The Administration & Economic College Journal
For Economics & Administration & Financial Studies
Vol. ٩,N.٣, P P. ١-٢٤
ISSN PRINT 2312-7813
ISSN ONLINE 2313-1012
مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية
المجلد ٩، العدد٣، ٢٠١٧ ص ص ٢٤-١

Role of Governance in Reducing the Audit Risks of computerized accounting Systeme Under COBIT Framework of Internal Control

دور حوكمة تكنولوجيا المعلومات في تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية في ظل إطار عمل (COBIT) للرقابة الداخلية

(*)أ.م.د.عقيل حمزة حبيب ألحسناوي. (**) م. م. إنعام محسن الموسوي.

Abstract

The rapid shift in accounting information systems from manual to electronic media has significant implications of Information Technology (IT) for the process of financial reporting. The intense dependency on computerized accounting information systems could expose company data to information security risk, and then may lead to increase audit risks. Therefore, this research aims to illustrate how can IT governance mechanisms support the information security of computerized accounting information systems. In particular, the research examines the role of IT governance under the COBIT framework of Internal control in reducing the audit risks in Iraqi private banks.

The findings reveal that application of IT governance in Iraqi private banks can reduce audit risks assessed by external IT auditors, increase the reliability of accounting information systems, and support information security under computerized accounting information systems. In addition, the empirical results reveal that there is a significant positive relation between reducing audit risks and IT Governance dimensions (tools and automation, policies, plans and procedures, responsibility and accountability, and skills and expertise, awareness and communications, and goal setting and measurement) respectively. Finally the research recommends adopting the COBIT framework as a tool to IT governance framework that support risk management in computerized accounting systems.

المستخلص:-

إن التحول المتسارع في نظم المعلومات المحاسبية من النظام اليدوي إلى الوسائط الالكترونية حمل الكثير من الآثار المتعلقة بتكنولوجيا المعلومات على عملية الإبلاغ المالي. فالاعتماد المكثف على نظم المعلومات المحاسبية الالكترونية قد يعرض قواعد بيانات الشركة إلى مشاكل تتعلق بأمن المعلومات والتي تقود إلى زيادة مخاطر التدقيق. لذا فان هذا البحث يهدف إلى بيان كيف يمكن لآليات حوكمة تكنولوجيا المعلومات أن تدعم امن المعلومات في ظل نظم المعلومات المحاسبية الالكترونية. ويختبر البحث دور تعزيز حوكمة تكنولوجيا المعلومات في ظل إطار عمل COBIT للرقابة الداخلية في تقليل مخاطر التدقيق في المصارف الأهلية العراقية. وقد بينت النتائج أن تطبيق آليات حوكمة تكنولوجيا المعلومات في المصارف الأهلية العراقية يمكن أن تؤدي إلى تقليل مخاطر التدقيق المقدرة من قبل المدققين الخارجيين وزيادة معوليه نظم المعلومات المحاسبية و دعم امن المعلومات في ظل نظم المعلومات المحاسبية الالكترونية. أظهرت النتائج الميدانية وجود علاقة موجبة وذات دلالة إحصائيا بين تقليل مخاطر التدقيق وأبعاد حوكمة تكنولوجيا المعلومات(الآليات والأتمتة، السياسات والخطط والإجراءات، المسؤولية والمساءلة، المهارات والخبرة، المعرفة والاتصالات، ووضع الأهداف

(*)جامعة الكوفة – كلية الادارة والاقتصاد.
(**)جامعة الكوفة – كلية الادارة والاقتصاد.

والقياس) على التوالي. وأخيرا يوصي البحث باعتماد إطار عمل COBIT للرقابة الداخلية في المصارف الأهلية العراقية بوصفها آلية لحوكمة تكنولوجيا المعلومات التي تدعم إدارة المخاطرة في نظم المعلومات المحاسبية الالكترونية.

المقدمـــة:-

شهد استخدام تكنولوجيا المعلومات في المجالات المحاسبية والمالية تزايداً مضطرداً في المؤسسات المالية العاملة في العراق في السنوات العشرة الأخيرة، وبالأخص في مؤسسات القطاع المصرفي مما أدى إلى زيادة اهتمام المهنيين والباحثين الأكاديميين بدراسة مخاطر، ووسائل الرقابة وتدقيق النظم المحاسبية الالكترونية المطبقة في هذه المؤسسات. في هذا السياق فان المخاطرة والرقابة على نظم المعلومات المحاسبية الالكترونية تعد جوهر العمليات التدقيقية التي تتم في المؤسسات التي تعتمد أنظمة معلومات ذات تكنولوجيا عالية في مجالات تدقيق تكنولوجيا المعلومات، التدقيق المالي فضلاً عن حوكمة تكنولوجيا المعلومات. وقد أكدت الدراسات الحديثة في مجال التدقيق في بيئة تكنولوجيا المعلومات من أمثال Von solms (2005), Iliescu(2010), Alfarajet et al.(2011), Haseley and Brucker(2012), Walker et al.(2012), Rubino and Vitolla (2014a) وغيرهم على الدور الذي آليات حوكمة تكنولوجيا المعلومات في تحقيق أهداف المنظمة، حيث إن التطبيق الفاعل لحوكمة تكنولوجيا المعلومات يساعد في التأكيد أن تكنولوجيا المعلومات تدعم تحقيق أهداف المنظمة وتحسين فاعلية الاستثمار فيها، و تؤدي إلى توفير آلية لرقابة مخاطر تكنولوجيا المعلومات. ويعد إطار عمل COBIT للرقابة الداخلية أنموذجا عاما للرقابة الداخلية على تكنولوجيا المعلومات وحماية امن المعلومات، وكذلك يمثل منهاجاً لإدارة تكنولوجيا المعلومات بشكل أفضل وتوظيف قدراتها لتوفير قيمة مضافة للمنظمة وتأسيس برنامج إدارة مخاطرة لحل المشاكل الجديدة الناتجة عن استخدام تكنولوجيا المعلومات في عمليات المنظمة. من هذا المنطلق تركز الدراسة الحالية على تقويم الدور المحتمل لتعزيز آليات حوكمة تكنولوجيا المعلومات على وفق إطار عمل COBIT للرقابة الداخلية في تقليل مخاطر تدقيق النظم المحاسبية الالكترونية. فتقويم المدقق الخارجي لمخاطر التدقيق يعد عنصراً مهما في عملية التدقيق ويتحكم بشكل كبير بتحديد حجم العينة، تكاليف التدقيق فضلاً عن جودة التدقيق الخارجي ومدى ثقة المستخدمين بالنظام المحاسبي ككل.

المبحث الأول
(منهجية البحث والدراسات السابقة)

<u>أولا: منهجية البحث</u>

مشكلة البحث:-

على الرغم من الدور الذي تلعبه نظم المعلومات الالكترونية في تسهيل عملية الإبلاغ المالي للشركات إلا أن ظهورها اقترن بازدياد مخاطر امن المعلومات من خلال اختراق نظم المعلومات أو محاولات التلاعب بالمعلومات المحاسبية وخصوصاً في القطاع المالي، مما يوثر سلباً على تقدير المدقق الخارجي لدرجة المخاطرة المتأصلة المرتبطة بكل بند من بنود القوائم المالية. وعلى هذا الأساس فان مشكلة البحث تكمن في الحاجة إلى بيان أهمية تطبيق آليات حوكمة تكنولوجيا المعلومات في تعزيز امن النظم المحاسبية الالكترونية، وتقويم دور تعزيز آليات حوكمة تكنولوجيا المعلومات في تقليل مخاطر التدقيق في ظل نظم المعلومات المحاسبية الالكترونية.

أهمية البحث:-

إن الاستخدام المتزايد لتكنولوجيا المعلومات في المجالات المحاسبية والمالية ادى إلى زيادة الاهتمام بالرقابة على نظم المعلومات الالكترونية، إذ أن المخاطر التي تتعرض لها تلك النظم قد تقود إلى فقدان الثقة في المعلومات المحاسبية، وظهور أخطاء جوهرية في عملية القياس الإبلاغ المالي. إذ تؤثر مخاطر نظم المعلومات المطبق في الشركات سلباً في نزاهة ودقة المعلومات المعلنة في القوائم المالية. على أساس ذلك فان أهمية البحث تنبع من الأهمية التي تحظى بها عملية تقدير المخاطرة المرتبطة بنظم المعلومات المحاسبية الالكترونية، ذلك أن تقدير المدقق الخارجي لمخاطر التدقيق يؤثر في الطريقة التي تتم من خلالها أداء المهام التدقيقية، و

على جودة التدقيق ككل. فضلاً عن ذلك فان تقدير مخاطر تدقيق نظم المعلومات المحاسبية تعد عنصراً أساسيا في عمليات التدقيق المالي في ظل تكنولوجيا المعلومات.

