AL KUT JOURNAL OF ECONOMIC AND ADMINISTRATIVE SCIENCES
Publisher: College of Economics and Management - Wasit University

دليل استرشادي مقترح لتدقيق الحسابات في بيئة الحوسبة السحابية على وفق معايير التدقيق المعتمدة

Proposed Guidelines for the Auditing of Accounts in the Cloud Computing Environment in Accordance with the Adopted Auditing Standards

احمد ساطع مظفر[1] أ. د. زياد هاشم السقا[2]

Ahmed Sateh Mudhaffar Prof. Dr. Ziad Hashem Al-Saqqa

ahmed.23bap76@student.uomosul.edu.iq zyad_hashim@uomosul.edu.iq

قسم المحاسبة / كلية الإدارة والاقتصاد / جامعة الموصل

المستخلص: تتناول هذه الدراسة مشكلة غياب معايير تدقيق إجرائية واضحة ومحددة يمكن الاسترشاد بها عند تنفيذ عمليات تدقيق الحسابات في بيئة الحوسبة السحابية، وهي بيئة تتسم بالتعقيد والتطور المستمر وتعدد الأطراف المشاركة في تقديم الخدمة، مما يجعل من الصعب تطبيق أساليب التدقيق التقليدية بصورة فعّالة. وتنطلق الدراسة من فرضية مفادها أن تطبيق معايير التدقيق الدولية (ISA) ودمجها مع أطر الأمن والحوكمة الدولية مثل ISO/IEC 27001 و ISO/IEC 27017و COBIT 2019 و ITIL يمكن أن يسهم في تصميم دليل إجرائي استرشادي موحّد يواكب التطورات التقنية في بيئات الحوسبة السحابية ويعزز جودة عمليات التدقيق. وتهدف الدراسة إلى اقتراح إطار عملي وتطبيقي يساعد المدققين على ضمان الدقة والموثوقية والشفافية في نتائج التدقيق السحابي، من خلال وضع إرشادات تفصيلية وخطوات عملية وقوائم تحقق تدعم استناد القرارات التدقيقية إلى أدلة رقمية موثوقة. كما تسعى إلى توضيح كيفية تكييف منظومة معايير ISA مع نموذج "المسؤولية المشتركة "الذي يميز بيئات السحابة، مع تحديد الأدوار والمسؤوليات بين مزود الخدمة والمستخدم النهائي لضمان فاعلية الرقابة والمساءلة.

وتتوصل الدراسة إلى أن تحقيق جودة عالية في تدقيق الحسابات السحابية يتطلب تطوير منظومة تدقيق هجينة تجمع بين الضوابط التقنية الصارمة ومتطلبات الحوكمة ومعايير التدقيق الدولية، إلى جانب التحقق من سلامة وموثوقية الأدلة الرقمية وتطبيق ضوابط دقيقة لإدارة الهوية والصلاحيات وإجراء اختبارات دورية لاستمرارية الخدمة وسلامة البيانات.

وتوصي الدراسة بضرورة إعداد دليل تدقيق استرشادي متكامل يعتمد على المعايير والأطر الدولية المذكورة، بما يسهم في توحيد إجراءات التدقيق وتعزيز الثقة والشفافية في بيئات الحوسبة السحابية.

الكلمـات المفتاحيـة: تـدقيق الحسـابات، الحوسـبة السـحابية، معـايير التـدقيق الدوليـة(ISA) ، أطـر الحوكمـة والأمـن المعلوماتي، الدليل الإجرائي الاسترشادي.

Abstract: This study addresses the problem of the absence of well-defined procedural auditing standards that can be used as guidance when conducting audit engagements in cloud computing environments—an environment characterized by complexity, constant technological evolution, and the involvement of multiple service providers and clients. These conditions make the application of traditional auditing approaches insufficient and often ineffective. The study is based on the assumption that international auditing standards (ISA) can be integrated with global security and governance frameworks such as ISO/IEC 27001, ISO/IEC 27017, COBIT 2019, and ITIL to design a unified procedural audit guideline capable of meeting the specific requirements of cloud-based systems and improving audit quality and reliability.
The study aims to propose a practical and applicable framework that enables auditors to ensure accuracy, reliability, and transparency in cloud auditing processes through the development of detailed guidelines, practical steps, and checklists that enhance the credibility of digital audit evidence. Furthermore, it seeks to adapt ISA standards to the "shared responsibility" model that defines cloud environments, clarifying accountability and responsibility boundaries between service providers and users to enhance control effectiveness.
The study concludes that achieving high-quality cloud auditing requires the development of a hybrid auditing framework that combines **s**trict technical controls, governance requirements, and international auditing standards**,** along with the validation of digital evidence reliability, identity and access management controls, and continuity testing to ensure service resilience and data integrity.

Finally, the study recommends developing a comprehensive and integrated audit guideline that aligns ISA standards with the mentioned frameworks to unify auditing practices and strengthen trust and transparency in cloud-based environments.

Keywords: Auditing, Cloud Computing, International Standards on Auditing (ISA), Governance and Information Security Frameworks, Procedural Audit Guideline.

المبحث الأول / منهجية البحث ودراسات سابقة

أولاً: منهجية البحث

1. مشكلة البحث:

تتمثل المشكلة الرئيسة للبحث في تساؤل رئيس هو:

كيف يمكن تدقيق الحسابات في بيئة الحوسبة السحابية في ظل عدم وجود معايير تدقيق يمكن الاسترشاد بها لهذا الغرض؟

ومنه تتفرع التساؤلات الآتية:

أ. ما الإرشادات التي يمكن اقتراحها لضمان دقة وسلامة تدقيق الحسابات في بيئة الحوسبة السحابية؟
ب. ما أهم معايير التدقيق المعتمدة التي يمكن الاستفادة منها في تدقيق الحسابات في بيئة الحوسبة السحابية؟

2. أهمية البحث

تأتي أهمية البحث من خلال:

أ. الحاجة إلى ما يمكن أن يسترشد به مراقبو الحسابات عند العمل في بيئة الحوسبة السحابية.
ب. تعزيز دقة وموثوقية الحسابات المالية في بيئة الحوسبة السحابية من خلال وضع ارشادات تدقيق واضحة ومبنية على المعايير المعتمدة.
ت. تمكين مراقبي الحسابات من أداء مهامهم بفعالية أكبر عبر تزويدهم بإرشادات ومعايير واضحة لتدقيق الحسابات السحابية.

3. هدف البحث

يسعى البحث الى تحقيق الأهداف الآتية:

1. توضيح أهمية تدقيق الحسابات في بيئة الحوسبة السحابية والحاجة إليه في ظل التطورات التقنية الحديثة.
2. تحديد معايير التدقيق التي يمكن الاستفادة منها في تحديد إرشادات تدقيق الحسابات في بيئة الحوسبة السحابية.
3. اقتراح دليل استرشادي لتدقيق الحسابات في بيئة الحوسبة السحابية في ضوء معايير التدقيق المعتمدة.

4. فرضية البحث

لغرض الإجابة على التساؤلات المحددة في مشكلة الدراسة والمسأهمة في تحقيق أهدافها يتم الاعتماد على فرضية رئيسة هي:

((يمكن الاستفادة من مجموعة من معايير التدقيق المعتمدة في تحديد بعض الارشادات التي يمكن ان تسهم في تحديد ممارسة العمل في بيئة الحوسبة السحابية)).

وتتفرع منها الفرضية الآتية:

أ. يسهم تطبيق الإرشادات التقنية والتنظيمية المقترحة في بيئة الحوسبة السحابية في تحسين دقة وسلامة عمليات تدقيق الحسابات، من خلال تعزيز أمن البيانات وموثوقية المعلومات المالية.

ب. تسهم معايير التدقيق المعتمدة في تحديد إرشادات يمكن ان تدخل في تحديد بعض الإجراءات التي يمكن الاعتماد عليها في تدقيق الحسابات في بيئة الحوسبة السحابية.

5. منهج البحث

يُعتمد على المنهج الاستنباطي: إذا أُنطلِقَ من معايير التدقيق الدولية (ISA) والأطر المهنية ذات الصلة ISO/IEC (27001و27017، COBIT 2019، ITIL) لاشتقاق مبادئ وضوابط لتدقيق الحسابات في بيئة الحوسبة السحابية. ثم جرى تحويل هذه المبادئ إلى دليل استرشادي لتدقيق الحسابات في بيئة الحوسبة السحابية على وفق معايير التدقيق المعتمدة.

