تقييم مستوى تطبيق حوكمة البيانات باستخدام إجراءات التدقيق الداخلي في ظل التحول الرقمي– منهج مقترح

Assessing the Level of Data Governance Implementation Using Internal Audit Procedures in the Context of Digital Transformation – A Proposed Methodology

أ.م.د.سُهاد صبيح الصفار

الجامعة التقنية الوسطى، الكلية التقنية الادارية– بغداد

sohadalsaffar72@mtu.edu.iq

رقم التصنيف الدولي ISSN 2709-2852

تاريخ استلام البحث : ٢٠٢٦/٣/٦ تاريخ قبول النشر: ٢٠٢٦/٣/٣٠

المستخلص

يهدف البحث توظيف متطلبات حوكمة البيانات بوصفها أساساً منهجياً لدعم المدقق الداخلي في تصميم إجراءات فحص ذات فاعلية عالية، وبناء إطار إجرائي يمكن من خلاله تنفيذ برامج التدقيق في ظل بيئة التحول الرقمي. ينصب التركيز على إبراز مجالات توظيف مفهوم حوكمة البيانات بما يعزز كفاءة تصميم إجراءات التدقيق الداخلي في تقييم مستوى الالتزام بتلك المتطلبات، وتحديد مجالات التدقيق ذات الأولوية، وتطوير أدلة الإثبات الملائمة، بما يؤدي إلى بلورة منهج عملي يساعد المدقق الداخلي على أداء مهامه في بيئات الأعمال الرقمية.

مجلة العلوم المالية والمحاسبية

AFSJ

ACCOUNTING & FINANCIAL SCIENCES JOURNAL

مجلة العلوم المالية والمحاسبية
العدد الثاني والعشرون/ حزيران ٢٠٢٦
الصفحات ١٩١– ٢٣٠

اعتماداً على الجانب التطبيقي للبحث، اتبعت الباحثة المنهج الوصفي – التحليلي من خلال دراسة حالة مصرف عراقي، جرى في إطارها تحليل السياسات والإجراءات التقنية الصادرة عن البنك المركزي وانعكاسها على حوكمة البيانات المصرفية، فضلاً عن تحليل التقارير المالية للفترة (٢٠٢٠–٢٠٢٤) والتقارير المنشورة الخاصة بحوكمة المصارف، بهدف تشخيص وتحليل متطلبات الحوكمة المطبقة فعلياً. وبناءً على نتائج هذا التحليل، تم تصميم قائمة فحص تضمنت سبعة متطلبات رئيسة لقياس مستوى التطبيق، وتحديد مجال التدقيق، وتوثيق أدلة الإثبات الداعمة لإجراءات التدقيق الداخلي، وبيان علاقتها بمسارات التحول الرقمي في القطاع المصرفي.

أظهرت نتائج فحص مستوى التطبيق وجود ضعف في الفصل بين أدوار ومسؤوليات مجلس الإدارة والإدارة التنفيذية فيما يتعلق بحوكمة البيانات، مما أدى إلى قصور في السياسات والإجراءات الرقابية. كما بينت النتائج ضعف الاهتمام بتطوير إدارة البيانات وسياساتها، وعدم كفاية الالتزام بالمتطلبات القانونية وضمان سلامة البيانات.

كلمات مفتاحية: حوكمة البيانات، مبادئ حوكمة البيانات، إجراءات التدقيق الداخلي، أدلة الاثبات، التحول الرقمي.

Abstract

This research aims to utilize data governance requirements as a methodological foundation to support internal auditors in designing highly effective audit procedures and building a procedural framework for implementing audit programs within a digital transformation environment. The focus is on highlighting the applications of the data governance concept to enhance the efficiency of internal audit procedure design in assessing compliance with these requirements, identifying priority audit areas, and developing appropriate audit evidence. This leads to the development of a practical methodology that helps internal auditors perform their tasks effectively in digital business environments.

Based on the applied aspect of the research, the researcher adopted an analytical and descriptive approach through a case study of an

Iraqi bank. This case study analyzed the policies and technical procedures issued by the Central Bank and their impact on banking data governance. It also analyzed financial reports for the period (2020–2024) and published reports on bank governance to diagnose and analyze the governance requirements actually implemented. Based on the results from this analysis, a checklist was developed comprising seven key requirements to measure the level of implementation, define the scope of the audit, document supporting evidence for internal audit procedures, and demonstrate their relationship to digital transformation pathways in the banking sector.

The results of the implementation level assessment revealed a weakness in the separation of responsibilities and roles between the board of directors and executive management regarding data governance, leading to deficiencies in policies and control procedures. The results also indicated insufficient attention to developing data management and its policies, and inadequate compliance with legal requirements and data integrity assurance.

Keywords: Data governance, Data governance principles, internal audit procedures, Evidence, Digital transformation.

المقدمة

تمثل حوكمة البيانات عنصرا اساسياً ضمن مفهوم حوكمة الشركات، للدور المباشر الذي تتمتع به في حماية اصحاب المصلحة من خلال تعزيز الرقابة على أداء الإدارة التنفيذية، بما ينسجم مع أهداف التدقيق الداخلي. مع التطور المتسارع في بيئة الأعمال الرقمية، ازداد الاهتمام بالبيانات بوصفها موردا استراتيجيا، الأمر الذي صاحبه تصاعد في مخاطر الاختراق وسوء الاستخدام. كما أن التوسع في حجم البيانات وتعدد مصادرها، إلى جانب تشابك عمليات جمعها ومعالجتها وتداولها بين البيئة الداخلية والخارجية، فرض على الوحدات الاقتصادية تبني أطر حوكمة فعالة لإدارة البيانات. وانطلاقًا من ذلك، يضطلع المدقق الداخلي بدور مهم في تقييم حوكمة البيانات من خلال إجراءات فحص مصممة لهذا الغرض، تعظيماً للقيمة المتحققة من البيانات،

ودعم الشفافية، وحماية الخصوصية، وضمان أمن البيانات، فضلاً عن تحقيق الرقابة على التكاليف والعوائد والمخاطر في ظل التحول الرقمي.

يستعرض البحث إبتداءاً المنهجية المتبعة في إعدادهِ، يليها مدخل نظري عن مفهوم حوكمة البيانات، والعلاقة بين متطلبات حوكمة البيانات وتصميم اجراءات فحص لتقييم مستوى تطبيق المتطلبات في ظل التحول الرقمي. ثم يُعزز هذا العرض بتحليل مدى تطبيق حوكمة البيانات، يلي ذلك إدراج لأهم ما تم التوصل اليه من إستنتاجات وتوصيات.

١- المبحث الاول/ منهجية البحث

١. ١- مشكلة البحث

تتمثل مشكلة البحث في الحاجة إلى تطوير منهج واضح ومتكامل لتقييم مستوى تطبيق حوكمة البيانات داخل الوحدات الاقتصادية في ظل التحول الرقمي، يعتمد على تصميم إجراءات تدقيق داخلي فاعلة تسهم في الحصول على أدلة إثبات كافية وملائمة تدعم رأي المدقق الداخلي بشأن مستوى التطبيق الفعلي. ومن ثم، يسعى البحث إلى الإجابة عن التساؤلات الآتية:

- ما الإجراءات المنهجية التي يمكن أن يعتمدها المدقق الداخلي لتقييم مستوى تطبيق حوكمة البيانات في بيئة التحول الرقمي؟
- إلى أي مدى تستند إجراءات التقييم المعتمدة من قبل المدقق الداخلي، إلى مراجعة متطلبات حوكمة البيانات بوصفها أدلة إثبات تدعم نتائج تقريره عن مستوى التطبيق في ظل التحول الرقمي؟

١. ٢- هدف البحث

يهدف البحث إلى بيان مجالات توظيف مفهوم حوكمة البيانات، بما يسهم في دعم تصميم إجراءات تدقيق داخلي فاعلة لتقييم مستوى التطبيق، وتحديد مجال التدقيق، وأدلة إثبات بما يؤدي إلى بناء منهج يساعد المدقق الداخلي في أداء مهامه في ظل بيئة التحول الرقمي.

١. ٣- أهمية البحث

تنبع أهمية البحث من تناوله لموضوع حوكمة البيانات في بيئة التحول الرقمي للمصارف، وما يطرحه ذلك من تحديات على مهنة التدقيق الداخلي، وذلك من خلال:

١. سد فجوة معرفية المتعلقة بدور حوكمة البيانات في دعم فعالية التدقيق الداخلي في الوحدات المصرفية.

٢. توضيح الكيفية التي يمكن من خلالها لتطبيق أطر حوكمة البيانات، أن يدعم متطلبات التحول الرقمي عبر تطوير أساليب رقابية وتدقيقية حديثة قائمة على البيانات.

٣. تقديم مخرجات تطبيقية يمكن للإدارة التنفيذية ووحدات التدقيق الداخلي، الاستفادة منها في قياس وتقويم مستوى الالتزام بسياسات حوكمة البيانات داخل البيئة الرقمية.

٤. توضيح دور حوكمة البيانات في الحد من المخاطر المرتبطة بالبيانات، ولاسيما مخاطر الأمن السيبراني وسلامة البيانات والحماية من إساءة استخدامها، بما يدعم تحسين جودة أعمال التدقيق الداخلي.

٥. مساعدة المهنيين في مجالات التدقيق الداخلي والتحول الرقمي، بإطار يمكن اعتماده عند تعزيز مواءمة وظيفة التدقيق الداخلي مع متطلبات البيئة الرقمية.

١. ٤- فرضية البحث

ينطلق البحث من فرضية رئيسة مفادها: "توافر منهج لتقييم تطبيق حوكمة البيانات في ظل التحول الرقمي، يُسهم في تصميم منهجية تدقيق داخلي قائمة على مجموعة من الإجراءات، التي تحدد طبيعة أدلة الإثبات الداعمة لنتائج تقرير المدقق الداخلي".

تقسم الفرضية الرئيسة إلى فرضيات فرعية بحسب المتغيرات وكالآتي:

الفرضية الفرعية الأولى. يُسهم تطبيق مبادئ وأطر حوكمة البيانات، في تعزيز موثوقية منهجية التدقيق الداخلي.

الفرضية الفرعية الثانية. يُعزز التحول الرقمي العلاقة بين حوكمة البيانات ومنهجية التدقيق الداخلي من خلال توظيف التقنيات الرقمية في جمع وتحليل أدلة الإثبات.

الفرضية الفرعية الثالثة. يُسهم تصميم منهجية تدقيق داخلي مبنية على إجراءات محددة لتقييم حوكمة البيانات، في توفير أدلة إثبات أكثر موضوعية وموثوقية.