أهداف البحث

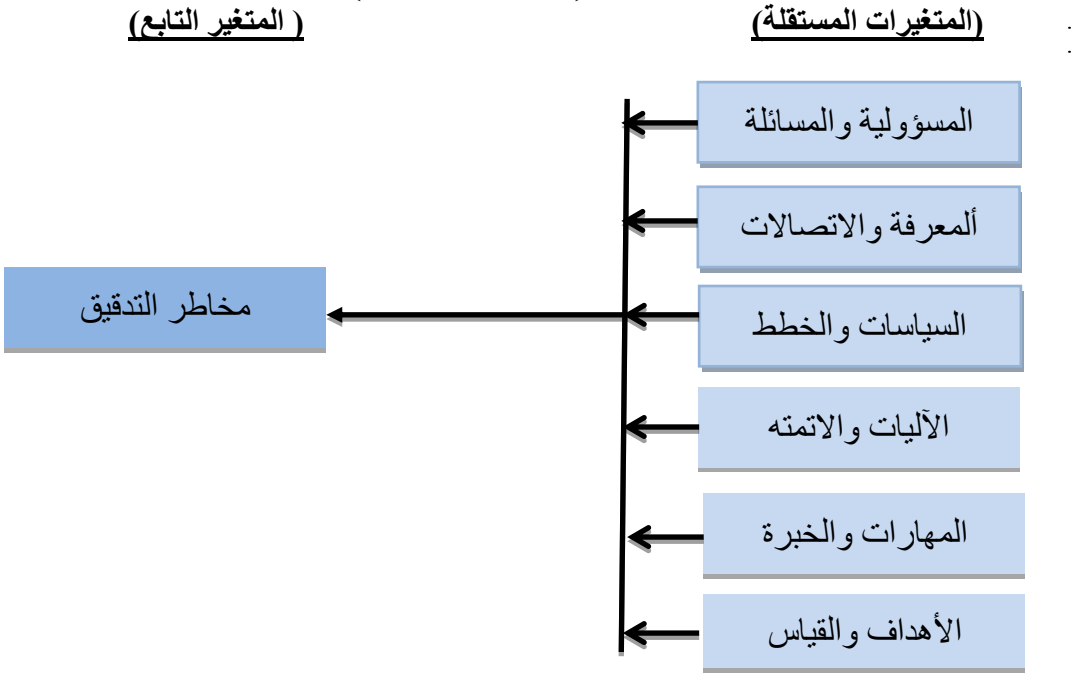
يهدف البحث إلى تحقيق الأتي:

١. توضيح أهمية تطبيق آليات حوكمة تكنولوجيا المعلومات في تعزيز امن المعلومات في ظل النظم المحاسبية الالكترونية
٢. بيان نظري لإطار عمل COBIT للرقابة الداخلية على نظم المعلومات الالكترونية.
٣. تقويم دور تعزيز حوكمة تكنولوجيا المعلومات في تقليل مخاطر تدقيق النظم المحاسبية الالكترونية.

متغيرات البحث

يتكون أنموذج البحث من جانبين، الجانب الأول يضم المتغيرات المستقلة. وتتمثل بالسمات الستة الأساسية لحوكمة تكنولوجيا المعلومات والجانب الثاني يضم المتغير التابع المتمثل بمخاطر التدقيق. ويبين الشكل رقم (١) أنموذج البحث، اذ تشمل ستة متغيرات المستقلة هي (المسؤولية والمساءلة، المعرفة والاتصالات، السياسات والخطط، الآليات والأتمتة، المهارات والخبرة، والأهداف والقياس). أما المتغير التابع فيتمثل بمخاطر التدقيق.

الشكل (١)
(متغيرات البحث)



فرضيات البحث

في ضوء مشكلة البحث ولغرض تحقيق أهدافه في اختبار تأثير تعزيز حوكمة تكنولوجيا المعلومات في الشركة على تقويم المدقق الخارجي لمخاطر التدقيق يقوم البحث على فرضية رئيسة واحدة مفادها أن:

" توجد علاقة ذات دلالة إحصائيا بين تعزيز حوكمة تكنولوجيا المعلومات في الشركة وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية "

وتتفرع عن هذه الفرضية الفرضيات الفرعية الآتية:-

- الفرضية الفرعية الأولى / **Ho1**: توجد علاقة ذات دلالة إحصائيا بين متغير **المسؤولية و المسائلة** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.
- الفرضية الفرعية الثانية / **Ho2**: توجد علاقة ذات دلالة إحصائيا بين متغير **المعرفة والاتصالات** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.
- الفرضية الفرعية الثالثة / **Ho3**: توجد علاقة ذات دلالة إحصائيا بين متغير **السياسات والخطط** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.
- الفرضية الفرعية الرابعة / **Ho4**: توجد علاقة ذات دلالة إحصائيا بين متغير **الآليات والاتمته** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.
- الفرضية الفرعية الخامسة / **Ho5**: توجد علاقة ذات دلالة إحصائيا بين متغير **المهارات والخبرة** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.
- الفرضية الفرعية السادسة / **Ho6**: توجد علاقة ذات دلالة إحصائيا بين متغير **الأهداف والقياس** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.

ثانياً : الدراسات السابقة

تنوعت الدراسات التي تناولت موضوع حوكمة تكنولوجيا المعلومات منها ما ركز على امن المعلومات المالية المعلنة في القوائم المالية في حين حظيت جوانب أخرى باهتمام الباحثين منها العلاقة نظام الرقابة الداخلية، غسيل الأموال، وكذلك فاعلية تطبيق آليات الحوكمة في ظل نظم المعلومات المحاسبية الالكترونية. من هذه الدراسات دراسة أبو حجر وعابدين(٢٠١٤) التي سعت بصورة أساسية إلى محاولة وضع إطار نظري لاستخدام آليات حوكمة تكنولوجيا المعلومات في تخفيض المخاطر التي تواجه أمن المعلومات في الوحدات الحكومية، وذلك من خلال الحد من التلاعب المالي الإلكتروني في ظل نظام الحكومة الإلكترونية. وقد بينت نتائج هذه الدراسة إن التلاعب المالي في ظل الحكومة الالكترونية يزداد ليس فقط بسبب الفساد الإداري وإنما أيضا نتيجة ضعف نظام الرقابة الداخلية، كما أن آليات حوكمة تكنولوجيا المعلومات من مبادئ وأهداف ومعايير تسهم في الحد من التلاعب المالي الالكتروني وتحقيق متطلبات امن المعلومات في الوحدات الحكومية في ظل تطبيق نظام الحكومة الالكترونية.

أما دراسة Tuttle& Vandervelde (2007) فقد هدفت إلى اختبار الإطار النظري لحوكمة تكنولوجيا المعلومات في ظل إطار عمل COBIT للرقابة الداخلية في مجالات التدقيق المختلفة بما في ذلك التدقيق التشغيلي، الامتثال للأنظمة والتعليمات وكذلك التدقيق المالي. وقد بينت نتائج هذه الدراسة أن من المهم والمفيد لمهنة التدقيق البحث عن اختبارات أكاديمية لتطبيقاتها والتي توفر دليل ميداني لواضعي السياسات في تعزيز تطبيقات التدقيق الحالية من عدمه. كما أظهرت النتائج وجود علاقة ارتباط بين تطبيق إطار عمل COBIT للرقابة الداخلية والتقويم الكلي لمخاطر عمليات COBIT في ظل النظم المحاسبية الالكترونية، وبينت النتائج أيضا أن أطار عمل COBIT يمكن أن يستخدم للتنبؤ بسلوك المدققين في مجال توفير مساعدة في عمليات تدقيق تكنولوجيا المعلومات.