6. دراسات سابقة:

أ- دراسات عربية

الدراسة الأولى	**دراسة (2023) السقا، زياد هاشم: إطار مقترح لتدقيق الحسابات في بيئة السحابة الإلكترونية، بحث منشور**
أهداف الدراسة	الإطار العملي للتدقيق في بيئة السحابة الالكترونية. المتطلبات اللازمة للتدقيق في بيئة السحابة الالكترونية. مجموعة من الإجراءات المقترحة في بيئة السحابة الالكترونية.
أبرز الاستنتاجات	في ظل التطورات المتلاحقة لاستعمال تقنيات المعلومات في تدقيق الحسابات ومنها ما يتعلق بالخدمات التي يمكن ان تقدمها تقنية السحابة الكترونية وعليه فقد سعى الباحثون الى دراسة التأثيرات المحتملة لاستعمال السحابة الكترونية في تدقيق الحسابات وقد ظهرت الكثير من المفاهيم التي صاحبها الخلط من الناحية العلمية مما يتطلب ضرورة توحيدها واستعمالها الاستعمال العلمي الصحيح والدقيق. يتعلق التدقيق باستعمال السحابة الالكترونية بثلاثة مفاهيم أساسية تحدد من خلالها طبيعة التعامل مع السحابة الالكترونية وكيفية الاستفادة من خدماتها المقدمة من خلال مزودي هذه الخدمة، وتشمل هذه المفاهيم كلاً من: التدقيق السحابي، تدقيق الحسابات عن بعد باستعمال السحابة الالكترونية، التدقيق في بيئة السحابة الالكترونية. يتطلب التدقيق في بيئة السحابة الالكترونية ضرورة توافر مجموعة من المتطلبات المتعلقة بطبيعة العمل في بيئة السحابة الالكترونية منها ما يتعلق بالمدقق نفسه ومنها ما يتعلق بكل من الوحدة محل

	التدقيق. تم وضع أنموذج لتدقيق الحسابات في بيئة السحابة الالكترونية شمل إجراءات مقترحة تتعلق بكل من: إجراءات تتعلق بشركات تقديم خدمة السحابة الالكترونية، إجراءات تتعلق بتدقيق عمليات التخزين السحابي ومخاطره، إجراءات تتعلق بتدقيق الحوسبة السحابية.
أهم التوصيات	ضرورة استمرار الباحثين في تحديد الاطر العلمية التي تتوافق وفقها المفاهيم والمصطلحات المستعملة من لدن الباحثين والمدققين والجمعيات المهنية والأكاديمية التي يقع ضمن اهتماماتها البحث العلمي في مجال تدقيق الحسابات في بيئة السحابة الالكتروني. ضرورة القيام بإعداد الدورات والندوات العلمية والمهنية اللازمة لزيادة إدراك المدققين بأهمية تدقيق الحسابات في بيئة السحابة الالكترونية؛ لأنها خدمة تأكيدية يتطلبها العمل في بيئة تقنيات المعلومات الحديثة ولجوء مختلف الوحدات الاقتصادية للتعامل معها والاستفادة من خدماتها. تضمين المناهج الدراسية في الجامعات لأهم المستجدات في مجالات استعمال تقنيات المعلومات في تدقيق الحسابات وكيفية الاستفادة منها في عمل مدققي الحسابات؛ لدورهم المهم في تقديم الخدمات التأكيدية في بيئة تقنيات المعلومات بصورة عامة وبيئة السحابة الالكترونية بصورة خاصة؛ لتوسع الوحدات الاقتصادية المختلفة في التعامل معها والاستفادة من خدماتها المقدمة.
الدراسة الثانية	**دراسة (2023) سلطان، تيسير جواد: أثر فاعليه التدقيق الداخلي في إدارة مخاطر الحوسبة السحابية، بحث منشور**
أهداف الدراسة	توضيح أهم الادوار المعاصرة لنشاط التدقيق الداخلي، ومنها اضافه قيمه للشركة عن طريق إدارة المخاطر المختلفة منها مخاطر تطبيق الحوسبة السحابية. التعرف على ادبيات موضوع الحوسبة السحابية بوصفها تقنية رقميه مجانية تحقق مزايا عديدة ومنها تخفيض التكاليف والسرعة في الاداء والانجاز وتقليل الوقت وامكانيه الولوج اليها في أي جهاز نقال ذكي أو حاسب الكتروني مكتبي أو محمول.
أبرز الاستنتاجات	تؤثر فعالية التدقيق الداخلي بشكل كبير في عمليه إدارة مخاطر تقنيه الحوسبة السحابية لما لها نشاط من ادوار استباقيه واستشارية لكافة المخاطر التي تعرضت لها الشركات ومنها مخاطر تطبيق تقنيه الحوسبة السحابية. تطور ادوار ومسؤوليات التدقيق الداخلي من الادوار والمسؤوليات التقليدية الى الادوار والمسؤوليات الحديثة والتي تضيف قيمه مهمه للشركة.
أهم التوصيات	ان تحرص إدارة الشركات ومجالس الإدارات فيها على اعطاء أهمية كبيره لنشاط التدقيق الداخلي لما له من ادوار معاصره من عمليه إدارة المخاطر المختلفة التي ترافق اعمال الشركات وبالنتيجة تحقيق قيمه مضافه تعزز من موقف الشركة التنافسي. ان تكون إدارات الشركات سباقه ورائده في تطبيق التقنيات الرقمية المعاصرة ومنها تقنيه الحوسبة

	السحابية لما لهذه التقنية من مزايا متنوعة تسهم في زيادة كفاءه الأنظمة المحاسبية المعتمدة التي تعزز من الميزة التنافسية للشركات في البيئة التي تعمل بها.
الدراسة الثالثة	**دراسة (2023) مجي، احمد، كاظم، تيسير: إثر كفاءه مراقب الحسابات على ممارسه التدقيق السحابي دارسه استطلاعيه لعينه من الأكاديميين والمهنيين في اختصاص المحاسبة والتدقيق، بحث منشور**
أهداف الدراسة	التعرف على مدى قدره وكفاءه مراقبه الحسابات على ممارسه التدقيق السحابي. بيان مفهوم التدقيق السحابي وأهميته وتطوره ومدى ممارسه هذا النوع الحديث من التدقيق في البيئة العراقية.
أبرز الاستنتاجات	يسهم تفعيل البرامج والدورات التدريبية المتخصصة في مجال الكمبيوتر وتكنولوجيا المعلومات بشكل مستمر في تحسين الكفاءة واداء مراقبي الحسابات بما يتماشى مع التطورات المستمرة في بيئة الأنظمة السحابية والبيانات الكبيرة.
أهم التوصيات	رفع كفاءه العمل المحاسبي والتدقيقي معا في عن طريق اهتمام الوحدات الاقتصادية بتنظيم وتطوير النظام المحاسبي فيها وذلك بإدخال مفهوم الحوسبة السحابية في اعمالها والاعتماد على ادوات التدقيق السحابي الالكترونية. مع ضرورة التأكيد على اهتمام شركات التدقيق في العراق بالمسأهمة في تطوير مهنه التدقيق باستمرار عن طريق اجراء دورات تدريبيه للموظفين في شركات التدقيق والاطلاع على أهم مستجدات تطبيقات تقنيه الحوسبة السحابية الإلكترونية.
الدراسة الرابعة	**دراسة (2022) حبيب، سمير: دور المحاسبة ومعايير التدقيق السحابي في تأكيد أمن البيانات والمعلومات دارسه ميدانيه من وجهه نظر مدققي الحسابات الخارجية في سوريا، بحث منشور**
أهداف الدراسة	استقصاء اراء مدققي الحسابات الخارجيين حول دور فوائد ومخاطر المحاسبة والتدقيق السحابي عند تبني الحلول السحابية. استقصاء اراء مدققي الحسابات الخارجية لدور معايير التدقيق السحابي (المعيار) TCISO 295، SSE 16، SAS 70.
أبرز الاستنتاجات	توجد فروق ذات دلالة إحصائية بين اراء مدققي الحسابات الخارجيين حول دور فوائد ومخاطر المحاسبة والتدقيق السحابي عند تبني الحلول السحابية (تبعا للمؤهل العلمي) مما يدل على انه بالرغم من الفوائد المتعددة التي يمكن تحقيقها عند استعمال السحابة في مجالي المحاسبة والتدقيق؛ ولاسيما فيما يتعلق بعمليات النسخ الاحتياطي التلقائي، ألا ان فكره تبني الحلول السحابية ما زالت تشكل مصدر قلق من نواحٍ عدة: أهمها وصول اشخاص غير مصرح لهم قانونيا الأمر الذي يتيح الاتلاف أو السرقة أو التلاعب بالبيانات والمعلومات والمحاسبية.

أهم التوصيات	السعي الى تحقيق التوازن والمواءمة بين فوائد ومخاطر المحاسبة والتدقيق السحابي عند تبني الحلول السحابية بالشكل الامثل من خلال التوجه نحو التحول الرقمي تدريجيا وفق استراتيجيات تنسجم مع نقاط عده أهمها تحديد مدى استعداد منظمات الاعمال لتبني هذه الحلول خصوصية، اعمالها وأهدافها، ودرجه حاجتها والاستفادة من الخدمات المدارة سحابيا. درجه استجابتها للمخاطر المحتملة والقدرة على تجاوزها في حال حدوثها، استراتيجية واضحة فيما يخص أمن البيانات والمعلومات؛ وذلك من خلال وضع مصفوفه الوصول لضمان عدم وصول الاشخاص غير مصرح لهم قانونيا، والتحديد الدقيق لصلاحيات المستخدمين.

