The Administration & Economic College Journal
For Economics & Administration & Financial Studies
Vol.18,N 1, P P - 208-224
ISSN PRINT 2312-7813
ISSN ONLINE 2313-1012
رقم الايداع 1557 لسنة 2011
مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية
المجلد 18 العدد1كانون الثاني 2026 ص ص 208- 224

إطار مقترح للمحافظ الالكترونية في تعزيز الرقابة والشفافية في البيئة المالية الرقمية (المصارف الأهلية نموذجاً)

A Proposed Audit Framework for E-Wallets to Enhance Control and Transparency in the Digital Financial Environment (private banks as a model)

م.د. شهلاء نعمه عنون
Shehlaa.neamah@atu.edu.iq
جامعة الفرات الاوسط التقنية
الكلية التقنية الادارية/كوفة

المستخلص:

يهدف هذا البحث إلى بناء إطار تدقيق مقترح للمحافظ الإلكترونية يسهم في تعزيز الرقابة والشفافية في البيئة المالية الرقمية، وذلك استجابةً للتوسع المتزايد في استخدام المحافظ الإلكترونية وما يرافقه من ارتفاع مستويات الاحتيال، وغسل الأموال، والاختراقات، وضعف حماية البيانات، وانطلاقاً من حاجة هذا الموضوع إلى تحليل علمي ومنهجي يكشف مكامن الخلل ويقترح معالجات عملية اعتمد البحث المنهج الوصفي التحليلي ومنهج دراسة الحالة من خلال تحليل بيئة عمل المحافظ الإلكترونية في ثلاثة مصارف أهلية عراقية، وتشخيص واقع الضوابط التشغيلية وبرامج التدقيق الحالية والكشف عن أوجه القصور المرتبطة بضعف تتبع العمليات الإلكترونية واعتماد إجراءات تدقيقية تقليدية لا تتلاءم مع طبيعة المخاطر الرقمية، كما حلّل البحث البرنامج التدقيقي المطبق فعلياً لتحديد فجواته مقارنة بمتطلبات التدقيق المبني على المخاطر، ثم صاغ الباحث إطاراً تدقيقياً متكاملاً يربط بين المخاطر الرقمية والضوابط الرقابية وإجراءات التدقيق المناسبة لكل فئة خطر انطلاقاً من النتائج التشخيصية وما أظهرته من فجوات مؤثرة في فعالية التدقيق حيث سعى البحث إلى التحقق من جدوى الإطار المقترح عملياً واختبار الإطار المقترح تطبيقياً من خلال مقارنته بالبرنامج القائم، وأظهرت النتائج تحسناً واضحاً في قدرة الكشف عن الاحتيال، وتحديد العمليات المشبوهة، ورصد الثغرات الأمنية، إضافة إلى رفع مستوى الشفافية وإمكانية تتبع العمليات وبناءً على ما تقدّم من نتائج وتحليلات منهجية، تتبلور أهمية الإطار المقترح ودوره في معالجة فجوات التدقيق القائمة، ليأتي هذا البحث ليسهم في تقديم نموذج عملي لتطوير برامج التدقيق على المحافظ الإلكترونية، ويدعم الجهات الرقابية والمصارف في مواجهة التحديات الرقمية وتحسين جودة الرقابة المالية.

الكلمات المفتاحية: المحافظ الإلكترونية – التدقيق المبني على المخاطر – الرقابة الرقمية – الشفافية – مكافحة غسل الأموال.

Abstract

This study aims to develop a proposed audit framework for e-wallets that enhances control and transparency within the digital financial environment. The increasing adoption of e-wallets has been accompanied by higher levels of fraud, money laundering risks, cybersecurity threats, weak data protection, and limited user safeguards. Using a descriptive-analytical approach combined with a case study methodology, the research examines the operational reality of e-wallet systems in three Iraqi private banks, identifying key weaknesses in internal controls and in the existing audit programs. The analysis shows that current audit practices rely heavily on traditional accounting-based procedures that lack the ability to trace digital transactions, detect behavioral anomalies, or address cybersecurity vulnerabilities. Based on these findings, the researcher develops an integrated risk-based audit framework that links digital risks to appropriate internal controls and tailored audit procedures. The proposed framework incorporates digital tracing, automated data analysis, AML red-flag detection, access-control evaluation, and end-to-end process verification. Experimental application of the framework demonstrates substantial improvements in fraud detection, identification of suspicious patterns, exposure of security weaknesses, and enhancement of transaction transparency. The study provides a practical model that financial institutions and regulatory authorities can use to strengthen their oversight of e-wallet operations and reduce digital financial risks.

Keywords: E-wallets – Risk based auditing - Digital control - Transparency Anti-money laundering.

1- المقدمة:

شهدت السنوات الأخيرة توسعاً كبيراً في استخدام المحافظ الإلكترونية كأحد أهم أدوات الدفع في البيئة المالية الرقمية، إذ أسهمت في خفض تكاليف التعاملات وتسريع إنجازها وتوسيع قاعدة الشمول المالي لفئات واسعة من الأفراد والمنشآت، غير أنّ هذا التوسع ترافق مع ارتفاع ملموس في مخاطر الاحتيال وغسل الأموال وتمويل الأنشطة غير المشروعة وتسرب البيانات وضعف حماية حقوق المستخدمين، الأمر الذي دفع الجهات الرقابية والمؤسسات المالية إلى تشديد الاهتمام بمتطلبات الرقابة والشفافية في أنظمة الدفع الرقمية وتعزيز دور التدقيق المتخصص في هذا المجال، وفي هذا السياق يكتسب موضوع إطار تدقيق مقترح للمحافظ الإلكترونية أهميته بوصفه استجابة عملية لحاجة بيئات العمل الرقمية إلى أدوات تدقيق تتلاءم مع طبيعة العمليات الإلكترونية وتعقيداتها وتدعم قدرة المؤسسات على الوقاية من المخاطر واكتشافها مبكراً وترسيخ الثقة في منظومة المدفوعات غير النقدية، حيث يركز هذا البحث على بناء إطار تدقيق مقترح للمحافظ الإلكترونية بوصفه المتغير المستقل وقياس أثره في تعزيز مستوى الرقابة والشفافية في البيئة المالية الرقمية بوصفهما المتغير التابع وذلك من خلال تحديد مكونات الإطار وأبعاده وإجراءاته وآليات تنفيذه ومؤشرات تقييمه وربطها بواقع الممارسة المهنية في بيئات عمل المحافظ الإلكترونية، وينطلق البحث من دراسة حالة تطبيقية يتم فيها أولاً تشخيص واقع عمل المحافظ الإلكترونية والإجراءات الرقابية والتدقيقية المعمول بها حالياً وتحليل المخاطر الرئيسة المرتبطة بها، كما يجري تحليل منهجي لبرنامج التدقيق الذي يعتمده مراقب الحسابات الخارجي أو الداخلي على هذه المحافظ للكشف عن أوجه القصور في تصميم إجراءات التدقيق أو تنفيذها أو توثيقها بالتوازي مع دراسة الأطر التشريعية والتنظيمية والمعايير المهنية ذات الصلة ومقارنتها بالممارسة الفعلية للكشف عن الفجوات وصولاً إلى صياغة إطار تدقيق متكامل قابل للتطبيق والتقويم يعتمد على إعادة بناء خطوات التدقيق ومجالات الفحص واختبارات الرقابة والجوهر وتحديد مؤشرات كمية ونوعية لقياس مستوى الرقابة والشفافية في نشاط المحافظ الإلكترونية بما يسمح بعرض الإطار المقترح على بيئة ميدانية مناسبة وتحليل نتائجه واستخلاص التوصيات التي يمكن أن تفيد الجهات الرقابية والمؤسسات المالية ومقدمي خدمات الدفع الرقمي في تعزيز متانة منظومة الرقابة والتدقيق على المحافظ الإلكترونية.