الفرضية الفرعية الرابعة. يؤدي تفاعل مكونات حوكمة البيانات مع متطلبات التحول الرقمي، تطوير إطار متكامل لاجراءات تدقيق داخلي وتحسين جودة التقارير التدقيقية.

١. ٥- مجتمع وعينة البحث

١. مجتمع البحث. تم اختيار القطاع المصرفي العراقي مجتمع للبحث كونه من أكثر القطاعات التي تعتمد على البيانات في مختلف عملياتها التشغيلية، وباعتباره من أكثر القطاعات تأثرا بالتحول الرقمي في البيئة الاقتصادية العراقية. كما تتميز المصارف بامتلاكها أنظمة معلومات مالية ومحاسبية رقمية، مما يجعلها بيئة مناسبة لتطبيق مفاهيم حوكمة البيانات وتصميم إجراءات للتدقيق الداخلي عند تقييمها.

٢. عينة البحث. تمثلت العينة أحد المصارف العراقية الخاصة (الأهلية)، التي تبنت خلال السنوات الأخيرة برامج للتحول الرقمي في أعمالها وخدماتها المالية، الأمر الذي يجعلها نموذج ملائم لدراسة مستوى تطبيق حوكمة البيانات وتقييم كفاءة ممارسات التدقيق الداخلي في ظل هذا التحول. يتيح هذا الاختيار إمكانية الوصول إلى بيانات وبيئة غنية بالتطبيقات الرقمية التي تدعم تحقيق أهداف البحث.

١. ٦- منهجية البحث

لغرض وضع مفاهيم البحث موضع التطبيق العملي، اعتمدت الباحثة المنهج الوصفي – التحليلي من خلال دراسة حالة مصرفية. إذ تم تحليل السياسات والإجراءات التقنية المصرح عنها من قبل البنك المركزي وانعكاسها على حوكمة البيانات المصرفية، فضلاً عن تحليل التقارير المالية للمدة (٢٠٢٠–٢٠٢٤)، وتقارير حوكمة المنشورة، بهدف التعرف تحليل متطلبات حوكمة فعليا. بناءً على ذلك، تم تصميم قائمة فحص تضمنت (7) متطلبات وذلك لغرض تقييم مستوى التطبيق، وتحديد مجال وادلة الإثبات الدعمة لإجراءات التدقيق الداخلي وعلاقتها بالتحول الرقمي. التزاماً بمبادئ حوكمة البيانات وأخلاقيات مهنة التدقيق الداخلي، ولاسيما مبدأ سرية البيانات، تم إجراء التطبيق العملي

في أحد المصارف الاهلية دون الإفصاح عن اسمه، وذلك لحماية البيانات وضمان عدم استخدامها المعلومات خارج نطاق البحث العلمي، وقد تم الحصول على موافقة المصرف لإجراء الدراسة واستخدام البيانات لأغراض البحث العلمي فقط.

ويوضح جدول (١) متطلبات حوكمة البيانات المعتمدة في البحث.

جدول (١) متطلبات حوكمة البيانات

ت	المتطلب	مجال الفحص	اجمالي التقييم لايفاء المتطلب	عدد فقرات كل متطلب
١	تنظيم وتصنيف البيانات	يشمل التدقيق تقييم السياسات والإجراءات الخاصة بهيكلة البيانات وتصنيفها وفق مستويات الأهمية والحساسية، والتحقق من وجود معايير موحدة لتسمية البيانات، وفهرستها، وتحديد مالكي البيانات، ومدى توافق عمليات التصنيف مع متطلبات العمل والضوابط التنظيمية.	٥٥	٧
٢	سلامة ونزاهة البيانات	يركز التدقيق على فحص دقة البيانات واكتمالها واتساقها عبر الأنظمة المختلفة، والتحقق من وجود ضوابط تمنع التعديل غير المصرح به، وآليات التحقق، وإجراءات كشف الأخطاء ومعالجتها لضمان موثوقية المعلومات المالية والتشغيلية.	٥١	٦
٣	أمن البيانات	تقييم ضوابط حماية البيانات من الوصول غير المصرح به أو الاختراق أو الفقدان، بما يشمل إدارة صلاحيات المستخدمين، التشفير، النسخ الاحتياطي، إدارة الهوية والوصول وخطط الاستجابة للحوادث الأمنية.	٥٤	٦

٤	امكانية الوصول للبيانات	التحقق من توفر البيانات للمستخدمين المخولين في الوقت المناسب، وتقييم سياسات منح الصلاحيات، وكفاءة أنظمة الاسترجاع، وضمان تحقيق التوازن بين سهولة الوصول ومتطلبات السرية والأمن.	٢٨	٤
٥	مراقبة البيانات	فحص آليات المراقبة المستمرة لاستخدام البيانات، وسجلات التتبع (Audit Trails)، ومراقبة التعديلات، وتحليل الأنشطة غير الطبيعية، ومدى استخدام أدوات تحليلية للكشف عن المخاطر المرتبطة بالبيانات.	١٨	٣
٦	متابعة وتدقيق حوكمة البيانات	وجود إطار رقابي واضح لحوكمة البيانات، الالتزام بالسياسات، وقياس مؤشرات الأداء الخاصة بالحوكمة، ومراجعة التقارير الدورية الخاصة بإدارة البيانات.	٥١	٦
٧	التحسين المستمر	آليات تطوير ممارسات حوكمة البيانات بشكل مستمر، واستخدام التقييمات السابقة في تحسين الضوابط.	٥١	٦

المصدر: اعداد الباحثة

حددت الباحثة منهجاً لتقويم تطبيق متطلبات حوكمة البيانات في احد المصارف. عند التقييم المدقق بتتبع مجموعة خطوات ضمن نطاق فقرات المتطلبات السبعة المحددة في جدول (١) السابق. تمثل هذه خطوات نظامية وجد بعضها مُطبقاً في المصرف موضوع البحث والبعض الآخر غير مُطبق. يمثل عدم تطبيق المتطلب ضعف يُصنف من قِبل الباحثة عند ثلاث مستويات في ضوء حجم تأثير الضعف بالنسبة للبيانات المصرفية وإنتهاكه للتعليمات والسياسات والإجراءات. كما يعتمد تحديد مداه أيضاً على تقدير المدقق الداخلي المبني على خبرته. يُعطى الضعف تدريجاً رقمياً حسب مستوى التصنيف. يبين جدول (٢) تصنيفات الضعف والدرجات المقابلة لها.

جدول (٢) التدريج الرقمي لمستويات الضعف

صغير	متوسط	كبير
٠ – ٤	٥ – ٧	٨ – ١٠

المصدر: اعداد الباحثة

توضح الجداول (٣) الى (٩)، متطلبات حوكمة البيانات. فضلا عن، تصنيف ضعف عدم توافر المتطلب، في ضوء اجابات المبحوثين على الاسئلة والاستفسارات المطروحة. وكانت درجات التقويم ضمن الحد الاقصى (٤، ٧، ١٠). على سبيل التوضيح، التكامل بين متطلب تنظيم البيانات وتصنيفها وإجراءات التدقيق، كان تقويم الضعف للمتطلب الاول ١١ درجة من اجمالي ٥٥ درجة، إذ يتضمن ثلاثة بتقييم كبير، وثلاثة بتقييم متوسط، وواحد بتقييم صغير [(٣×١٠)+(٣×٧)+(١×٤)]. اما تكامل متطلب سلامة ونزاهة البيانات واجراءات التدقيق، كان التقييم الضعف للمتطلب الثاني ١٧ درجة من اجمالي ٥١ درجة، إذ تضمن ثلاثة كبير، ثلاثة متوسط [(٣×١٠)+(٣×٧)]. وكذلك الحال بالنسبة لبقية الجداول.

٢- المبحث الثاني/ الابعاد المفاهيمية لحوكمة البيانات والتدقيق الداخلي

ظهرت أهمية الحوكمة بعد أزمات مالية وانهيارات اقتصادية شهدها العالم نتيجة حالات تحريف القوائم المالية وتعظيم الأرباح، مما أضر بأصحاب المصلحة وفي مقدمتهم المستثمرين والمقرضين. وقد اقتُرحَت الحوكمة كأحد الحلول للحد من تأثير ممارسات للتحريف (Pazarskis & Kostyuk, 2024, 6)

٢. ١- حوكمة البيانات – منظور مفاهيمي

تُعد حوكمة البيانات أحد المكونات الجوهرية لمفهوم حوكمة المعلومات، إذ تمثل البعد التنفيذي الخاص بتنظيم إدارة البيانات داخل الوحدة الاقتصادية وضبط آليات التعامل معها (Brous, 2016: 115). عُرفت حوكمة البيانات بأنها مجموعة من الأنشطة والإجراءات التنظيمية التي تهدف إلى تحديد صلاحيات اتخاذ القرار المتعلقة بالبيانات وتوضيح مسؤوليات المساءلة المرتبطة بإدارتها واستخدامها، وذلك وفق قواعد ونماذج حوكمة متفق عليها تحدد آليات الوصول للبيانات واستخدامها وتوقيتاتها وشروطها، بما يضمن إدارتها

بصورة منضبطة وفعّالة (Liaw et al., 2014: 199–206). كما يشير Smallwood إلى أنها إطاراً يضم السياسات والإجراءات والهياكل الرقابية التي تنظم عمليات إنشاء البيانات وإدارتها وحمايتها واستخدامها، بما يعزز التعامل معها كموجود استراتيجي يدعم القرارات ويعزز الامتثال وإدارة المخاطر (Smallwood, 2016: 16). كما انها تُعد عملية تنظيمية منهجية تهدف إلى ضمان موثوقية البيانات ودقتها واتساقها، الأمر الذي يجعلها ركناً أساسياً في استراتيجية إدارة البيانات داخل الوحدات الاقتصادية (الأسدي، ٢٠٢٢: ٣٧). وفي الاتجاه ذاته، ينظر (Burmeister et al., 2020: 5595) إلى حوكمة البيانات بوصفها آلية تعظم القيمة الاقتصادية للبيانات من خلال تقليل المخاطر المرتبطة بها وخفض تكاليف إدارتها وتشغيلها. وهناك من يرى انها لا تقتصر على الأبعاد التقنية، بل تمتد لتشكل إطاراً تنظيمياً ورقابياً شاملاً يتطلب تحديداً واضحاً للأدوار والمسؤوليات، مثل مالكي البيانات وأمنائها، إلى جانب تطبيق ضوابط رقابية وإجراءات تدقيق دورية تسهم في تعزيز سلامة البيانات وجودتها. يُعد التدقيق أداة رئيسة في تقييم مستوى تطبيق حوكمة البيانات والكشف عن أوجه القصور، بما ينعكس إيجاباً على موثوقية المعلومات وفاعلية القرار في بيئات التحول الرقمي (Thompson et al., 2015: 118).

