دور التدقيق الداخلي في تقييم حوكمة تقنية المعلومات كأحد ابعاد الصمود السيبراني دراسة تطبيقية

The Role of Internal Audit in Evaluating it Governance as a Dimension of Cyber Resilience: an applied study

الباحث / فيان سمير عبد الصاحب أ.د ابتهاج اسماعيل يعقوب

الجامعة المستنصرية / كلية الادارة والاقتصاد

alyaravalayra@gmail.com

hussainalaa10000@uomustansiriyah.edu.iq

رقم التصنيف الدولي ISSN 2709-2852

تاريخ استلام البحث : ٢٠٢٥/١١/١٢ تاريخ قبول النشر: ٢٠٢٥/١٢/٧

المستخلص

يهدف البحث الحالي الى التعرف على دور التدقيق الداخلي في تقييم بعد حوكمة تقنية المعلومات كاحد ابعاد الصمود السيبراني في القطاع المصرفي العراقي من خلال مجموعة من الضوابط االتي اقرتها تعليمات البنك المركزي العراقي لعام ٢٠٢٤، ومدى امكانيتها في معرفة تاثير التهديدات والهجمات السيبرانية على هذا القطاع ودعمها بالاستمرار بالعمل بعد تلك الهجمات، وذلك من خلال استخدام المنهج الوصفي التحليلي للاستبانة الموضوعة لهذا الغرض فضلاً عن المقابلات الشخصية لسبعة مصارف عراقية. اذ استند البحث على مشكلة مفادها " هل للتدقيق الداخلي دور في تقييم ضوابط الصمود السيبراني" ومن خلال البحث توصل البحث الى مجموعة من النتائج اهمها " امتثال المصارف العراقية عينة البحث بضوابط المتعلقة بالصمود السيبراني وعلى وفق تعليمات البنك النركزي العراقي".

مجلة العلوم المالية والمحاسبية
ACCOUNTING & FINANCIAL SCIENCES JOURNAL

مجلة العلوم المالية والمحاسبية
العدد الحادي والعشرون /اذار ٢٠٢٦
الصفحات ١ــ ٢٠

بحث مستل من رسالة ماجستير

الكلمات الافتتاحية : الصمود السيبراني، التدقيق الداخلي، مخاطر الامن السيبراني، ابعاد الصمود السيبراني.

Abstract

This research aims to identify the role of internal auditing in evaluating the IT governance dimension as a key aspect of cyber resilience in the Iraqi banking sector. This evaluation is conducted through a set of controls stipulated by the Central Bank of Iraq's 2024 directives, and assesses the extent to which these controls can identify the impact of cyber threats and attacks on the sector and support its continued operation after such attacks. The research employs a descriptive-analytical methodology, utilizing a questionnaire developed specifically for this purpose, as well as conducting personal interviews with seven Iraqi banks. The research problem is based on the question: "Does internal auditing play a role in evaluating cyber resilience controls?" The research concluded that the Iraqi banks in the sample comply with the cyber resilience controls as outlined in the Central Bank of Iraq's directives.

Keywords: Cyber resilience, internal auditing, cybersecurity risks, dimensions of cyber, resilience

المقدمـــــة

يعد تقييم الضوابط الرقابية للصمود السيبراني من اهم المهام الذي يضطلع بها وظيفة التدقيق الداخلي، اذ يهدف تقييم الضوابط الرقابية الى التاكد من ان الضوابط الرقابية في الوحدة الاقتصادية تعمل بشكل يخدم تلك الوحدة فضلاً عن التعرف على الفجوة المسجلة بين ماهو مطلوب وملزم على المصارف مقارنة بما مطبق في تلك المصارف وحسب تعليمات البنك المركزي العراقي لعام ٢٠٢٤ والمتعلقة بالصمود السيبراني. تبرز اهمية الصمود السيبراني في حماية المعلومات والبيانات التي لها اهمية كبيرة خاصة في المجال المالي والمصرفي والتي تتميز بتعاملها المباشر من الاشخاص والوحدات الاقتصادية وتعمل باموالهم مما يتطلب توفير حماية كبيرة لبياناتهم، فضلاً عن حماية .

١-المبحث الاول/ منهجية البحث

١.١- اهمية البحث

تنبع اهمية البحث من اهمية الدور الذي يضطلع به التدقيق الداخلي في تقييم حوكمة تقنية المعلومات كأبعاد للصمود السيبراني في القطاع المصرفي وفق متطلبات وتعليمات البنك المركزي .

٢.١- اهداف البحث

يهدف البحث الى الاتي :

١ – التعرف الى الاطر المفاهيمي للتديق الداخلي والصمود السيبراني

٢- التعرف على اهم ابعاد الضوابط الرقابية للصمود السيبراني حسب تعليمات البنك المركزي لعام ٢٠٢٤

٣- دور التدقيق الداخلي في تقييم بعد حوكمة تقنية المعلومات فيما يتعلق بلصمود السيبراني.

٣.١-فرضيات البحث

يستند البحث على فرضية رئيسة مفادها " للتدقيق الداخلي دور في تقييم ضوابط الصمود السيبراني على وفق التعليمات والضوابط التي اصدرها البنك المركزي العراقي في عام ٢٠٢٤ "

٤.١- بعض الدراسات السابقة

١.٤.١-دراسة عربية

_ المشهداني ٢٠٢٥

دور التدقيق الداخلي في تعزيز اليات حوكمة التحول الرقمي دراسة تطبيقية .

يهدف البحث الى التعرف على التدقيق الداخلي والدور الذي يلعبه في تعزيز اليات حوكمة التحول الرقمي وتحليل طبيعة ونطاق انشطة التدقيق الداخلي

كما تمثلت عينة البحث : ٧٩ قائمة استقصاء موزعة على مراجعين داخليين وخارجيين ومحاسبين واكاديميين اما اداة البحث استبانة موزعة .