أ. الدراسات الاجنبية

الدراسة الأولى	**دراسة Emad Kendry (2022)** **Adoption of cloud computing by external auditors in raq Exploratory Study** **اعتماد الحوسبة السحابية من لدن المدققين الخارجيين في العراق دراسة استكشافية بحث منشور**
أهداف الدراسة	تهدف الدراسة الى استكشاف فوائد وتحديات وفرص الحوسبة السحابية في العراق، فضلا عن معرفة ما إذا كان المدققون الخارجيون في العراق يستعملون خدمات الحوسبة السحابية أم لا.
أبرز الاستنتاجات	أظهرت نتائج الدراسة أن غالبية المستجيبين يوافقون على اعتماد الحوسبة السحابية من لدن المدققين الخارجيين، مما يدل على أن للحوسبة السحابية دوراً مهماً في عملية التدقيق في العراق.
أهم التوصيات	يقترح الباحث اجراء دراسات مستقبلية لاستكشاف تأثير استعمال الحوسبة السحابية على عملية التدقيق من وجهة نظر المدققين الخارجيين في البيئة العراقية.
الدراسة الثانية	**دراسة (2022)** **Cloud auditing Assurance resources & pooled audits** **تدقيق السحابة وموارد الضمان والتدقيق المجمع**
أهداف الدراسة	تهدف الدراسة الى تقديم توجيهات للبنوك حول كيفية التدقيق على مقدمي خدمات السحابة وضمان الامتثال لمتطلبات الأمان والامتثال التنظيمي. تعزيز فهم المؤسسات المالية حول كيفية إدارة مخاطر الاعتماد على الحوسبة السحابية وضمان استمرارية الالتزام بالقوانين المنظمة في أوروبا. تقديم أفضل الممارسات للدراسات المشتركة (التدقيق الجماعي) لتحسين كفاءة وفعالية التدقيق على

	الخدمات السحابية.
أبرز الاستنتاجات	التحول الرقمي: أثرت التكنولوجيا الرقمية على عملية التدقيق، وهذه التكنلوجيا مستمرة في تشكيل الحوسبة السحابية واعتمادها، مما يتطلب المزيد من الرقابة التنظيمية. تحديات التدقيق السحابي: تتطلب طبيعة البيئة السحابية التحديث المستمر الأنموذج الخطوط الثلاثة للدفاع، وتوزيع المسؤوليات بين مقدمي الخدمات السحابية والمؤسسات المالية. كفاءة عمليات التدقيق: هناك أدوات تدقيق متقدمة يمكن أن تقلل من التكاليف والوقت، مثل: التدقيق الجماعي، والتقارير الداخلية لمقدمي الخدمات.
أهم التوصيات	على المؤسسات المالية اتباع نهج قائم على المخاطر في التدقيق على مقدمي الخدمات السحابية، مع الاخذ في الاعتبار أهمية الوظائف والامتثال للمعايير الدولية. يشدد على ضرورة التحوّل نحو أدوات التدقيق الرقمية والآلية لمواكبة التطور التكنولوجي وتقليل الاعتماد على التدقيق التقليدي المباشر.
الدراسة الثالثة	**دراسةGunjan Gupta (2022)** **Managing Compliance and Auditing in Cloud** **إدارة الامتثال والتدقيق في السحابة، بحث منشور**
أهداف الدراسة	هدفت الدراسة إلى تحليل كيفية إدارة الامتثال والتدقيق في بيئة الحوسبة السحابية، والبحث في المجالات التي تحتاج فيها عمليات التدقيق والامتثال التقليدية إلى التعديل؛ لتتناسب مع خصائص الحوسبة السحابية وتقديم توصيات تسهم في تحسين هذا المجال.
أبرز الاستنتاجات	تؤكد الدراسة على ضرورة أن يكون المدققون على دراية بالمجالات الخاصة بالحوسبة السحابية، ونماذج تقديم الخدمات، والمخاطر الرئيسة، وتوزيع الأدوار والمسؤوليات، وأطر التدقيق الخاصة بالسحابة. ويؤكّد البحث على أهمية فهم المخاطر الأمنية والامتثال في بيئة السحابة قبل تبني هذه التكنولوجيا
أهم التوصيات	يوصي البحث بإنشاء قائمة تحقق للتدقيق السحابي، تشتمل على المجالات الرئيسة التي يجب تدقيقها، وتوضيح مسؤوليات الجهات المزودة للخدمات السحابية والعملاء.
الدراسة الرابعة	**دراسة Sergi Serra Aloy (2021)** **AUDITING MODELS OF CLOUD COMPUTING SERVICE FOR PUBLIC ADMINISTRATIONS** **نموذج تدقيق لخدمات الحوسبة السحابية للإدارات العامة، رسالة ماجستير**

أهداف الدراسة	تطوير أنموذج تدقيق قوي لتقديم خدمات الحوسبة السحابية للإدارات العامة اقتراح عمليات قائمة على معايير ISO/IEC لضمان التوافق والتكامل بين الخدمات السحابية العامة. تحسين الكفاءة التشغيلية وتخفيض البيروقراطية من خلال أنموذج تبادل بيانات سحابية فعال للإدارات العامة في الاتحاد الأوروبي.
أبرز الاستنتاجات	يُعدُّ تبني الحوسبة السحابية أداة فعالة لتمكين التحوّل الرقمي للإدارات العام هناك تحديات كبيرة تتعلق بالتشريعات وعدم وجود هيكل محدد لتحقيق تكامل فعال بين الأنظمة أنموذج التفاعل الديناميكي بين السحب المختلفة يُعدُّ عاملاً أساسًا لمستقبل التكنولوجيا في الإدارات العامة، كما أن تشجيع التكامل بين المؤسسات السحابية يعزز الأداء والكفاءة
أهم التوصيات	التعاون بين المؤسسات العامة: تعزيز التعاون بين الإدارات العامة لتبادل البيانات والمعلومات بفعالية وأمان تحديث البنية التحتية: الاستثمار في تطوير البنية التحتية السحابية لتحقيق التكامل بين الأنظمة المختلفة تعزيز أمن المعلومات: يجب أن تكون المعايير الأمنية قوية ومتوافقة مع اللوائح التنظيمية، لضمان حماية البيانات الخاصة والمعلومات الشخصية.

المصدر: الجدول من إعداد الباحث

المصدر: من إعداد الباحث

في ضوء مراجعة الأدبيات السابقة، يمكن استخلاص ما يأتي:

(1) العوامل المشتركة في الدراسات السابقة:

يتضح من مجمل الدراسات السابقة أنّ الحوسبة السحابية أثرت بشكل مباشر على مهنة التدقيق؛ إذ وفرت مزايا تتعلق بسرعة إنجاز العمل وجودة المخرجات، لكنها في المقابل طرحت تحديات مهمة أبرزها أمن البيانات وإدارة المخاطر. كما أكدت الأبحاث على ضرورة وضع أطر ومعايير مهنية تنظم التدقيق السحابي وتضمن الامتثال للمعايير الدولية، إضافةً إلى الحاجة المستمرة لتطوير مهارات المدققين لمواكبة التطورات التقنية. وبالرغم من الفوائد الكبيرة التي تحققها السحابة في مجال التدقيق، فإن معظم الدراسات أكدت على أهمية إيجاد توازن بين هذه الفوائد والمخاطر المترتبة عليها.

(2) ما يُميز الدراسة الحالية عن الدراسات السابقة:

سعت الدراسة إلى الربط المباشر بين بيئة الحوسبة السحابية ومعايير التدقيق المعتمدة، عن طريق وضع إرشادات عملية واضحة تساعد المدققين على التعامل مع التحديات التي تفرضها البيئة الرقمية. فهي لم تقتصر على استعراض المخاطر أو الفوائد، بل ركزت على تقديم إطار إجرائي تطبيقي يوجه عملية التدقيق السحابي وفقاً للمعايير الدولية والمهنية. كما تميزت الدراسة بأنها تناولت أدلة الإثبات وأساليب جمعها في البيئة السحابية، مع التأكيد على ملاءمتها وكفايتها لدعم رأي المدقق. ومن جهة أخرى، فهي تسهم في سد فجوة معرفية قائمة بين الجانب النظري المتعلق بالتقنيات

السحابية والتطبيق العملي لعمليات التدقيق، عن طريق مقترحات يمكن أن يستفيد منها المدققون والممارسون بشكل مباشر.

المبحث الثاني

معايير التدقيق ذات العلاقة بتدقيق الحسابات في بيئة الحوسبة السحابية

تُعد معايير التدقيق المعتمدة الإطار المهني الرئيس الذي يستند إليه المدققون في ممارسة أعمالهم؛ إذ تحدد المبادئ والإجراءات الواجب اتباعها لضمان جودة عملية التدقيق ودقتها. ومع الانتشار المتزايد لتبني الحوسبة السحابية في إدارة الأنظمة المحاسبية، برزت الحاجة إلى تكييف تطبيق هذه المعايير مع خصوصية البيئة الرقمية الجديدة. فالمعايير المتعلقة بأدلة الإثبات، وتقييم المخاطر، وفهم بيئة الرقابة الداخلية، أصبحت أكثر ارتباطًا عند تدقيق الحسابات في بيئة تعتمد على نظم سحابية، حيث يواجه المدقق تحديات تتعلق بمكان تخزين البيانات، والتحكم في الوصول إليها، وأمن المعلومات. ومن ثم فإنَّ الالتزام بمعايير التدقيق ذات الصلة يشكل الأساس لضمان موثوقية القوائم المالية وشفافيتها في ظل التحوّل نحو الحوسبة السحابية.

2-1معايير أمن المعلومات وضوابط الحوسبة السحابية

أولا- ISO/IEC 27001 معيار نظم إدارة أمن المعلومات(ISMS) (ISO/IEC,2022)

إنَّ هذا المعيار ليس معياراً تدقيقياً فحسب، لكنه إطار مرجعي مفيد لفهم البيئة الأمنية لدى مزود السحابة حيث يُقدّم هذا المعيار متطلبات لإنشاء نظام إدارة أمن المعلومات وتنفيذه وصيانته وتحسينه باستمرار. ويُعد اعتماد نظام إدارة أمن المعلومات قرارًا استراتيجيًا للمنظمة، ويتأثر تنفيذه باحتياجات المنظمة وأهدافها ومتطلباتها الأمنية والعمليات التنظيمية والحجم والتركيبة حيث يهدف نظام إدارة أمن المعلومات إلى الحفاظ على سرية وتكامل وتوافر المعلومات من خلال تطبيق عمليات إدارة المخاطر، ويمنح الثقة للأطراف المعنية بأن المخاطر مُدارة بشكل كافٍ. يُتوقع أن يتم دمج نظام إدارة أمن المعلومات ضمن عمليات المنظمة وبنيتها الإدارية الشاملة، وأن يتم أخذ الأمن المعلوماتي في الحسبان عند تصميم العمليات ونظم المعلومات والضوابط.