1-1 مشكلة البحث:

تتمثل مشكلة البحث في أن التوسع المتسارع في استخدام المحافظ الإلكترونية في البيئة المالية الرقمية لا يرافقه في كثير من الأحيان تطوير مكافئ في أنظمة التدقيق والرقابة التي تتلاءم مع طبيعة هذه المحافظ وخصائصها التقنية حيث تعتمد العديد من المؤسسات المالية ومقدمي خدمات الدفع الرقمي على إجراءات رقابية وتجميعية تقليدية لا تغطي بشكل كاف مخاطر الاحتيال والاختراق الإلكتروني وغسل الأموال وضعف حماية بيانات المستخدمين وعدم كفاية الإفصاح والشفافية في عرض العمليات والرسوم والسياسات للمستفيدين والجهات الرقابية إذ يظهر هذا القصور في غياب إطار تدقيق متكامل ومحدد للمحافظ الإلكترونية يحدد بوضوح الأهداف الرقابية ومجالات الفحص وأدوات التدقيق القائمة على البيانات الرقمية ومؤشرات قياس مستوى الرقابة والشفافية الأمر الذي يخلق فجوة بين حجم المخاطر القائمة والآليات المتاحة لإدارتها ومتابعتها ويحتم الحاجة إلى بناء إطار تدقيق مقترح يمكن تطبيقه وتقويمه في البيئة المالية الرقمية، ويكون سؤال البحث الرئيس: ما أثر تطبيق إطار تدقيق مقترح للمحافظ الإلكترونية في تعزيز الرقابة والشفافية في البيئة المالية الرقمية؟

1-2 أهمية البحث:

تظهر الأهمية النظرية لهذا البحث في مساهمته في بناء إطار علمي منظم لتدقيق المحافظ الإلكترونية في ظل التحول نحو البيئة المالية الرقمية حيث إنه يقدم مفهوما أكثر دقة لعلاقة التدقيق بالرقابة والشفافية في أنظمة الدفع الرقمية ويحدد أبعاد إطار التدقيق ومتغيراته ومؤشراته بشكل واضح وقابل للقياس كما إنه يسد فراغا في الأدبيات المحاسبية والرقابية التي ما زالت تركز في أغلبها على الأنشطة التقليدية ويضيف بعدا جديدا يتعلق بتوظيف أدوات التدقيق في بيئة تقوم على البيانات الضخمة والعمليات الفورية والمعاملات غير الملموسة ويساعد بناء هذا الإطار في فتح مسار لبحوث لاحقة يمكن أن تختبر أجزاءه أو تطوره أو تقارنه بأطر أخرى في مجالات مالية رقمية مختلفة.

أما الأهمية التطبيقية فتتمثل في أن إطار التدقيق المقترح يمكن أن يقدم أداة عملية للجهات الرقابية والمصارف ومقدمي خدمات الدفع الرقمي لتقييم مستوى الرقابة والشفافية في أنظمة المحافظ الإلكترونية وتحسينهما كما يساعد الإطار متخذي القرار في التعرف على نقاط الضعف في إجراءات التدقيق الحالية وترتيب المخاطر الرقمية حسب أولويتها وتصميم اختبارات تدقيق أكثر ملاءمة لطبيعة العمليات الرقمية وإنه يدعم جهود الامتثال للمعايير والقوانين الخاصة بمكافحة غسل الأموال وتمويل الأنشطة غير المشروعة وحماية بيانات المستخدمين من خلال إجراءات تدقيق واضحة وخطوات تنفيذ محددة ومؤشرات أداء قابلة للمتابعة الأمر الذي يسهم في تعزيز ثقة المستخدمين والجهات الرقابية في خدمات المحافظ الإلكترونية.

1-3 أهداف البحث:

1- بناء إطار تدقيق مقترح للمحافظ الإلكترونية يحدد المكونات والأبعاد والإجراءات اللازمة لتعزيز الرقابة والشفافية في البيئة المالية الرقمية.
2- تشخيص واقع التدقيق والرقابة على المحافظ الإلكترونية ورصد أهم أوجه القصور والمخاطر المرتبطة بها في البيئة المالية الرقمية.
3- تحليل أثر تطبيق إطار التدقيق المقترح للمحافظ الإلكترونية في تحسين مستوى الرقابة وكفاءة إجراءاتها وزيادة مستوى الشفافية في عرض المعلومات والعمليات.
4- تقديم مجموعة من التوصيات العملية للجهات الرقابية والمصارف ومقدمي خدمات الدفع الرقمي لاعتماد وتفعيل إطار التدقيق المقترح وتطوير السياسات والضوابط المرتبطة بالمحافظ الإلكترونية.

1-4 فرضيات البحث:

الفرضية الرئيسة: لا يوجد أثر لتطبيق إطار التدقيق المقترح للمحافظ الإلكترونية في تعزيز مستوى الرقابة والشفافية في البيئة المالية الرقمية.

الفرضية الفرعية الأولى: لا يوجد أثر لتطبيق إطار التدقيق المقترح للمحافظ الإلكترونية في تحسين مستوى الرقابة على عمليات المحافظ الإلكترونية في البيئة المالية الرقمية.

الفرضية الفرعية الثانية: لا يوجد أثر لتطبيق إطار التدقيق المقترح للمحافظ الإلكترونية في رفع مستوى الشفافية في عرض والإفصاح عن معلومات وعمليات المحافظ الإلكترونية في البيئة المالية الرقمية.

1-5 الدراسات السابقة:

اتجهت الأدبيات نحو بناء نماذج تقنية وتنظيمية لتعزيز أمان المحافظ الإلكترونية والمعاملات الرقمية والرقابة عليها ومنها:

1- تبحث دراسة Ibitoye 2025 بعنوان نظم ذكاء اصطناعي متعددة الوكلاء لمراقبة الاحتيال في عمليات التكنولوجيا المالية العابرة للحدود في بيئة المدفوعات الرقمية، مجتمع الدراسة يتمثل في بيئات المدفوعات

الرقمية العابرة للحدود ومقدمي خدمات FinTech والجهات الرقابية ذات الصلة، نوع الدراسة تطوير نموذج تقني تطبيقي يربط الأمن بالشفافية والامتثال، وخلصت إلى أن المراقبة متعددة الوكلاء تدعم كشف الاحتيال بشكل مبكر وتحسن قابلية التتبع وتدعم متطلبات الامتثال التنظيمي.

2- تناولت دراسة Al-Qubati 2024 بعنوان نموذج جاهزية المحافظ الإلكترونية الآمنة مرحلة ما قبل الإطلاق الفعلي للخدمة، مجتمع الدراسة يتمثل في المؤسسات التي تخطط لإطلاق محافظ إلكترونية أو تطويرها ضمن بنية تقنية وتنظيمية محددة، نوع الدراسة بناء نموذج جاهزية تقني تنظيمي يحدد المتطلبات السابقة للتشغيل، توصلت النتائج إلى أن نجاح التشغيل الآمن يعتمد على جاهزية أمن المعلومات والبنية التقنية والحوكمة والإجراءات التنظيمية قبل الإطلاق.

3- ناقشت دراسة Kamis 2024 بعنوان منافع المحافظ الإلكترونية وتحدياتها في عالم ما بعد الجائحة واقع الاستخدام الواسع للمحافظ الإلكترونية، مجتمع الدراسة يتمثل في بيئة المستخدمين والجهات المقدمة للخدمة في مرحلة ما بعد الجائحة وسوق المدفوعات الرقمية، نوع الدراسة تحليل وصفي لواقع المنافع والتحديات والمخاطر، أظهرت النتائج اتساع الاعتماد على المحافظ مع تصاعد مخاطر الخصوصية والاحتيال والحاجة إلى رقابة أشد وإجراءات حوكمة أكثر صرامة.

4- قدمت دراسة Oriento 2023 بعنوان مخاطر المعاملات غير النقدية عبر المحافظ الإلكترونية والحماية القانونية للمستخدمين زاوية قانونية وحقوقية، مجتمع الدراسة يتمثل في مستخدمي المحافظ الإلكترونية والأطراف المتعاملة معهم ضمن معاملات غير نقدية وما ينشأ عنها من نزاعات، نوع الدراسة تحليل قانوني معياري لأطر الحماية وحقوق المستخدم، خلصت إلى أن فجوات التنظيم والحماية تزيد النزاعات والاحتيال وأن وضوح الحقوق وآليات التعويض والإفصاح يقلل المخاطر ويرفع ثقة المستخدم.

5- عرضت دراسة Nordin 2024 بعنوان إطار حماية مستخدمي مؤسسات النقود الإلكترونية منظور التنظيم والحوكمة والترخيص، مجتمع الدراسة يتمثل في مؤسسات النقود الإلكترونية ومستخدميها والجهات المنظمة، نوع الدراسة اقتراح إطار تنظيمي حمائي يركز على الترخيص والحوكمة وحماية الأموال الإلكترونية، توصلت إلى أن قوة الحماية ترتفع عندما تتكامل متطلبات الترخيص والحوكمة مع آليات فصل أموال العملاء وإدارة المخاطر والإشراف.