اظهرت نتائج الدراسة وجود علاقة ايجابية بين التحول الرقمي وجودة المراجعة الداخلية وتحسين جودة التقارير المالية

٢.٤.١- دراسة اجنبية

(Hsien wu , huang , others) 2024_
IT governance and it controls : analysis from an internal auditing perspective

حوكمة تكنلوجيا المعلومات وضوابطها : تحليل من منظور التدقيق الداخلي

تستكشف هذه الدراسة خصائص ادارات التدقيق الداخلي في حوكمة تكنلوجيا المعلومات وتتحقق مما اذا كانت هذه المشاركة تعزز ضوابط تكنلوجيا المعلومات

عينة البحث هي تم توزيع الاستبيان على المدققين الداخليين في الشركات التايوانية المدرجة في البورصة , وبلغ حجم العينة ٤١٤ مدققا .

واظهرت النتائج ان معرفة تكنلوجيا المعلومات وادوار التدقيق الداخلي ترتبط ارتباطا ايجابيا كبيرا بجودة العلاقة بين IAF وتكنلوجيا المعلومات .

٢- المبحث الثاني : الجانب النظري

١.٢- : تعريف التدقيق الداخلي

عرف معهد المدققين الداخليين (IIA) التدقيق الداخلي على انه نشاط مستقل وموضوعي يهدف الى تقديم ضمانات وخدمات استشارية، بما يعزز قيمة الوحدة الاقتصادية ويحسن عملياتها، ويساعد في تحقيق اهدافها من خلال اتباع منهج منظم ومنضبط لتقييم وتحسين فعالية عمليات ادارة المخاطرة والرقابة والحوكمة (IIA,2019:11). كما عرفه مجلس معايير التدقيق والتاكيد الدولي على وفق المعيار ٦١٠ بانه " نشاط تقييم يتم تحديده او تقديمه كخدمة للوحدة الاقتصادية ومن ضمن وظائفه فحص وتقييم ومراقبة مدى كفاية وفاعلية الرقابة الداخلية (IFAC , : 40 2006). وتم تعريفه من قبل لجنة بازل للرقابة المصرفية على ان التدقيق الداخلي هو وظيفة مستقلة تهدف الى تقييم كفاية وفعالية نظام الرقابة الداخلية وادارة المخاطر والحوكمة مما يضمن استقرار المسسات المالية (Basel,2021:13). كما عرف على

انه عملية تقييم منهجية ومستقلة لمخاطر وانشطة الوحدة الاقتصادية تنفذ باستخدام تقنية الذكاء الاصطناعي لتحسين كفاءة وفاعلية عمليات التدقيق وتقديم ضمانات معقولة حول فاعلية نظام الرقابة الداخلية وادارة المخاطر وحوكمة الوحدات الداخلية . (الوردات , ٢٠٢٤ : ٢٧) وعرف بانه " منهج مستقل لمطابقة منتجات وعمليات البرمجيات مع اللوائح والمعايير والمبادئ التوجيهية وابلاغ الادارة بهذه النتائج لغرض اتخاذ القرار والاجراءات والخطط المعمول بها" (Raji , 2020 : 33).

٢.٢-التدقيق الداخلي المستند الى المخاطر

يعد التدقيق الداخلي المستند الى المخاطر منهجية حديثة تركز على توجيه جهود التدقيق نحو الحالات والانشطة ذات ألتاثير الاكبر على المخاطر التي تهدد تحقيق اهداف الوحدة الاقتصادية بدلا من استنادها على القوائم الدورية، اذ يقوم هذا النوع بربط انشطة التدقيق الداخلي بادارة المخاطر التشغيلية الاسترتيجية، كما تعد عملية تقييم على مستوى المخاطر المرتبطة بها. يركز التدقيق الداخلي على فحص وتحسين فعالية الضوابط الداخلية وادارة المخاطرة وحوكمة الوحدات الاقتصادية في المجالات الاكثر عرضة للمخاطر, (جمال ,٢٠٢٢ : ٣٢) وقد غير مفهوم التدقيق الداخلي المستند الى المخاطر مفهوم التدقيق الداخلي من التقليدي الى المعاصر اذ يعتمد حاليا على مواجهة المخاطر , ونتيجة لتغير الاحتياجات التنظيمية والتطورات التكنولوجية تغيرت طبيعة الخدمات التي يقدمها المدققون الداخليون عبر السنوات واصبح التدقيق التقليدي يتحول تدريجيا الى التدقيق القائم على اساس المخاطر، وهو ما يضيف قيمة للاعمال من خلال الخدمات التأكيدية والاستشارية والمساهمة في تقليل التعرض للمخاطر وتحقيق الاهداف وتحسين الاداء، ويعود هذا التحول بشكل رئيسي الى تطور مهام المدقق وظهور بيانات داخلية وخارجية متعددة، اضافة الى تنوع المتطلبات التي تؤكد ضرورة تطوير دور المدقق الداخلي والتحقق من امتثاله للمعايير والقواعد(Faiteh,Aasri, 2022:17)

وتدور احداث التدقيق الداخلي الذي تم دعمة من قبل معايير التدقيق العالمية الصادرة

في ٢٠٢٤ واصبحت واجبة التنفيذ في ٢٠٢٥ وتوضح هذه المعايير ان المخاطر وتقييمها وقبولها والابلاغ عنها تم التاكيد عليها في المجال الرابع (ادارة وظيفة التدقيق الداخلي) حيث تضم المبادئ (٩ و ١١) التي تم ربطها بالمبدأ ١١_٥ المتعلق بالابلاغ عن قبول المخاطر والذي يحمل مسؤولية التأكد من عدم قبول مخاطر تتجاوز حدود المؤسسة، ويهدف المعيار الى ضمان ان المخاطر التي تتحملها المؤسسة تقع ضمن حدود قدرتها على التحمل، كما يوضح دور الرئيس التنفيذي للتدقيق في الابلاغ عندما تتجاوز المخاطر المستوى المقبول (معايير التدقيق العالمية , ٢٠٢٤ : ٨٧).

