامر "الهجمات على شبكات الحاسوب في القانون الدولي الإنساني "هاتريك للتوزيع والنشر الطبعة الأولى 2023.
9. الشريف .مصطفى كامل "موسوعة الامن السيبراني "دار القناديل للتوزيع والنشر الطبعة الأولى 2024 .
10.جيرارد كومو، المفردات القضائية، جمعية هنري كابيتانا، P.U.F 4eme الطبعة 1994 ص: 155

- **الرسائل والاطاريح والبحوث:**

1. د. الياس ناصيف، الكامل في قانون التجارة ، ج٣، الشركات التجارية، المؤسسة الحديثة للكتاب ، طرابلس ، لبنان، ٢٠٠٨ ، ص ٧٦-٧٧
2. احمد محمد محرز ، الشركات التجارية ، القاهرة ، ط 1 ، منشأة دار المعارف، ٢٠٠٩ ، ص ٥٦٨ .
3. د. عيسى ابو الطبل، وعبد المنعم محمود، المراجعة اصولها العلمية والعملية، دار النهضة العربية ، القاهرة ، ١٩٦٧ ،
4. نهلة طعمة خلف ، التنظيم القانوني لمراقب الحسابات في شركات القطاع الخاص ، رسالة ماجستير ، كلية القانون ، جامعة بغداد ، ٢٠٠٦ ، ص ١٥.
5. علي , عبد الوهاب نصر , شحاته السيد شحاته , الرقابة والمراجعة الداخلية الحديثة في بيئة تكنولوجيا المعلومات وعولمة اسواق المال (الواقع والمستقبل) , الدار الجامعية , الاسكندرية , 2006 سندس ماجد رضا اليات حوكمة الشركات ودورها في تقليص فجوة التوقعاتالحسابات ومستخدمي القوائم المالية ، بحث منشور في مجلة الغرب للعلوم الاقتصادية والادارية ، المجلد (٤) ، العدد ٢٠١١،.
6. د. احمد عبد الرحمن المجالي، المفهوم القانوني لمهمة مراقب الحسابات في الشركة الخاضعة لرقابته وفقاً للانظمة السعودية، بحث منشور في مجلة الفكر الصادرة عن كلية الحقوق والعلوم السياسية بجامعة محمد خضير بسكرة ، العدد ٢٠١٦ ، ١٣ ، ص ١٨
7. دحدوح، حسين أحمد والقاضي، حسين يوسف، مراجعة الحسابات المتقدمة الإطار النظري والإجراءات العملية، ج1، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009م
8. (صالح واخرون) التحول الرقمي من الأرض إلى الفضاء فرص للنمو الاقتصادي أم تهديد للأمن القومي 2022
9. الحسيني والمعموري 2022.استخدام شبكات الاعصاب في تطوير دور مراقب اصطناعي في اكتشاف الأخطاء
10. المعموري ,الاحمدي (2023) تدقيق النظام المصرفي الالكتروني الشامل للكشف عن مخاطر الاعمال التشغيلية
11. التويجري، محمد، مهنة التدقيق المحاسبي بين الواقع والمنشود (مراقب الحسابات مسؤول عن صحة البيانات الواردة في تقريره، بحث منشور، صحيفة القبس الكويتية– يومية سياسية مُستقلة، الكويت، 2009م.
12. أحمد عبيس نعمة الفتلاوي الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، كلية جامعة2016 بابل، العراق

References

1. HAJRA BIBI & MAHR MUHAMMAD SAEED AKHTAR, Relationship between Leadership Commitment and Performance of Public Sector Universities of Punjab, Pakistan, 2020.
2. Mardiana, Mardiana, and Puji Endah Purnamasari. "The effect of risk management on financial performance with good corporate governance as a moderation variable." Management and Economics Journal (MEC-J) 2.3 (2018): 257-268.
3. Middleton, Bruce. A history of cyber security attacks: 1980 to present. Auerbach Publications, 2017.
4. Whitman, M. E., and H. J. Mattord. "Management of Information Security . Cengage Learning." Inc., Boston, MA 2210 (2019).
5. Julio C. Rodriguez, Public Servants' Perceptions of the Cybersecurity Posture of the Local Government in Puerto Rico, 2019.
6. Johnny Fadel Rawass, Cybersecurity Strategies to Protect Information Systems in Small Financial Institutions, 2019
7.Murphy, F., &13-2 Materne, S. (2022) Cyber risk and cyber security