6- قدمت دراسة Karthikeyan 2025 بعنوان مراجعة شاملة لأساليب كشف غسل الأموال الذكية في البنوك والمحافظ الإلكترونية مراجعة بحثية تقنية، مجتمع الدراسة يشمل قطاع البنوك والمحافظ الإلكترونية من حيث تقنيات الرصد والامتثال ومراقبة العمليات، نوع الدراسة مراجعة منهجية لأساليب التعلم الآلي وتحليل الأنماط السلوكية للكشف عن الاشتباه، خلصت إلى أن النماذج الذكية ترفع القدرة على اكتشاف الأنماط المعقدة لكنها تتطلب بيانات عالية الجودة وحوكمة بيانات وتفسير نتائج يدعم الامتثال.

7-ناقشت دراسة Wibisono 2025 بعنوان التحول نحو اقتصاد رقمي نزيه عبر تحسين المعاملات غير النقدية العلاقة بين التوسع غير النقدي والنزاهة العامة، مجتمع الدراسة يتمثل في الاقتصاد الرقمي والقطاع العام والخاص من زاوية تتبع التدفقات المالية والحد من الفساد، نوع الدراسة تحليل سياساتي يربط أدوات الدفع غير النقدية بتحسين التتبع والشفافية، أظهرت النتائج أن توسيع المعاملات غير النقدية يحسن قابلية التتبع ويقلل فرص الفساد عندما ترافقه حوكمة ورقابة فعالة. والجدول التالي يبين أوجه الشبه والاختلاف:

الدراسة	محور التركيز	مجتمع الدراسة	نوع الدراسة	أبرز النتائج	أوجه الشبه مع بحثك	أوجه الاختلاف عن بحثك
Ibitoye 2025	مراقبة الاحتيال بالذكاء الاصطناعي متعددة الوكلاء مع ربط الأمن الشفافية الامتثال	بيئات FinTech العابرة للحدود ومقدمو الدفع الرقمي	تطوير نموذج تقني تطبيقي	كشف مبكر وتحسن تتبع ودعم امتثال	تشترك في هدف خفض الاحتيال وتعزيز الشفافية	لا يقدم إطار تدقيق مهني وخطوات تدقيق ومؤشرات قياس كمية للرقابة والشفافية ولا يختبره كبرنامج تدقيق داخل مصارف عراقية
Al-Qubati	جاهزية المحافظ	مؤسسات تخطط	نموذج	الجاهزية الأمنية	يشترك في	يركز على ما قبل الإطلاق

2024	الإلكترونية الآمنة قبل الإطلاق	لإطلاق محفظة وبناها التنظيمية والتقنية	جاهزية تقني تنظيمي	والتنظيمية شرط لنجاح التشغيل	الاهتمام بأمن المعلومات والضوابط	وليس على تدقيق التشغيل الفعلي ولا على مقارنة برنامج تدقيق قائم ببرنامج مقترح
Kamis 2024	منافع وتحديات المحافظ بعد الجائحة	سوق المستخدمين ومقدمي الخدمة بعد الجائحة	تحليل وصفي	تصاعد مخاطر الخصوصية والاحتيال والحاجة لرقابة	يشترك في تشخيص المخاطر الدافعة لتطوير الرقابة	لا يبني إطار تدقيق تفصيلي ولا يربط المخاطر بضوابط وإجراءات تدقيق قابلة للقياس
Oriento 2023	المخاطر القانونية وحماية المستخدم في معاملات المحفظة	مستخدمون وأطراف معاملات غير نقدية ونزاعات	تحليل قانوني	تقوية الحماية والحقوق تقلل النزاعات والاحتيال	يشترك في دعم الشفافية وحماية المستخدم	يركز على التشريع والحقوق أكثر من إجراءات التدقيق الرقمي والأدلة الرقمية وتتبع العملية من البداية للنهاية
Nordin 2024	إطار حماية مؤسسات النقود الإلكترونية عبر الترخيص والحوكمة	مؤسسات نقود إلكترونية ومستخدمون وجهات منظمة	إطار تنظيمي مقترح	الترخيص الحوكمة حماية الأموال ترفع الحماية	يشترك في تركيز الامتثال والحوكمة	لا يقدم برنامج تدقيق عملي ولا يضم أدوات تتبع رقمي وتحليل بيانات وتطبيق تجريبي على مصارف
Karthikeyan 2025	كشف غسل الأموال الذكي بالتعلم الآلي وتحليل الأنماط	بنوك ومحافظ إلكترونية من زاوية AML	مراجعة شاملة	الأساليب الذكية ترفع الكشف وتتطلب حوكمة بيانات	يشترك في محور غسل الأموال والتحليل السلوكي	مراجعة تقنية وليست إطار تدقيق متكامل يحدد اختبارات رقابة وجوهر ومؤشرات شفافية ويطبق على حالة عراقية
Wibisono 2025	المعاملات غير النقدية كأداة للحد من الفساد عبر التتبع	اقتصاد رقمي وجهات عامة وخاصة	تحليل سياساتي	التتبع يحسن النزاهة مع حوكمة فعالة	يشترك في فكرة التتبع والشفافية	لا يصوغ خطوات تدقيق وإجراءات اختبار ولا يقيس التحسن عبر مقارنة برنامج قائم وبرنامج مقترح

ميزة البحث عن الدراسات السابقة:

تتمثل ميزة هذا البحث عن الأدبيات السابقة في أنه لا يكتفي بعرض مخاطر المحافظ الإلكترونية أو تقديم نماذج أمنية وتشريعية عامة كما ركزت عليه معظم الدراسات السابقة، بل ينتقل إلى بناء إطار تدقيق تطبيقي متكامل ومحدد لعمليات المحافظ الإلكترونية يربط بصورة مباشرة بين فئات المخاطر الرقمية والضوابط الرقابية وإجراءات التدقيق المناسبة لكل خطر ضمن مصفوفة تشغيلية قابلة للتنفيذ والقياس، مع إدراج أدوات تتبع رقمي وتحليل بيانات ورصد أنماط غسل الأموال وتقييم صلاحيات الوصول واختبار سلامة دورة العملية من البداية حتى الإغلاق، ثم يختبر هذا الإطار ميدانياً عبر دراسة حالة في ثلاثة مصارف أهلية عراقية ويقدّم دليلاً مقارناً على التحسن عند تطبيقه مقابل البرنامج القائم من خلال نتائج كمية واضحة في قدرة الكشف والإنذار ورصد الثغرات ورفع شفافية تتبع العمليات، وبذلك يسد فجوة معرفية وتطبيقية في الأدبيات التي تناولت المحافظ من زاوية الأمن أو الامتثال دون تقديم برنامج تدقيق عملي مبني على المخاطر ومقاس على خصائص العمليات الرقمية.

1-6 منهجية البحث:

يعتمد البحث المنهج الاستقرائي والاستكشافي عبر تطبيقه على بيئة عمل فعلية للمحافظ الإلكترونية في أحد المصارف الأهلية العراقية إذ يبدأ الباحث بمراجعة الأدبيات والمعايير المهنية والمتطلبات التنظيمية لبناء إطار نظري يحدد خصائص المحفظة الإلكترونية ومراحل تشغيلها ومخاطرها الرئيسة ثم يوصف برنامج التدقيق المطبق فعلياً على عمليات المحفظة ويحلل في ضوء خريطة المخاطر لتحديد جوانب القصور في تتبع مسار العملية الرقمية وتغطية غسل الأموال وضوابط الدخول والتشفير والسجلات الإلكترونية ثم بعد ذلك يصاغ برنامج تدقيق مقترح مبني على المخاطر يتضمن توصيف دورة العمل ومصفوفة تربط المخاطر

بالضوابط وإجراءات التدقيق وقوائم تحقق للامتثال وأمن المعلومات مع توظيف أدوات تدقيق بمساعدة الحاسوب لتحليل البيانات وتتبع العمليات ويعرض البرنامج على خبراء وممارسين لتقويمه وتعديله ثم يطبق تجريبياً عبر مقارنة نتائج البرنامج القائم والبرنامج المقترح وتوثيق الفروق نوعياً لاستخلاص الاستنتاجات والتوصيات.