٣.٢ – مهام واجراءات التدقيق الداخلي في المصارف .

١– بحسب التعليمات الصادرة من البنك المركزي العراقي لتقييم فعالية نشاط التدقيق الداخلي في المصارف، وهو جزء من الجهود المستمرة التي يبذلها البنك لمعالجة المسائل الرقابية وتعزيز الرقابة المصرفي اذ اشار دليل العمل الرقابي للبنك المركزي العراقي مهام واجراءات التدقيق الداخلي في المصارف وهي : (دليل العمل الرقابي ٢٠١٩, ٣:).

٢– يقوم قسم التدقيق الداخلي بوضع خطة عمل واجراءات يتم تحديثها، وتركز على المخاطر ومراجعتها بشكل سنوي، ويتم المصادقة عليها من قبل مجلس الادارة او لجنة التدقيق التابعة له في بداية العام .

٣– الكفاءة المهنية ، ويشمل المعرفة والخبرة لدى كل مدقق داخلي وهي ضرورية لفعالية نشاط التدقيق الداخلي في المصرف، وعلى الادارة العليا تعزيز وتطوير هذه الكفاءة من خلال اكتساب المهارات لموظفي التدقيق الداخلي بوسائل عدة ومنها عقد الدورات التدريبية خارج وداخل العراق، ويقوم البنك المركزي العراقي بمتابعة مثل هذه الدورات لاهميتها. ويشمل مسؤوليات قسم التدقيق الداخلي تدقيق معاملات الانفاق قبل عملية الصرف وبعدها حسب المعايير الدولية .

٤– يجب ان يكون لكل مصرف ميثاق للتدقيق الداخلي يوضح الغرض من نشاط التدقيق الداخلي ومكانته وصلاحيته داخل المصرف بطريقة تعزز من النشاط الفعال

للتدقيق الداخلي كما هو موصوف في المتطلب رقم (١)، علماً ان هذا الميثاق هو جزء من متطلبات الحوكمة المؤسسية .

٥- يجب ان يضمن نطاق الانشطة الخاصة بالتدقيق الداخلي التغطية الكافية للامور المدرجة في في خطة التدقيق .

٤.٢- مفهوم الصمود السيبراني :

ظهر مصطلح الصمود السيبراني كمفهوم جديد في اوائل القرن الماضي ومع بداية العقد الاول من القرن الحادي والعشرين وتحديدا في عام ٢٠٠٠، بدأ التركيز يتجه نحو الامن السيبراني والمخاطر والتهديدات المرتبطة بالانظمة الرقمية مما ابرز الحاجة الى تبني مفهوم الصمود السيبراني بوصفه اطارا قادرا على مواجهة الهجمات السيبرانية. واصبح هذا المفهوم عنصرا رئيسياً في اي استراتيجية تعني بتوضيح الامن السيبراني سواء في القطاع العام او الخاص، كما استمرت النقاشات المتعلقة بتعزيز مستويات الامن وتحديد السبل المثلى لتحقيق صمود سيبراني فعال، اذ اشار تقرير مجلس الوزراء البريطاني عام ٢٠٠٥ الى ضرورة تمكن الوحدة الاقتصادية من التكيف مع التهديدات في عصر التكنولوجيا الرقمية والحفاظ على حرية تدفق المعلومات والدعوة الى توفير التمويل اللازم ضمن اطر الدولة لحماية المنجزات الرقمية، كما اعلنت الولايات المتحدة الامريكية الصمود السيبراني كاستراتيجية وطنية ونصت عليه في دستورها وحددت شهر تشرين الاول من كل عام شهرا للتوعية به , وتزايدت بعد ذلك المؤتمرات المتخصصة التي تعقد تحت شعار اهمية الصمود السيبراني , وكان اول مؤتمر دولي في استراليا عام ٢٠١٠, الامر الذي مهد الطريق لتطورات واسعة النقاشات المستقبلية المتعلقة بالصمود السيبراني ومنها المؤتمر الثاني للصمود السيبراني الذي انعقد في استراليا لاحقا. وبعدها توالت الاهتمامات والادبيات بها وعلى الصعد المهنية الدولية. عرف البنك المركزي الصمود السيبراني قدرة الوحدات الاقتصادية على مواصلة اداء مهامها ووظائفها من خلال التنبؤ والتكيف مع المخاطر والتهديدات والهجمات السيبرانية اثناء حدوثها والتغيرات المرتبطة بالبيئة التقنية للمعلومات، والصمود والتحديد والكشف

والاحتواء والاستجابة والتعافي السريع من جميع الاحداث السيبرانية (البنك المركزي , ٢٠٢٤ : ٦). كما تم تعريفه من قبل المعهد الوطني للمعايير والتكنلوجيا (NIST) هي القدرة على توقع الضغوط او الهجمات او الاختراقات على الانظمة التي تتضمن موارد سيبرانية ومقاومتها والتعافي منها والتكيف معها (NIST, 2021 : 73).

٥.٢- ابعاد الصمود السيبراني ومؤشراته :

تمثلت الابعاد الرقابية للصمود السيبراني ومؤشراته حسب تعليمات البنك المركزي العراقي ٢٠٢٤ بالاتي :

١- حوكمة تقنية المعلومات : يركز مبدأ حوكمة الامن السيبراني على التحقق من مواءمة استراتيجية الامن السيبراني مع استراتيجية ادارة المخاطر، اذ تعد انظمة الحوكمة ضرورية لدمج الامن السيبراني ضمن الاطار الشامل لادارة مخاطر المؤسسة (ERM) من خلال تحديد السياسات والمسؤوليات، وضمان الاستجابة الاستراتيجية للمخاطر السيبرانية ضمن منهج مؤسسي متكامل.