كما هدفت دراسة Abu-Musa, (2009) إلى اختبار مدى أهمية وتطبيق أهداف الرقابة على المعلومات والتكنولوجيا المتصلة بها على وفق إطار عمل COBIT في الشركات السعودية. استندت الدراسة إلى عينة مكونة من ١٢٧ مستجيب للاستبانة المصممة لهذا الغرض. وقد بينت نتائج الدراسة إن اغلب المستجيبين من أفراد العينة يدركون أهمية تطبيق إطار عمل COBIT للرقابة الداخلية في شركاتهم، في حين أن عدد قليل منهم أكدوا تطبيق آليات حوكمة تكنولوجيا المعلومات في منظماتهم بشكل مناسب. وبينت النتائج أيضا أن البنوك والمؤسسات المالية والمؤسسات الخدمية تهتم أكثر بتطبيق إطار عمل COBIT مقارنة مع المنظمات الأخرى وان المتخصصون بتكنولوجيا المعلومات، والمدققين الداخليين والمدراء التنفيذيون أكثر إدراكا لأهمية تطبيق إطار COBIT بالمقارنة مع الآخرين. أما Pramod, Li, and Gao(2011) فقد اقترحوا إطارا لمكافحة غسيل الأموال في المصارف من خلال الجمع بين عمليات إطار عمل COBIT للرقابة على المعلومات والتكنولوجيا المتصلة بها ومكونات إطار عمل COSO للرقابة الداخلية. وقد بينت الدراسة أن الإطار المقترح

يدعم بفاعلية جميع أنشطة القطاع المالي من خلال تحديد تكنولوجيا المعلومات الكفوءة القائمة على أساس عمليات وأساليب الرقابة في النظم المحاسبية الالكترونية.

من جانب آخر سعت دراسة Rubino & Vitolla(2014b) إلى توضيح كيف تدعم حوكمة تكنولوجيا المعلومات نظام إدارة مخاطر المشروع ERM، وعلى وجهة الخصوص ركزت الدراسة على إيضاح كيف تساعد أهداف الرقابة على المعلومات والتكنولوجيا المتصلة بها الشركات في الوصول إلى أهدافها من خلال التكامل بين نظام إدارة مخاطر المشروع وإطار عمل COBIT للرقابة الداخلية. وقد بينت نتائج الدراسة أن التكامل بين إطار عمل COBIT وإطار عمل COSO ERM يمكن أن يمثل لأي منظمة طريقة جيدة لتحقيق أهداف الرقابة الداخلية وإدارة المخاطر وكذلك حوكمة الشركة.

وأخيرا سعت دراسة Fazlida & Said (2015) إلى وضع إطار نظري لمخاطر امن المعلومات والحوكمة والعقبات التي تعيق تطبيقها. وقد بينت نتائج هذه الدراسة أن امن المعلومات يعد جزءاً متمماً لحوكمة تكنولوجيا المعلومات في مجال التأكيد على السرية والنزاهة وتوفر المعلومات. فوجود إطار متكامل لحوكمة تكنولوجيا المعلومات كإطار عمل COBIT للرقابة الداخلية يمكن أن يستخدم من قبل المنظمات كآلية للمساعدة في تطبيق حوكمة امن المعلومات.

استنادا إلى ما تقدم يمكن القول أن الدراسة الحالية تتميز عن الدراسات السابقة في كونها تسلط الضوء على أهمية تطبيق آليات حوكمة تكنولوجيا المعلومات في القطاع المصرفي العراقي لما له من فائدة في مجال دعم امن المعلومات وزيادة ثقة المتعاملين في هذا القطاع بالصناعة المصرفية عموماً، فضلاً أن الدراسة الحالية تركز على تقويم دور حوكمة تكنولوجيا المعلومات في تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية المطبقة في المصارف الأهلية العراقية وهو الأمر الذي لم يخضع للاختبار في معظم الدراسات السابقة.

المبحث الثاني
(الإطار النظري للبحث)

حوكمة تكنولوجيا المعلومات

حوكمة تكنولوجيا المعلومات هي إحدى المفاهيم التي حظيت باهتمام كبير في الآونة الأخيرة وأصبحت من المواضيع المهمة في مجال تكنولوجيا المعلومات. وقد أشار معهد تكنولوجيا المعلومات إلى أن الحوكمة هي مسؤولية مجلس الإدارة والإدارة التنفيذية وهي جزء مكمل لحوكمة الشركة وتتكون من القيادة والهيكل التنظيمي والعمليات التي تؤكد على دعم تكنولوجيا المنظمة وتضمن تحقيق إستراتيجية المنظمة وأهدافها (Mirela,2010:33) .

أما Van Grembergen, (2002) فقد أكد على أن حوكمة تكنولوجيا المعلومات هي القدرة التنظيمية التي يمارسها كل من مجلس الإدارة والإدارة التنفيذية وإدارة تكنولوجيا المعلومات للرقابة على تصميم وتنفيذ إستراتيجية تكنولوجيا المعلومات والتأكيد على الاندماج بين المنظمة وتكنولوجيا المعلومات. في حين عرفها Moeller,(2013:42) بأنها مجموعة من السياسات وأفضل التطبيقات التي تخدم كقوة تمكين إستراتيجية لتحسين عمليات المشاريع التجارية وتضم جميع المستويات في المنظمة. وتتضمن حوكمة تكنولوجيا المعلومات إدارة عمليات ومشاريع تكنولوجيا المعلومات و التأكيد على التوافق بين تلك الأنشطة واحتياجات المنظمة المحددة في استراتيجياتها. ويعني التوافق بين تكنولوجيا المعلومات والمنظمة ما يأتي:

١. إن إدارة المنظمة تفهم المحددات المحتملة لتكنولوجيا المعلومات

٢. إن وظيفة تكنولوجيا المعلومات تفهم أهداف واحتياجات المنظمة المرتبطة بتلك الأهداف.
٣. هذا الفهم المتبادل يتم ويراقب من قبل المنظمة عبر المسائلة وهيكل حوكمة مناسب.

إن فهم قيمة وتكلفة تكنولوجيا المعلومات تعد مهمة بالنسبة للمدير ومجلس الإدارة وإدارة تكنولوجيا المعلومات على حد سواء. حيث يتطلب تحقيق التوافق الناجح بين المنظمة وتكنولوجيا المعلومات أن تتوافق أهداف وأغراض المنظمة مع احتياجات المنظمة من نظم المعلومات وعندما تكون تكنولوجيا المعلومات قادرة على تلبية تلك الاحتياجات بالتعاون مع الإدارة. وعلى هذا الأساس يقع على عاتق الإدارة مسؤولية الأخذ بنظر الاعتبار المجالات الرئيسة لحوكمة تكنولوجيا المعلومات. وتتمثل هذه المجالات بخمسة عناصر أساسية، كل

عنصر في هذه العناصر يحمل أهمية بالنسبة لجميع مجالات تكنولوجيا المعلومات الأخرى (Hardy, 2006:56):

١. التوافق الاستراتيجي Strategic Alignment. يقع على الإدارة مسؤولية إدارة التوافق والانسجام داخل المنظمة من خلال التأكيد على أن استراتيجيات تكنولوجيا المعلومات تتوافق مع استراتيجيات المنظمة، وان توفير تكنولوجيا المعلومات يتم في الوقت المناسب وضمن الموازنة المخصصة له وتحمل توصيف وظيفي ملائم وتوازن في استثمارات تكنولوجيا المعلومات التي تدعم المنظمة ككل وتلك التي تساعدها في النمو والمنافسة. إذ يسهم التوافق الاستراتيجي في تعظيم الفرص لاستخدام تكنولوجيا المعلومات مع توفير الشفافية والتوكيد التي تحققها تكنولوجيا المعلومات بما يؤدي إلى زيادة الفاعلية الإدارية.

٢. توفير القيمة Value Delivery. وهو تحسين العائد من الاستثمار في تكنولوجيا المعلومات من خلال تنفيذ مشروع توفير القيمة للزبون، وتلبية متطلبات قطاع الأعمال والتحقق من نزاهة ودقة المعلومات. إن فاعلية توفير القيمة تتحقق فقط عندما تتم الموازنة بين التكاليف والعائد على الاستثمار في تكنولوجيا المعلومات، فالإدارة ينبغي أن تؤمن تكنولوجيا المعلومات التي تتوافق مع توفير القيمة من خلال تأمين البنى التحتية التكنولوجية التي تمكن المنظمة من النمو والنفوذ في أسواق جديدة، زيادة العائد الكلي، تحسين رضا الزبائن، ضمان المحافظة على الزبون و إدارة الاستراتيجيات التنافسية.

٣. إدارة المخاطرة Risk Management . وتهتم معالجة احتياجات الامتثال القانوني والتنظيمي وفهم وإدارة مخاطر العمليات الرئيسة. إن الدافع لإدارة المخاطرة هو حاجة الإدارة لإثبات وجود حوكمة في الشركة لمختلف المستخدمين منهم على سبيل المثال المساهمين، المنظمين،المستخدمين، والعملاء والمجهزين. لذا ينبغي على مجلس الإدارة التأكد من وجود شفافية تتعلق بالمخاطر الجوهرية على المنظمة. وهذا يتضمن تحديد تقبل وتحمل المخاطرة ، تقدير المعرفة بمخاطر تكنولوجيا المعلومات، وتحديد حالات التعرض للمخاطرة. كما ينبغي أن تكون إدارة المخاطرة في المنظمة جزء لا يتجزأ من عملياتها وذلك لضمان الاستجابة السريعة لتحديات المخاطرة التي تتسم بالتغير المستمر.