وبناءً على ما ذكر من تعاريف ترى الباحثة أن حوكمة البيانات تمثل إطاراً حوكمياً متكاملاً يتجاوز الإدارة التقنية للبيانات ليشمل تنظيم العلاقات والمسؤوليات المرتبطة باستخدام البيانات داخل الوحدة الاقتصادية. إذ تؤكد الأدبيات على مركزية مبدأ المساءلة من خلال تحديد الجهات المخولة بالوصول إلى البيانات وآليات استخدامها، بما يعزز الشفافية الوحدة والالتزام التنظيمي. كما تؤدي حوكمة البيانات دوراً محورياً في إنجاح التحول الرقمي عبر مواءمة الوظائف التنظيمية لمواجهة تحديات تضخم البيانات، وتطوير آليات اتخاذ القرار القائم على البيانات لدعم التخطيط الاستراتيجي، فضلاً عن تحسين كفاءة استثمار الموارد الرقمية وتعزيز تكامل تقنيات البيانات بما يحقق مرونة العمليات واستدامة الأداء المؤسسة التنظيمية.

٢. ٢- العلاقة بين حوكمة البيانات، وإجراءات التدقيق الداخلي، والتحول الرقمي

أولاً: العلاقة بين حوكمة بيانات الوحدة الاقتصادية وإجراءات التدقيق الداخلي

يُعد التدقيق الداخلي بوصفه نشاطاً تأكيدياً واستشارياً مستقلاً يسهم في تقييم كفاءة وفعالية الحوكمة (IIA, 2024: 12)، ولاسيما حوكمة البيانات، من خلال تصميم وتنفيذ إجراءات تدقيق تسهم بالاتي (الوثيري، ٢٠٢٤: ٤٢-٤٣)

- تقييم مدى وضوح سياسات وإجراءات حوكمة البيانات.
- فحص الضوابط الرقابية المرتبطة بإدارة البيانات.
- التحقق من الالتزام بالمتطلبات التنظيمية والمعايير المهنية ذات العلاقة.
- توفير أدلة إثبات كافية وملائمة تدعم استنتاجات المدقق الداخلي بشأن مستوى التطبيق.

يمكن القول تمثل إجراءات التدقيق الداخلي أداة منهجية رئيسة لقياس وتقييم نضج تطبيق حوكمة بيانات الوحدة الاقتصادية.

ثانياً: دور التحول الرقمي في تصميم إجراءات التدقيق الداخلي

انعكس التحول الرقمي على إحداث تغييرات جوهرية في بيئة أعمال الوحدة، بشكل مباشر في طبيعة عمليات التدقيق الداخلي، من حيث أساليب جمع الأدلة، وتحليل البيانات، وتوقيت تنفيذ الإجراءات (Jabur & Ibrahim, 2025: 211).

تتركز إسهامت التقنيات الرقمية من خلال تعزيز كفاءة وفاعلية إجراءات التدقيق بالاتي (رشوان وهبة، ٢٠٢٢: ٤٣-٤٤)، (امين و عبد الحق، ٢٠٢٣: ٣٤٣):

- أتمتة إجراءات التدقيق وتحسين سرعة الإنجاز.
- استخدام تحليلات البيانات الضخمة في اكتشاف الانحرافات والمخاطر.
- تعزيز القدرة على التدقيق المستمر بدلًا من التدقيق الدوري.
- تعزيز جودة أدلة الإثبات ودقتها وموثوقيتها.

ثالثاً: التحول الرقمي كعامل مؤثر في العلاقة بين حوكمة البيانات وإجراءات التدقيق الداخلي

في ظل بيئة التحول الرقمي المتسارعة، تزداد تعقيدات إدارة البيانات بصورة ملحوظة، بالتوازي مع تصاعد المخاطر المرتبطة بالأمن السيبراني، وحماية الخصوصية،

واستمرارية الأنظمة الرقمية (حمني وطوبال، ٢٠٢٠: ١١٨٧)، الأمر الذي يجعل تبنّي حوكمة البيانات ضرورة تنظيمية واستراتيجية لضمان الاستخدام الآمن والفعّال للبيانات داخل الوحدات الاقتصادية (Karimallah & Drissi, 2024: 864). وفي هذا السياق، يتعاظم دور التدقيق الداخلي المدعوم بالتقنيات الرقمية بوصفه حلقة وصل بين متطلبات الحوكمة والإجراءات التطبيقية، من خلال تعزيز قدرته على تقييم نظم حوكمة البيانات الرقمية، وتوسيع نطاق إجراءات التدقيق ليشمل قواعد البيانات والمنصات الإلكترونية والبنى التحتية الرقمية، فضلاً عن دعم موثوقية نتائج تقييم الحوكمة عبر توظيف أدوات تحليل البيانات والتقنيات الذكية.

يرى معهد المدققين الداخليين (IIA) أن وظيفة التدقيق الداخلي تمثل أحد المرتكزات الأساسية في حوكمة البيانات، إذ تضطلع بمسؤولية تقييم الأطر التنظيمية والسياسات والإجراءات المرتبطة بإدارة البيانات وأخلاقياتها داخل الوحدة الاقتصادية، والتحقق من فاعليتها في ضمان الاستخدام المسؤول والآمن للبيانات. وعليه، ينبغي أن ينظر المدقق الداخلي إلى أخلاقيات البيانات باعتبارها جزءاً متكاملاً من نطاق تدقيق أوسع يشمل حوكمة البيانات والعمليات التنظيمية المرتبطة بها، من خلال تحديد المخاطر ذات الصلة وتحليل الممارسات التشغيلية المتعلقة بجمع البيانات وتخزينها ومعالجتها ونقلها والإفصاح عنها. يتطلب ذلك تنفيذ عمليات رسم خرائط البيانات وجردها بهدف تحديد مصادر البيانات ومسارات تدفقها والجهات المخوّلة بالوصول إليها، فضلاً عن التحقق من الالتزام بالتشريعات والقواعد المنظمة لاستخدام البيانات وحمايتها. كما يؤدي التدقيق الداخلي دوراً محورياً في تقييم مخاطر البيانات بالتنسيق مع إدارة تقنية المعلومات، بما يسهم في فهم المخاطر المرتبطة بجودة البيانات وأمنها وخصوصيتها وتكاملها، خاصة في ظل انتشار البيانات عبر أنظمة متعددة، الأمر الذي يزيد من احتمالات التعرض للاختراقات الأمنية. ويمتد نطاق التدقيق ليشمل فحص مؤشرات الأداء المرتبطة بحوكمة البيانات، مثال ذلك وجود سياسات أخلاقية معتمدة لاستخدام البيانات، مستوى الامتثال، عدد المخالفات المرتبطة بأمن البيانات، مجالات تدريب العاملين على أخلاقيات البيانات وإدارة تضارب المصالح. إضافةً إلى ذلك، يركز التدقيق الداخلي على تقييم آليات الإبلاغ عن المخالفات

الأخلاقية وضمان معالجتها وفق سياسات واضحة تحمي المبلّغين من الممارسات الانتقامية، فضلاً عن تحليل الحوادث الأخلاقية لقياس فاعلية الضوابط الرقابة. ونظراً للطبيعة الديناميكية لحوكمة البيانات، فإن دور التدقيق الداخلي لا يقتصر على الفحص الدوري، بل يمتد إلى المراقبة والمتابعة المستمرة لضمان استدامة الامتثال وكفاءة الضوابط، بما يعزز الثقة في إدارة البيانات ويدعم منظومة الحوكمة (IIA, 2020: 10–12).

من خلال العرض السابق، ترى الباحثة أن حوكمة البيانات تمثل إطاراً تنظيمياً ورقابياً متكاملاً يتقاطع بصورة مباشرة مع وظائف التدقيق الداخلي، إذ تسهم في تعزيز الشفافية والمساءلة من خلال تدقيق صلاحيات الوصول إلى البيانات وآليات استخدامها، الأمر الذي يدعم قدرة التدقيق الداخلي على تقديم تأكيد موضوعي بشأن موثوقية المعلومات وجودة التقارير. كما تؤدي حوكمة البيانات دوراً محورياً في دعم التحول الرقمي عبر تمكين التدقيق الداخلي من تبني منهج تدقيق قائم على البيانات، بما يعزز كفاءة تقييم المخاطر ويرفع جودة الرقابة ويسهم في تحسين التخطيط الاستراتيجي وكفاءة استثمار الموارد الرقمية داخل الوحدة الاقتصادية.

٣. المبحث الثالث/ الجانب العملي. الإطار المقترح لربط متغيرات البحث

انطلاقاً مما عرض في منهجية البحث، والجانب النظري، يقوم الإطار المقترح على افتراض أن:

– حوكمة بيانات الوحدة الاقتصادية تمثل المتغير الرئيس المراد تقييمه.

– إجراءات التدقيق الداخلي تمثل الأداة المنهجية للتقييم والحصول على أدلة الإثبات.

– التحول الرقمي يمثل عاملا يعزز إجراءات التدقيق الداخلي.

٣. ١– تأثير مستوى تطبيق متطلب تنظيم وتصنيف البيانات في إجراءات التدقيق

تخضع قاعدة بيانات المصرف لإدارة وإشراف قسم تقنية المعلومات والاتصالات، بما يضمن ضبط عمليات التخزين والمعالجة واستمرارية الرقابة تقنية المعلومات. وفي إطار الضوابط التطبيقية، يتحقق تأكيد صحة ترحيل المعاملات من قبل القسم المستخدم من خلال كشوف مطابقة تُستخرج مباشرة من النظام، إذ يتم سحب كشف لكل قيد يجري

ترحيله من قبل أي مستخدم، بما يعزز مبدأ التتبع الإلكتروني (Audit Trail) ويوفر تسلسلاً رقابياً يدعم إمكانية التحقق من دقة القيود.

يساعد توافر هذه المرتكزات ضمن العمل الرقمي قوة وحيادية أدلة الإثبات التي يعتمد عليها المدقق الداخلي، كونها أدلة ناتجة عن نظام يخضع إلى رقابات تقنية وإجرائية متكاملة، إضافة إلى قيود أمنية ونظم تقارير رقمية تُصعب فرص الغش البيانات أو تعديلها دون كشف. يتيح التحول الرقمي دمج الملفات المحاسبية ضمن منظومة معلومات متكاملة تدعم التوثيق الإلكتروني، والرقابة المستمرة، وإمكانية الفحص والتتبع عند تنفيذ أعمال التدقيق الداخلي.

يستعرض جدول (٣)، مدى تطبيق متطلب تنظيم البيانات وتصنيفها كأحد متطلبات حوكمة البيانات في المصرف موضوع البحث.