ثانيا- معيار ISO/IEC 27017 لتدقيق الحسابات في بيئة الحوسبة السحابية (ISO/IEC,2015)

يعد ISO/IEC 27017 معيارًا مكملًا لـISO/IEC 27002 ، يوفّر إرشادات إضافية وضوابط جديدة تُعنى بأمن المعلومات في خدمات الحوسبة السحابية، موجهًا لكلٍّ من:

1. مزودي خدمات السحابة (Cloud Service Providers – CSPs)
2. زبائن السحابة (Cloud Service Customers – CSCs)

اما يهم المدقق في بيئة الحوسبة السحابية:

يهتمّ المدقّق في بيئة الحوسبة السحابية أولًا بتحديد الأدوار والمسؤوليات الأمنية في العقود بشكل واضح بين مزوّد الخدمة والعميل، خاصة ما يتصل بحماية البيانات وتشفير الاتصالات والنسخ الاحتياطي وإدارة الحوادث. ثم يراجع ضوابط الوصول وإدارة الهوية عبر التحقق من تفعيل المصادقة متعددة العوامل وتطبيق مبدأ "أقل امتياز" وتتبع

سجلات الدخول والأنشطة الإدارية. ويُقيّم حماية البيانات السحابية من خلال سياسات تصنيف المعلومات والتشفير في النقل والسكون، مع وجود إجراءات مُحكمة لحذف بيانات العملاء عند إنهاء العقود. كما يتثبت من مواقع مراكز البيانات (Data Residency)وتوافقها مع القوانين المحلية والدولية لحماية البيانات مثل الـ GDPR أو القوانين العراقية. ويُدقّق في ضوابط المورّدين من الباطن بفحص عقود الأطراف الثالثة والتأكد من التزامهم بذات ضوابط أمن المعلومات. ويختبر جاهزية الاستجابة للحوادث واستمرارية الأعمال بوجود خطط واضحة ومُختبرة للتعافي من الكوارث وقنوات موثّقة للإبلاغ عن الحوادث. وأخيرًا، يتحقق من أدلة التحقق عبر مراجعة سجلات التدقيق وضمان تأمينها وقابليتها للتتبّع ووجود نظام إنذار مبكر لأي خرق أو اختراق.

2-2معايير الحوكمة والتقارير الأخرى ذات العلاقة

أولا: إطار COBIT 2019هو إطار شامل لحوكمة وإدارة تقنية المعلومات، تم تطويره من لدن جمعية تدقيق وضبط نظم المعلومات ISACA يستعمل هذا الإطار من لدن المدققين لتقييم مدى فعالية الرقابة على تقنية المعلومات في الوحدات الاقتصادية، سواء كانت هذه الوحدات الاقتصادية زبائن أو مزودي خدمات حيث يساعد COBIT 2019 في تحديد نقاط القوة والضعف في الرقابة الداخلية المرتبطة بتقنية المعلومات، ويُمكّن المدقق من قياس مستوى النضج والقدرة (Capability Level) للعمليات التقنية داخل الوحدة الاقتصادية كما يتيح الإطار تقييم مجالات متعددة مثل: تحسين المخاطر(EDM03) ، إدارة المخاطر(APO12) ، إدارة التغيير(BAI06) ، أمن المعلومات(DSS05) ، والتحكم في العمليات(DSS06) كما أن عند قيام المدقق بتطبيق أو استعمال COBIT 2019، فإنه **(**Jamal,**2023** Kusuma Wati,**):**

1. يقيّم مدى امتثال الوحدة الاقتصادية لمبادئ حوكمة تقنية المعلومات.
2. يحدد الفجوات بين الأداء الحالي والمستوى المستهدف.
3. يصدر توصيات لتحسين العمليات وتعزيز الأمن المعلوماتي والكفاءة التشغيلية.

ثانيا مكتبة البنية التحتية لتقنية المعلومات تفيد في تقييم العمليات التشغيلية المرتبطة بالخدمات السحابية

ITIL (Information Technology Infrastructure Library)هي مكتبة من أفضل الممارسات والمعايير لإدارة خدمات تقنية المعلومات(ITSM) ، وتهدف إلى تحسين جودة الخدمات التقنية المقدمة في المؤسسات من خلال تنظيم العمليات والمهام المرتبطة بها.

تُستخدم ITILبشكل فعال في تقييم وتحسين العمليات التشغيلية، وخاصة في بيئات الخدمات السحابية (Cloud Services)، حيث تساعد في (Bayastura, Krisdina,2021)

1. تحديد مدى كفاءة إدارة الحوادث (Incidents) والمشكلات (Problems) في بيئة الحوسبة السحابية.
2. ضمان استمرارية الخدمة من خلال إدارة التكوين (Configuration Management) وإدارة التغيير (Change Management).
3. تحقيق التكامل بين خدمات البنية التحتية السحابية والعمليات الداخلية للمؤسسة.

4. رفع مستوى رضا المستخدمين من خلال ممارسات إدارة طلبات الخدمة (Service Request Management) واتفاقيات مستوى الخدمة.(SLA)

5. عند دمج ITIL مع أطر مثل COBIT 2019، يمكن الحصول على تغطية شاملة للجوانب الرقابية (Governance) والتشغيلية في بيئة الخدمات السحابية.

ويرى الباحث أن معايير منظمة الايزو لم لا تكفي وحدها لتدقيق الحسابات في بيئة الحوسبة السحابية وذلك للأسباب الآتية:

أولاً :طبيعة معايير الأيزو وأهدافها

1. **معايير الأيزو (ISO/IEC 27001, 27017, 27002)** صممت أساسًا لإرساء إطار إدارة أمن المعلومات ووضع ضوابط إجرائية وتقنية لتحقيق مستوى مقبول من حماية البيانات والمعلومات في مختلف البيئات (تقليدية أو سحابية).

2. **تركز هذه المعايير على:**

a. حماية البيانات(Confidentiality, Integrity, Availability)

b. السياسات والإجراءات والضوابط التقنية والتنظيمية.

c. الإدارة المستمرة للمخاطر وتحسين نظام الإدارة الأمن ية.

وعليه، فان معايير الأيزو مثل (ISO/IEC 27001, 27017) ضرورية وتُعد "مرجعية أساسية لضبط أمن المعلومات"، لكنها غير كافية لوحدها لتدقيق الحسابات في بيئة الحوسبة السحابية؛ لأنها:

1. تركز على الضبط والأمن لا على إجراءات التدقيق المالي نفسه.

2. لا تضع منهجية اختبارات مالية أو أدلة إثبات محاسبية تفصيلية.

3. تحتاج إلى التكامل مع معايير التدقيق الدولية وأطر الحوكمة لتغطية كافة الجوانب المالية، التقنية، والقانونية؛ لذلك يجب دمجها مع معايير التدقيق المالي وأطر الحوكمة مثل COBIT وITIL، وتكييف إجراءات التدقيق بما يتناسب مع طبيعة المخاطر والتحديات في البيئة السحابية.

وعليه، سيتم اخذ جزء من كلِّ معيار تدقيق دولي الذي يمكن الاستفادة منه عند تدقيق الحسابات في بيئة الحوسبة السحابية وكما يأتي:

2-3معايير التدقيق الدولية

أولا: معيار التدقيق الدولي رقم 265: التواصل بشأن أوجه القصور في نظام الرقابة الداخلية (IAASB,2009).

يتناول معيار ISA 265 مسؤولية المدقق في التواصل الكتابي المناسب مع المسؤولين عن الحوكمة والإدارة بشأن أوجه القصور في نظام الرقابة الداخلية التي يُحددها خلال تدقيق القوائم المالية. لا يفرض هذا المعيار التزامات إضافية على المدقق لفهم أو اختبار الرقابة الداخلية بما يتجاوز ما تطلبه المعايير الأخرى، مثل ISA 315 و ISA 330.

ربط معيار التدقيق الدولي رقم 265 بالحوسبة السحابية(Cloud Computing) :

في بيئة الحوسبة السحابية، يتعيّن على المدقق التعامل مع ضوابط ليست داخلية بالكامل، بل موزّعة بين الشركة، ومزوّدي خدمات مثل: AWS وAzure، ما يفرض فهم ضوابط الحوكمة السحابية (الوصول، التشفير، مراقبة الأنشطة) بوصفها جزءاً من الرقابة الداخلية. ويجب فحص إدارة الهوية والصلاحيات لاكتشاف ثغرات قد تؤدي لتحريفات غير مكتشفة، والإبلاغ عن أي قصور في الالتزام بضوابط أمن البيانات) مثل ISO/IEC 27017 أو تقارير (SOCبوصفه قصورًا رقابيًا. كما يستلزم الأمر توثيقًا دقيقًا لمسؤوليات الطرفين ضمن نموذج المسؤولية المشتركة؛ لتفادي فجوات رقابية في التقييم والتواصل.

ثانيا: معيار التدقيق الدولي التخطيط لعملية التدقيق رقم 300 (IAASB,2009):

معيار التدقيق الدولي رقم 300 يركّز على أهمية تخطيط عملية التدقيق لضمان تنفيذ التدقيق بفعالية وكفاءة عند تدقيق الحسابات في بيئة تقليديه، حيث يشمل التخطيط تحديد نطاق العمل، وتوزيع المهام بين الفريق، وتقييم المخاطر، وفهم بيئة الزبون ونظامه المحاسبي.