٢- البنية التحتية لتقنية المعلومات: تشمل البنية التحتية لتكنلوجيا المعلومات على خليط من اجهزة الحاسوب جرى تجهيزها من مجهزين مختلفيين ويلعب الانترنت بشكل خاص دور مهم في البنية التحتية لتكنلوجيا المعلومات اذ يقدم الخدمات كقناة اتصال رئيسية مع الزبائن والعاملين والوسطاء والموزعين، بالاضافة الى ان تطور وسائل تكنلوجيا الاتصال عمل على توفير المرونة وفرص الاختيار من حيث طرق تجهيز خدمات الاتصال وامكانية تجميع نظم تكنلوجية وهي النظم المرتبطة بعمليات الاتصال التي تسهم في رفع اداء داخل المؤسسة (الطائي , العبادي , ٢٠٢٢ : ٢) .

٣- ادارة المخاطر السيبرانية : تشير إدارة المخاطر إلى الاستراتيجيات والأساليب والأدوات الداعمة لتحديد المخاطر والسيطرة عليها إلى مستوى مقبول. بالإضافة إلى ذلك، يمكن أيضًا الإشارة إلى إدارة المخاطر على أنها مجموعة متزامنة من الإجراءات والأساليب لتوجيه المنظمة لتقليل المخاطر لتحقيق الأهداف التنظيمية. تسمح إدارة المخاطر لصانع القرار بفهم وتقييم تأثير المخاطر في شبكة سلسلة التوريد. يؤدي

التحكم في التعقيد إلى كفاءة تكلفة أعلى ويقلل من المخاطر(johny , 2021 : 6 , Gurtu).

٤- التحديد : يتعلق هذا البعد بتحديد الاصول والبنى التحتية وتقييم التهديدات ونقاط الضعف المحتملة التي قد تؤثر عليها، ويساهم هذا الجانب في تعزيز الهوية الرقمية للمؤسسة، والهدف الاساسي لهذا البعد هو انشاء خريطة شاملة للمخاطر وضمان السيطرة عليها.

٥- الحماية : يعني هذا المبدأ وضع الضوابط الامنية الملائمة لحماية الاصول وضمان سرية وسلامة وتوافر المعلومات والانظمة الحساسة، وتشمل اجراءات الحماية تحديد الاصول ذات الاولوية وتطبيق سياسة امنية فعالة كالتشفير والمراقبة الى جانب تأمين الاجهزة والبرامج والخدمات المرتبطة بالمنصات الرقمية مما يعزز قدرة البنية التحتية على مقاومة الهجمات الالكترونية.

٦- الاكتشاف : يركز هذا المبدأ على تطوير القدرات اللازمة لاكتشاف الانشطة او الاحداث الامنية غير المصرح بها في الوقت المناسب , ويتضمن ذلك مراقبة الشبكات وتحليل البيانات الامنية للكشف عن الانماط المشبوهة باستخدام تقنيات الذكاء الاصطناعي، مما يتيح سرعة التنبه للحوادث والتعامل معها قبل ان تتسبب باضرار واسعة .

٧- الاستجابة : يركز هذا المبدأ على وضع الخطط والاجراءات الفعالة للاستجابة للحوادث الامنية , بما في ذلك احتواء الاضرار واستعادة الانظمة المتأثرة، كما يهدف الى تعزيز القدرة المؤسسية على تقليل اثر الحوادث السيبرانية المستقبلية من خلال تحليل النتائج والدروس المستفادة وتحديث خطط الاستجابة وفقا لها .

٨- الاسترجاع : يهتم بوضع وتنفيذ الخطط اللازمة لاستعادة الانظمة والعمليات الى حالتها الطبيعية بعد وقوع الحوادث , كما يسهم في تعزيز صمود المؤسسة من خلال تطوير القدرات الكفيلة بضمان استمرارية الخدمات وتقليل تأثير الاضرار الناتجة عن الحوادث السيبرانية .

٩- التوعية : تزويد الأفراد بالمعرفة والمهارات اللازمة للتعرف على التهديدات المحتملة والاستجابة لها وتعزيز ثقافة واعية بالأمن السيبراني داخل المؤسسة، وتشمل برامج التوعية السيبرانية مجموعة متنوعة من المناهج التعليمية المصممة خصيصًا لإشراك الموظفين بشكل فعال.

١٠-الفحص : تقييم الثغرات الامنية واختبار الاختراق لتحديد ومعالجة نقاط الضعف الامنية في انظمة الكمبيوتر والشبكات والتطبيقات الخاصة بالوحدة الاقتصادية.

٦: مراحل لجنة بازل (٣) لتحقيق استراتيجية الصمود السيبراني

تعد لجنة بازل (BCBS) وهي لجنة دولية انشأت عام ١٩٧٤ من قبل بنك التسويات الدولية (BIS) في مدينة بازل السويسرية _ لجنة تهدف الى وضع معايير وقواعد رقابية لتعزيز سلامة واستقرار النظام المصرفي العالمي , اضافة الى تطوير أطر عمل وارشادات للبنوك والجهات الرقابية الوطنية بشأن ادارة المخاطر , فضلا عن التنسيق والتعاون بين السلطات الرقابية في مختلف دول العالم فيما يتعلق بالعمل المصرفي. ومن ابرز انجازات لجنة بازل اصدارها ثلاث اتفاقيات رئيسية هي :

١- اتفاقية بازل (١٩٨٨)

٢- اتفاقية بازل ٢ (٢٠٠٤) التي اضافت ثلاث ركائز اساسية تشمل , المتطلبات الرأسمالية , المراجعة الرقابية , الانضباط السوقي .

٣- اتفاقية بازل ٣ (٢٠١٠ _ ٢٠١٧) التي جاءت بعد الازمة المالية العالمية عام ٢٠٠٨ , وركزت على معايير السيولة وجودة رأس المال ونسب الرافعة المالية وادارة المخاطر النظامية .

واقرت اللجنة من خلال اتفاقية بازل (٣) بانه يمكن تحقيق استراتيجية الصمود السيبراني على سبع مراحل هي (Basel , 2021 : 16) :

المرحلة الاولى قدرات التحديد : تشمل الادراة السيبرانية والهيكلية والقدرة على الاستشعار لتوقع ومعالجة الاعمال السلبية او الاحداث السيبرانية.