جدول (٣) تكامل متطلب تنظيم وتصنيف البيانات مع إجراءات التدقيق الداخلي المنفذة

متطلبات حوكمة البيانات في البيئة الرقمية/ تنظيم وتصنيف البيانات	التطبيق / مُطبق ✓ / غير مُطبق ×	تحليل المتطلب في ظل التحول الرقمي	أدلة الإثبات المطلوب فحصها	اجراءات الفحص المعتمدة عند تقييم المدقق الداخلي لمستوى تطبيق متطلبات حوكمة البيانات
١. أمن قواعد البيانات رقمياً، الحماية من الأعطال والاختراقات.	كبير	التحكم في الوصول، وجود ملفات احتياطية مدعومة سحابياً	تقارير قسم البيانات والاتصالات حول اداء قواعد بيانات، كشف الاعطال والخروقات	– التأكد من عدم سماح برامجيات قواعد البيانات أداء نفس المستخدم أو المشغل الجميع بين الوصول والمعالجة للمعاملة والتحقق منها. – المطابقة بين قواعد البيانات الفرعية وقواعد البيانات العامة. – تقييم معايير إنشاء قاعدة بيانات، ومجالات التخزين.
تصنيف خطر عدم توفير المتطلب	✓			

٤. البيانات والمستندات مصنفة إلكترونياً	٣. تطبيق منهجية رقمية لإدارة مخاطر البيانات واقتراح حلول تحميها.	٢. توحيد برامج جمع البيانات ومعايير إدخالها رقمياً
صغير	كبير	متوسط
×	✓	✓
تصنيف البيانات والمستندات حسب الوظائف الإدارية والتشغيلية	تقييم المخاطر المحيطة بالبيانات الإلكترونية (مخاطر سيبرانية ومخاطر سلامة البيانات)	التكامل بين الأنظمة المالية والمصرفية ضمن التحول الرقمي.
سجلات النظام الالكتروني، تقارير ادارة المستندات، صلاحيات الوصول	تقارير تقييم مخاطر البيانات الرقمية، النسخ الاحتياطية واستعادة البيانات، مراقبة الحوادث الامنية	السجلات المحاسبية، نماذج من مخرجات قواعد البيانات
– فحص تقارير حوادث عمليات المصرف. – مراجعة آلية تصنيف البيانات والمستندات الإلكترونية للتحقق من توافقها مع سياسات حوكمة المعتمدة، وأن التصنيف يتم وفق معايير السرية، الأهمية، نوع البيانات، فترة الاحتفاظ.	الفحص الدوري لقواعد بيانات وسجلات المصرف وتحديثها بإستمرار. يُحَدِّث المصرف كل وحدة (فرع او قسم) مرة في السنة ويمكن زيادة عدد المرات حسب طلب الادارة العليا. فضلا عن فحص جودة البيانات واستمرارية حمايتها رقمياً.	– تدقيق الجدول الزمني لحفظ وحذف البيانات. إذ ينبغي بقائها على برنامج الارشفة حسب مدد محددة من قبل البنك المركزي متوسط الوقت ١٥ سنة حسب نوع الوثيقة في عمليات السحب او الايداع قد تصل مدة الحفظ ٢٠ سنة

٥. تصنيف البيانات رقمياً وفق احتياجات المعالجة.	متوسط	×	البيانات موزعة حسب فئات المعالجة
البيانات المفصح عنها، تقارير صلاحية الوصول والاجراءات الرقابية، هيكل قواعد البيانات، مستويات تصنيف البيانات	– اختبار آليات التحكم في صلاحيات الوصول للتأكد من أن المستخدمين يحصلون فقط على البيانات المنسجمة مع طبيعة مهام المعالجة الموكلة إليهم. – مراجعة الخدمة الالكترونية ومؤشرات الاداء. متوسط عدد مرات المراجعة من ٦ الى ١٠ مرات. تقرير فصلي ٢ مرات وممكن اكثر حسب الحاجة، او عند وجود عطل وذلك من قبل مدقق داخلي معتمد.		
٦. رقمنة المستندات، لضمان سرعة معالجة البيانات	متوسط	✓	التصوير الإلكتروني وأتمتة أرشفة المستندات
تقارير اداء النظام ومؤشرات زمن المعالجة، المستندات الرقمية المؤرشفة والتوقيع الالكتروني	تفحص الارشفة الالكترونية كل مرة عند تدقيق اعمال الوحدة مع اخذ نماذج من مستندات مؤرشفة. – مراجعة سياسات التحول الرقمي للمصرف. – اختبار عينة من المستندات المرقمنة ومقارنتها بالاصل. – اختبار سرعة البحث عن مستند معين		

٧. تعزيز أمن الأرشفة الإلكترونية، وتقييد الوصول اليها	كبير	٧	أجهزة الأرشفة والوسائط الرقمية في أماكن آمنة	سجلات الوصول المرتبطة بالارشفة، الاوامر الادارية بمنح او الغاء الصلاحيات
مستوى الضعف	٥٥	١١		

الاطلاع على اماكن حفظ أجهزة الارشفة، وتجهيزات مكافحة الحريق، ووجود ابواب حصينة. - التحقق من استخدام التشفير الالكتروني للملفات، وفحص محاولات الاختراق. - تحليل سجلات الدخول والخروج والتعديلات على الملفات المؤرشفة

المصدر: إعداد الباحثة إستنادا للمعلومات الواردة في القوائم المالية ودليل الحوكمة

٣. ٢- تأثير مستوى تطبيق متطلب سلامة ونزاهة البيانات في إجراءات التدقيق

تأثير مستوى تطبيق متطلب سلامة ونزاهة البيانات في إجراءات التدقيق

ينشأ القسم المالي البيانات والإحتفاظ بها وتوزيعها وتتبعها لضمان صحتها وموثوقيتها، من خلال إزالة تكرار البيانات وتكاليف التخزين والمخاطر. تفرض إدارة المصرف سياسات تلبي المعايير القانونية وتحافظ على سلامة البيانات من أي تغيير او حذف مع المحافظة على مسارات التدقيق ومراقبتها لضمان الإمتثال وتأكيد سلامة البيانات. يمتلك المصرف لجنة تدقيق إستناداً إلى قانون المصارف العراقي (٩٤) لسنة ٢٠٠٤ ضمن المادة (٢٤)، تتركز مسؤولية اللجنة التي أشارت إليها تعليمات المادة (٤) لسنة ٢٠١٠ الصادرة عن البنك المركزي العراقي، على فحص صدق وعدالة التقارير المالية ومراقبة الإفصاح والتحقق من تطبيق تعليمات البنك المركزي ومعايير المحاسبة الدولية ومتطلبات هيئة الأوراق المالية. يعزز توافر هذا المتطلب المدقق الداخلي في الحصول على ادلة (مذكورة ضمن الجدول)، حول تفويض بالمعاملات من قبل المخولين (أ و ب) وإدخالها في الملفات.

يستعرض الجدول (٤)، مدى تطبيق متطلب سلامة ونزاهة البيانات كأحد متطلبات حوكمة البيانات في المصرف موضوع البحث.

جدول (٤) تكامل متطلب سلامة ونزاهة البيانات مع إجراءات التدقيق الداخلي المنفذة

متطلبات حوكمة البيانات في البيئة الرقمية/ سلامة ونزاهة البيانات	١. الاتساق في دورة حياة البيانات ضمن البيئة الرقمية من خلال انسيابية البيانات الرقمية	٢. الالتزام بممارسات حوكمة البيانات رقمياً
تصنيف خطر عدم توفير المتطلب	كبير	متوسط
التطبيق / مُطبق ✓ / غير مُطبق ×	✓	×
تحليل المتطلب في ظل التحول الرقمي	إنشاء المعلومة والاحتفاظ بها وتحديثها وتوزيعها إلكترونيا	السياسات والمعايير الرقمية تضمن دقة ومؤثوقيته البيانات
أدلة الإثبات المطلوب فحصها	تقارير تتبع مصدر البيانات، التشفير والحماية،سجلات المعالجة	تقارير تقييم الحوكمة من قبل لجنة التدقيق، تقارير مراقبة استخدام البيانات، تصنيف البيانات
اجراءات الفحص المعتمدة عند تقييم المدقق الداخلي لمستوى تطبيق متطلبات حوكمة البيانات	– التحقق من توافر انظمة ضبط داخلية لانشطة المصرف والفروع التابعه. – فحص ملفات اجراءات سحب ودفع النقد، وحسابات التوفير والودائع. الخ. – تتبع مسار البيانات عبر الانظمة – التحقق من تطبيق اجراءات الاتلاف الامن للبيانات.	– مراجعة التقرير السنوي بما يتضمنه من معلومات تهم اصحاب المصالح – فحص مستوى تطبيق دليل حوكمة المصرف مقارنة بحوكمة الشركات المقرة من البنك المركزي. – وجود اليات اختبار الكتروني لتتبع التعديلات على البيانات.

مستوى الضعف		٦. الالتزام بالرقابة الداخلية الرقمية، بما يعزز الحوكمة.	متوسط	✓	فصل الوظائف وتوزيع الصلاحيات رقمياً	لاجراءات الرقابية، تقارير الاستلال لتعليمات البنك المركزي أو سياسات IT	فحص السياسات والاجراءات الرقابية، التي تحدد فصل وظائف حفظ الموجودات عن التسجيل في السجلات. – فحص تقارير ادارة تقنية المعلومات. – فحص ضوابط الوصول والهوية الرقمية.
٥١	١٧	٥. تفعيل إدارة البيانات الداعمة للامتثال وحمايتها من خلال مسارات التدقيق الإلكترونية.	كبير	×	السياسات الرقمية تتماشى مع المتطلبات القانونية والتنظيمية	سجلات مسار التدقيق الالكتروني، تقارير منح الصلاحيات	فحص الإجراءات التشغيلية التي تحكم تحويل الأموال، وسياسات أمنية تحمي تحويل الأموال، والبرمجيات، والإحصالات. علما ان متوسط عدد مرات الفحص مرتين سنوياً.
		٤. تعزيز الرقابات الرقمية لضمان سلامة استخدام البيانات	متوسط	✓	وجود آمن للبيانات، يحد من الإساءة للبيانات الرقمية.	تقارير التدقيق الداخلي	يحتوي تقرير التدقيق الداخلي عدد المخالفات القانونية والاخطاء المحاسبية المكتشفة في الملفات المحاسبية للمصرف.
		٣. رفع جودة البيانات في الأنظمة الرقمية بخفض مخاطر البيانات وتقليل تكاليف التخزين	كبير	✓	عدم التكرار وإزالة الازدواجية وتحسين بنية البيانات	تقارير تصحيح الاخطاء، الالتزام بادارة البيانات، تكاليف التخزين.	– التأكد من دقة الاجراءات المحاسبية وسلامتها والتقيد بها، وان اي تعديلات على البيانات نتجت من عملية التدقيق الداخلي. – تدقيق كفاءة تخزين البيانات وإدارة المخاطر الرقمية. – مقارنة تكلفة التخزين قبل وبعد تطبيق الحوكمة.