أما عند تطبيق المعيار في بيئة الحوسبة السحابية، فيبرز عدد من الجوانب الخاصة يجب على المدقق أخذها بعين الاعتبار أثناء التخطيط:

يتطلّب التخطيط لتدقيق الحسابات في بيئة الحوسبة السحابية فهمًا دقيقًا لطبيعة الخدمات المستعملة (SaaS/PaaS/IaaS)ونوع السحابة (عامة/خاصة/هجينة) ومسارات تخزين ومعالجة البيانات المالية. ويجب تقييم مخاطر الاعتماد على المزوّدين من حيث التوافر والسرية والسلامة، ثم وضع استراتيجية واضحة لجمع الأدلة من المنصات السحابية (الوصول للبيانات، مراجعة سجلات الاستعمال والوصول). كما يلزم اختيار فريق تدقيق يمتلك خبرة تقنية بالسحابة والضوابط الإلكترونية، مع تنظيم قنوات اتصال وتنسيق فعّالة مع مزوّد الخدمة للحصول على الأدلة والتوضيحات حول الحماية والنسخ الاحتياطي والتشفير. وأخيرًا، ينبغي اعتماد تخطيط مستمر يواكب التحديثات السريعة في البيئة السحابية طوال مدة التدقيق؛ لضمان بقاء الإجراءات مناسبة وفعّالة.

ثالثا: معيار التدقيق الدولي رقم 315 :(ISA 315) تحديد وتقييم مخاطر الأخطاء الجوهرية من خلال فهم المنشأة وبيئتها (IAASB,2020):

يتناول معيار ISA 315 مسؤولية المدقق في تحديد وتقييم مخاطر التحريفات الجوهرية في القوائم المالية، سواء كانت ناتجة عن الغش أو الخطأ، من خلال فهم شامل للمنشأة وبيئتها، بما يشمل نظام الرقابة الداخلية .يمثل هذا الفهم قاعدة أساسية لتصميم وتنفيذ الإجراءات التدقيقية المناسبة.

ربط معيار التدقيق الدولي رقم 315 بالحوسبة السحابية:

أوجد التحوّل الرقمي واعتماد الحوسبة السحابية مخاطر رقابية جديدة يتعيّن على المدقّقين تقييمها على وفق ISA315؛ إذ بات فهم نظام المعلومات يشمل منصّات سحابية تُعالج وتُخزّن البيانات المالية، ما يستلزم فحص ضوابط الوصول والنسخ الاحتياطي والتشفير لدى المزوّد. كما يجب تقييم فعالية الضوابط السحابية المؤثرة في التسجيل وإعداد التقارير، خاصةً الخدمات المؤتمتة المستضافة عبر Azure أو AWS. وتتبع مخاطر جوهرية خاصة من فقدان السيطرة المباشرة على البنية التحتية أو من غموض المسؤوليات المشتركة بين المنشأة والمزوّد. كذلك يقتضي المعيار فهم الاتصالات الإلكترونية بين الإدارة ومزوّدي الخدمات بوصفها جزءًا من نظام المعلومات والاتصال. لذلك، يظل ISA 315 محورًا لضمان جودة التدقيق في عصر السحابة، ويستلزم دمج فهمٍ تقني للسحابة ضمن فهم بيئة الوحدة الاقتصادية ورقابتها الداخلية لتقييم دقيق للمخاطر الجوهرية.

رابعا: معيار التدقيق الدولي رقم 330 استجابة المدقق للمخاطر المقدّرة (IAASB,2009):

يحدد معيار ISA 330 مسؤولية المدقق في تصميم وتنفيذ استجابات فعالة لمخاطر الأخطاء الجوهرية المقدّرة بالقوائم المالية، سواء على مستوى القوائم ككل أو على مستوى التأكيدات (المعاملات، الأرصدة، الإفصاحات).

تطبيق معيار التدقيق الدولي رقم ISA 330 في بيئة الحوسبة السحابية:

تزداد أهمية ISA 330 في التدقيق السحابي؛ لأنه يوجّه المدقق إلى تصميم استجابات عامة تراعي مخاطر الاعتماد على مزوّد الخدمة (مثل فقدان البيانات أو تعذّر الوصول للأدلة)، وتنفيذ إجراءات تقنية متخصّصة كفحص سجلات الوصول الرقمية واختبار سلامة النسخ الاحتياطية. كما يقتضي اختبار فعالية الضوابط الإلكترونية لدى المزوّد (التشفير، إدارة الهوية، التحكم في الوصول)، وتوظيف تحليلات بيانات متقدمة لاكتشاف علاقات غير منطقية أو فروقات مفاجئة. ويُلزم بتقييم كفاية وموثوقية الأدلة الإلكترونية عندما تكون المصدر الوحيد المتاح. وإذا قيّدت سياسات المزوّد أو التشفير وصول المدقق إلى أدلة أساسية، فيجب توثيق ذلك بوضوح وتقييم أثره على الرأي المهني النهائي.

خامسا: معيار التدقيق الدولي402 ISA الاعتبارات الخاصة بالتدقيق عند استعمال خدمات مؤسسة تقدم خدمات (مقدم الخدمة) (IAASB,2009):

يتناول معيار ISA 402 مسؤولية مدقق الحسابات تجاه الوحدات الاقتصادية التي تستعمل خدمات جهات خارجية (مقدمي الخدمة) لتنفيذ عمليات قد تؤثر على إعداد القوائم المالية .ويمتد نطاق المعيار ليشمل العمليات التي تُنفذ خارجيًا، خاصة إذا أثرت على نظام الرقابة الداخلية أو البيانات المحاسبية ذات الصلة.

ربط معيار التدقيق الدولي ISA 402 بالحوسبة السحابية(Cloud Computing)

يكتسب ISA 402 أهمية خاصة في بيئة الحوسبة السحابية؛ لأن جزءًا من نظام المعلومات والرقابة الداخلية ينتقل فعليًا إلى مزوّد الخدمة .(AWS/Azure/Google Cloud) على المدقق تقييم ضوابط الأمان والوصول وتكامل البيانات لدى المزوّد، والاستفادة من تقارير SOC 1 Type II أو ISAE 3402 لفهم تصميم الضوابط وفاعليتها—بما في ذلك الضوابط المكملة على عاتق المنشأة. وإذا تعذّر الحصول على أدلة كافية وملائمة من المزوّد أو بدائلها، فقد ينشأ قيد على نطاق التدقيق يجب توثيقه وأخذ أثره على الرأي المهني. كما ينبغي تقييم الحاجة للإفصاح في القوائم المالية عن الاعتماد

على خدمات سحابية عندما يكون له أثر جوهري على معالجة البيانات أو الرقابة. بهذا الإطار، يمكّن ISA 402 المدقق من التعامل المهني المرن مع مخاطر الاعتماد على خدمات خارجية ضمن التحول الرقمي.

سادسا: معيار التدقيق الدولي رقم 500 ادلة الاثبات (IFAC,2016)

يُعد معيار ISA 500 من المعايير الأساسية التي تُحدد مسؤولية المدقق في الحصول على أدلة إثبات كافية وملائمة لدعم رأيه في القوائم المالية ويؤكد المعيار أن جودة عملية التدقيق ترتبط ارتباطًا مباشرًا بمدى ملاءمة وموثوقية الأدلة التي جُمعت من مصادر متعددة، سواء كانت داخلية أو خارجية.

ربط معيار التدقيق الدولي رقم 500 ISAبالحوسبة السحابية:

إدارة الأدلة في السحابة تتطلّب من المدقّق توثيقًا وتقنيات تدقيق أدقّ من المعتاد: أولًا، يتحقّق من موثوقية الأدلة الإلكترونية المخزّنة لدى المزود عبر مراجعة الضوابط التقنية والأمن ية) مثل امتثال ISO/IEC 27001 وتقارير (2 SOCوآليات حماية السجلات من العبث. ثانيًا، عند الاعتماد على الأدلة الرقمية (سجلات الخوادم، تقارير النشاط، قواعد البيانات) يُقيِّم مخاطر التعديل غير المرئي عبر تتبّع الأثر، الطوابع الزمنية، وسلاسل الحفظ. ثالثًا، يفحص تكامل وشفافية البيانات المستخرجة من الأنظمة السحابية خصوصًا عندما تتم المعالجة خارج سيطرة المنشأة. رابعًا، يطالب بإثباتات التعاقد وسياسات حفظ/استرجاع البيانات لضمان توافر الأدلة. أمّا اعتبارات التدقيق المهمة: فإذا ظهر تناقض أو شكّ في الموثوقية فيوسّع الإجراءات (اختبارات إضافية، مصادر بديلة، تأكيدات خارجية)، كما يراجع مخرجات خبراء الإدارة أو الأنظمة الذكية السحابية من حيث الكفاءة والموضوعية والدقة قبل اعتمادها بوصفها أدلة كافية وملائمة

سابعا: معيار التدقيق الدولي رقم 505 ISA التأكيدات الخارجية(IAASB,2004) :

يُعالج معيار ISA 505 استعمال التأكيدات الخارجية كوسيلة موثوقة للحصول على أدلة تدقيق كافية وملائمة لدعم رأي المدقق بشأن القوائم المالية ويُركّز المعيار على الحالات التي يكون فيها مستوى مخاطر التحريف الجوهري مرتفعًا، مما يتطلب أدلة من مصادر مستقلة خارجية.