7-1مجتمع وعينة البحث:

يتكون مجتمع البحث من المصارف الأهلية العراقية التي تعتمد خدمة المحافظ الإلكترونية وتمارس عمليات تشغيلها ورقابتها في إطار أنظمة الدفع الرقمي، ولأغراض دراسة الحالة تم اختيار ثلاث مصارف أهلية هي بنك بغداد، والمصرف الأهلي العراقي، ومصرف الخليج التجاري لتمثل عينة البحث بصورة قصدية استنادا إلى معايير علمية تتمثل في امتلاك هذه المصارف برامج فعلية لتشغيل المحافظ الإلكترونية، وارتفاع حجم وعدد العمليات المنفذة عبر هذه المحافظ مقارنة بمصارف أخرى، إضافة إلى تنوع قاعدة عملائها وتغطيتها لشرائح مختلفة من المستخدمين، فضلا عن تباين حجمها التنظيمي بما يسمح برصد فروق محتملة في تطبيق الرقابة والتدقيق، وتوفر درجة مناسبة من التعاون وإمكانية الوصول إلى المعلومات والوثائق التدقيقية اللازمة للتحليل. وبناء على ذلك تعتمد الدراسة على تحليل برنامج التدقيق الذي يطبقه مدقق الحسابات الداخلي أو الخارجي في هذه المصارف على عمليات المحافظ الإلكترونية وتشخيص أوجه القصور في تصميمه أو تنفيذه أو توثيقه، ثم مقارنته بما يقدمه برنامج تدقيق مقترح يعاد بناؤه وفق منهج التدقيق المبني على المخاطر ومتطلبات البيئة الرقمية بهدف بيان مقدار التحسن الممكن تحقيقه في جودة الرقابة وكفاءة متابعة العمليات الإلكترونية في المصارف المشمولة بالدراسة.

2. الإطار النظري والمفاهيمي:

2-1 المحور الأول: المحفظة الإلكترونية في البيئة المالية الرقمية

2-1-1 مفهوم المحفظة الإلكترونية وطبيعتها التشغيلية

تمثل المحفظة الإلكترونية إحدى أدوات الدفع الرقمية التي تعمل من خلال بيئة إلكترونية تعتمد على الهواتف الذكية وأنظمة الاتصال الحديثة، بهدف تنفيذ عمليات مالية تشمل الدفع والتحويل واستلام الأموال دون الحاجة للتعامل النقدي المباشر، وتُعد المحافظ أحد أهم ركائز التحول الرقمي في القطاع المالي لما توفره من سرعة في إنجاز المعاملات وتقليل كلف التشغيل ورفع مستوى الشمول المالي، وتستند المحافظ الإلكترونية في طبيعتها التشغيلية إلى بيئة متكاملة تشمل المستخدم، والمصرف أو جهة الإصدار، ومقدم خدمة الدفع، إضافة إلى شبكة من قواعد البيانات التي تحفظ عمليات المستخدم وتسلسلها وعمليات المصادقة والتحقق الأمني كما أوضح (Al-Qubati, 2024, 4) عند مناقشة نموذج الجاهزية التقنية للمحافظ، ويعتمد نجاح تشغيل المحفظة على كفاءة البنية الرقمية واستقرار الاتصال والقدرة على حماية بيانات المستخدمين، الأمر الذي يفسّر التركيز المتزايد على تطوير الأطر التشغيلية والرقابية المصاحبة لها انسجاماً مع ما أشار إليه الشبلي (2023) حول أثر التحول الرقمي في إعادة تشكيل بيئة العمل الحكومي والمالي.

جدول 1: مقارنة بين الوظائف الأساسية للمحافظ الإلكترونية والعمليات المصرفية التقليدية

البعد	المحافظ الإلكترونية	العمليات المصرفية التقليدية
سرعة التنفيذ	فوري	يتطلب وقتاً لمعالجة الطلب
طبيعة السجلات	رقمية ومباشرة	ورقية أو مزيج ورقي–رقمي
سهولة الاستخدام	عالية عبر الهاتف	أقل لارتباطها بالمراجعة المباشرة

مخاطر الأمان	مرتفعة رقمياً	مرتفعة مالياً وتقليدياً

المصدر: إعداد الباحث بالاعتماد على الدراسات السابقة

2-1-2 البنية التقنية والوظيفية للمحافظ الإلكترونية

تعتمد المحفظة الإلكترونية على منظومة تقنية تشمل واجهات التطبيقات، وأنظمة الهوية الرقمية، وخوارزميات التحقق والمصادقة، إضافة إلى قواعد بيانات متصلة تحفظ جميع التحويلات والحركات المالية، وهو ما يجعلها عرضة لمخاطر تقنية خاصة تتطلب بناء ضوابط قوية، وقد أشار Nordin وآخرون (2024) إلى أن أي نظام نقدي إلكتروني يحتاج إلى بنية تقنية ثابتة تتضمن التشفير، وإدارة الامتيازات، وسياسات حماية الأموال الإلكترونية لضمان سلامة المعاملات وحماية المستخدمين أما الوظائف التشغيلية للمحافظ فتتكون من عدة مراحل تمسّ دورة حياة العملية المالية، ابتداءً من تسجيل المستخدم والتحقق من هويته مروراً بتنفيذ العمليات عبر خوادم الدفع وانتهاءً بإغلاق الحركة وتسجيلها بما يضمن إمكانية تتبعها وهي عناصر أكد (Oriento, 2023, 112) أهميتها في حماية المتعاملين قانونياً وتقليل النزاعات، وتفرض هذه البنية متطلبات رقابية خاصة تتعلق بإدارة الوصول للنظام والتحكم بامتيازات المستخدمين وفحص سلامة البرمجيات دورياً، بما ينسجم مع ما أشار إليه (Ibitoye, 2025, 28) عند مناقشة نظم المراقبة الذكية متعددة الوكلاء للكشف عن الاحتيال في بيئات الـFinTech.

جدول 2 أبرز المكونات التقنية في المحافظ الإلكترونية وعلاقتها بالمخاطر

المكون التقني	وظيفته الرئيسة	نوع الخطر المرتبط
الهوية الرقمية	التحقق من المستخدم	انتحال الهوية
التشفير	حماية البيانات	الاختراق والتجسس
قواعد البيانات	حفظ العمليات	فقدان السجلات أو تلاعبها
أنظمة الامتيازات	التحكم بالمستخدمين	إساءة الاستخدام الداخلي

المصدر: إعداد الباحث بالاعتماد على الدراسات السابقة

2-1-3 خصائص عمليات المحافظ الإلكترونية وأثرها في العمل المصرفي

تتميز عمليات المحافظ الإلكترونية بكونها آنية، ومرتبطة بأنظمة تشغيل ذكية تعمل على مدار الساعة مما يخلق بيئة عمليات ذات حجم كبير من البيانات التي تتطلب مراقبة دقيقة وتحليلاً متواصلاً لسلوك المستخدمين، وتُعد سرعة العمليات وغياب التفاعل البشري المباشر من أبرز الخصائص التي تعزز الكفاءة من جهة، وترفع مستوى المخاطر الرقمية من جهة أخرى كما أوضح (Wibisono, 2025, 717) في تحليله لدور المعاملات الرقمية في مكافحة الفساد عبر تعزيز التتبع المالي، ويؤثر هذا التحول في طبيعة العمل المصرفي من خلال تقليص الحاجة إلى الإجراءات التقليدية وتوسيع دور الأنظمة الرقمية في التسجيل والمتابعة، مما يعزز الاعتماد على الرقابة الإلكترونية والاختبارات الرقمية بدلاً من المراجعة اليدوية، وهو ما يتفق مع ما ذكره الاعمر (2023) بشأن دور الحوكمة الإلكترونية في رفع كفاءة الأداء المالي عبر تقليل الأخطاء وتعزيز الشفافية، وتُظهر خصائص هذه العمليات ضرورة امتلاك المصارف لبرامج تدقيق متخصصة تستند إلى تقييم المخاطر وتحليل البيانات الضخمة، خصوصاً مع بروز تحديات مثل عمليات غسل الأموال الرقمية، والتي ناقشها (Karthikeyan, 2025, 9) بوصفها من أكثر الأنشطة تطوراً في بيئة الدفع الإلكتروني.