٤. إدارة الموارد Resource Management . وتعني التوفيق بشكل مناسب بين إمكانات تكنولوجيا المعلومات واحتياجات قطاع الأعمال، بما في ذلك تحسين موارد تكنولوجيا المعلومات، تحسين المعرفة، والتوافق مع الإمكانات المتاحة. ولتحقيق ذلك، على الإدارة أن تسعى للتأكيد على توفير الطرق الملائمة والمهارات المطلوبة في المنظمة لإدارة مشاريع تكنولوجيا المعلومات وان تكون الأهداف واقعية وقابلة للتحقيق. إذ أن الحوكمة الفاعلة للإنفاق على تكنولوجيا المعلومات يمكن أن تؤدي إلى تحقيق وفورات جوهرية في التكاليف.

٥. قياس الأداء Performance Measurement . قياس أداء تكنولوجيا المعلومات من خلال استخدام بطاقة الأداء المتوازن تعد أداة غاية في الفاعلية لمجلس الإدارة وذلك لتحقيق التوافق بين نظم المعلومات وإستراتيجية المنظمة. كما ينبغي على الإدارة استخدم بيانات الوقت الحقيقي أو البيانات الفورية real time data لتحسين عملية الإبلاغ الفوري عن المعلومات في نظم تكنولوجيا المعلومات.

إطار عمل COBIT للرقابة الداخلية

يعد إطار عمل COBIT للرقابة الداخلية واحد من أهم التطورات في مجال حوكمة تكنولوجيا المعلومات، إذ يهدف هذا الإطار إلى مجموعة من أفضل ممارسات الحوكمة والعمليات التدقيقية لنظم المعلومات الالكترونية والتكنولوجيا المتصلة بها مع التأكيد على التوفيق بين أهداف تكنولوجيا المعلومات المطبقة في الشركات وأهداف تلك الشركات. و يختص إطار عمل COBIT بالرقابة الداخلية على نظم المعلومات الالكترونية وتكنولوجيا المتصلة بهذه النظم وحماية امن المعلومات. هذا الإطار تم تطويره من قبل جمعية تدقيق ورقابة نظم المعلومات Information systems Audit and Control Association واختصارها ISACA، ويرجع ظهور هذا الإطار إلى منتصف تسعينيات القرن الماضي[١]. نتيجة لما يواجهه المدققين من

[١] للمزيد من التفاصيل انظر Sigler, and Rainey(2016) De Haes and Van Grembergen (2015)

صعوبات متزايدة عند العمل في ظل أنظمة محاسبية مؤتمته ولخلق دليل عمل للمدققين في بيئة تكنولوجيا المعلومات.و قد تم تطوير إطار عمل COBIT أساسا كإطار لتنفيذ مهام التدقيق في بيئة تكنولوجيا المعلومات والتي تتمحور حول مجموعة من الأهداف الرقابية لعمليات تكنولوجيا المعلومات. ظهرت النسخة الأولى لهذا الإطار عام ١٩٩٦ في حين تم إصدار النسخة الثانية عام ١٩٩٨ ،وقد شهد إطار COBIT العديد من التطورات اللاحقة التي استندت بمجملها على أساس تدقيق تكنولوجيا المعلومات، حيث خضع هذا الإطار لعملية تطوير أكثر أصبح بموجبها إطارا شاملا لإدارة تكنولوجيا المعلومات. وفي عام ٢٠٠٠ تم إضافة المبادئ التوجيهية لإدارة تكنولوجيا المعلومات ضمن الإصدار الثالث لإطار COBIT3 والتي ضمت المقاييس وعوامل النجاح الأساسية ونماذج النضج Maturity Models لعمليات تكنولوجيا المعلومات.

ولم تقتصر التطورات في مجال حوكمة تكنولوجيا المعلومات على هذا الحد بل استمرت لتنتج في عام ٢٠٠٥ الإصدار الرابع COBIT4 والذي تضمن العديد من المفاهيم التي توضح آليات الحوكمة والإدارة منها على سبيل المثال:

- التوافق بين أهداف المنظمة وأهداف تكنولوجيا المعلومات وعلاقتها بدعم عمليات تكنولوجيا المعلومات.
- المهام والمسؤوليات داخل عمليات تكنولوجيا المعلومات.
- العلاقات المتداخلة بين عمليات تكنولوجيا المعلومات.

أما أخر إصدارات COBIT فكانت النسخة الخامسة COBIT5 التي صدرت عام ٢٠١٢ ، وقد أكدت على مفهوم حوكمة تكنولوجيا المعلومات داخل المنظمة، ووفقاً لـ ISACA (2012) فان هذا الإصدار يوفر أطارا أكثر شمولية يساعد المنظمات في تحقيق أهدافها في مجالات الحوكمة وإدارة تكنولوجيا المعلومات فيها. إذ يوفر الدعم اللازم للمنظمة في إدارة تكنولوجيا المعلومات بطريقة شاملة لكامل المشروع أخذة بالاعتبار تحديد المجالات الوظيفية وتحديد المسؤوليات وكذلك مصالح المستفيدين الداخليين والخارجيين من تكنولوجيا المعلومات.

وفي هذا السياق حدد الإصدار الخامس لإطار عمل COBIT المبادئ ألأساسية للرقابة الداخلية (De Haes and Van Grembergen,2015:104) والمتمثلة بخمسة مبادئ أساسية يبينها الشكل (١) وهي كالأتي:

١. **تلبية احتياجات المستخدمين Meeting Stakeholder Needs**– ويعني هذا المبدأ أن علىCOBIT أن يوفر جميع العمليات والعوامل الأخرى التي تدعم عملية خلق القيمة للمنظمة من خلال استخدام تكنولوجيا المعلومات على النحو الذي يؤدي إلى تلبية احتياجات المستفيدين(أصحاب المصالح). ويرتبط هذا المبدأ بشمل وثيق مع بالتوافق الاستراتيجي المبين في الإصدارات السابقة لإطار COBIT. ويعد هذا المبدأ بالغ الأهمية للمنظمات وذلك لاختلاف الأهداف الموضوعة لكل منظمة مما يتطلب منها تكييف أهداف تكنولوجيا المعلومات المستخدمة فيها لتلاءم أهدافها. إلا أن التحدي الذي يمكن أن تواجه المنظمات هو كيفية تحقيق هذا التوافق بين أهداف المنظمة وأهداف تكنولوجيا المعلومات، هذا التحدي دفع العديد من الباحثين إلى السعي لإيجاد دليل عمل لفهم كيف يمكن أن تؤثر أهداف المنظمة في أهداف تكنولوجيا المعلومات ذات الصلة والعكس صحيح.

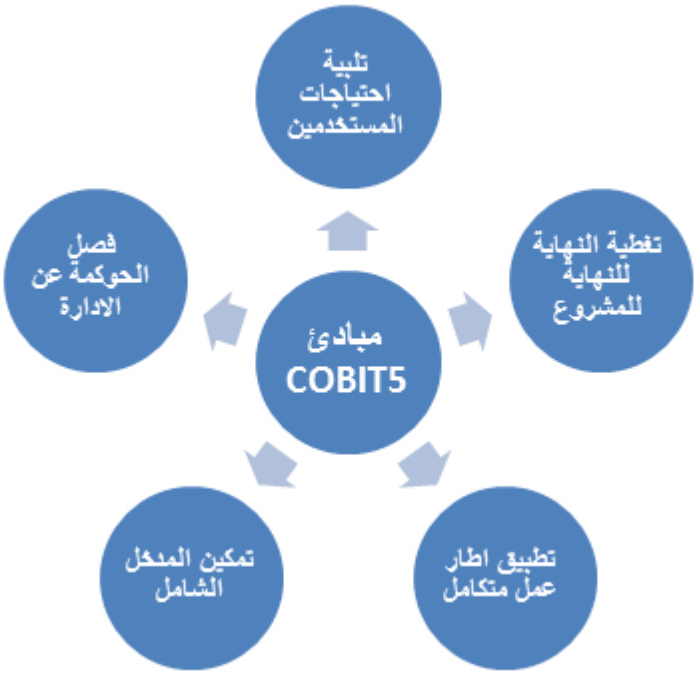
٢. **تغطية النهاية للنهاية للمشروع[٢] Covering the Enterprise End-to-end**– من خلال هذا المبدأ يعمل إطار COBIT على دمج حوكمة تكنولوجيا المعلومات في حوكمة الشركة ككل، فهو:

٢,١. يغطي جميع الوظائف والعمليات داخل المنظمة، فإطار COBIT لا يركز فقط على وظيفة تكنولوجيا المعلومات وإنما يعامل المعلومات والتقنيات المتعلقة بها كأصول ينبغي أن تعالج كأي أصل أخر في المنظمة.