ربط التدقيق الدولي رقم 505 ISA بالحوسبة السحابية:

في بيئة الحوسبة السحابية تتخذ التأكيدات الخارجية بُعدًا تقنيًا إضافيًا؛ إذ يستعمل المدقق تأكيدات من أطراف ثالثة (مزودي التخزين/المعالجة) للتحقق من وجود العقود، مستوى الامتثال، أو الالتزامات، ويمكن الاستناد إلى تقارير ضمان مستقلة (SOC 1/SOC 2) كجزء من الأدلة—مع التنبيه أنها لا تُغني عن تأكيدات أرصدة/عمليات محددة عند الحاجة) وفق ISA 500 و .(ISA 505وعند تلقي التأكيدات عبر وسائل رقمية، يُتحقق من هوية المستجيب وموثوقية القناة (تواقيع رقمية، بروتوكولات أمن ة، بوابات مخصصة، أو إجراءات "اتصال عكسي" للتحقق)، مع توثيق المصدر ووقت الاستلام. وللأرصدة أو العمليات المُدارة سحابيًا) حسابات بنكية إلكترونية، إدارة مخزون عبر (SaaS يُفضَّل الجمع بين تأكيدات خارجية مباشرة من الجهة المالكة للبيانات ومراجعة سجلات المنصة السحابية لتقليل مخاطر الاعتماد على نظام واحد. وأخيرًا، تُعالَج الاستثناءات والتناقضات بإجراءات بديلة (مطابقات مستقلة، أدلة من مصدر ثانٍ)، ويُوثَّق نطاق التأكيدات وحدودها وأثر أي قيود على رأي المراجعة.

ثأمن ا: معيار التدقيق الدولي رقم 520 ISA الإجراءات التحليلية(ISA 520, 2016)

يتناول هذا المعيار مسؤولية المدقق في استعمال الإجراءات التحليلية خلال مراحل مختلفة من التدقيق، سواء بوصفها إجراءات موضوعية للحصول على أدلة تدقيقية مباشرة، أو كإجراء عام يُستعمل في نهاية التدقيق لتكوين استنتاج شامل حول القوائم المالية.

ربط معيار التدقيق الدولي رقم 520 ISA بالحوسبة السحابية:

يُمكّن الاعتماد على الأنظمة السحابية (ERP/CRM) المدقّق من إجراء تحليلات فورية تعزز سرعة كشف التحريفات، لكن يستلزم التحقق من موثوقية البيانات المجلوبة عبر واجهات API ودمج بيانات تشغيلية غير مالية بحذر وتقييم نتائج الأدوات الذكية بما يضمن قابليتها للتفسير. وتتحول المعايير إلى خارطة طريق تبدأ بـ 300ISA لتخطيط نموذج الخدمة ومسارات البيانات، ثم 315ISA مع الاستناد إلى 27001ISO/IEC و27017 لتقييم ضوابط الأمن. وبعد تقدير المخاطر، يطبّق 330ISA باختبارات رقابة تقنية وإجراءات موضوعية مدعومة بـ 520ISA و 500ISA. وعند الاعتماد على مزوّد خدمة، يُستعمل 402ISA (تقارير 3402SOC/ISAE) وتُستكمل الأدلة بتأكيدات خارجية وفق 505ISA، مع الاسترشاد بـ COBIT 2019 وITIL، وتوثيق أي قصور رقابي وفق 265ISA.

ومن خلال ما تقدم؛ يتبين ضرورة تكييف معايير التدقيق الدولية مع بيئة الحوسبة السحابية، بحيث يشمل فهم الضبط الداخلي والسحابي معًا (الوصول والهوية، التشفير، مواقع البيانات) واعتماد أدلة رقمية موثوقة وافصاحات مناسبة. وتُعد معايير ISO/IEC 27001 و27017 مرجعية أمنية مهمة لكنها غير كافية وحدها، لذا يلزم دمجها مع أطر الحوكمة والتشغيل مثل COBIT 2019 و .ITILعمليًا، يرتكز التدقيق السحابي على منظومة300) ISA ، 315، 330، 402، 500، 505، 520، 265 (لتخطيط العمل وتقدير المخاطر والاستجابة لها، والتحقق من الأدلة الخارجية والإلكترونية، وتوثيق أوجه القصور والتواصل بها مهنيًا.

المبحث الثالث

دليل استرشادي مقترح لتدقيق الحسابات في بيئة الحوسبة السحابية في ضوء معايير التدقيق المعتمدة

في ضوء ما نُوقش في المبحث السابق، يمكن توضيح ما يجب الاستناد عليه لمراقب الحسابات عند العمل في بيئة الحوسبة السحابية بحيث تتضمن الآتي:

أولا فهم بيئة الحوسبة السحابية والضبط الداخلي في عمليات التدقيق الخارجي

يعد فهم بيئة الحوسبة السحابية (Cloud Environment) والضبط الداخلي (Internal Control) من أولى وأهم مراحل التدقيق الخارجي عند تدقيق حسابات الوحدة الاقتصادية التي تعتمد على خدمات الحوسبة السحابية؛ وذلك لأن الاعتماد على السحابة يؤثر على هيكل تقنية المعلومات، طبيعة إدارة البيانات، توزيع المسؤوليات، ونوعية المخاطر التي قد تواجهها الوحدة الاقتصادية.

كما يشمل هذا الفهم عدة أمور وهي:

1. تحديد نموذج السحابة والخدمات المستعملة مثل:

أ. نموذج الخدمة: هل تعتمد الوحدة الاقتصادية على البرمجيات كخدمة(SaaS) ، أو المنصة كخدمة(PaaS) ، أو البنية التحتية كخدمة(IaaS) ؟

ب. نموذج النشر: سحابة عامة(Public) ، خاصة(Private) ، أو هجينة(Hybrid) ؟

ت. الأطراف ذات العلاقة: تحديد العلاقة بين الزبون (الوحدة الاقتصادية)، ومزود الخدمة السحابية مثل(AWS ، Azure، وأي أطراف خارجية أخرى) .

2. فهم الهيكل التقني والحوكمة وكما يأتي:

أ. رسم خريطة تدفق البيانات: كيف تنتقل البيانات من/إلى السحابة؟ ما نقاط الدخول والخروج؟

ب. توزيع المسؤوليات: ما مسؤولية كل طرف في حفظ البيانات، حماية الخصوصية، إجراء النسخ الاحتياطي، واستعادة البيانات؟

ت. سياسات إدارة الموظفين: كيف يتم التحكم في الصلاحيات والوصول إلى البيانات والتطبيقات؟

3. دراسة الضبط الداخلي في بيئة السحابة من خلال:

أ. فحص إجراءات الضبط الداخلي الجديدة أو المعدلة: ما التغيرات التي طرأت على الضبط الداخلي عند الانتقال للسحابة (مثلاً، هل لا تزال الضوابط الخاصة بالتوثيق، الموافقات، الفصل بين المهام فعالة)؟

ب. تحليل الاعتماد على مزود الخدمة: هل لدى المدقق إمكانية الوصول إلى سجلات وأنظمة السحابة أم يعتمد على تقارير مزود الخدمة مثل تقارير(SOC) ؟

ثانياً: تقييم المخاطر المرتبطة بالحوسبة السحابية

يعد تقييم المخاطر (Risk Assessment) خطوة محورية في أي عملية تدقيق خارجي، وتزداد أهميتها في بيئة الحوسبة السحابية نظرًا لتعدد الأطراف، وتشعب مصادر الخطر، وتحول الكثير من عناصر التحكم إلى مزودي الخدمة السحابية حيث ان الهدف هذه الخطوة هو تحديد وفهم وتقييم مدى احتمالية حدوث أخطاء جوهرية في البيانات المالية أو فقدان أو تسريب البيانات نتيجة العمل في بيئة سحاب، كما تشمل عملية تقييم المخاطر المرتبطة بالحوسبة السحابية عدة نقاط وهي:

1. التعرف أنواع المخاطر في الحوسبة السحابية وهي:

أ. مخاطر فقدان البيانات: بسبب أعطال تقنية، هجمات إلكترونية، أو سوء إدارة النسخ الاحتياطية.

ب. مخاطر سرية المعلومات: مثل الوصول غير المصرح به إلى البيانات أو انتهاك الخصوصية.

ت. مخاطر توافر الخدمة: توقف الخدمة أو تعطل النظام السحابي مما يؤثر على استمرارية العمليات.

ث. مخاطر الاعتماد على طرف ثالث: ضعف الضوابط أو الأهمال أو التقصير من جانب مزود الخدمة السحابية.

ج. مخاطر الامتثال للأنظمة والتشريعات: مثل عدم التوافق مع متطلبات حماية البيانات المحلية والدولية(GDPR) ، ISO (27001)

2. تحديد خطوات تقيم المخاطر في عند تدقيق الحسابات في بيئة الحوسبة السحابية كما يأتي:

أ. **جمع المعلومات حول البيئة السحابية:** ويتم ذلك من خلال تحديد الخدمات والتطبيقات التي تعمل على السحابة والتعرف على نوع وأهمية البيانات المخزنة (مالية، شخصية، سرية).

ب. **تحليل سياسات وإجراءات إدارة المخاطر:** ويتم ذلك من خلال مراجعة سياسات الوحدة الاقتصادية لإدارة مخاطر العمل مع أطراف خارجية مع فحص وجود خطة لإدارة الكوارث وخطة استمرارية الأعمال.(BCP/DRP)

ت. **تدقيق التعاقدات مع مزود الخدمة:** ويتم ذلك من خلال دراسة شروط اتفاقية مستوى الخدمة(SLA) كما يجب التأكد من وجود بنود واضحة بشأن أمن البيانات، مسؤولية حماية البيانات، والتزامات التعويض في حالة الفقد أو التلاعب.