2- 2المحور الثاني: مخاطر المحافظ الإلكترونية ومتطلبات الرقابة

2-2-1 مخاطر الاحتيال والاختراق وغسل الأموال في المحافظ الإلكترونية

تتعرض المحافظ الإلكترونية لمستوى مرتفع من مخاطر الاحتيال بسبب طبيعتها القائمة على العمليات الفورية وضعف التفاعل المباشر بين المستخدم والمؤسسة المالية، إذ تشمل هذه المخاطر استخدام هويات رقمية مزيفة واستغلال ثغرات التطبيقات لإجراء تحويلات غير مصرح بها، إضافة إلى محاولات اختراق الأنظمة أو إعادة توجيه العمليات عبر برمجيات خبيثة، وقد أشار Karthikeyan (2025, 11) إلى أن تقنيات الاحتيال في بيئات الدفع الرقمي تطورت بشكل كبير، خاصة عبر استخدام خوارزميات التلاعب والروبوتات التي تخفي مصدر العملية، مما يصعّب على الأنظمة التقليدية اكتشافها في الوقت المناسب، كما تمثل عمليات غسل الأموال أحد أخطر التحديات في المحافظ الإلكترونية نتيجة سهولة فتح الحسابات وتعدد القنوات المرتبطة بها وضعف الربط بين المستخدمين وهوياتهم الحقيقية الأمر الذي يجعل تتبع التدفقات المالية أكثر تعقيداً، ويدعم هذا ما أكده(2025, 29) Ibitoye بشأن صعوبة مراقبة التدفقات في البيئات المالية العابرة للحدود، حيث تتطلب هذه العمليات أنظمة ذكاء اصطناعي متقدمة لضبط الأنماط غير الطبيعية واكتشاف التحويلات المشبوهة، وتظهر كذلك مخاطر ناتجة من التلاعب في البيانات أو اعتراضها أثناء انتقالها بين المستخدم ونظام المعالجة وهو ما يزيد أهمية بناء ضوابط رقابية تعتمد على تشفير قوي وأنظمة تحقق متعددة الخطوات كما شدد Al-Qubati (2024, 4)في نموذج الجاهزية التقنية للمحافظ.

جدول 3. أنواع مخاطر الاحتيال والاختراق وغسل الأموال الأكثر شيوعاً في المحافظ الإلكتروني

نوع الخطر	الوصف	مستوى الخطورة
الاحتيال بالهويات	إنشاء حسابات مزوّرة أو استخدام بيانات مسروقة	مرتفع
الاحتيال في العمليات	تحويلات غير مصرح بها داخل النظام	مرتفع
الاختراق السيبراني	الوصول غير المشروع لبيانات النظام	مرتفع
غسل الأموال	تمرير تحويلات متعددة لإخفاء المصدر	مرتفع

المصدر: إعداد الباحث بالاعتماد على الدراسات السابقة

2-2-2 مخاطر حماية البيانات والخصوصية واستمرارية الخدمة

تتضمن المحافظ الإلكترونية بيانات حساسة تشمل هويات المستخدمين وسجلات العمليات والمعلومات البنكية الأمر الذي يجعلها هدفاً رئيسياً للهجمات السيبرانية، وتبرز مخاطر الخصوصية نتيجة ضعف سياسات إدارة البيانات أو قصور آليات التشفير والتخزين وهو ما يدعم ما ذكره (Hassan et al., 2022, 7) عند فحصهم لثغرات المحافظ الأكثر استخداماً، حيث أظهروا قدرة بعض البرمجيات على استخراج بيانات المستخدم عبر نقاط ضعف في التطبيقات، كما تتأثر المحافظ بمخاطر التشغيل المرتبطة بتوقف الخدمة بسبب أعطال تقنية أو ضغط عالٍ على الخوادم مما يسبب تعطلاً في قدرة المستخدمين على تنفيذ عملياتهم المالية، ويضعف الثقة في النظام، وترتبط هذه التحديات ضعفاً بغياب خطط استمرارية الأعمال وبروتوكولات النسخ الاحتياطي الفعال وهو ما يتفق مع تحليل Oriento (2023, 111) حول المخاطر القانونية للمستخدمين عند حدوث توقف في الخدمة أو ضياع السجلات الإلكترونية، وتزيد هذه المخاطر عندما تكون البنية التحتية للمحافظ منشأة دون معايير تقنية صارمة كما ناقش Nordin (2024, 58) في إطار حماية المستخدمين للمؤسسات النقدية الإلكترونية وتشير هذه الأدبيات إلى ضرورة دمج آليات حماية البيانات ضمن العمليات اليومية إضافة إلى تصميم تدفق معلومات آمن يُمكّن من اكتشاف أي محاولة اختراق أو تسريب.

جدول 4. أبرز مصادر مخاطر حماية البيانات والخصوصية في المحافظ الإلكترونية

مصدر الخطر	أثره على المستخدم	أثره على المؤسسة
ضعف التشفير	تسريب البيانات الحساسة	فقدان الثقة والمساءلة القانونية
سوء إدارة الامتيازات	الوصول غير المصرح به	زيادة مخاطر الاحتيال الداخلي
ثغرات البرمجيات	اختراق الحسابات والعمليات	تكاليف إصلاح مرتفعة
ضعف النسخ الاحتياطي	ضياع السجلات	توقف العمليات وتضرر السمعة

المصدر: إعداد الباحث بالاعتماد على الدراسات السابقة

2 3-2-دور الأطر التشريعية والرقابية في ضبط مخاطر المحافظ الإلكترونية

تؤدي الأطر التشريعية والرقابية دوراً محورياً في الحد من مخاطر المحافظ الإلكترونية من خلال وضع قواعد تنظيمية صارمة تحكم عمل مقدمي الخدمة، وتحدد مسؤوليات المصارف وشركات الدفع وتفرض إجراءات اعرف عميلك والإبلاغ عن العمليات المشبوهة ومتطلبات حماية البيانات، وقد أكدت الدراسات مثل Oriento (2023, 112) أن الإطار القانوني يمثل خط الدفاع الأول للمستخدمين خصوصاً مع تزايد حالات الاحتيال والنزاعات المرتبطة بالمحافظ، كما يوضح الاعمر (2023، 595) أن الحوكمة الرقمية ترفع مستوى الانضباط المالي وتقلل الأخطاء الناتجة من غياب الضوابط مما ينعكس مباشرة على كفاءة المتابعة والرقابة في المؤسسات المالية، ويؤكد Karthikeyan (2025, 22) أن التشريعات يجب أن تركز على تحديث سياسات مكافحة غسل الأموال لتشمل الأنماط الرقمية المعقدة التي تُستغل في المحافظ الإلكترونية نظراً لسرعة العمليات وصعوبة تتبعها، وتُظهر الأدبيات كذلك أهمية وضع معايير تشغيل تقنية موحدة تتعلق بالتشفير وإدارة الهوية وحماية الامتيازات وتدقيق العمليات وهو ما يتوافق مع ما طرحه Nordin (2024, 55) حول ضرورة امتلاك المؤسسات النقدية الإلكترونية إطار حماية متكامل يتمتع بقوة قانونية ملزمة.

2-3 المحور الثالث: التدقيق في بيئة المحافظ الإلكترونية وإطار التدقيق المقترح

3-2-1 التدقيق المبني على المخاطر في أنشطة الدفع الرقمي

يعتمد التدقيق في بيئة المحافظ الإلكترونية على منهج التدقيق المبني على المخاطر والذي يتطلب تحليل بيئة التشغيل الرقمية وتحديد مصادر الخطر الأكثر تأثيراً على سلامة العمليات وجودة التقارير المالية ويُعد هذا المنهج أكثر ملاءمة من الأساليب التقليدية لأن المحافظ تعتمد على عمليات فورية ومعاملات ذات حجم كبير ما يفرض الحاجة إلى إجراءات تدقيق تركز على تقييم الضوابط الإلكترونية وتحديد الثغرات التقنية ومراقبة الأنماط غير الطبيعية، وقد أكد (Ibitoye et al., 2025) أهمية الانتقال إلى نظم مراقبة ذكية تعتمد على تحليل سلوك العمليات للكشف المبكر عن الاحتيال في البيئات الرقمية العابرة للحدود، مما يدعم تطبيق منهج التدقيق المبني على المخاطر، كما ترتبط فعالية هذا المنهج بقدرة المؤسسة على تحديث خرائط المخاطر بشكل مستمر وفقاً لتغير التهديدات السيبرانية، وهو ما يتسق مع تحليل (Kamis et al., 2024, 4) حول تغير طبيعة مخاطر المحافظ الإلكترونية بعد الجائحة وتوسع استخدامها، ويظهر كذلك أن تطبيق هذا المنهج يعزز قدرة المدققين على تقييم الامتثال للمتطلبات التنظيمية المتعلقة بمكافحة غسل الأموال وحماية البيانات، وهو ما أكده (Nordin et al., 2024, 57) عند مناقشة الإطار التنظيمي للمؤسسات النقدية الإلكترونية.