المصدر: إعداد الباحثة إستنادا للمعلومات الواردة في القوائم المالية ودليل الحوكمة

٣. ٣- تأثير مستوى تطبيق متطلب أمن البيانات في إجراءات التدقيق

يمتلك المصرف قسماً متخصصاً بإدارة المخاطر، ترتكز استراتيجياته على تجنب المخاطر والحد من آثارها بما يضمن استمرارية الأنشطة التشغيلية وعدم تعطل العمليات المصرفية. وفي إطار التحول الرقمي وتوسع الاعتماد على الأنظمة الإلكترونية، يولي المصرف اهتماماً بتطوير خطة حماية وإدارة لمخاطر الأمن السيبراني وفقاً لتعليمات البنك المركزي العراقي، لاسيما ما يتعلق بمخاطر الاختراقات الرقمية وسرقة البيانات وتعطيل الخدمات. تشمل حماية البيانات ضمان أمنها في حالات المعالجة كافة، أي أثناء التخزين والتوزيع/النقل والاستخدام، بما يحقق المحافظة على خصائص البيانات (السرّية، والسلامة، والإتاحة)، من خلال اتخاذ إجراءات وقائية تمنع التلف أو السرقة أو التعديل غير المصرّح به من قبل غير المخولين. يتحقق عبر تشفير البيانات والمستندات، وتعزيز ضوابط الوصول والصلاحيات، والحماية من التجسس والاختراق عبر البريد الإلكتروني ووسائل الاتصال الإلكترونية. كما ألزم البنك المركزي المصارف بموجب كتابه ١٢٥٩/٦/١٤ بتاريخ ٢٠٢٢/٧/٢١ بضرورة تطبيق مواصفة ISO 27001 الخاصة بإدارة أمن البيانات، بوصفها إطاراً يضمن تعزيز الضوابط الرقابية الرقمية، ويدعم انتظام العمليات الإلكترونية بأمان.

وفي هذا المجال، يبرز دور التدقيق الداخلي كوظيفة رقابية لينفذ إجراءات تدقيق رقمية حول التزام المصرف بالامتثال لأحكام قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (٣٩) لسنة ٢٠١٥ الذي ألزم المصارف بالمحافظة على سرية حسابات الزبائن وودائعهم ومنع الإفصاح عنها إلا بموجب تصريح قانوني أو بموافقة خطية من الزبون. التزام الإدارة والموظفين (الحاليين والسابقين) بعدم تمكين أي طرف ثالث من الاطلاع أو فحص بيانات الزبائن خارج الحالات التي أجازها القانون، وذلك انسجاماً مع ما ورد في المادة (٥٠) من قانون المصارف رقم (٩٤) لسنة ٢٠٠٤، بما يعزز فعالية الرقابة الداخلية ويحد من مخاطر التسرب البياناتي والانتهاكات الرقمية.

يستعرض الجدول (٥)، مدى تطبيق متطلب أمن البيانات كأحد متطلبات حوكمة البيانات في المصرف موضوع البحث.

جدول (٥) تكامل متطلب أمن البيانات مع إجراءات التدقيق الداخلي المنفذة

متطلبات حوكمة البيانات في البيئة الرقمية/ أمن البيانات	تصنيف خطر عدم توفير المتطلب	التطبيق / مُطبق ✓ / غير مُطبق ×	تحليل المتطلب في ظل التحول الرقمي	أدلة الاثبات المطلوب فحصها	اجراءات الفحص المعتمدة عند تقييم المدقق الداخلي لمستوى تطبيق متطلبات حوكمة البيانات
١. توظيف برامج تكشف الاختراقات المحتملة للمصرف.	كبير	✓	رصد التهديدات السيبرانية والكشف المبكر عن محاولات الاختراق، لتعزيز الاستجابة وتقليل آثار المخاطر الرقمية	تقارير انظمة كشف التسلل، سجلات الاحداث الامنية، تقرير المسؤوليات	– مراجعة تقارير قسم تقنيات البيانات عند حدوث عطل. اجتماع لجنة تقنية البيانات فصلية كل ٣ اشهر (اجندة الاجتماع). – تقييم كفاءة وفاعلية نظام كشف الاختراقات – تقييم ضوابط الاستجابة للحوادث السيبرانية
٢. تشفير البيانات المرسلة عبر الشبكات الداخلية والخارجية.	كبير	✓	تطبيق تقنيات تشفير قوية للبيانات المتبادلة عبر الشبكات الداخلية والخارجية، لضمان سرية البيانات وحمايتها عند تداولها	سياسات أمن المعلومات وتقارير الاختبارات الأمنية، تقارير سجلات الشبكة وأنظمة الحماية	– يتم التقييم مرتين سنوياً. – مراجعة سياسة أمن المعلومات للتأكد من وجود سياسة رسمية لتشفير البيانات أثناء النقل – التأكد من توافق السياسة مع المعايير مثل ISO 27001. – اختبار تطبيق بروتوكولات التشفير على الشبكات – مراجعة آلية إنشاء وتخزين وتغيير مفاتيح التشفير.

٤. وجود حماية كافية لودائع الزبائن والموجودات المالية.	٣. وجود إجراءات تضمن عدم تسريب المستخدمين للبيانات
كبير	متوسط
✓	×
تطبيق ضوابط إلكترونية متقدمة، ونظم مراقبة فورية للعمليات، بما يقلل الاحتيال والاختلاس	رقابات تمنع تسريب البيانات، مع تعزيز الالتزام بضوابط الأمن والصلاحيات
نسخة من السياسات والاجراءات الرقابية	نسخة من سياسات واجراءات المصرف، اقرارات سرية البيانات، تقارير العقوبات عن تسريب البيانات، برامج التدريب على أمن البيانات
التأكد من الالتزام بالسياسات والاجراءات الرقابية ذات العلاقة، حسب كتاب البنك المركزي بتاريخ ٧-١١-٢٠١٦	– تدقيق تحكم المصرف في البيانات، إذ تكون متاحة ومحمية وموزعة ومخزنة ومحتفظ بها وقابلة للتغيير بشكل كاف. – فحص سياسات وإجراءات منح صلاحيات الوصول إلى قواعد البيانات. – فحص سجلات النظام (Logs) للتأكد من وجود آلية لرصد عمليات تحميل أو نسخ أو إرسال البيانات. – مراجعة توقيع المستخدمين على تعهد سرية البيانات، وتنفيذ برامج التوعية الأمنية، التزام الموظفين بسياسات الحماية.

٥. الجدران نارية Firewalls فاعلة ضد الوصول غير المصرح به.	كبير	✓	منع الوصول غير المصرح به إلى أنظمة المصرف وقواعد بياناته، وتعزز مستوى أمن الشبكات وحماية الموارد الرقمية.	– البرامج المعتمدة من قبل المصرف، تقييد عناوين IP غير المصرح بها، قيام الجدار الناري بحظر الاتصالات المشبوهة، سياسات أمن الشبكة المعتمدة.
٦. تعزيز التحول الرقمي من خلال الامتثال ومتابعة الأنشطة غير الاعتيادية	متوسط	×	الالتزام بإجراءات الوقاية من مخاطر المعاملات المشبوهة	– فحص خطة معالجة مخاطر أمن البيانات – الحوادث التي تسببت بخسائر مالية أو انقطاع في العمليات أو أثرت في السمعة، (لم تحدث مثل هكذا حوادث خلال فترة البحث). – يقوم المدقق الداخلي بمراجعة إعدادات الجدار الناري والتحقق من أن قواعد التحكم بالوصول (Access Rules) مهيأة وفق مبدأ الحد الأدنى من الصلاحيات (Least Privilege). – مراجعة أدلة التحديثات الأمنية (Firmware & Security Updates) للتأكد من إجراء التحديثات الدورية وتصحيح الثغرات الأمنية.
مستوى الضعف	٥٤	١٤		

المصدر: إعداد الباحثة إستنادا للمعلومات الواردة في القوائم المالية ودليل الحوكمة

٣. ٤- تأثير مستوى تطبيق متطلب إمكانية الوصول للبيانات في إجراءات التدقيق

يعمل التدقيق الداخلي على تصميم اختبارات فحص رقمية للتحقق من سلامة بيئة نظم البيانات الالكترونية ومنع مخاطر الاختراق، عبر التأكد من عدم وجود محاولات دخول غير مصرح بها للنظام كإدخال هوية مزيفة أو توقيع رقمي وهمي، فضلاً عن اختبار فعالية الضوابط الآلية التي تُغلق الحساب تلقائياً عند تكرار الفشل في إدخال بيانات الدخول بصورة صحيحة. كما تشمل الاختبارات التحقق من عدم منح نفس الهوية التعريفية لأكثر من مستخدم، مما يحد من مخاطر إساءة الاستخدام أو تضارب الصلاحيات. كذلك ينفذ المدقق الداخلي اختبارات لحقوق الوصول للملفات التي تتضمن بيانات المعاملات، وفق مستويات الصلاحيات (للقراءة فقط، السماح بالكتابة، السماح بالتعديل)، وبما يتوافق مع احتياجات المستخدمين المخولين ومبدأ الحد الأدنى من الصلاحيات (Least Privilege). من جانب آخر، يقوم المدقق الداخلي باعداد تقارير رقابية تؤكد التزام المصرف بمتطلبات الإفصاح والرقابة، بما يدعم الامتثال الرقمي للجهات الرقابية، وذلك من خلال الاتي:

١. إعداد المصرف تقارير تلبي متطلبات رقابة ومتابعة البنك المركزي العراقي، ومن أمثلة ذلك:

أ. كشف الموجودات واندثاراتها، كشف المدينون، كشف القروض المستلمة، كشف القروض والتسليفات، كشف الدائنون، كشف رأس المال والاحتياطيات.

ب. كشف تقييم الحسابات الدائنة والمدينة بالعملة الأجنبية، وكشف الالتزامات المتقابلة لقاء العمليات المصرفية، وكشف إيرادات العمليات المصرفية، وكشف الودائع لأجل وحين الطلب.

٢. التحقق من كفاءة الأنظمة الإلكترونية المستخدمة في المصرف (وخاصة وحدة المدفوعات) والتأكد من عملها وفق ما هو مصرح به وبما ينسجم مع متطلبات التحول الرقمي، ومن ذلك: نظام التسوية الإجمالي في الوقت الفعلي (RTGS)، ونظام تسجيل السندات الحكومية (GSRS)، ونظام المقاصة الآلي (ACH).