[٢] النهاية للنهاية هي وسيلة اتصال امن تمنع الطرف الثالث من الوصول إلى البيانات عند نقلها من نظام إلى أخر أو من جهاز إلى أخر

٢,٢. يأخذ بالاعتبار جميع عوامل حوكمة وإدارة تكنولوجيا المعلومات بشكل واسع وضمن طريقة النهاية للنهاية، على سبيل المثال يجب أن تتضمن كل شيء داخلي كان أم خارجي قد يعتبر ملائم لحوكمة وإدارة معلومات المنظمة.

الشكل رقم ٢
(مبادئ حوكمة تكنولوجيا المعلومات)



المصدر: COBIT 5, www.isaca.org/COBIT

٣. **تطبيق إطار عمل متكامل Applying an Integrated Framework** – هنالك العديد من المعايير والتطبيقات الجيدة المتعلقة بتكنولوجيا المعلومات كل منها يوفر دليل عمل لمجموعة فرعية من أنشطة تكنولوجيا المعلومات، ويقوم إطار عمل COBIT على التنسيق والتوافق مع المعايير والأطر الملائمة الأخرى لخلق منهج موحد، وعلية فان إطار عمل COBIT يعد بمثابة إطار شامل للحوكمة وإدارة تكنولوجيا المعلومات في المنظمة.

٤. **تمكين المدخل الشامل Enabling a Holistic Approach** – إن وجود حوكمة وإدارة كفوءة وفاعلة لتكنولوجيا المعلومات في المنظمة يتطلب وجود منهج شامل يأخذ بالحسبان عدد من العناصر المتفاعلة مع بعضها البعض. وقد حدد إطار عمل COBIT سبعة أصناف من العوامل المساعدة التي تدعم تنفيذ إطار شامل لنظم حوكمة وإدارة تكنولوجيا المعلومات في الشركة. وتعرف هذه العوامل على إنها كل شيء يمكن أن يساعد في تحقيق أهداف المشروع ويشمل الأتي:

١. المبادئ والسياسات والأطر.
٢. العمليات.
٣. الهياكل التنظيمية.
٤. الثقافة، الأخلاق، والسلوك.
٥. المعلومات.
٦. الخدمات، البنى التحتية والتطبيقات.

٧. الأشخاص، المهارات، والاختصاصات.

٥. **فصل الحوكمة عن الإدارة Separating Governance From Management** – يميز إطار عمل COBIT تتميزاً واضحاً بين الحوكمة والإدارة، إذ إنها تشمل أنواع مختلفة من الأنشطة وتتطلب هياكل تنظيمية مختلفة و وتخدم أغراض مختلفة.

بالاستناد إلى ما تقدم يمكن القول أن إطار عمل COBIT للرقابة الداخلية يمثل إطار متكامل لحوكمة تكنولوجيا المعلومات يتعامل بشكل أساس مع الأنظمة المحاسبية الالكترونية ويختص بتوفير آليات للرقابة على تكنولوجيا المعلومات المستخدمة في إعداد الكشوفات المالي. من هذا المنطلق فان تطبيق آليات حوكمة تكنولوجيا المعلومات يؤدي إلى زيادة ثقة المستخدمين بالمعلومات المعلنة بالكشوفات المالية للشركات وقد لخص ألركابي (٢٠٠٩:٧٣) فوائد تطبيق إطار عمل COBIT للرقابة الداخلية بثلاث نقاط هي:-

1. إتاحة الفرصة لإدارة المنظمة للقيام بالمقارنة المرجعية (Benchmark) فيما يتعلق بحماية تكنولوجيا المعلومات والرقابة عليها.
2. اطمئنان مستخدمي خدمات تكنولوجيا المعلومات على كفاية الحماية وتوفر اليات ألرقابه المناسبة.
3. يستطيع المدقق من إبداء رأيه بالرقابة الداخلية وتقديم نصائحه على مدى توفر الأمن لتكنولوجيا المعلومات.

مخاطر التدقيق في النظم المحاسبية الالكترونية

تعرف مخاطر التدقيق بأنها المخاطر المتعلقة بفشل المدقق بدون قصد بتعديل راية بشكل مناسب حول الكشوفات المالية التي هي أساسا تشوبها أخطاء جوهري. ويتطلب المعيار الثاني من معايير العمل الميداني من المدقق أن يفهم طبيعة الوحدة وبيئتها بما في ذلك نظام الرقابة الداخلية لتحديد مخاطر الأخطاء الجوهرية في الكشوفات المالية للعميل. ويعتبر أنموذج مخاطر التدقيق الأساس الذي يعتمد عليه المدققون بنظر الاعتبار المخاطر في إجراءات التخطيط للحصول على أدلة الإثبات التدقيق. إذ يساعد هذا الأنموذج المدققين في تقرير مقدار أدلة الإثبات الواجب تجميعها في كل مرحلة من مراحل التدقيق(Arens et al., 2012:259).

وعادة ما يتم صياغة هذا الأنموذج بالشكل الأتي:

$$PDR = \frac{\text{AAR}}{\text{IR} \times \text{CR}}$$

حيث إن:

PDR= مخاطر الاكتشاف المخططة.

AAR= مخاطر التدقيق المقبولة.

IR= المخاطرة المتأصلة.

CR= مخاطر الرقابة.

١. **مخاطر الاكتشاف المخطط Planned Detection Risk** وهي المخاطر المتعلقة بأن دليل الإثبات لجزء أو مفردة معينه يفشل في اكتشاف الأخطاء التي تتجاوز مستوى الأخطاء المسموح بها. و توجد نقطتان يجب معرفتهما عند الحديث عن مخاطر الاكتشاف المخطط. الأولى أن مخاطر الاكتشاف المخطط تعتمد على العوامل الثلاثة الأخرى في أنموذج مخاطر التدقيق(مخاطر التدقيق المقبولة، مخاطر التدقيق المتأصلة، ومخاطر الرقابة)، فهي تتغير فقط عندما يغير المدقق واحد من عوامل المخاطرة الأخرى. أما النقطة الثانية فهي أن مخاطر الاكتشاف المخطط تحدد مقدار أدلة الإثبات الواجب على المدقق تجميعها وبما يتناسب عكسيا مع حجم مخاطر الاكتشاف المخطط. فإذا انخفض مستوى مخاطر الاكتشاف المخطط فيحتاج المدقق إلى تجميع أدلة إثبات أكثر لتحقيق مستوى مخاطر اكتشاف مخطط اقل. مثال ذلك تكون مخاطر الاكتشاف المخطط للمخزون ذات مستوى منخفض نسبياً، لذا يتوجب على المدقق تجميع مقدار اكبر من أدلة الإثبات. وعلى العكس من ذلك نجد أن مستوى مخاطر الاكتشاف المخطط للرواتب عالية مما يتوجب تقليل حجم أدلة الإثبات الواجب تجميعها حول عنصر الرواتب.

٢. **المخاطرة المتأصلة Inherent Risk** وتقيس تقدير المدقق لاحتمال أن يكون هناك أخطاء جوهرية نتيجة للخطأ أو الغش في جزء معين أو بند معين قبل الأخذ الاعتبار فاعلية نظام الرقابة الداخلية. فإذا

استنتج المدقق احتمالا عاليا بوجود أخطاء فهذا يعني أن هناك مستوى عالي من المخاطرة المتأصلة. ويرجع السبب في إهمال وسائل الرقابة الداخلية عند تحديد المخاطرة المتأصلة لأنها تؤخذ بالاعتبار بشكل منفصل عند تحديد مخاطر الرقابة. وتتفاوت بنود القوائم المالية في مستوى المخاطرة الذي تحمله فتتمتع حالات الاكتساب للموجودات الثابتة، والمخزون، والمدفوعات النقدية بمستوى عالي من المخاطرة المتأصلة، في حين تكون المخاطرة اقل في بنود أخرى مثل الرواتب و الموارد البشرية وغيرها. مثل هذه التقديرات يقوم بها المدقق بالتشاور مع الإدارة، من خلال المعرفة السابقة بنشاط الشركة، أو بالاعتماد على نتائج التدقيق في السنوات السابقة. وترتبط المخاطر المتأصلة عكسيا مع مخاطر الاكتشاف المخطط وبشكل مباشر مع مقدار أدلة التدقيق.