المرحلة الثانية الصمود: تشمل وضع اطار دفاعي الكتروني متكيف يحافظ على المهام ويساعد في التصدي للتهديدات التي تتعرض لها الوحدة الاقتصادية .

المرحلة الثالثة الدفاع : تشمل الدفاع ضد الاحداث السيبرانية التخريبية والتحوط بمناعة رقمية قوية ذاتية الشفاء ودفاع الكتروني نشط.

المرحلة الرابعة الفحص : تشمل مراقبة الشبكات الالكترونية والانترنت في الوقت الفعلي للكشف عن التهديدات السيبرانية في الوقت الفعلي.

المرحلة الخامسة الملاحظة : تشمل الاعتماد على الاتمتة والتعلم الالي لمواجهة التهديدات السيبرانية المستقبلية .

المرحلة السادسة الاسترداد : تشمل القدرة على استعادة المنصات الرقمة بسرعة، والتكييف، واستعادة الانظمة ذات المهام الحرجة لتجنب انقطاع الاعمال في حال حصول اي تهديدات سيبرانية.

المرحلة السابعة التكييف : تشمل التقييم الذاتي المستمر وقياس الاداء السيبراني والتحسين المستمر لدعم الاعمال التجارية.

٦.٢- المخاطر السيبرانية

ترتبط المخاطر السيبرانية بمفهوم الامن السيبراني الذي يشير الى مجموعة الوسائل التقنية والادارية المستخدمة لمنع الاستغلال غير المشروع او اساءة استخدام المعلومات واستعادتها , اضافة الى حماية انظمة المعلومات الالكترونية وتنظيم امن البيانات وضمان سريتها وخصوصية المعلومات الشخصية للمواطنين (السراي , ٢٠٢٥ : ٢١) , وتبرز اهمية الامن في الحفاظ على البيانات الشخصية وسلامتها وحماية الاجهزة والشبكات باعتبارها خط الدفاع الاول عن البيانات والعلومات .

وتتمثل المخاطر الالكترونية او السيبرانية في نقاط الضعف الموجودة في تكنلوجيا المعلومات التي يمكن للمتسللين استغلالها لاختراق اي نظام , وتشمل المخاطر السيبرانية فقدان البيانات نتيجة للهجمات الالكترونية او اختراق البيانات الحساسة للوحدة الاقتصادية , فاذا تمكن المهاجمون من اختراق البيانات فأن ذلك يترتب عليه خسائر

كبيرة سواء من خلال تعطيل عمليات التشغيل او تسريب البيانات الحساسة ووفق الاستراتيجية الوطنية للامن السيبراني, تعد حماية الاصول الرقمية داخل الفضاء الالكتروني عنصراً رئيسيا في الامن المعلوماتي (استراتيجية الامن الالكتروني الوطنية , ٢٠١٩:٤) وفي دراسة اصدرتها جمعية المدققين الداخليين بالولايات المتحدة في مارس ٢٠٢٢ , تبين ان المخاطر السيبرانية تأتي في صدارة المخاطر التي تهدد منظمات الاعمال في مختلف القطاعات , كما صنفت المرتبة الاولى بين ١٣ مخاطرة رئيسية (IIA, 2019:4).

٧.٢- تقييم التدقيق الداخلي لضوابط الصمود السيبراني

مع ظهور تقنيات المعلومات والاتصالات بدأت ادوار التدقيق الداخلي تتطور بادوات عدة لتحليل البيانات وتقييم المخاطر حيث ساعدت المدققين على اتمت المهام , فالتدقيق الداخلي تتمحور مهمته في معرفة وتحديد وتقييم الاحداث المحتملة والتحكم والسيطرة عليها حيث يتم التوصل الى تأكيدات معقولة بخصوص تحقيق اهداف الوحدة الاقتصادية , فالمدقق الداخلي يقيم المخاطر التي تواجه الوحدة الاقتصادية والضوابط المصممة للتخفيف من تلك المخاطر وفاعلية تطبيق تلك الضوابط حيث يوظف المدقق الداخلي العديد من اساليب التدقيق الداخلي مثل الملاحضة والمقابلات والاستقصاء والتحليل لتحقيق هدفه في تقييم الضوابط .والمدقق الداخلي لا تقع على عاتقه مسؤولية تصميم الضوابط الرقابية حيث يقتصر دوره في تقييم كفاءة وفاعلية الرقابية ومدى تطبيق الجهات لتلك الضوابط وتقديم التوصيات لغرض التحسين ولا يطبق الضوابط الرقابية فوظيفته تقتصر على تطبيق الضوابط بشكل فاعل من خلال الاختيارات التي يقوم بها ولا يدير الضوابط الرقابية فهذه الضوابط تقع مسؤوليتها على عاتق ادارة الوحدة الاقتصادية ويقتصر دوره على تقديم تقارير وتوصيات حول فاعلية الضوابط ويساعد الادارة على تحسينها فضلا على انه لا ينفذ الضوابط الرقابية ولا يتحمل مسؤولية الضوابط الرقابية , فالمدقق الداخلي يقع على عاتقه التأكد من تنفيذ الضوابط الرقابية بشكل فاعل من خلال اختبارات التدقيق الداخلي وتقع المسؤولية النهائية على ادارة

الوحدة الاقتصادية اذ يقدم المدقق تقييما موضوعيا مستقلاً لفاعلية الضوابط ويساعد الادارة على اتخاذ القرارات اللازمة لتحسينها (الوردات , ٢٠٢٥ : ٣٠) ويحدد الاطار المهني الدولي لممارسة اعمال التدقيق الداخلي (IPPF) الصادر عن معهد المدققين الداخليين ٢٠٢٤ بالتفصيل دور نشاط التدقيق الداخلي في تقييم الضوابط الرقابية من خلال تنفيذه للمهام الاستشارية (Assurance Engagment) ومهام تأكيدية (consulting Engagements)

٣- المبحث الثالث: الجانب العملي .