جدول 5. علاقة أنواع المخاطر بإجراءات التدقيق المبني على المخاطر

نوع الخطر	إجراء التدقيق المناسب	النتيجة المتوقعة
الاختراق السيبراني	تقييم ضوابط التشفير والاختبار الأمني	خفض احتمالية الوصول غير المشروع
الاحتيال	تحليل أنماط العمليات واستخدام أدوات ذكية	كشف العمليات غير الطبيعية
غسل الأموال	وتتبع التحويلات KYC فحص الامتثال لإجراءات	تحديد العمليات المشبوهة

المصدر: إعداد الباحث بالاعتماد على الدراسات السابقة

2-3-2 متطلبات تطوير برامج التدقيق على المحافظ الإلكترونية

تتطلب طبيعة المحافظ الإلكترونية تطوير برامج تدقيق قادرة على التعامل مع الحجم الكبير للبيانات الرقمية، وسرعة العمليات، وتعدد الأطراف المرتبطة بتنفيذ العملية الواحدة، ويشمل تطوير هذه البرامج دمج أدوات تحليل بيانات متقدمة تمكن المدقق من فحص جميع العمليات وليس عينات محدودة، وهو ما أشار إليه (Karthikeyan et al., 2025, 13) عند مناقشة أساليب كشف غسل الأموال التي تعتمد على تحليل الأنماط الرقمية المعقدة، كما يستلزم تطوير البرنامج وجود فهم عميق لدورة عمل المحفظة الإلكترونية من حيث التسجيل وأذونات الوصول وتنفيذ العمليات وإغلاق الحركة لأن أي خلل في هذه الدورة قد يؤدي إلى مخاطر تشغيلية ومالية، وقد أظهر (Hassan et al., 2022, 9) أن جزءاً كبيراً من المخاطر التقنية في المحافظ الإلكترونية ناتج عن ضعف الاختبارات الأمنية قبل الإطلاق أو بعد التحديثات الدورية مما يعزز الحاجة إلى تضمين الفحص التقني ضمن إجراءات التدقيق، ويعد بناء قواعد تحقق إلكترونية (Checklists) خاصة بضوابط أمن المعلومات ومتطلبات الامتثال التنظيمي ضرورة لضمان شمولية الفحص الرقابي وهو ما يتوافق مع توجهات (Oriento et al., 2023, 112) في تعزيز الحماية القانونية للمستخدمين.

جدول 6. متطلبات تطوير برنامج تدقيق فعال في بيئة المحافظ الإلكترونية

المطلب	أهميته	أثره على جودة التدقيق
أدوات تحليل البيانات	فحص شامل للعمليات	رفع معدل الاكتشاف
فهم الدورة الرقمية	تقييم المخاطر بدقة	تجنب الثغرات التشغيلية
اختبارات أمنية	حماية النظام	خفض الاختراقات
قوائم تحقق تنظيمية	الامتثال للقوانين	تقليل المخاطر القانونية

المصدر: إعداد الباحث بالاعتماد على الدراسات السابقة

2-3-3 مكونات وأبعاد إطار التدقيق المقترح لتعزيز الرقابة والشفافية:

يقوم إطار التدقيق المقترح على مجموعة من المكونات التي تشمل تحديد دورة التشغيل الرقمية للمحفظة وبناء مصفوفة تربط بين المخاطر والضوابط والإجراءات المناسبة واستخدام الأدوات الرقمية لكشف التلاعب والانحرافات، ويرتكز الإطار على دمج اختبارات الرقابة واختبارات الجوهر بطريقة تتناسب مع طبيعة العمليات الإلكترونية بحيث يبدأ بفهم النظام ثم تقييم الضوابط التقنية ثم تحليل البيانات المالية وغير المالية ثم إصدار الأحكام المهنية بناءً على الأدلة الرقمية، وقد أكد (Nordin et al., 2024, 57) أهمية وجود إطار حماية شامل يشمل الجوانب التشغيلية والقانونية لضمان حماية المستخدمين واستقرار النظام وهو ما يعد جزءاً أساسياً من الإطار المقترح كما يدعم الإطار تعزيز الشفافية من خلال تتبع مسار كل عملية منذ إنشائها وحتى إغلاقها وتوثيق كل خطوة بطريقة رقمية قابلة للمراجعة وهو ما يتسق مع رؤية Wibisono

(et al., 2025, 719) في استخدام المعاملات غير النقدية كوسيلة لتعزيز النزاهة ومنع الفساد عبر قابلية التتبع، ويستند الإطار كذلك إلى تحليل متطلبات الأمان والتدقيق المستمر وذلك لملاحقة تحديثات التطبيقات والتهديدات السيبرانية الجديدة مما يضمن الحفاظ على مستوى رقابة مستدام يلائم بيئة الدفع الرقمي المتغيرة.

3. الإطار التحليلي:

يستند الإطار التحليلي لهذا البحث إلى تطبيق منهج دراسة الحالة ضمن بيئة عمل فعلية للمحافظ الإلكترونية في المصارف الأهلية العراقية، وذلك من خلال الاعتماد على مزيج من التحليل الوصفي والفحص الميداني لبرامج التدقيق المطبقة داخل المؤسسة محل الدراسة إذ بدأ التحليل بجمع البيانات الأولية عبر مراجعة السجلات الإلكترونية للمحافظ والاطلاع على الأدلة التدقيقية ودراسة الوثائق التنظيمية والسياسات المعتمدة إضافة إلى مقابلات مباشرة مع المدققين الداخليين والخبراء العاملين في مجال المخاطر الرقمية، كما تم دمج البيانات الثانوية من الأدبيات المهنية والمعايير الدولية الخاصة بالتدقيق الرقمي ومكافحة غسل الأموال، واعتمد الباحث على تحليل متسلسل يبدأ بتشخيص البيئة الرقمية ثم تقييم برنامج التدقيق القائم ثم بناء إطار مقترح وتطبيقه بشكل تجريبي لقياس الفروق بين النتائج المتحققة قبل وبعد تطبيق البرنامج، وقد تم تنظيم المخرجات ضمن أربعة جداول رئيسية تعكس مراحل التحليل المختلفة:

الجدول 7. تحليل واقع بيئة المحافظ الإلكترونية في المصارف الأهلية العراقية (مرحلة التشخيصية)

البعد التحليلي	الوضع الفعلي في المؤسسة محل الدراسة	الدلالات على الرقابة الداخلية
هيكل النظام	وجود وحدات تقنية منفصلة وضعف في تتبع العملية	ضعف القدرة على تتبع مسار العملية الإلكترونية كاملة
مستوى التعرض للاحتيال	مرتفع بسبب ضعف إجراءات التحقق من الهوية	ازدياد احتمالية تنفيذ عمليات غير مصرح بها
ضوابط مكافحة غسل الأموال	اعتماد فحص يدوي دون تحليل نمط العمليات	ضعف القدرة على كشف السلوك المالي غير الطبيعي
أمن البيانات	تشفير أساسي وضوابط وصول تقليدية	ارتفاع احتمالات الاختراق وتسريب البيانات
استمرارية الخدمة	غياب دورة نسخ احتياطي كاملة	تعرض النظام للتوقف وفقدان البيانات

المصدر: إعداد الباحث بالاعتماد على تحليل المصارف

يوضح الجدول 7 صورة دقيقة لواقع بيئة المحافظ الإلكترونية في المؤسسة محل الدراسة حيث يُبين وجود فجوة واضحة بين متطلبات التشغيل الرقمي السليم والواقع الفعلي المعمول به وتُظهر البيانات أن هيكل النظام يعاني من التجزئة وضعف الترابط بين الوحدات وهو ما ينعكس سلباً على القدرة على تتبع مسار العملية الإلكترونية من بدايتها إلى نهايتها، كما يشير الجدول إلى ارتفاع مستوى التعرض للاحتيال بسبب ضعف أنظمة التحقق من الهوية الأمر الذي يسمح بإمكانية تنفيذ عمليات غير مشروعة، أما فيما يتعلق بضوابط مكافحة غسل الأموال فقد تبين اعتماد المؤسسة على فحص يدوي غير قائم على تحليل الأنماط السلوكية مما يقلل من قدرة النظام على اكتشاف الأنشطة المشبوهة، ويبرز كذلك قصور في حماية البيانات نتيجة استخدام أساليب تشفير تقليدية وضعف ضوابط الصلاحيات وأخيراً، فإن غياب خطط نسخ احتياطي متكاملة يعرّض النظام لمخاطر فقدان البيانات أو توقف الخدمات ويؤسس هذا التحليل لضرورة وجود إطار تدقيق رقمي أكثر قوة وشمولية.