٣. **مخاطر الرقابة Control Risk** وهي المخاطر الناتجة عن حدوث خطأ جوهري في احد البنود ولا يمكن منعه أو اكتشافه في وقت مناسب عن طريق إجراءات الرقابة الداخلية. فهي تقيس تقدير المدقق فيما إذا كانت الأخطاء التي تزيد عن المقدار المسموح به في جزء معين أو بند معين سوف يتم منعها أو اكتشافها بواسطة وسائل الرقابة الداخلية للعميل. وهنالك علاقة قوية بين المخاطر المتأصلة ومخاطر الرقابة، حيث يوثر كلا النوعين على مستوى مخاطر الاكتشاف المخطط.

٤. **مخاطر التدقيق المقبولة Acceptable Audit Risk** وتقيس كيفية استعداد المدقق لاحتمال أن يكون هناك أخطاء جوهرية في الكشوفات المالية بعد اكتمال عملية التدقيق والوصول إلى رأي غير متحفظ. وعندما يقرر المدققون مستوى اقل من مخاطر التدقيق المقبولة، فأنهم سوف يكونون متأكدين بان الكشوفات المالية لا تحتوي أخطاء جوهرية. وحالة المخاطرة صفر تعني التأكد التام و ١٠٠% مخاطرة تعني عدم التأكد بشكل كامل.

وعادة ما يقبل المدققين بمستوى معين من المخاطرة أو عدم التحقق عند أدائهم لوظيفة التدقيق. فالمدقق يدرك على سبيل المثال المخاطرة المتأصلة المتعلقة بملائمة دليل الإثبات، وعدم التأكد المقترنة بفاعلية نظام الرقابة الداخلية للعميل، وعدم التحقق المتعلق فيما إذا كان عرض القوائم المالية منصفاً بعد اكتمال عملية التدقيق. أن المدقق الكفء يدرك بان المخاطر موجودة ويتعامل مع تلك المخاطر بطريقة مناسبة. إن معظم المخاطر التي يواجهها المدققين صعبة القياس وتتطلب عناية فائقة قبل أن يتمكن المدقق من الاستجابة لها بشكل ملائم.إذ أن الاستجابة لتلك المخاطر بشكل مناسب يعد عنصراً أساسيا لتحقيق تدقيق عالي الجودة. ومن هذا المنطلق فان وجود نظام فاعل للرقابة الداخلية يسهم في الحد من مخاطر التدقيق وبالأخص في النظم المحاسبية الالكترونية التي تعتمد تكنولوجيا معلومات متقدمة. وفي هذا السياق أشار Messier et al. (2008:14) إلى أن على المدققين أن يفهموا المخاطر المرتبطة بالتغيرات التكنولوجية المتسارعة وكيفية تقويم تلك المخاطر لعميل معين. فقد تختلف مخاطر التدقيق من عميل يطبق نظام معلومات محاسبي الكتروني معقد إلى أخر يطبق نظام تقليدي، لذا فان الخبرة المهنية والأحكام الشخصية للمدقق تلعب دوراً بالغ الأهمية في تقويم مخاطر المرتبطة بالتقنيات والأنظمة الالكترونية المطبقة في المهمة محل التدقيق. ولا يقتصر تأثير المخاطر على نظم المعلومات المحاسبية الالكترونية فحسب وإنما يتعرض لها النظام اليدوي أيضا ولكن بدرجات متفاوتة تبعاً لمستوى تعقيد النظام المطبق في الشركة، حيث يزداد المخاطر كلما ازداد استخدام تكنولوجيا معلومات أكثر تطوراً. على أساس نرى من الضروري للمؤسسات التي تطبق نظم محاسبية الكترونية أن تضمن بيئة فاعلة للرقابة الداخلية تساعد على الحد من المخاطر المتصلة باستخدام تكنولوجيا المعلومات.

دور آليات حوكمة تكنولوجيا المعلومات وفقاً لـ COBIT في تقليل مخاطر التدقيق

لقد أصبحت تكنولوجيا المعلومات عنصراً استراتيجياً لخلق الفرص والابتكار وتحقيق الميزة التنافسية للمنظمات، إلا أنها في الوقت نفسه تستلزم زيادة المخاطرة المتأصلة Inherent Risk المتعلقة بالثقة، النزاهة، وكذلك بأمن المعلومات الناتجة عنها. لذا فان وجود آليات فاعلة لحوكمة تكنولوجيا المعلومات يمكنها أن تضيف قيمة للمنظمة من وجهة نظر مستخدميها. ويوفر أطار عمل cobit إطارا شاملاً يساعد المنظمات في تحقيق أهدافها وخلق قيمة مضافة من خلال إيجاد آليات حوكمة تكنولوجيا معلومات فاعلة داخل المنظمة.

وفي هذا البحث تم اعتماد عناصر أو مكونات إطار عمل COBIT للرقابة الداخلية كأساس لتقويم دور تعزيز آليات حوكمة تكنولوجيا المعلومات في تقليل مخاطر التدقيق. وهذه العناصر تتضمن ست سمات أساسية لحوكمة تكنولوجيا المعلومات هي(COBIT4.1: 2007:21):

١. المسؤولية والمساءلة Responsibility and Accountability- وتشير إلى إجراءات حوكمة تكنولوجيا المعلومات المتعلقة بتحديد الصلاحيات والمسؤوليات داخل المنظمة والتي قد تشمل تحديد واضح للمسؤوليات والصلاحيات في إدارة تكنولوجيا المعلومات، إعداد دليل سلوك مهني للمتعاملين بتكنولوجيا المعلومات، إضافة إلى التقارير الخاصة بتقويم سلوك المستخدَمين داخل المنظمة.

٢. المعرفة والاتصالات Awareness and Communication. تتضمن مجموعة من إجراءات الحوكمة التي تهدف إلى تامين قنوات الاتصال بين المستويات الإدارية المختلفة ذات العلاقة بإدارة تكنولوجيا المعلومات. مثل هذه الإجراءات قد تشمل تقارير دورية تقدم للإدارة حول مدى توافق تكنولوجيا المعلومات مع إستراتيجية المنظمة، تقارير حول المشاكل التقنية التي تطرأ والحلول المناسبة لها.

٣. السياسات والخطط والإجراءات Policies, plans and procedures- وتشير إلى إجراءات الحوكمة المتعلقة بتقويم فاعلية وسائل الرقابة على عملية انتقال البيانات داخل النظام، مثل هذه الإجراءات قد تتضمن وجود إجراءات رقابية صارمة على انتقال البيانات خلال عمليات إدخال البيانات، المعالجة، وكذلك المخرجات، كما قد تشمل تقديم تقارير دورية من قسم تكنولوجيا المعلومات للكشف عن حالات الدخول غير المصرح للشبكة.

٤. الأدوات والاتمته Tools and Automation- يركز هذا العنصر على إجراءات الحوكمة المتعلقة بالبرمجيات وأنظمة الرقابة على نشاط قاعدة البيانات. هذه الإجراءات قد تشمل وجود برمجيات تعمل على منع الدخول غير المصرح للنظام، ووجود برمجيات رقابية تسمح باكتشاف الثغرات في النظام وتصحيحها الكترونياً، وكذلك وجود برامج متكاملة تسمح بانتقال البيانات داخل المنظمة بسهولة وأمان.

٥. المهارات والخبرة Skills and Expertise- وهي إجراءات الحوكمة المتعلقة بمستوى الكفاءة والاختصاص المطلوبة للمتعاملين بتكنولوجيا المعلومات. وهذه الإجراءات قد تتضمن وجود متطلبات توظيف صارمة للعاملين في مجال تكنولوجيا المعلومات منها ما يتعلق بالكفاءة والاختصاص أو ما يتعلق بالنزاهة والكتمان. فضلاً عن إجراءات التقويم المستمر والتدريب بهدف الارتقاء بمستوى الأداء للعاملين في المنظمة.

٦. الأهداف والقياس Goals and Measurement- يهتم العنصر الأخير بإجراءات الحوكمة المتعلقة بوضع أهداف تكنولوجيا المعلومات وقياسها وكذلك تقويم أداء قسم تكنولوجيا المعلومات المنظمة. وهذه الإجراءات قد تتضمن تحديد واضح لأهداف قسم تكنولوجيا المعلومات ،تحفيز المدراء على تطوير خططهم التشغيلية، فضلاً عن وجود آلية لتقويم فاعلية وكفاءة أداء تكنولوجيا المعلومات ومدى تحقيقه لأهدافه.