يستعرض الجدول (٦)، مدى تطبيق متطلب إمكانية الوصول للمعلومات كأحد متطلبات حوكمة البيانات في المصرف موضوع البحث.

جدول (٦) تكامل متطلب إمكانية الوصول للبيانات مع إجراءات التدقيق الداخلي المنفذة

متطلبات حوكمة البيانات في البيئة الرقمية/ إمكانية الوصول للبيانات	تصنيف خطر عدم توفير المتطلب	التطبيق / مطبق ✓ / غير مطبق ×	تحليل المتطلب في ظل التحول الرقمي	أدلة الإثبات المطلوب فحصها	اجراءات الفحص المعتمدة عند تقييم المدقق الداخلي لمستوى تطبيق متطلبات حوكمة البيانات
١. تستلزم عملية إدارة المعلومات توفير معالجة للبيانات وايصال المعلومات إلى مستخدميها بكفاءة وفاعلية.	كبير	✓	اعتماد الأنظمة المحوسبة في إعداد التقارير المالية	برامج معالجة البيانات، سجلات المعالجة، مقابلات مع مديري الاقسام	– فحص امكانية الوصول الى قاعدة البيانات حسب الصلاحيات المحددة من قبل المصرف. إذ يوجد جدول بالصلاحيات يسمح بالتحديث، أو القراءة – اختبار الية استخراج التقارير وارسالها الى المستخدمين
٢. إنشاء هوية تعريفية للمستخدمين أو المشغلين لنظام التشغيل	صغير	✓	الموافقات الإدارية الضمان الحوكمة	معلومات عن المشغلين والمبرمجين، الغاء الحسابات غير المستخدمة	– فحص إدامة وتحديث معلومات المشغلين او المستخدمين (تتم المراجعة سنويا وعند استقالة افراد) – إدارة الوصول وتقديم البيانات. – مراجعة اعدادات كلمة المرور – تعطيل حسابات الموظفين المنقولين او ذوي الخدمة المنتهية.

٤. تغلق برمجية النظام حساب هوية المستخدم والمشغل بعد عدد معين من المحاولات الفاشلة لإدخال كلمة المرور.	متوسط	✓	٧	
منع مخاطر الاختراق وتعزيز موثوقية النظام.				
معلومات عن طبيعة كلمات المرور (عدد الرموز ونوعها نصي، او رقمي او الاثنين معا)				
– مراجعة إدامة وتحديث كلمات المرور من قبل نظام التشغيل لتجنب تكرار إستعمال نفس الكلمات مرة ثانية. – الاطلاع على التقارير التي تبين حالات الوصول غير الناجحة، واجراءات منعها.				
٣. السيطرة على حقوق الوصول لنظام التشغيل، وملفات البيانات، وإنشاء وتهيئة قواعد بيانات.	متوسط	×		
تعزيز إجراءات الحماية التقنية.				
تقارير فحص الصلاحيات الدورية المعتمدة من الإدارة، تقارير محاولات الدخول الناجحة والفاشلة، سجلات إنشاء أو تعديل قواعد البيانات.				
– فحص محاولات الوصول غير المصرحة من قبل النظام إستناداً للسياسة الأمنية. – إقتصار إدامة وتحديث مَطَمات رقابة النظام، على مستخدم بمستوى خاص لهُ صلاحية كافية. – التحقق من أن ضوابط التحكم بالوصول إلى نظام التشغيل وقواعد البيانات مصممة ومطبقة بفعالية بما يضمن: حماية سرية وسلامة البيانات. منع الوصول غير المصرح به. الالتزام بسياسات أمن المعلومات.				

المصدر. إعداد الباحثة إستنادا للمعلومات الواردة في القوائم المالية ودليل الحوكمة

٣. ٥- تأثير مستوى تطبيق متطلب مراقبة البيانات في إجراءات التدقيق

يمتلك المصرف لجنة لتقنية البيانات والإتصالات تجتمع شهرياً. مهام اللجنة مراجعة وتطوير إستخدام تقنية البيانات والاتصالات والتحقق من أمن البيانات وكفاية البنية التحتية وأنظمة البيانات والشبكات الإلكترونية وبرمجيات المصرف، والتحقق من إجراءات حفظ نسخ إحتياطية مُحدَّثة من البيانات لمواجهة كوارث محتملة وفقدان قواعد البيانات، والتأكد من جودة إدارة الشبكة الداخلية للمصرف وموقعه الإلكتروني. فضلا عن مراقبة الوصول إلى الوثائق والتقارير وكيفية إنشائها وتحديثها وطباعتها.

يستعرض جدول (٧)، مدى تطبيق متطلب مراقبة البيانات كأحد متطلبات حوكمة البيانات في المصرف.

جدول (٧) تكامل متطلب مراقبة البيانات مع إجراءات التدقيق الداخلي المنفذة

متطلبات حوكمة البيانات في البيئة الرقمية/ مراقبة البيانات	تصنيف خطر عدم توفير المتطلب	التطبيق / مُطبق ✓ / غير مُطبق ×	تحليل المتطلب في ظل التحول الرقمي	أدلة الإثبات المطلوب فحصها	اجراءات الفحص المعتمدة عند تقييم الدقق الداخلي لمستوى تطبيق متطلبات حوكمة البيانات
١. وجود توثيق كافٍ للبيانات، من خلال التسجيل في الملفات ذات العلاقة، وتحسين تتبع العمليات وأحكام الرقابة عليها، مما يدعم شفافية التقارير وسهولة تدقيقها	متوسط	✓	تنظيم البيانات وأرشفتها إلكترونياً، وتعزيز إمكانية الوصول للمعلومات	مستندات منظمة، تقارير الفحص حول الالتزام بإجراءات التوثيق، ملفات الأرشفة الرقمية أو الورقية التي تثبت تسجيل العمليات بصورة نظامية.	- يقوم التدقيق الداخلي بفحص عينة من مستندات للتحقق من الالتزام بمعايير الإبلاغ المالي من حيث الوضوح، الشمول، والدقة في عرض المعلومات. ويشمل ذلك مراجعة معاملات استلام ودفع النقد، وإجراءات فتح الحسابات بمختلف أنواعها، فضلاً عن عمليات الإيداع والسحب في حسابات التوفير والحسابات الجارية. ويتضمن الفحص التحقق من اكتمال المستندات المؤيدة، وصحة التفويضات، والتأكد من الالتزام بالإجراءات والسياسات، إضافة إلى مطابقة البيانات المسجلة مع القيود المحاسبية والأنظمة الإلكترونية، وتقييم كفاءة الضوابط الداخلية بدورة العمليات النقدية. - اختبار مسار تدفق البيانات.

٢. توفير برمجيات أرشفة الكترونية وتطبيقها في نظام معلومات الكتروني.	صغير	٧	ربط الأرشفة مع الأنظمة المحاسبية	البرامج المعتمدة في العمل	الإطلاع على المستندات المؤرشفة الكترونيا.
٣. إرسال نسخ الكترونية من المستندات للإدارة العامة خلال مدة زمنية معينة.	متوسط	×	الاحتفاظ بنسخ من أقراص تخزين البيانات.	سياسات وإجراءات الإرسال، رسائل البريد الإلكتروني للإدارة العامة من حيث تاريخ ووقت الإرسال.	– مقارنة تاريخ إعداد المستند مع تاريخ إرساله للإدارة العامة للتحقق من الالتزام بالمدة الزمنية المحددة في التعليمات. – اختيار عينة من المعاملات المرسلة إلكترونيًا ومطابقتها مع قائمة المستندات المطلوبة وفق الإجراءات. – فحص آلية حفظ النسخ الإلكترونية وإمكانية الرجوع إليها عند الحاجة لأغراض الرقابة أو التدقيق.
مستوى الضعف	١٨	٧			

المصدر: إعداد الباحثة إستنادا للمعلومات الواردة في القوائم المالية ودليل الحوكمة

٣. ٦- تأثير مستوى تطبيق متطلب متابعة وتدقيق حوكمة البيانات في إجراءات التدقيق

في ظل بيئة التحول الرقمي وتزايد الاعتماد على الأنظمة المصرفية الإلكترونية وقواعد البيانات، فإن توافر هذا المتطلب يعزّز قدرة التدقيق الداخلي على تصميم إجراءات رقابية وتدقيقية تتعلق بـ: التحقق من التزام الموظفين بسياسات أمن البيانات وإدارة الصلاحيات الرقمية، فحص كفاءة نظم التقارير الرقمية، تقييم سلامة تدفق البيانات وإتاحتها في الوقت المناسب وبصورة قابلة للمقارنة.

يرفع المدقق الداخلي تقريره عن مشكلات المصرف في تنفيذ أنشطته، ولاسيما تلك المرتبطة بجودة البيانات، وفعالية نظم المتابعة الرقمية، ومستوى الامتثال للتعليمات

الرقابية. كما يفحص التزام المصرف بتطبيق تعليمات البنك المركزي المتعلقة بنظام إدارة استمرارية الأعمال (ISO 22301)، استناداً إلى التعميم المرقم ١٢٥٩/٦/١٤ بتاريخ ٢٠٢٢/٧/٢١، لما لهذا النظام من دور في تعزيز استمرارية أعمال المصرف وتقليل الانقطاعات التشغيلية، وبما ينسجم مع متطلبات التحول الرقمي وضمان جاهزية الأنظمة والخدمات الإلكترونية.

يستعرض الجدول (٨)، مدى تطبيق متطلب متابعة وتدقيق حوكمة البيانات كأحد متطلبات حوكمة البيانات في المصرف موضوع البحث.