حوكمة تقنية المعلومات

لغرض تقييم التزام المصارف عينة البحث بالضابط الرقابي (حوكمة تقنية المعلومات) والذي يتضمن (١٤) فقرة فرعية مرتبطة بحوكمة تقنية المعلومات. وتمت الاشارة الى الضوابط من خلال ربط الضابط بالرقم الفرعي (هل تم اعتماد هيكل تنظيمي رسمي لحوكمة تقنية المعلومات، اذ تمت الاشارة اليه بالرقم ١.١.١) وهكذا لبقية الضوابط.

وعلى وفق المقياس الثلاثي تم فان مطبق كلياً اعطي وزن (٣)، ومطبق جزئي وزن (٢)، اما غير مطبق فاعطي الوزن (١). ويوضح الجدول (١) اختبار الالتزام بتطبيق الضوابط الرقابية للصمود السيبراني لبعد حوكمة تقنية المعلومات.

جدول (١) تقييم الالتزام بضوابط حوكمة تقنية المعلومات على وفق المصارف عينة البحث

الضابط	مصرف المنصور	مصرف العراق الاول	مصرف المستشار	مصرف الناصك	مصرف المشرق	مصرف بغداد	مصرف الاهلي العراقي	الاهمية النسبية %	الانحراف	الوسط الحسابي
٢.١.١	٣	٣	٣	٣	٢	٢	٣	٩٠.٥	٠.٤٩	٢.٧١
٢.١.٢	٣	٣	٣	٣	٣	٢	١	٨٥.٧	٠.٧٩	٢.٥٧
٢.١.٣	٣	٣	٣	٣	٣	٣	١	٩٠.٥	٠.٧٦	٢.٧١

٢.١.٤	١	٣	٣	٣	٣	٣	٢	٨٥.٥	٠.٧٩	٢.٥٧
٢.١.٥	٢	٣	٢	٣	٣	٣	٣	٩٠.٥	٠.٤٩	٢.٧١
٢.٢.١	٢	٣	٣	٢	٣	٣	٣	٨٥.٥	٠.٥٣	٢.٥٧
٢.٢.٢	٢	٣	٣	٢	٢	٢	٣	٨١	٠.٥٣	٢.٤٣
٢.٢.٣	٣	٣	٣	٢	٣	٣	٣	٩٥.٢	٠.٣٨	٢.٨٦
٢.٢.٤	٣	٣	٣	٣	٣	٣	٢	٩٥.٢	٠.٣٨	٢.٨٦
٢.٣.١	٢	٣	٣	٣	٢	٣	١	٨١	٠.٧٩	٢.٤٣
٢.٣.٢	٣	٣	٣	٣	٣	٣	٣	١٠٠	٠.٠٠	٣
٢.٣.٣	٣	٣	٣	٢	٣	٣	٣	٩٥.٢	٠.٣٨	٢.٨٦
٢.٣.٤	٣	٣	٣	٣	٢	٢	٢	٨٥.٧	٠.٥٣	٢.٥٧
٢.٤.١	٣	٣	٢	٣	٢	٢	٣	٨٥.٧	٠.٥٣	٢.٥٧
٢.٤.٢	٣	٣	٣	٣	٢	٢	٣	٩٠.٥	٠.٤٩	٢.٧١
٢.٤.٣	٣	٣	٢	٣	٣	٣	٣	٩٥.٢	٠.٣٨	٢.٨٦
٢.٤.٤	٣	٣	٣	٣	٣	٣	٣	١٠٠	٠.٠٠	٣
٢.٤.٥	٣	٣	٢	٢	٣	٢	٣	٨٥.٧	٠.٥٣	٢.٥٧
	البنيـة التحتيـة لتقنيـة المعلومـات							٨٩.٩	٠.٤٩	٢.٧٠
	الفجـــوة							١٠.١ %		

بوضح الجدول (١) ضوابط حوكمة تقنية المعلومات، ومن خلال التحليل الاحصائي لمؤشرات البعد الاول (حوكمة تقنية المعلومات والتي تتضمن (١٤) مؤشر تم تحليلها من خلال الاسئلة (١.١.١ – ١.٤.٣) يتضح الاتي :

١- الفجوة بين المطبق والملتزم به من قبل المصارف عينة البحث مقارنة بغير المطبق: اذ تظهر فجوة ضعيفة وبنسبة (7.79%) وهي تمثل نسبة ضعيفة مما يفسر ان المصارف عينة البحث مطبقة للمؤشرات ذات الصلة للضابط الرقابي لحوكمة تقنية المعلومات بشكل كبير، اي ان المصارف تلتزم بتعليمات وضوابط المركزي بخصوص ضابط حوكمة تقنية المعلومات كأحد ضوابط الامن السيبراني.