مثل هذه الإجراءات من المتوقع أن يكون لها تأثيرا ايجابياً في مستوى المخاطرة المرتبطة بتدقيق نظم المعلومات المحاسبية الالكترونية. لذا يُكرس المبحث الثالث من هذا البحث لاختبار دور تعزيز آليات حوكمة تكنولوجيا المعلومات في تقليل مخاطر التدقيق في بيئة التدقيق الالكترونية.

المبحث الثالث
(الجانب التطبيقي للبحث)

مقياس البحث

يهتم هذا المبحث بتحليل و اختبار فرضيات البحث الرئيسة والفرعية، و لهذا الغرض تم استخدام مقياس (Likert) الخماسي الذي يتوزع من أعلى وزن له والذي أعطى (٥) درجات لتمثل حقل الإجابة (اتفق تماما) إلى اقل وزن له والذي أعطي (١) درجة لتمثل حقل الإجابة (لا اتفق تماما) وبينهما ثلاثة أوزان أخرى هي (٢،٣،٤) لتمثل حقول الإجابة (اتفق، محايد، لا اتفق) على التوالي. ومن جانب آخر اعتمد الوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقويم الدرجة المتحصل عليها، علما أن الوسط الفرضي يمثل (١+ ٢+ ٣+ ٤ +٥) /٥ = ٣. والجدول (١) يبين توزيع فقرات الاستبانة على المحاور الرئيسية للبحث.

الجدول 1
(توزيع فقرات الاستبانة)

ت	أبعاد أداة القياس	الاختصار	الفقرات	عدد الفقرات
١	**تعزيز حوكمة تكنولوجيا المعلومات**	**X**	**1-18**	18
١	المسؤولية والمساءلة	*x1*	1-3	**3**
٢	المعرفة والاتصالات	*x2*	4-6	**3**
٣	السياسات والخطط	*x3*	7-9	**3**
٤	الآليات والاتمته	*x4*	10-12	**3**
٥	المهارات والخبرة	*x5*	13-15	**3**
٦	**الأهداف والقياس**	***X6***	**16-18**	**3**

صدق و ثبات المقياس

من اجل التحقق من صدق أداة القياس المتمثلة بالاستبانة تم عرضها على مجموعة من أساتذة كلية الإدارة والاقتصاد في جامعة الكوفة وقد تم الأخذ بملاحظاتهم واقتراحاتهم المتعلقة بتصويب الاستبانة، كما تم اعتماد معامل كرونباخ الفا (Cronbach Alpha) كأداة للتأكد من الثبات والاتساق الداخلي لفقرات هذا المقياس. وقد أظهرت النتائج المبينة في الجدول (٢) أن قيمة معامل الثبات كرونباخ الفا قد تجاوزت النسبة المقبولة لاعتماد نتائج الدراسة وهي ٦٠% ولجميع متغيرات الدراسة.

الجدول 2
(ثبات مقياس الدراسة)

المتغير	الاختصار	قيمة الفا
تعزيز حوكمة تكنولوجيا المعلومات	**X**	.849
المسؤولية والمساءلة	*x1*	.861
المعرفة والاتصالات	*x2*	.883
السياسات والخطط	*x3*	.887
الآليات والاتمته	*x4*	.865
المهارات والخبرة	*x5*	.888
الأهداف والقياس	*X6*	.901
كافة المتغيرات		٩٢.8

عينة البحث

تمثلت عينة البحث بالمصارف التجارية العراقية العاملة في محافظة النجف الأشرف، إذ أن التعاملات التجارية للقطاع المصرفي تتم من خلال النظم المحاسبية الالكترونية ومن ثم يمكن أن تلبي الغرض الرئيس للبحث وهو اختبار دور آليات حوكمة تكنولوجيا المعلومات في تقليل مخاطر عملية التدقيق. وقد تم اختيار عينة البحث بشكل عشوائي لتشمل ٦٠ شخصاً يمثلون ٢٠ من المصارف التجارية العراقية العاملة في محافظة النجف من أصل ٢٤ مصرف تمثل مجتمع الدراسة. على هذا الأساس تم توزيع ٦٠ استمارة استبيان على أفراد العينة

على اختلاف مستوياتهم الإدارية محاسبين، مدققين، ومدراء فروع ، وقد استرجع منها ٤٨ استمارة بنسبة استرجاع ٨٠%.

وصف خصائص العينة وتحليلها

أما تحليل البيانات الديموغرافية لعينة البحث فتظهر في الجدول (٣).

الجدول 3
(الخصائص الديموغرافية لعينة البحث)

المتغير	الفئات	العدد	%
طبيعة العمل	مدير	٢٤	٥٠
	محاسب	١٨	٣٨
	مدقق	٦	١٢
	المجموع	**٤٨**	**١٠٠**
المؤهل العلمي	دكتوراه	٠	٠
	ماجستير	٦	١٩
	بكالوريوس	٣٣	٥٦
	دبلوم	٩	٢٥
	المجموع	**٤٨**	**١٠٠**
الخبرة	١ ــ ٥ سنوات	١٢	٢٥
	٥ ــ ١٠ سنوات	١٥	٣١
	١٠ ــ ٢٠ سنة	١٨	٣٨
	٢٠ سنة وأكثر	٣	٦
	المجموع	**٤٨**	**١٠٠**

نتائج اختبار الفرضيات

تختص هذه الفقرة بقياس علاقات الارتباط بين متغيرات البحث والتي تضمنتها الفرضية الرئيسية الأولى والتي تنص على الأتي:-

H0 فرضية العدم : **" لا توجد علاقة ذات دلالة إحصائيا بين تعزيز حوكمة تكنولوجيا المعلومات في الشركة وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية"**

H1 الفرضية البديلة : **" توجد علاقة ذات دلالة إحصائيا بين تعزيز حوكمة تكنولوجيا المعلومات في الشركة وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية"**

وقد تم استخدام اختبار (One-Sample T-Test) عند مستوى معنوية (٥ %) بمستوى ثقة (٩٥ %) للمنحنى ذي الطرفين من أجل اختبار فرضية الدراسة الرئيسية والفرضيات الفرعية المنبثقة عنها، إذ يبين الجدول ٤ نتائج اختبار T للفرضية الرئيسة وفرضياتها الفرعية.

الجدول ٤

(نتائج اختبار الفرضية الرئيسية للبحث)

One-Sample Test						
	Test Value = 3					
	t	do	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
X1	28.341	47	.000	1.31896	1.2253	1.4126
X2	25.255	47	.000	1.14563	1.0544	1.2369
X3	24.082	47	.000	1.64583	1.5083	1.7833
X4	44.610	47	.000	1.68792	1.6118	1.7640
X5	26.299	47	.000	1.27104	1.1738	1.3683
X6	16.619	47	.000	.85396	.7506	.9573

ويتضح من الجدول (٤) بأن مستوى المعنوية للمتغيرات كافة كان صفراً، وأن المتوسطات للمتغيرات الستة التي خضعت للاختبار كانت أكبر من القيمة الافتراضية البالغة (٣)؛ فضلاً عن أن قيمة t المحسوبة لجميع المتغيرات تزيد عن القيمة الجدولية البالغة ١,٦٨ عند مستوى معنوية ٥%. مما يشير إلى رفض فرضية العدم وقبول الفرضية البديلة التي تنص على وجود علاقة ذات دلالة إحصائيا بين تعزيز حوكمة تكنولوجيا المعلومات في الشركة وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية. فضلاً عن ذلك فان النتائج أعلاه تشير إلى وجود مؤشرات لتأثيرات إيجابية لمتغيرات الدراسة المتعلقة بتعزيز حوكمة تكنولوجيا المعلومات على مستوى مخاطر التدقيق في النظم المحاسبية الالكترونية.

ولتحديد مستوى العلاقة بين متغيرات الدراسة ومستوى تقويم المدقق لمخاطر التدقيق تم استخدام معامل الارتباط البسيط بيرسون لاختبار كل فرضية فرعية على حده. والأتي نتائج اختبار الفرضيات الفرعية للدراسة:

نتائج اختبار الفرضية الفرعية الأولى:

تختص الفرضية الفرعية الأولى باختبار العلاقة بين متغير **المسؤولية والمساءلة** وتقليل مخاطر التدقيق وتنص على الأتي:-

H0 فرضية العدم: لا توجد علاقة ذات دلالة إحصائيا بين متغير **المسؤولية و المسائلة** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.