الجدول 8. تحليل برنامج التدقيق القائم مقارنة بمتطلبات التدقيق المبني على المخاطر

مكوّن التدقيق	برنامج التدقيق القائم	المتطلب وفق التدقيق المبني على المخاطر	حجم الفجوة
التخطيط	التركيز على الأرصدة المحاسبية	التركيز على فهم دورة العملية الرقمية	كبيرة
تقييم المخاطر	محصور بالمخاطر المالية	يشمل المخاطر السيبرانية وغسل الأموال والبيانات	كبيرة
اختبارات الرقابة	إجراءات يدوية قائمة على عينات	اختبارات آلية تشمل كل العمليات	كبيرة جداً
جمع الأدلة	أوراق عمل تقليدية	سجلات رقمية ومسارات إلكترونية للعمليات	كبيرة
إجراءات غسل الأموال	فحص تقليدي بسيط	تحليل سلوكي للعمليات وأنماطها	فجوة حرجة

المصدر: إعداد الباحث بالاعتماد على تحليل المصارف

يعرض الجدول 8 المقارنة بين برنامج التدقيق الحالي في المؤسسة ومتطلبات التدقيق المبني على المخاطر ويكشف عن فجوات جوهرية تعوق تحقيق رقابة فعالة على المحافظ الإلكترونية فالبرنامج القائم يركز على فحص الأرصدة المحاسبية أكثر من اهتمامه بفهم دورة العملية الرقمية مما يحد من قدرته على التعامل مع المخاطر التقنية، كما تُظهر البيانات أن تقييم المخاطر ينحصر في المخاطر المالية التقليدية دون امتداد إلى المخاطر السيبرانية أو مخاطر غسل الأموال الرقمية التي تُعد عناصر محورية في بيئة المحافظ وتعتمد الاختبارات الحالية على إجراءات يدوية تستخدم عينات محدودة بينما يتطلب التدقيق الرقمي فحصاً شاملاً لجميع العمليات باستخدام أدوات تحليل البيانات، كما أن عملية جمع الأدلة تظل تقليدية وغير مستندة إلى سجلات رقمية أو مسارات إلكترونية واضحة مما يقلل من موثوقية النتائج، ويؤكد الجدول أيضاً وجود فجوة حرجة في إجراءات مكافحة غسل الأموال حيث يفتقر البرنامج إلى التحليل السلوكي الذي يُعد أساسياً في كشف الأنشطة المشبوهة وتدعم هذه النتائج الحاجة لتطوير برنامج تدقيق رقمي متقدم.

الجدول 9. مصفوفة ربط المخاطر بالضوابط وإجراءات التدقيق في الإطار المقترح

فئة الخطر	الضابط المطلوب	إجراء التدقيق المقترح	النتيجة المتوقعة
الاحتيال الإلكتروني	المصادقة متعددة العوامل	فحص سجلات الدخول وتحليل الشذوذ	خفض العمليات غير المصرح بها
مخاطر غسل الأموال	مراقبة فورية للعمليات	تحليل أنماط التحويل عبر خوارزميات	زيادة كشف العمليات المشبوهة
خروقات البيانات	تشفير قوي وضبط صلاحيات	اختبار اختراق ومراجعة امتيازات المستخدمين	تقليل احتمالية تسريب البيانات
الأعطال التشغيلية	نسخ احتياطي واستعادة منتظمة	مراجعة دورة النسخ الاحتياطي وإجراء محاكاة تشغيل	رفع مستوى استمرارية الخدمة

المصدر: إعداد الباحث بالاعتماد على تحليل المصارف

يمثل الجدول 9 جوهر الإطار المقترح من خلال ربط فئات المخاطر بالضوابط المناسبة وإجراءات التدقيق الملائمة لكل منها ويوضح التحليل أن مخاطر الاحتيال الإلكتروني يمكن الحد منها عبر تطبيق

ضوابط قوية مثل المصادقة متعددة العوامل وفحص سجلات الدخول وتحليل الشذوذ مما يسهم في خفض العمليات غير المصرح بها أما مخاطر غسل الأموال فيقترح الإطار استخدام المراقبة الفورية والتحليل الخوارزمي لأنماط التحويل وهو ما يعزز القدرة على كشف الأنشطة غير القانونية. وفيما يتعلق بخروقات البيانات فإن الاعتماد على التشفير المتقدم وضبط الصلاحيات يرافقه تنفيذ اختبارات اختراق دورية لضمان سلامة النظام ويعالج الإطار أيضاً مخاطر الأعطال التشغيلية من خلال مراجعة منهجية لدورات النسخ الاحتياطي ومحاكاة إجراءات الاستعادة للتأكد من استمرارية الخدمة، ويؤكد هذا الجدول أن الإطار المقترح يوفر معالجة شاملة ومباشرة لكل فئة من المخاطر عبر إجراءات تدقيق واضحة، مما يرفع من مستوى الرقابة والشفافية.

الجدول 10. نتائج التطبيق التجريبي للبرنامج المقترح مقارنة بالبرنامج القائم

البعد المُقَيَّم	نتائج البرنامج القائم	نتائج البرنامج المقترح	مستوى التحسن
كشف الاحتيال	اكتشاف حالتين فقط	اكتشاف 11 حالة	عالي
إنذارات غسل الأموال	غياب الإنذارات الممنهجة	ظهور 7 إنذارات قائمة على النمط	عالٍ جداً
نقاط الضعف الأمنية	مشكلات بسيطة 3	مشكلة تقنية وأمنية محددة 14	حرج
فحص النظام التشغيلي	غير متوفر	فحص كامل لدورة النظام	عالي
مؤشرات الشفافية	تتبع جزئي للعمليات	تتبع كامل للعمليات الإلكترونية	عالٍ جداً

المصدر: إعداد الباحث بالاعتماد على تحليل المصارف

يسلط الجدول 10 الضوء على النتائج الفعلية للتطبيق التجريبي للبرنامج المقترح بالمقارنة مع البرنامج القائم، وهو ما يوفر دليلاً عملياً على فعالية الإطار التدقيقي الجديد وتوضح النتائج أن برنامج التدقيق الحالي تمكن من اكتشاف حالتين فقط من حالات الاحتيال بينما كشف البرنامج المقترح إحدى عشرة حالة عند تطبيقه على نفس البيانات مما يشير إلى ارتفاع كبير في قدرة الكشف، وفيما يتعلق بإنذارات غسل الأموال فقد أظهر الإطار المقترح سبع إشارات مبنية على التحليل السلوكي في حين لم يولد البرنامج القديم أي إنذارات ذات معنى، كما كشف الإطار المقترح أربع عشرة نقطة ضعف أمنية متنوعة مقارنة بثلاث نقاط فقط في النظام التقليدي، مما يعكس شمولية الفحص الرقمي، وأثبت الإطار أيضاً إمكانية فحص النظام التشغيلي بالكامل مقابل غياب هذا الجانب في البرنامج السابق وتعد أبرز النتائج تحسين مستوى الشفافية من تتبع جزئي إلى تتبع كامل لمسار العملية. وتؤكد هذه النتائج مجتمعة قوة الإطار المقترح وفعاليته في تحسين الرقابة.

وباختبار الفرضيات نجد:

- الفرضية الرئيسة: نص الفرضية لا يوجد أثر لتطبيق إطار التدقيق المقترح للمحافظ الإلكترونية في تعزيز مستوى الرقابة والشفافية في البيئة المالية الرقمية
- الاستنتاج رفض الفرضية الصفرية وقبول الفرضية البديلة بوجود أثر.

التحليل أظهر تطبيق الإطار المقترح انتقال التدقيق من فحص نتائج محاسبية مجمعة إلى تتبع مسار العملية الرقمية وربط المخاطر بالضوابط وباختبارات تدقيق محددة مع أدلة إلكترونية قابلة للتحقق وهذا يرفع فعالية الرقابة ويزيد شفافية التتبع ويقلل فجوة المعلومات بين الإدارة والمدقق والجهات التنظيمية كما ان الأثر الاقتصادي يظهر عبر خفض خسائر الاحتيال وتقليل تكلفة عدم الامتثال وتحسين الثقة بالخدمة الرقمية بما يدعم استمرارية الاستخدام وتوسعها.

- الفرضية الفرعية الأولى: نص الفرضية لا يوجد أثر لتطبيق إطار التدقيق المقترح للمحافظ الإلكترونية في تحسين مستوى الرقابة على عمليات المحافظ الإلكترونية في البيئة المالية الرقمية
- الاستنتاج رفض الفرضية الصفرية وقبول وجود أثر في تحسين الرقابة.

التحليل تحسن مستوى الرقابة لأن الإطار المقترح يقدم مصفوفة تشغيلية تربط كل خطر بضابط وبإجراء تدقيق مناسب ويغطي نقاط التحكم الحرجة في دورة المحفظة مثل فتح الحساب والتحويل والسحب والدفع والإغلاق كما يعالج جوانب كانت غالباً أقل حضوراً في البرامج التقليدية مثل ضوابط الدخول والصلاحيات وحفظ السجلات وقابلية التتبع، النتيجة رقابة أكثر وقائية بدلاً من رقابة لاحقة ما يقلل احتمالات الاختراق والتلاعب ويرفع جودة الضبط الداخلي.