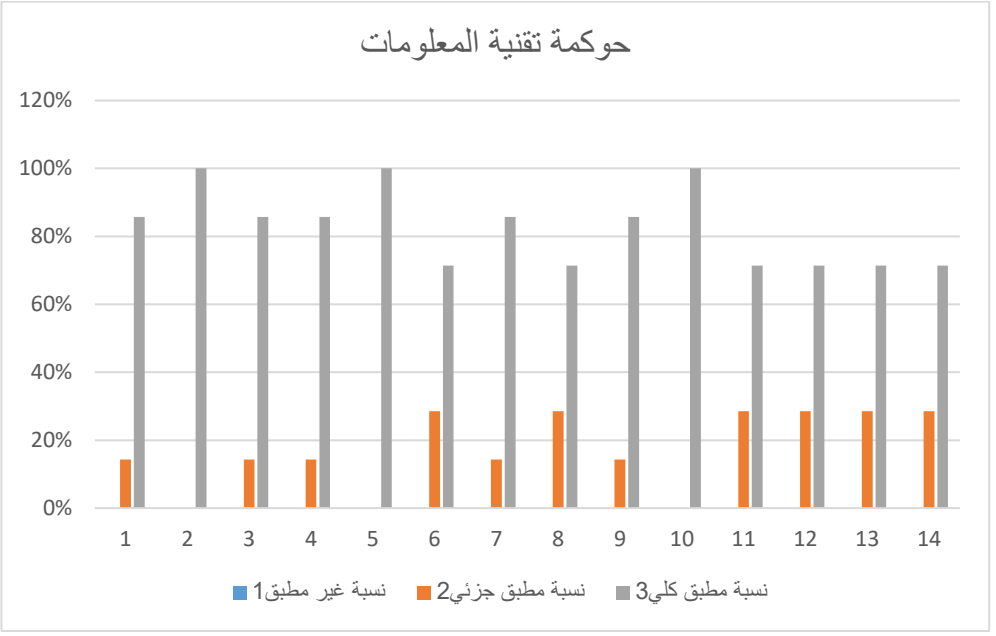
٢- حققت المصارف عينة البحث نسبة (% 100) وبوسط حسابي بلغ (٣) للمؤشرات (١.١.٢، ١.١.٥، ١.٣.٢) فيما يخص ادوار اللجان ذات العلاقة بضوابط حوكمة تقنية المعلومات ووجود مؤشرات تختص باداء حوكمة تقنية المعلومات تعتمدها المصارف عينة البحث في التقييم فضلاً عن وجود تدقيق ومراجعة مستمرة للسياسات الامنية ذات الصلة بامن المعلومات مما يفسر ان المصارف عينة البحث تتمتع بالاهتمام الواضح لمتطلبات البنك المركزي بخصوص مرونة السياسات وتحديثها ووجود لجان وسياسات مختصة بالامن السيبراني لتحقيق الصمود السيبراني.

٣- من جهة اخرى، تفاوتت المصارف فيما يتعلق بالالتزام بالضوابط الرقابية ذات الصلة بحوكمة تقنية المعلومات، فنسبة (% 95.2) وبمتوسط حسابي (2.86) وللمؤشرات (١.١.١، ١.١.٣، ١.١.٤، ١.٢.٢، ١.٣.١) فيما يتعلق اعتماد هيكل تنظيمي رسمي لحوكمة تقنية المعلومات فالمصارف عينة البحث لديها لحوكمة تقنية المعلومات وبشكل واضح في هيكلها التنظيمي باستثناء مصرف المنصوروالذي هو بطور اتمام كافة الاجراءات بهذا الخصوص، فالتطبيق غير تام وانما جزئي. وباتجاه اخر، فان المصارف عينة البحث تطبق وتلزم بشكل كامل بتشكيل لجان حوكمة تقنية المعلومات وحسب تعليمات البنك المركزي العراقي باستثناء مصرف المنصور والذي يسير بخطى حثيثة بتشكيل اللجنة الانفة الذكر. وتشير الاحصاءات الوصفية ان المصارف عينة البحث وفق المؤشر توثق الاجتماعات في لجنة الحوكمة وتتابع القرارات وتنفذها بشكل كامل باستثناء مصرف المنصور فانه باتجاه تشكيل اللجنة وتوثيق الاجتماعات في المستقبل القريب والتي تم تأكيدها من خلال اللقاءات (المقابلات) التي قامت بها الباحثة مع مسؤولي (IT) في المصرف، وبشكل منطقي فان المصارف التي لها حوكمة تقنية المعلومات فانها تحدد صلاحيات ومهام لجنة الامن السيبراني باستثناء مصرف المنصور الذي يطبق هذا المؤشر بشكل جزئي، وبنفس الاتجاه فان المصارف تطبق وبشكل كامل اعتماد سياسات امن سيبراني محدثة ومعتمدة باستثناء مصرف بغداد الذي لديه هذه السياسات الا ان تحديثها يكون

وفق اجتماعات وموافقات مجلس الادارة في المصرف.

٤- تفاوتت المصارف بنسبة (90.5%) وبمتوسط (2.71) فيما يتعلق بامتثال المصارف وتطبيقها للمؤشرات الفرعية لبعد حوكمة تقينية المعلومات فيما يتعلق بالمؤشرات (١.٢.١، ١.٢.٣، ١.٣.٣، ١.٤.١، ١.٤.٢، ١.٤.٣) حيث توافقت المصارف عينة البحث فيما يتعلق بتشكيل لجنة الامن السيبراني وتشمل في اعضاءها اشخاص ذوي علاقة باستثناء مصرفي المشرق والاهلي العراقي وقد يكون هذا نتيجة تشكيل لجنة حوكمة تقنية المعلومات واعتبارها هي اللجنة البديلة، وبنفس السياق، كان هناك اتفاق تام بالتطبيق الكامل بعقد اجتماعات دورية ذات صلة بالامن السيبراني باستثناء مصرفي المشرق والاهلي العراقي. واتفقت المصارف على التنطبيق التام بخصوص توافق او تماشي السياسات مع المتطلبات التنظيمية والمعايير مع المتطلبات المحلية والدولية التي تضعها المصارف باستثناء مصرفي بغداد والاهلي، ويمكن تفسير ذلك ان مصرف بغداد ينتمي الى مجموعة بنك برقان الكويتي وقد يتبع في هذا الجزء مايصدر عن البنك الام رغم انه يعمل كمؤسسة مصرفية مستقلة في العراق، وبينت المصارف وبالتطبيق التام ان المصارف بادارتها العليا الدعم الكافي لمبادرات الامن السيبراني باستثناء مصرف المشرق والمستشار الذي كان التطبيق الجزئي لادارة المصرفين بهذا الخصوص، واكدو انه تم الاستفسار من ادارة المصرفين بان النظم السيبرانية يتم التعهيد الخارجي مع شركات عربية واجنبية بهذا الخصوص، وكان التطيق التام باعتبار الامن السيبراني هم استراتيجية اساسية في المصرف ويعد احد استراتيجيات المصرف باستثناء مصرفي المشرق والمستشار وقد يكون لحداثة هذين المصرفين ان استراتيجية الامن السيبراني تكون استراتيجية مستقلة بهذا الخصوص، ويمكن تفسير استثناء مصرفي بغداد والمشرق بخصوص مراجعة الادارة العليا لتقارير الامن السيبراني وبشكل تطبيق جزئي، على خلاف ذلك فان عينة البحث اكدت على ان مراجعة تقارير الامن السيبراني يكون من قبل الادارة العليا لان المصرفنت لديهما قسم متخصص بالامن السيبراني داخل المصرف هو الذي يقوم بهذه المهمة.