جدول (٨) تكامل متطلب متابعة وتدقيق حوكمة البيانات مع إجراءات التدقيق الداخلي المنفذة

متطلبات حوكمة البيانات في البيئة الرقمية/ متابعة وتدقيق حوكمة البيانات	تصنيف خطر عدم توفير المتطلب	التطبيق / مُطبق ✓ / غير مُطبق ×	تحليل المتطلب في ظل التحول الرقمي	أدلة الإثبات المطلوب فحصها	إجراءات الفحص المعتمدة عند تقييم المدقق الداخلي لمستوى تطبيق متطلبات حوكمة البيانات
١. تقييم الحوكمة المطبقة من قبل المصرف.	كبير	✓	تقييم الحوكمة بالاعتماد تقارير تحليل الضعف الرقابي	تقارير الالتزام بتعليمات البنك المركزي، دليل الحوكمة المطبق، محاضر اجتماعات مجلس الإدارة ولجان التدقيق.	فحص وجود ضوابط رقابية تمكن مجلس الإدارة من مساءلة الإدارة التنفيذية. مثال الزيادة في النقد، والتأخر في معالجة المعاملات، التأخر في تجاوز الاخطاء وعدم تكرارها. – فحص الهيكل التنظيمي للتأكد من وضوح الأدوار والمسؤوليات بين مجلس الإدارة، لجان التدقيق، الإدارة التنفيذية، ووحدات الرقابة الداخلية. – تحليل جودة الإفصاح والالتزام بمتطلبات الجهات الرقابية

٤. التحري عن الانحرافات في ادخال ومعالجة واخراج البيانات، والإجراءات المناسبة لتصحيحها.	صفير	×	اعتماد اجراءات رقابية وتصحيحية مدعومة بمسارات التدقيق
٣. الامتثال لسياسات المصرف الداخلية والمعايير الدولية والقوانين والتعليمات.	متوسط	✓	أنظمة امتثال إلكترونية تضمن التتبع، والتوثيق،
٢. تطوير الهيكل التنظيمي للمصرف ومراجعته من قبل مجلس الادارة والإدارة التنفيذية تماشياً مع المتطلبات	كبير	×	تصميم المهام والصلاحيات رقمياً ووضوح المتابعة
– الهيكل التنظيمي يعكس خطوط المسؤولية. يشمل على الاقل المستويات الرقابية مثل مجلس الادارة، ادارة المخاطر، والامتثال، والتدقيق. – مراجعة الهيكل التنظيمي المعتمد ومقارنته مع تعليمات البنك المركزي ومتطلبات الحوكمة – تقييم آلية رفع التقارير من الإدارة التنفيذية إلى مجلس الإدارة – تقييم مدى مساهمة الهيكل التنظيمي في تحقيق الكفاءة التشغيلية وإدارة المخاطر.	الهيكل التنظيمي، المسؤوليات والصلاحيات، محاضر مجلس الإدارة تتضمن اعتماد أو تعديل الهيكل التنظيمي، توصيفات وظيفية محدثة	تعليمات الامتثال من البنك المركزي	تدقيق الامور الإدارية والمالية وعلى أن تتوافر فيها الدقه والتوقيت المناسب.
	نسخ من تقارير المتابعة، تقارير معالجة النظام وتقارير الأخطاء، مقارنة المخرجات الفعلية مع النتائج المتوقعة	– الاطلاع على تقارير قسم حوكمة تقنية البيانات، التدقيق الداخلي. – مطابقة التقارير الصادرة مع مصادر بيانات مستقلة. – استخدام أدوات تحليل البيانات (Data Analytics) لاكتشاف القيم المتطرفة. – فحص عينات من المعاملات ومقارنتها بالمستندات الأصلية	

٥. يتمتع قسم التدقيق الداخلي باستقلال عمله، وعدم وجود تضارب بالمصالح.	كبير	٢	موضوعية التدقيق الداخلي وفاعلية دوره	ميثاق عمل التدقيق الداخلي	يمتلك نشاط التدقيق الداخلي ميثاقاً ينماشى مع رسالته. ولكن لا يراجع دورياً.
٦. التزام التدقيق الداخلي بالإبلاغ عن المخالفات القانونية.	كبير	٢	نظم توثيق توفر أدلة رقمية	تقارير التدقيق الداخلي	الاطلاع على تقارير قسم تقنية المعلومات والاتصالات البيانات، التدقيق الداخلي.
مستوى الضعف	٥١	١٤			

المصدر: إعداد الباحثة إستنادا للمعلومات الواردة في القوائم المالية ودليل الحوكمة

٣. ٧- تأثير مستوى تطبيق متطلب التحسين المستمر في إجراءات التدقيق

تُراجع متطلبات الحوكمة دوريا بما ينسجم مع تغيرات بيئة الأعمال والتحول الرقمي. يوجد توثيق للمعاملات، إلا أن التوثيق الإلكتروني ما يزال ينفذ بأسلوب يدوي لمستندات المصرف الورقية، فضلاً عن ضعف نظام توثيق إلكتروني، الأمر الذي يؤثر في إدارة البيانات الرقمية

يمكن للمدقق الداخلي من تصميم وتنفيذ إجراءات تدقيق رقمية للحصول بشأن الآتي:

– متابعة سياسات وإجراءات الرقابة الداخلية بصورة مستمرة عبر تطبيق آليات تقييم رقابي ذاتي، مع تحديث اجراءات تقييم السياسات والاجراءات الرقابية بما يتلاءم مع بيئة التشغيل الرقمية.

– فحص عناصر وأجهزة الشبكات والبنية التحتية الرقمية وفق قواعد تدقيق تقنية، للتحقق من عدم وجود ثغرات أمنية قد تؤدي إلى اختراق البيانات أو الأنظمة أو تعطيل العمليات المصرفية.

– بناء وتقييم فاعلية خطط التعافي من الكوارث واستمرارية الأعمال وفقاً لآليات التصميم والتشغيل والاختبار والتحديث والتدريب، بما يعزز جاهزية المصرف للاستجابة للمخاطر التشغيلية والسيبرانية في ظل التحول الرقمي.

يستعرض الجدول (٩)، مدى تطبيق متطلب التحسين المستمر كأحد متطلبات حوكمة البيانات في المصرف موضوع البحث.

جدول (٩) تكامل متطلب التحسين المستمر مع إجراءات التدقيق الداخلي المنفذة

١	يعتمد المصرف إطاراً موثقاً لحوكمة البيانات يحدد السياسات والأدوار والمسؤوليات ويخضع للفحص الدوري	متوسط	×	ربط إطار حوكمة البيانات بالاستراتيجية الرقمية للمصرف بحيث تتحول البيانات من مجرد مورد تشغيلي إلى أصل استراتيجي داعم للابتكار	تقارير التحسين المستمر، محاضر اجتماعات تحديث نظم الأرشفة، استرجاع عينة من الملفات للتحقق من سهولة الوصول.
	متطلبات حوكمة البيانات في البيئة الرقمية/ التحسين المستمر	تصنيف خطر عدم توفير المتطلب	التطبيق / مُطبق ✓ / غير مطبق ×	تحليل المتطلب في ظل التحول الرقمي	أدلة الاثبات المطلوب فحصها
					– فحص تأكيدات إدارية بشأن تنفيذ برامج التحسين المستمر. – يتحقق المدقق الداخلي من وجود آلية رسمية للتحسين المستمر عبر: ■ مراجعة تقارير التقييم الدوري التي يعدها رئيس قسم تقنية المعلومات. ■ التأكد من معالجة نقاط الضعف المكتشفة وتنفيذ الإجراءات التصحيحية. ■ متابعة مؤشرات الأداء المرتبطة بكفاءة معالجة البيانات. ■ مطابقة الوثائق مع متطلبات البنك المركزي ومعايير الحوكمة المعتمدة. ■ فحص وثيقة إطار حوكمة البيانات المعتمدة رسمياً.	اجراءات الفحص المعتمدة عند تقييم المدقق الداخلي لمستوى تطبيق متطلبات حوكمة البيانات

٤	٣	٢
جمع وتحليل ملاحظات مستخدمي البيانات (الإدارة، المدققين، منخذي القرار) لتحسين جودة المعلومات	يعتمد المصرف مؤشرات أداء لقياس جودة البيانات وكفاءة إداريتها واستخدام نتائجها في التحسين المستمر	سياسات إدارة البيانات بصورة منتظمة استناداً إلى نتائج التقييمات والتدقيقات السابقة
كبير	كبير	متوسط
٧	٧	٧
تبني منهجيات تحليل متقدمة لتحديد الأسباب الجذرية لأخطاء البيانات، أدوات تحليل السبب والأثر	تحديد المسؤوليات المتعلقة بملكية البيانات، وتطبيق سياسات أمن، واستخدام تقنيات الأتمتة والذكاء الاصطناعي في مراقبة البيانات	تعتمد إدارة البيانات في بيئة التحول الرقمي على مبدأ التحسين المستمر المستند إلى نتائج التقييمات والتدقيقات السابقة
تقارير قسم تقنية المعلومات، تقارير تقييم رضا مستخدمي البيانات	تقارير مؤشرات اداء جودة البيانات، مقابلة مسؤولي ادارة البيانات.	تقارير تقييم والتدقيق السابقة، سجلات تحديث سياسات ادارة البيانات، نسخ من السياسات قبل وبعد التحديث.
– فحص إسترجاع البيانات المطلوبة في الوقت المناسب وبكفاءة ودقة. مقارنة المشكلات المتكررة اجراءات التحسين المتخذة. – اختيار عينة من التحسينات المنفذة ومقارنتها بالوضع السابق	– الاطلاع على التقارير المرفوعة من قبل لجنة التدقيق. – اختبار عينة من البيانات للتحقق من الدقة والاكتمال والانسجام – خطط التحسين المستمر المبنية على نتائج القياس.	– محاضرة اجتماعات لجان حوكمة وادارة المخاطر، وتقارير متابعة تنفيذ التوصيات. – التحقق من تاريخ اخر تحديث للسياسة. – التحقق من مناقشة نتائج التقييمات والتدقيق. – التحقق من اشعار المستخدمين بالتحديثات الجديدة. – تقييم مدى انخفاض المخاطر المتكررة

٥	ربط نتائج تقييم مخاطر البيانات بخطط التحسين المستمر ضمن نظام إدارة مخاطر المصرف	متوسط	×	تحليل الملاحظات الوظيفية والرقابية للنظام المعلوماتي	تقارير الامتثال	– فحص المتطلبات القانونية والتنظيمية والمالية والتشغيلية. – تقارير المتابعة الدورية لإدارة المخاطر – تقارير لجنة التدقيق حول توثيق إغلاق الملاحظات وتحسين الضوابط.
٦	تقوم لجنة التدقيق بمتابعة تقييم فعالية حوكمة البيانات بصورة دورية وتقديم توصيات تطويرية	كبير	✓	تحديث سياسات إدارة البيانات، تعزيز الضوابط الداخلية الرقمية، تطوير مهارات العاملين	تقييم جودة اداء التدقيق الداخلي، خلال السنة	الاطلاع على تقارير الاداء، وخطة التدقيق بداية السنة، والبرامج المنفذة، ومستوى التقارير المرفوعة، وحجم الاخطأ المكتشفة، والتوصيات المقترحة.
مستوى الضعف		٥١	٧			

المصدر: إعداد الباحثة إستنادا للمعلومات الواردة في القوائم المالية ودليل الحوكمة

٣. ٨- مناقشة النتائج

يبين الجدول (١٠) ملخصاً للمنهج المقترح لتقويم الإلتزام بحوكمة بيانات للمصرف موضوع البحث.