ث. **اختبار الضوابط التقنية:** التأكد من آليات التشفير، النسخ الاحتياطي، إدارة الوصول والصلاحيات، ومراقبة الأنشطة كما يجب التأكد من إجراء اختبارات دورية على الضوابط الأمن ية.

ج. **الاعتماد على تقارير الطرف الثالث:** الاستفادة من تقارير تدقيق مزود الخدمة مثل SOC 1/SOC2أو تقارير الامتثال لمعايير .ISO/IEC 27001

3. كما ان دور المدقق الخارجي في هذه المرحلة يستطيع المدقق تحديد الاتي:

أ. تحديد المخاطر الجوهرية التي قد تؤثر على جودة وموثوقية البيانات المالية.

ب. تقديم التوصيات بشأن تعزيز ضوابط التحكم وإدارة المخاطر.

ت. توجيه عمليات الفحص التفصيلي والتركيز على النقاط الحرجة التي قد تمثل فجوات في الضبط الداخلي.

ثالثاً: فحص ضوابط الوصول والصلاحيات(Access & Privilege Controls)

ضوابط الوصول والصلاحيات (Access Controls) تعني السياسات والإجراءات التي تضمن أن الوصول إلى الأنظمة والبيانات السحابية مقتصر فقط على الأشخاص المخولين بذلك، على وفق حدود واختصاصات كل موظف في بيئة الحوسبة السحابية، حيث تكتسب هذه الضوابط أهمية خاصة بسبب تعدد الموظفين، وتوزيع الإدارة بين الوحدة الاقتصادية ومزود الخدمة، وخطورة اختراق البيانات المالية أو الحساسة.

رابعا التحقق من سلامة البيانات واستمرارية الأعمال في التدقيق الخارجي

سلامة البيانات:(Data Integrity)

يقصد بها التأكد من أن البيانات المخزنة والمعالجة في البيئة السحابية صحيحة، مكتملة، لم تتعرض للتغيير أو التلاعب غير المصرح به، ويمكن الاعتماد عليها في التقارير المالية والقرارات الإدارية.

استمرارية الأعمال:(Business Continuity)

تعني قدرة الوحدة الاقتصادية على الاستمرار في أداء عملياتها الحيوية (وخاصة المالية) حتى في حال وقوع حوادث أو كوارث أو توقف مؤقت في الخدمات السحابية، من خلال خطط واضحة لاستعادة الأنظمة والبيانات (Disaster Recovery Plans).

إجراءات التحقق في التدقيق الخارجي

1. **التأكد من سياسات النسخ الاحتياطي واستعادة البيانات:**

أ. التأكد من وجود سياسة واضحة للنسخ الاحتياطي (Backup Policy) تتضمن تكرار النسخ، أماكن التخزين (محلي/سحابي)، وفترات الاحتفاظ.

ب. التحقق من اختبار خطط استعادة البيانات (Disaster Recovery Testing) بانتظام، وعدم الاعتماد فقط على النظري أو الوثائق.

2. **فحص آليات حماية وسلامة البيانات:**

أ. التأكد من تطبيق تقنيات التشفير (Encryption) خلال نقل البيانات وتخزينها في السحابة.

ب. التأكد من إجراءات التحقق من سلامة الملفات بعد الاسترجاع مثل (التحقق من التوقيع الرقمي)

3. **تدقيق ضوابط الحماية من الفقد أو التلاعب:**

أ. التحقق من وجود آليات لمنع التلاعب أو التغيير غير المصرح به في قواعد البيانات أو الملفات الحساسة.

ب. تدقيق سجلات التغييرات (Change Logs) وسجلات العمليات (Audit Trails) لتحديد أي تعديلات أو محاولات وصول غير مشروعة.

4. **اختبار استمرارية الأعمال وخطط الطوارئ:**

أ. التأكد من وجود خطة استمرارية أعمال (Business Continuity Plan, BCP) متكاملة تغطي جميع أنشطة الوحدة الاقتصادية الحرجة.

ب. فحص مدى جاهزية خطة التعافي من الكوارث(Disaster Recovery Plan, DRP) ، والتأكد من إجراء اختبارات دورية عليها.

5. **تقييم دور مزود الخدمة السحابية:**

أ. التأكد من التزام مزود الخدمة بمعايير الاعتمادية واستمرارية الأعمال مثلاً22301 (ISO/IEC :، ISO/IEC 27017)

ب. التأكد من تقارير التدقيق الخارجي مثل (SOC 2 Type II) الخاصة بسلامة البيانات واستمرارية الخدمة لدى مزود الخدمة.

خامسا تدقيق العمليات والبيانات المالية في بيئة الحوسبة السحابية:

تدقيق العمليات والبيانات المالية في السحابة أصبح من أهم التحديات للمدقق الخارجي؛ بسبب التغير في طريقة إدارة وتخزين ومعالجة البيانات. يجب التأكد من أنَّ جميع العمليات المالية والإجراءات المحاسبية المنفذة عبر الأنظمة السحابية دقيقة، كاملة، وموثوقة، ولم تتعرض لأخطاء أو تلاعب.

خطوات تدقيق العمليات والبيانات المالية

1. **فحص سير العمليات المحاسبية:**

أ. تدقيق دورة العمليات المالية (الشراء، البيع، الدفع، التحصيل، التسويات البنكية...) المنفذة عبر أنظمة الحوسبة السحابية.

ب. التأكد من وجود ضوابط للتحقق من صحة البيانات المدخلة، وحماية العمليات من الأخطاء أو الازدواجية.

2. **اختبار تكامل البيانات المالية:**

أ. التأكد من أن جميع العمليات التي تتم في النظام السحابي تنعكس بشكل صحيح ومتكامل في السجلات المحاسبية والتقارير المالية.

ب. فحص الربط بين الأنظمة السحابية المختلفة: (مثل الربط بين نظام الفواتير ونظام المخزون ونظام المحاسبة العامة).

3. **التدقيق التحليلي واستعمال الأدوات الرقمية:**

أ. إجراء اختبارات تحليلية (Substantive Analytical Procedures) لمقارنة الأرقام المالية الفعلية بالمتوقع، ورصد أي فروقات جوهرية.

ب. استعمال أدوات التحليل الرقمي (Data Analytics) والذكاء الاصطناعي لرصد الأنماط غير الطبيعية أو المعاملات الشاذة.(Outliers)

4. **التأكد آليات إدخال وتعديل وحذف البيانات:**

أ. التأكد من وجود ضوابط للموافقة على التعديلات في القيود المالية، وتوثيق عمليات الإضافة أو التعديل أو الإلغاء.

ب. فحص سجل العمليات (Audit Trail) لأي تغيير أو معالجة مالية تمت على النظام.

5. **مطابقة البيانات والتقارير:**

أ. إجراء مطابقة بين التقارير المالية الصادرة عن الأنظمة السحابية والسجلات الخارجية أو البنكية أو الوثائق الأصلية.

ب. التأكد من مطابقة القيود والبيانات بين الفترات المالية المختلفة.

6. **تقييم الاعتمادية على الضوابط التقنية:**

أ. التأكد من فعالية الضوابط الآلية المضمنة في النظام السحابي لمنع الأخطاء والتلاعب.

ب. التأكد من نتائج اختبارات التدقيق الداخلي أو تقارير SOC الخاصة بمزود النظام.

سادساً: التأكد من الامتثال للمعايير واللوائح:

الامتثال (Compliance) هو مدى الوحدة الاقتصادية – وكذلك مزود الخدمة السحابية – بالتشريعات والقوانين الوطنية والدولية، وأيضاً بالمعايير المهنية والإرشادات التقنية التي تحكم أمن المعلومات، حماية البيانات، والإفصاح المالي. يشمل ذلك كل ما يتعلق بحقوق وحماية بيانات الزبائن، السرية، الأمان، الاحتفاظ بالسجلات، التراخيص، والشفافية.

إجراءات التأكد من الامتثال في التدقيق الخارجي:

1. **التأكد التزام الوحدة الاقتصادية ومزود الخدمة بالمعايير الدولية:**

أ. التحقق من التزام الوحدة الاقتصادية ومزود الخدمة بمعايير أمن المعلومات مثل ISO/IEC 27001، ISO/IEC 27017(لحماية البيانات في السحابة)، ومعايير حماية البيانات الشخصية مثل GDPRأو أي متطلبات وطنية مماثلة.

ب. التأكد من توفر شهادات امتثال رسمية لدى مزود الخدمة.

2. **التأكد من الامتثال لمتطلبات الهيئات الرقابية والتشريعات المحلية:**

أ. فحص مدى التزام الوحدة الاقتصادية بالقوانين المحلية (مثل قوانين المصارف، قوانين حماية البيانات الوطنية، تعليمات البنك المركزي...إلخ).

ب. التأكد من بنود الاتفاق مع مزود الخدمة السحابية بخصوص الامتثال للمتطلبات التشريعية المحلية والدولية.

3. **تدقيق الاتفاقيات التعاقدية مع مزود الخدمة:**

أ. دراسة اتفاقيات مستوى الخدمة (SLA) للتأكد من احتوائها على بنود واضحة حول حماية البيانات، سرية المعلومات، وتحديد المسؤوليات في حال وقوع خرق أمن ي أو فقدان بيانات.

ب. التأكد من حق الوحدة الاقتصادية في إجراء تدقيق دوري على بيئة مزود الخدمة.