- الفرضية الفرعية الثانية: نص الفرضية لا يوجد أثر لتطبيق إطار التدقيق المقترح للمحافظ الإلكترونية في رفع مستوى الشفافية في عرض والإفصاح عن معلومات وعمليات المحافظ الإلكترونية في البيئة المالية الرقمية
- الاستنتاج رفض الفرضية الصفرية وقبول وجود أثر في رفع الشفافية.

التحليل رفع الإطار المقترح الشفافية عبر تعزيز الإفصاح القابل للتحقق عن العمليات من خلال أدلة رقمية وسجلات إلكترونية منظمة ومؤشرات قياس واضحة يمكن تتبعها ومقارنتها عبر الزمن عندما تصبح المعلومات قابلة للتتبع من المصدر إلى القيد إلى الأثر النهائي تقل مساحة الغموض في التقارير وتتحسن قابلية المراجعة والتفسير أمام الإدارة والرقابة والجهات التنظيمية وهذا يخفض مخاطر السمعة والغرامات ويقوي الثقة لدى المستخدمين والشركاء لأنه يحسن قابلية مساءلة الخدمة الرقمية.

الاستنتاجات:

1- توصل البحث من خلال التحليل النظري والتطبيقي ودراسة الحالة إلى مجموعة استنتاجات رئيسية تؤكد الحاجة الملحة لاعتماد إطار تدقيق متخصص يتناسب مع طبيعة المخاطر الرقمية في بيئة المحافظ الإلكترونية.
2- أظهر تشخيص الواقع العملي وجود قصور واضح في البنية التقنية وفي نظام الرقابة الداخلية للمؤسسة محل الدراسة، تمثل في ضعف تتبع مسار العمليات الإلكترونية واعتماد أساليب تحقق تقليدية غير قادرة على منع الاحتيال أو كشف الأنشطة المشبوهة في الوقت المناسب.
3- بيّنت نتائج تحليل برنامج التدقيق القائم أن إجراءات التدقيق الحالية تركز على الجوانب المحاسبية التقليدية وتفتقر إلى الأدوات الرقمية اللازمة لفحص حجم العمليات الكبير وتعقيدها، إضافة إلى غياب الربط بين تقييم المخاطر وتحديد طبيعة الاختبارات المناسبة مما أدى إلى انخفاض مستوى الكشف عن نقاط الضعف الجوهرية.
4- أظهر التطبيق التجريبي للإطار التدقيقي المقترح أن اعتماد نهج التدقيق المبني على المخاطر واستخدام أدوات تحليل البيانات والاعتماد على مصفوفة تربط بين المخاطر والضوابط وإجراءات التدقيق يؤدي إلى رفع مستوى القدرة على اكتشاف الاحتيال وغسل الأموال والاختراقات التقنية.
5- أثبت الإطار المقترح قدرته على تحسين مستوى الشفافية من خلال تعزيز إمكانية تتبع العملية الإلكترونية بالكامل وتوثيق الأدلة الرقمية بشكل منظم وتشير هذه النتائج إلى ضرورة تحديث أنظمة التدقيق في المصارف الأهلية العراقية لتواكب التحول الرقمي السريع ولتقلل الفجوة بين حجم المخاطر القائمة والآليات المستخدمة لإدارتها.

التوصيات:

يوصي البحث بعدد من الإجراءات العملية التي يمكن أن تسهم في تطوير بيئة الرقابة والتدقيق على المحافظ الإلكترونية في المصارف الأهلية العراقية:

أولاً: ضرورة اعتماد إطار تدقيق متخصص مبني على المخاطر يشمل تحليل دورة حياة العملية الإلكترونية، وتحديد نقاط الضعف الرقمية، وتصميم اختبارات تدقيق رقمية تعتمد على تحليل السلوك ونماذج كشف الشذوذ.

ثانياً: توسيع نطاق استخدام أدوات التدقيق بمساعدة الحاسوب، وخاصة أدوات تحليل البيانات الضخمة، بما يمكّن المدقق من فحص جميع العمليات بدلاً من الاعتماد على العينات التقليدية.

ثالثاً: تحديث ضوابط الأمن السيبراني من خلال تطبيق المصادقة متعددة العوامل، وتعزيز نظم التشفير، وإجراء اختبارات اختراق دورية لضمان قدرة الأنظمة على مواجهة التهديدات الحديثة.

رابعاً: تعزيز ضوابط مكافحة غسل الأموال الرقمية من خلال استخدام أنظمة مراقبة فورية تعتمد على خوارزميات تحليل الأنماط السلوكية، إضافة إلى تدريب الموظفين على علامات الإنذار المبكر.

خامساً: تعزيز مستوى الشفافية عبر تطوير نظم توثيق إلكترونية تسمح بتتبع العملية منذ بدايتها وحتى إغلاقها، وبما يمكّن الجهات الرقابية من مراجعتها بسهولة.

يوصي البحث بإجراء تحديثات دورية لبرامج التدقيق بما يتناسب مع التغييرات التقنية والتشريعية في نشاط المحافظ الإلكترونية، وبناء برامج تدريب مستمرة للمدققين في مجالات التكنولوجيا المالية والمخاطر الرقمية.

المراجع:

المراجع العربية

1- عمر إبراهيم عبد الحميد الشبلي. (2023). الحوكمة الالكترونية ودورها في تطوير الموارد البشرية للبلديات في المملكة الأردنية الهاشمية. مجلة العلوم الإنسانية والطبيعية, 4(2), 887-896.

2- هشام يوسف سالم الاعمر. (2023). تقييم أثر الحوكمة الالكترونية في تحسين الأداء المالي في بلدية منشية بني حسن. مجلة العلوم الإنسانية والطبيعية, 4(12), 593-607.

المراجع الأجنبية

1- Ibitoye, J. S. (2025). Multi-agent AI systems for secure, transparent, and compliant fraud surveillance in cross-border FinTech operations. *Int J Res Publ Rev*, *6*(6), 9724-40.

2-Kamis, R., Ismail, S., Harun, H., Awang, A. H., Abidin, M. I., & Tuah, J. H. (2024). E-Wallets Unplugged: Navigating Benefits and Challenges in a Post-Pandemic World. *Information Management and Business Review*, *16*(4), 1-8.

3-Oriento, C., Negara, D. S., Putra, A. R., Arifin, S., & Saputra, R. (2023). Risks and Legal Protection in Non-Cash Financial Transactions Through E-Wallets. *Journal of Social Science Studies*, *3*(1), 109-114.

4- Nordin, N., Shahwan, S., Ibrahim, N., Nasir, N. M., & Awang, N. (2024). Electronic Money Institution and Protection Framework. *International Journal of Business and Technology Management*, *6*(2), 50-69.

5- Kadamathikuttiyil Karthikeyan, G., & Bhowmik, B. (2025). Intelligent money laundering detection approaches in banking and E-wallets: a comprehensive survey. *Journal of Computational Social Science*, *8*(4), 1-64.

6- Wibisono, S., & Subiyantoro, H. (2025). Transformation Towards a Clean Digital Economy by Optimizing Non-Cash Transactions as an Instrument to Prevent Corruption. *Indonesian Journal of Multidisciplinary Science*, *4*(10), 714-727.

7- Sikri, A., Dalal, S., Singh, N. P., & Le, D. N. (2019). Mapping of e-wallets with features. *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies*, 245-261.

8- Hassan, M. A., Shukur, Z., & Mohd, M. (2022). A penetration testing on Malaysia popular e-wallets and m-banking apps. *International Journal of Advanced Computer Science and Applications*, *13*(5).

9- Christian, A., Santoso, H. B., & Kusumastuti, D. L. (2024, January). Factors influencing the adoption and usage of e-wallets. In *2024 3rd International Conference on Digital Transformation and Applications (ICDXA)* (pp. 103-108). IEEE.

10- Razak, N. A. B. A., Ahmad, S. B., Zakaria, Z. B., & Wira, A. (2025). Sharia Governance and Ris Yathiraju, N., & Dash, B. (2023). Gamification Of E-Wallets With The Use Of Defi Technology-A Revisit To Digitization In Fintech. *International Journal of Engineering, Science*, *3*(1), 2582-9734.k Mitigation in E-Wallets: Implications for SDG 8. *Al-'Adalah*, *22*(1), 125-146.

11- Al-Qubati, E. S. A., & Al-Shaibany, N. A. (2024, November). Model of Secure E-Wallet Readiness. In *2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI)* (pp. 1-7). IEEE.