جدول (١٠) خلاصة نتائج الالتزام بحوكمة البيانات من خلال متطلباتها للمصرف موضوع البحث

ت	متطلبات حوكمة البيانات	إجمالي درجات المتطلب	مصرف موضوع البحث			
			مجموع الضعف الكبير	مجموع الضعف لمتوسط	مجموع الضعف الصغير	مستوىالضعف الكلي	إجمالي درجات التقييم
١	تنظيم وتصنيف البيانات.	٥٥	–	١	١	١١	٤٤
٢	سلامة ونزاهة البيانات.	٥١	١	١	–	١٧	٣٤
٣	أمن البيانات.	٥٤	–	٢	–	١٤	٤٠
٤	إمكانية الوصول للبيانات.	٢٨	–	١	–	٧	٢١
٥	مراقبة البيانات.	١٨	–	١	–	٧	١١
٦	متابعة وتدقيق حوكمة البيانات.	٥١	١	–	١	١٤	٣٧

٧	A	–	B	C	D
التحسين المستمر	عدد نقاط الضعف المكتشفة	الوزن النسبي للضعف	مجموع نقاط تقويم الضعف (مجموع نقاط الضعف الفعلية×مستوى تقويم الضعف (كبير ١٠، متوسط ٧، ضعيف ٤	الحد الأقصى للضعف (عدم تلبية أية متطلب)	نسبة تقويم الضعف إلى الحد الأقصى (B ÷ C) × ١٠٠
٥١			٣٠٨		٪١٠٠
–	٢	١٠	٢٠	٢٠٠	٪١٠
٣	٩	٧	٦٣	١٤٧	٪٤٢.٨٦
–	٢	٤	٨	٢٤	٪٣٣.٣
٧			٧٧		
٤٤					

المصدر: إعداد الباحثة إستنادا للجداول المعروضة سابقا

في ضوء جدول (١٠) خلاصة النتائج، يمكن إستعراض الاتي:

١. تشير النتائج إلى أن تصنيف البيانات والمستندات وفقا للوظائف الإدارية والتشغيلية لا يقتصر على كونه إجراءً تنظيميا شكليا، بل يمثل إطارا منهجيا يسهم في تعزيز الحوكمة المعلوماتية، ويُحسن من كفاءة إدارة دورة حياة البيانات، ويقلل من التكرار والازدواجية في المعالجة.

٢. أظهرت عملية توزيع البيانات حسب فئات المعالجة وجود بنية تنظيمية واضحة تعكس مستوى متقدما من النضج الرقمي، إذ يتيح هذا التصنيف تحديد طبيعة البيانات،

وآليات التعامل معها، ومستوى حساسيتها، بما يدعم ضبط عمليات الوصول والاستخدام ويعزز إدارة المخاطر.

٣. كشفت النتائج أن السياسات والمعايير الرقمية المعتمدة تؤدي دورا محوريا في ضمان دقة البيانات وموثوقيتها، إذ تسهم في توحيد إجراءات الإدخال، والتحديث، والتحقق، والمراجعة الدورية، مما ينعكس إيجابا على جودة المعلومات المتاحة لصناع القرار.

٤. بينت الدراسة يساعد مواءمة السياسات الرقمية مع المتطلبات القانونية والتنظيمية لا تعكس فقط الامتثال التشريعي، بل تعزز الشفافية المؤسسية والمساءلة، وتحد من المخاطر القانونية والتشغيلية، الأمر الذي يدعم استدامة الأداء المؤسسي في البيئة الرقمية.

٥. تشير النتائج إلى أن تقييم المدقق الداخلي لمستوى عدم الالتزام بتعليمات الحوكمة الصادرة عن البنك المركزي يستند بصورة أساسية إلى تحليل منهجي لطبيعة المخالفات القانونية والأخطاء المحاسبية المكتشفة إلكترونيا ضمن الملفات والنظم المحاسبية للمصرف. ويعكس هذا التقييم درجة وعي المدقق الداخلي بأبعاد المخاطر المرتبطة بعدم الامتثال، ومدى قدرته على توظيف أدوات التحليل الرقمي في رصد الانحرافات وتحديد أنماطها وتوقيت حدوثها.

٦. كما أظهرت النتائج فعالية التقييم ترتبط مباشرا بكفاءة نظم الرقابة الرقمية المعتمدة في المصرف، إذ تسهم هذه النظم في تعزيز القدرة على الاكتشاف المبكر للمخالفات والحد من تكرارها، بما يدعم الالتزام بتعليمات الحوكمة ويقلل من مخاطر عدم الامتثال. ويؤكد ذلك الدور المحوري للرقابة الرقمية في دعم عمل التدقيق الداخلي وتعزيز بيئة الرقابة المؤسسية.

٧. تشير النتائج إلى أن تحديد محاولات الوصول غير المصرح به إلى الأنظمة وقواعد البيانات، في ضوء السياسات الأمنية الرقمية المعتمدة، يمثل مؤشرًا جوهريًا على فاعلية منظومة الضبط الرقمي داخل المنظمة. وقد تبين أن رصد هذه المحاولات يسهم في

الكشف المبكر عن نقاط الضعف المحتملة في بيئة نظم المعلومات، ويعزز من مستوى الامتثال للضوابط الرقابية المرتبطة بإدارة الهوية والصلاحيات.

٨. كما أظهرت النتائج أن الاعتماد على تلك المؤشرات يدعم توجيه إجراءات التدقيق الداخلي نحو توسيع نطاق الاختبارات الإلكترونية، بهدف التحقق من قصر صلاحيات الوصول إلى قواعد البيانات ونظم التشغيل على مستخدمين محددين وفق مستويات تفويض واضحة ومحددة مسبقًا. ويسهم ذلك في تعزيز سلامة المعاملات وحماية البيانات ضمن بيئة التحول الرقمي، بما يرسخ مبادئ الحوكمة والأمن السيبراني.

٤- المبحث الرابع/ الإستنتاجات والتوصيات

٤. ١- الإستنتاجات

خلص البحث لمجموعة إستنتاجات أهمها:

١. الحاجة لتقييم تطورات حوكمة بيانات المصرف ودراسة تأثيرها في أنشطة الاعمال اليومية.

2. تفعيل إدارة داعمة للامتثال وحماية البيانات من خلال مسارات التدقيق الإلكترونية.

٣. الالتزام بممارسات حوكمة البيانات رقمياً، بما يدعم اتخاذ القرار.

٤. يساعد إنموذج التقييم المقترح في تعزيز اجراءات التدقيق الداخلي عند تقييم حوكمة البيانات، مما ينعكس على المعلومات المفصح عنها التزاما بالمتطلبات والقوانين والتشريعات التي تدعم الحوكمة وتقليل من مخاطر التحريفات.

٤. ٢- التوصيات

١. تطوير قنوات اتصال فعالة لتدفق البيانات داخل المصرف.

٢. تصنيف البيانات المالية رقمياً وفق احتياجات المستخدمين

٣. كفاية الإفصاح عن تكاليف تقنية المعلومات ومنافعها ومخاطرها.

٤. تعزيز التحول الرقمي من خلال الامتثال ومتابعة الأنشطة غير الاعتيادية

٥. السيطرة على حقوق الوصول لنظام التشغيل، وملفات البيانات، وإنشاء وتهيئة قواعد بيانات.

٦. تطبيق الانموذج المستخدم في الورقة البحثية وبما يعزز حوكمة البيانات في اجراءات التدقيق.

المصادر العربية

١. امين، هروال محمد، زيان عبد الحق، (٢٠٢٣)، "واقع وظيفة التدقيق الداخلي في ظل التحول الرقمي: قراءة تحليلية في التجربة الرقمية الهولندية"، مجلة البحوث في العلوم المالية والمحاسبة، المجلد ٨، العدد ١.

٢. حمني، حورية، ابتسام طوبال، (٢٠٢٠)، "دور حوكمة تكنلوجيا المعلومات في إنجاح التحول الرقمي"، مجلة العلوم الانسانية لجامعة ام البواقي، المجلد ٧، العدد ٣.

٣. الإسدي، ذكرى مهدي صالح، (٢٠٢٢)، "إنموذج مقترح لإعداد تقارير مالية في ظل حوكمة المعلومات/ دراسة تطبيقية"، إطروحة مقدمة إلى كلية الإدارة والإقتصاد– الجامعة المستنصرية، جزء من متطلبات نيل شهادة الدكتوراه فلسفة في المحاسبة.

٤. رشوان،عبد الرحمن محمد، (٢٠٢٢)، "دور التحول الرقمي في تحسين جودة عملية التدقيق الداخلي "، مجلة دراسات محاسبية ومالية، مجلد ١٧، عدد ٥٩.

٥. الوثيري، عائشه خالد محمد، (٢٠٢٤)، "أثر التحول الرقمي على التدقيق الاستراتيجي: الدور الوسيط لجودة التدقيق الداخلي في البنوك التجارية الاردنية"، رسالة ماجستير في المحاسبة، قسم العلوم المالية والمحاسبية/ كلية الأعمال، جامعة الشرق الاوسط.

References

1. Brous, P., Janssen, M., Vilminko-Heikkinen, R., (2016), “Activities: A Systematic Review of Data Governance Principles”, In: IFIP International Federation for Information Processing.

2. Burmeister, Fabian , Dominik Huth, Paul Drews, (2020), “Enhancing Information Governance with Enterprise Architecture Management: Design Principles Derived from Benefits and Barriers in the GDPR Implementation”.

3. Central Bank of Iraq (CBI), (2019), "Governance controls and institutional management of information and communications technology in the banking sector", Pp. 1-72.
4. Institute of Internal Auditor (IIA), (2024), "Global Internal Audit Standards".
٥. The Institute of Internal Auditors (IIA), (2020), "Data Governance/ Providing assurance regarding data risk management".
6. Karimallah, Khawla, Hicham Drissi, (2024), "Assessing the Impact of Digitalization on Internal Auditing Function", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 15, No. 6.
7. Jabur, Hanan Salih, Yusra hadi Ibrahim, (2025), "Using the digital transformation techniques for improving the internal audit process", Al-Ghary Journal of Economic and Administrative Sciences Vol. 21, No.4.
8. Liaw, Siaw-Teng, Christopher Pearce, Harshana Liyanage, Gladys SS Liaw, (2014), "An integrated organisation-wide data quality management governance framework: theoretical and information underpinnings". Research article, theoretical underpinnings. Inform Prim Care. Vol. 21, No 4
9. Pazarskis Michail, Alexander Kostyuk, (2024), "Corporate Governance: Future Avenues and Perspectives", International Online Conference (November 28, 2024).
10. Thompson, N., Ravindran, R., Nicosia, S., (2015), "Government data does not mean data governance: Lessons learned from a public sector application audit", In: Government Information Quarterly, Vol. 32, No. 3, Pp. 316–322.
11. Smallwood, Robert. F., (2016), "Information governance: concepts, strategies and best practices". Hoboken, NJ: Wiley & Sons.