4. **مراجعة تقارير التدقيق والاختبارات المستقلة:**

أ. الاستفادة من تقارير الامتثال أو التدقيق الصادرة عن جهات خارجية مستقلة مثل (تقارير SOC 1 ، SOC 2).

ب. مراجعة نتائج عمليات تدقيق سابقة ومعالجة الملاحظات أو التحسينات المقترحة.

5. **تقييم الضوابط الرقابية الداخلية المتعلقة بالامتثال:**

أ. التأكد من وجود سياسات واضحة ومحدثة للامتثال.

ب. فحص آليات التدريب والتوعية للموظفين حول المتطلبات الرقابية والتشريعية الخاصة بالعمل في البيئة السحابية.

ت. مراجعة الإجراءات الخاصة بالإبلاغ الفوري عند وقوع خرق أو مخالفة تنظيمية.

6. نقاط رئيسة في تقرير التدقيق حول الامتثال:

أ. مدى التزام الوحدة الاقتصادية ومزود الخدمة بالمعايير الدولية والتشريعات المحلية.

ب. تقييم فعالية الضوابط والإجراءات المتعلقة بالامتثال.

ت. بيان أية فجوات أو نقاط ضعف أو مخاطر عدم الامتثال.

سابعا: توصيات لتحسين الضوابط في بيئة الحوسبة السحابية

1. تطوير سياسات وإجراءات واضحة ومحدثة

أ. صياغة وتحديث سياسات أمن المعلومات وحوكمة السحابة بما يتوافق مع أحدث التحديات والتقنيات، مع تدقيقها بشكل دوري.

ب. وضع سياسة رسمية لإدارة الهوية والصلاحيات (IAM) تشمل موافقات إدارية لكل إضافة أو تعديل على الصلاحيات.

2. تعزيز وميكنة ضوابط الوصول والصلاحيات

أ. تفعيل التوثيق المتعدد العوامل (MFA) لجميع الحسابات الهامة والامتيازات العالية.

ب. استعمال أدوات مراقبة الصلاحيات وتنبيه الإدارة عن أي تغييرات غير طبيعية في حسابات الموظفين.

3. تحسين خطط النسخ الاحتياطي والتعافي من الكوارث

أ. إجراء اختبارات دورية على خطط النسخ الاحتياطي وخطط التعافي من الكوارث(DRP) ، والتأكد من أن النسخ الاحتياطية مخزنة في مواقع منفصلة وأمن ة.

ب. توثيق عمليات استرجاع البيانات والتأكد من فاعلية خطط الاستمرارية العملية.(BCP)

4. تعزيز التدريب والتوعية

أ. تنظيم دورات تدريبية منتظمة لموظفي تقنية المعلومات والموظفين الرئيسيين حول التهديدات الأمنية الحديثة في الحوسبة السحابية وأفضل ممارسات الضبط الداخلي.

ب. إصدار نشرات توعوية دورية حول سياسات الامتثال وحماية البيانات.

5. مراجعة دورية للامتثال والضوابط التقنية

أ. إجراء مراجعات تدقيقية داخلية دورية وفجائية لضوابط السحابة بالتعاون مع مدققين خارجيين.

ب. الاستفادة من تقارير التدقيق الخارجية لمزودي الخدمة مثل (SOC 2، ISO 27001) ومراجعة معالجة الملاحظات السابقة.

6. تحديث الاتفاقيات مع مزودي الخدمة

أ. التأكد من أن عقود الخدمات السحابية تتضمن شروطًا واضحة حول التزامات الأمن، حماية البيانات، حق التدقيق، والتعويض في حالات الإخلال.

ب. التفاوض على بنود SLA أكثر صرامة فيما يخص توافر الخدمة ووقت الاستجابة للحوادث.

الاستنتاجات

1. لا توجد معايير تدقيق "خاصة بالسحابة" تكفي بذاتها؛ المطلوب تكييف منظومة ISA ودمجها مع أطر الأمن والحوكمة (ISO/COBIT/ITIL)لتغطية الجوانب المالية والتقنية معًا.
2. الانتقال إلى السحابة ينقل جزءًا من الرقابة إلى مزود الخدمة؛ لذا يصبح فهم "المسؤولية المشتركة" وضوابط الوصول والتشفير شرطًا أساسيًا لجودة التدقيق.
3. قوة التدقيق مرهونة بملاءمة وموثوقية الأدلة الرقمية وقابليتها للتتبّع؛ تقارير SOC تعزّز الفهم لكنها لا تغني عن إجراءات جوهرية واستقلالية الأدلة عند الحاجة.
4. التخطيط المستمر وفق ISA 300 وISA 315—مع فهم نموذج الخدمة (SaaS/PaaS/IaaS) ومسارات البيانات—هو الأساس لتقدير المخاطر وتصميم استجابات فعّالة.(ISA 330)
5. رفع الكفاءة التقنية للمدققين وتحسين الامتثال التعاقدي والتنظيمي يقللان فجوات المخاطر ويعظّمان موثوقية القوائم المالية في بيئة الحوسبة السحابية.

التوصيات

1. تطوير "إطار تدقيق سحابي مُهَجّن" يدمج معايير ISA مع أطر (ISO/COBIT/ITIL).
2. إلزامية "تدقيق نموذج المسؤولية المشتركة" للتحقق من ترسيم الحدود وضوابط الوصول.
3. اعتماد نموذج "الثقة مع التحقق" للأدلة (استعمال تقارير SOC لتقييم المخاطر، واستكمالها بإجراءات جوهرية).
4. التحول إلى "التخطيط المستمر للتدقيق" (تطبيق ISA 315 ديناميكيًا) مع "تدقيق مسارات البيانات".
5. الاستثمار المزدوج في "رفع الكفاءة التقنية للمدققين" و"إدراج تدقيق العقود (SLAs)" بوصفه إجراءً إلزامياً.

المصادر

1. السقا، زياد هاشم. (2023). إطار مقترح لتدقيق الحسابات في بيئة السحابة الالكترونية. مجلة دراسات متقدمة في المالية والمحاسبة، المجلد 6، العدد 1، العراق.
2. حبيب، سمير. (2022). دور المحاسبة ومعايير التدقيق السحابي في تأكيد أمن البيانات والمعلومات. مجلة جامعة تشرين، العلوم الاقتصادية والقانونية، المجلد 44، العدد 6، سوريا.

3. سلطان، تيسير جواد. (2023). أثر فاعليه التدقيق الداخلي في إدارة مخاطر الحوسبة السحابية، المجلد 19، العدد4، العراق.

4. مجي، احمد حسين، كاظم، تيسير جواد. (2023). أثر كفاءة مراقب الحسابات على ممارسة التدقيق السحابي دراسة استطلاعية لعينة من الأكاديميين والمهنيين في اختصاص المحاسبة والتدقيق. العدد 69، المجلد 2، مصر.

References

1. Al-Saqqa, Ziyad Hashim. (2023). A Proposed Framework for Auditing in the Electronic Cloud Environment. Journal of Advanced Studies in Finance and Accounting, Vol. 6, No. 1, Iraq.

2. Bayastura, Siti Fatimah, Krisdina, Sari, & Widodo, Agus Purnomo. (2021). Analysis and Design of Information Technology Governance Using the COBIT 2019 at PT XYZ. JIKO: Jurnal Informatika dan Komputer, Vol. 4, No. 1, Indonesia.

3. Habib, Samir. (2022). The Role of Accounting and Cloud Auditing Standards in Ensuring Data and Information Security. Tishreen University Journal for Economic and Legal Sciences, Vol. 44, No. 6, Syria.

4. International Auditing and Assurance Standards Board (IAASB). (2009). International Standards on Auditing: ISA 300 Planning an audit of financial statements (Translated by Chartered Accountants of Canada). IFAC, Canada.

5. International Auditing and Assurance Standards Board (IAASB). (2020). ISA 315 (Revised 2019): Identifying and assessing the risks of material misstatement. International Auditing and Assurance Standards Board (IAASB), IFAC, United States.

6. International Auditing and Assurance Standards Board (IAASB). (2009). International Standard on Auditing (ISA 265): Communicating deficiencies in internal control to those charged with governance and management. International Auditing and Assurance Standards Board (IAASB), IFAC, United States.

7. International Auditing and Assurance Standards Board (IAASB). (2009). ISA 402: Audit considerations relating to an entity using a service organization (Reaffirmed 2020). IFAC, United States.

8. International Auditing and Assurance Standards Board (IAASB). (2004). ISA 505: External confirmations. IFAC, United States.

9. International Federation of Accountants (IFAC). (2016). ISA 500: Audit evidence (Approved June 2018). Malaysian Institute of Accountants.

10. International Federation of Accountants (IFAC). (2016). ISA 520: Analytical procedures (Approved June 2018). Malaysian Institute of Accountants.

11. International Organization for Standardization / International Electrotechnical Commission (ISO/IEC). (2015). ISO/IEC 27017:2015 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. International Organization for Standardization / International Electrotechnical Commission, Switzerland.

12. Kusumawati, Ayu, Jamal, Dwi Kurniawan, & Haliah. (2023). Information System Audit Using COBIT 2019 Framework in Construction Companies. Journal of Software Engineering and Simulation, Vol. 9, No. 4, Indonesia.

13. Maji, Ahmed Hussein, & Kazem, Taysir Jawad. (2023). The Impact of Auditor Efficiency on the Practice of Cloud Auditing: An Exploratory Study of a Sample of Academics and Professionals in Accounting and Auditing. Vol. 69, No. 2, Egypt.

14. Sultan, Taysir Jawad. (2023). The Impact of Internal Audit Effectiveness on Cloud Computing Risk Management. Vol. 19, No. 4, Iraq.