مما سبق يتضح ان المصارف عينة البحث متوافقة مع بعد حوكمة تقنية المعلومات كاحد متطلبات الصمود السيبراني وبنسبة (92.21 %) على مستوى العينة وبمتوسط (2.83). والشكل (٨) يوضح الضوابط الرقابية لبعد البنية التحتية لتقنية المعلومات بشكل عام.



شكل (٨) الضوابط الرقابية لبعد حوكمة تقنية المعلومات

المصدر: من اعداد الباحثة بالاعتماد على بيانات الجدول (١)

٤-المبحث الرابـع : الاستنتاجات والتوصيات

٤.١- الاستنتاجات

١- امتثلت المصارف بتعليمات البنك المركزي العراقي بشكل تام فيما يخص بعد حوكمة تقنية المعلومات لتعزيز الصمود السيبراني واتضح ذلك من قيمة معدل الفجوة بين المطبق والملتزم به من قبل المصارف مقارنة بغير المطبق (7.79%).

٢- اهتم البنك المركزي العراقي بشكل متميز بالصمود السيبراني من خلال تعليماته التي تضمنت عشرة ابعاد مهمة لتعزيز الصمود السيبراني وفرض تطبيقها على المصارف العراقية.

٣- يساهم التدقيق الداخلي بادارة المخاطر السيبرانية بشكل واضح وبالتالي تعزيز الصمود السيبراني وباستمرار العمل.

٤- لاتزال هناك بعض التحديات التي تواجه المصارف في الامتثال الى كامل تعليمات البنك المركزي فيما يتعلق الابعاد الرقابية للصمود السيبراني.

٥- تساعد ابعاد الصمود السيبرانية في تعزيز القدرة على الاستجابة السريعة لاي هجمات سيبرانية مما يقلل تاثيرها على العمل.

٦- تدريب الموظفين على ادارة المخاطرة السيبرانية ووضع انظمة الانذار المبكر تساعد بشكل كبير على تعزيز الصمود السيبراني.

٢.٤ -التوصيات

١- اجراء تقييم شامل ودوري للمخاطر الالكترونية لتحديد نقاط الضعف الحالية والمحتملة واجراء محاكاة لتلك المخاطرة والعمل على معالجة الاخطاء.

٢- نشر المعرفة وتدريب الموظفين بشكل دوري وتوعيتهم والزبائن وتعريفهم بالانماط الحديثة والاساليب الخاصة بالهجمات السيبرانية وطرق تجنبها وكشفها والابلاغ عنها من خلال وسائل اتصال موثوقة.

٣- تبني نهج استباقي لادارة المخاطر السيبرانية وتشكيل فريق للاستجابة للتهديدات السيبرانية في المصارف بهدف الامتثال للابعاد الرقابية للصمود السيبراني وتطبيقها بشكل امثل للمعايير القياسية لادارة المخاطر السيبرانية .

٤- وضع الية تعاون بين البنك المركزي العراقي والمصارف العراقية لتقييم الالتزام بالمعايير الاساسية للصمود السيبراني والتعاون المشترك لمواجهة الهجمات السيبرانية وتعزيز الصمود السيبراني.

٥- التعاون مع جهات عالمية متخصصة للعمل على اجراء اختبارات ومحاكاة جدية للهجمات السيبرانية وكيفية مواجهتها واختبار اجهزة واساليب الانذار المبكر لتلك الهجمات.

المصادر :

اولا : المصادر العربية .

١_ البنك المركزي العراقي , ٢٠٢٤ , ضوابط الصمود السيبراني في القطاع المالي والمصرفي في العراق

٢_ معهد المدققين الداخليين , المعايير الدولية لممارسة مهنة التدقيق التدقيق الداخلي , ٢٠١٩

٣_ دليل العمل الرقابي , (٢٠١٩), متطلبات او مبأدئ مقترحة لنظام البنك المركزي العراقي الخاص بالتدقيق الداخلي .

٤_ المعايير الدولية لممارسة المهنية للتدقيق الداخلي , (٢٠٠٦) .

٥_ استراتيجية الامن السيبراني العراقية , (٢٠١٩) .

٦_ الوردات , خلف عبدالله , (٢٠٢٤) . دور التدقيق الداخلي في عصر الذكاء الاصطناعي , الاردن .

٧_ الطائي , الاء علي حسين عوني , (٢٠٢٢) . استراتيجية الامن السيبراني / دراسة حالة في وزارة الدفاع العراقية .

٨_ السراي , خلدون خضر باري , (٢٠٢٤) .دور التدقيق الداخلي في تقييم ادارة المخاطر السيبرانية في المصارف التجارية العراقية على وفق اطار (NIST)

ثانيا : المصادر الاجنبية .

1-the institute of internal auditor ,(2024), Global internal audit standards .

2-Basel ,(2021) , basel committee banking supervision .

3- National institute of standards and Technology (NIST) , (2018) , cyber security framework .
4-Raji, Inioluwa Deborah, et al. (2020) , "Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing.
5-Anouar Faiteh, Mohammed Rachid Aasri, " Internal Audit and Added Value: What is the Relationship", (2022).
6-Gurtu, Amulya, and Jestin Johny. "Supply chain risk management: Literature review." *Risks* 9.1 (2021) .