H1 الفرضية البديلة : توجد علاقة ذات دلالة إحصائيا بين متغير **المسؤولية و المسائلة** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

يبين الجدول (٥) نتائج علاقة الارتباط (باستخدام معامل بيرسون للارتباط البسيط) بين متغير المسؤولية و المسائلة وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

الجدول ٥
(نتائج اختبار الفرضية الفرعية الأولى)

Correlations			
		X	X1
Y	Pearson Correlation	1	.876**
	Sig. (2-tailed)		.000
	N	48	48
X1	Pearson Correlation	.876**	1
	Sig. (2-tailed)	.000	
	N	48	48
**. Correlation is significant at the 0.01 level (2-tailed).			

تشير النتائج في الجدول أعلاه إلى وجود علاقة ارتباط طردية (موجبة) وقوية وذات دلالة إحصائية عند المستوى المعنوي (١%) بين متغير المسؤولية و المسائلة كمتغير مستقل و تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية كمتغير تابع، إذ بلغت قيمة معامل بيرسون للارتباط البسيط بينهما (0,876) وتشير هذه النتيجة إلى قوة العلاقة بينهما، مما يعني قبول الفرضية الفرعية الأولى .

نتائج اختبار الفرضية الفرعية الثانية:

تختص الفرضية الفرعية الثانية باختبار العلاقة بين متغير **المعرفة والاتصالات** وتقليل مخاطر التدقيق وتنص على الأتي:

H0 فرضية العدم: لا توجد علاقة ذات دلالة إحصائيا بين متغير **المعرفة والاتصالات** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.

H1 الفرضية البديلة : توجد علاقة ذات دلالة إحصائيا بين متغير **المعرفة والاتصالات** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

ويظهر الجدول (٦) نتائج علاقة الارتباط بين متغير **المعرفة والاتصالات** وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

الجدول ٦
(نتائج اختبار الفرضية الفرعية الثانية)

Correlations			
		X	X2
Y	Pearson Correlation	1	.731**
	Sig. (2-tailed)		.000
	N	48	48
X2	Pearson Correlation	.731**	1
	Sig. (2-tailed)	.000	
	N	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

النتائج في الجدول ٦ تبين وجود علاقة ارتباط طردية (موجبة) وقوية نسبياً وذات دلالة إحصائية عند المستوى المعنوي (١%) بين متغير المعرفة والاتصالات كمتغير مستقل و تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية كمتغير تابع، وقد بلغت قيمة معامل بيرسون للارتباط البسيط بينهما (0,731)، هذه النتيجة تشير إلى قوة العلاقة بين المتغيرين، مما يعني قبول الفرضية الفرعية الثانية.

نتائج اختبار الفرضية الفرعية الثالثة:

تختص الفرضية الفرعية الثالثة باختبار العلاقة بين متغير **السياسات والخطط** وتقليل مخاطر التدقيق وتنص على الأتي:

H0 فرضية العدم: لا توجد علاقة ذات دلالة إحصائيا بين متغير **السياسات والخطط** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.

H1 الفرضية البديلة : توجد علاقة ذات دلالة إحصائيا بين متغير **السياسات والخطط** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

النتائج المبينة في الجدول (7) تتضمن معامل الارتباط بيرسون للعلاقة بين متغير السياسات والخطط وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

الجدول ٧

(نتائج اختبار الفرضية الفرعية الثالثة)

Correlations			
		Y	X3
Y	Pearson Correlation	1	.811**
	Sig. (2-tailed)		.000
	N	48	48
X3	Pearson Correlation	.811**	1
	Sig. (2-tailed)	.000	
	N	48	48
**. Correlation is significant at the 0.01 level (2-tailed).			

وتشير هذه النتائج إلى وجود علاقة ارتباط طردية (موجبة) وقوية وذات دلالة إحصائية عند المستوى المعنوي (١%) بين متغير السياسات والخطط كمتغير مستقل و تقليل مخاطر تدقيق نظم المعلومات المحاسبية

الالكترونية كمتغير تابع، إذ بلغت قيمة معامل بيرسون للارتباط البسيط بينهما (0,811) وتشير هذه النتيجة إلى قوة العلاقة بين المتغيرين، مما يدل على قبول الفرضية الفرعية الثالثة .

نتائج اختبار الفرضية الفرعية الرابعة:

تختص الفرضية الفرعية الرابعة باختبار العلاقة بين متغير **الآليات والأتمتة** وتقليل مخاطر التدقيق وتنص على الأتي:

H0 فرضية العدم: لا توجد علاقة ذات دلالة إحصائيا بين متغير **الآليات والأتمتة** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.

H1 الفرضية البديلة: توجد علاقة ذات دلالة إحصائيا بين متغير **الآليات والأتمتة** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

يبين الجدول (٨) نتائج اختبار بيرسون للعلاقة بين متغير الآليات والاتمته وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

الجدول رقم ٨

(نتائج اختبار الفرضية الفرعية الرابعة)

Correlations			
		Y	X4
Y	Pearson Correlation	1	.882**
	Sig. (2-tailed)		.000
	N	48	48
X4	Pearson Correlation	.882**	1
	Sig. (2-tailed)	.000	
	N	48	48
**. Correlation is significant at the 0.01 level (2-tailed).			

تشير النتائج في الجدول أعلاه إلى وجود علاقة ارتباط طردية (موجبة) وقوية وذات دلالة إحصائية عند المستوى المعنوي (١%) بين متغير الآليات والاتمته كمتغير مستقل وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية كمتغير تابع، إذ بلغت قيمة معامل بيرسون للارتباط البسيط بينهما (0,882) وتشير هذه النتيجة إلى قوة العلاقة المتغيرين، مما يشير إلى قبول الفرضية الفرعية الرابعة .

نتائج اختبار الفرضية الفرعية الخامسة:

تختص الفرضية الفرعية الخامسة باختبار العلاقة بين متغير **المهارات والخبرة** وتقليل مخاطر التدقيق وتنص على الأتي:

H0 فرضية العدم: لا توجد علاقة ذات دلالة إحصائيا بين متغير **المهارات والخبرة** ومخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.

H1 الفرضية البديلة : توجد علاقة ذات دلالة إحصائيا بين متغير **المهارات والخبرة** و مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

الجدول (٩) يبين نتائج علاقة الارتباط باستخدام معامل بيرسون للارتباط البسيط بين متغير المهارات والخبرة وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

الجدول ٩

(نتائج اختبار الفرضية الفرعية الخامسة)

Correlations			
		Y	X5
Y	Pearson	1	.704**

	Correlation		
	Sig. (2-tailed)		.000
	N	48	48
X5	Pearson Correlation	.704**	1
	Sig. (2-tailed)	.000	
	N	48	48
**. Correlation is significant at the 0.01 level (2-tailed).			

تشير النتائج في الجدول أعلاه إلى وجود علاقة ارتباط طردية (موجبة) وقوية نسبياً وذات دلالة إحصائية عند المستوى المعنوي (١%) بين متغير **المهارات والخبرة** كمتغير مستقل و تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية كمتغير تابع، إذ بلغت قيمة معامل بيرسون للارتباط البسيط بينهما (0,704) وتشير هذه النتيجة إلى قوة العلاقة بين المتغيرين، مما يعني قبول الفرضية الفرعية الخامسة .

نتائج اختبار الفرضية الفرعية السادسة:

تختص الفرضية الفرعية السادسة باختبار العلاقة بين متغير **الأهداف والقياس** وتقليل مخاطر التدقيق وتنص على الأتي:

H0 فرضية العدم: لا توجد علاقة ذات دلالة إحصائيا بين متغير **الأهداف والقياس** ومخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.

H1 الفرضية البديلة: توجد علاقة ذات دلالة إحصائيا بين متغير **الأهداف والقياس** ومخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

يبين الجدول (١٠) نتائج علاقة الارتباط باستخدام معامل بيرسون للارتباط البسيط بين متغير الأهداف والقياس وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية .

الجدول ١٠
(نتائج اختبار الفرضية الفرعية السادسة)

Correlations			
		Y	X6
Y	Pearson Correlation	1	.624**
	Sig. (2-tailed)		.000
	N	48	48
X6	Pearson Correlation	.624**	1
	Sig. (2-tailed)	.000	
	N	48	48
**. Correlation is significant at the 0.01 level (2-tailed).			

النتائج في الجدول ١٠ يشير إلى وجود علاقة ارتباط طردية (موجبة) وقوية نسبياً وذات دلالة إحصائية عند المستوى المعنوي (١%) بين متغير الأهداف والقياس كمتغير مستقل و تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية كمتغير تابع، إذ بلغت قيمة معامل بيرسون للارتباط البسيط بينهما (0,624) وتشير هذه النتيجة إلى قوة العلاقة بين المتغيرين، مما يدل على قبول الفرضية الفرعية السادسة .

مناقشة وتفسير النتائج

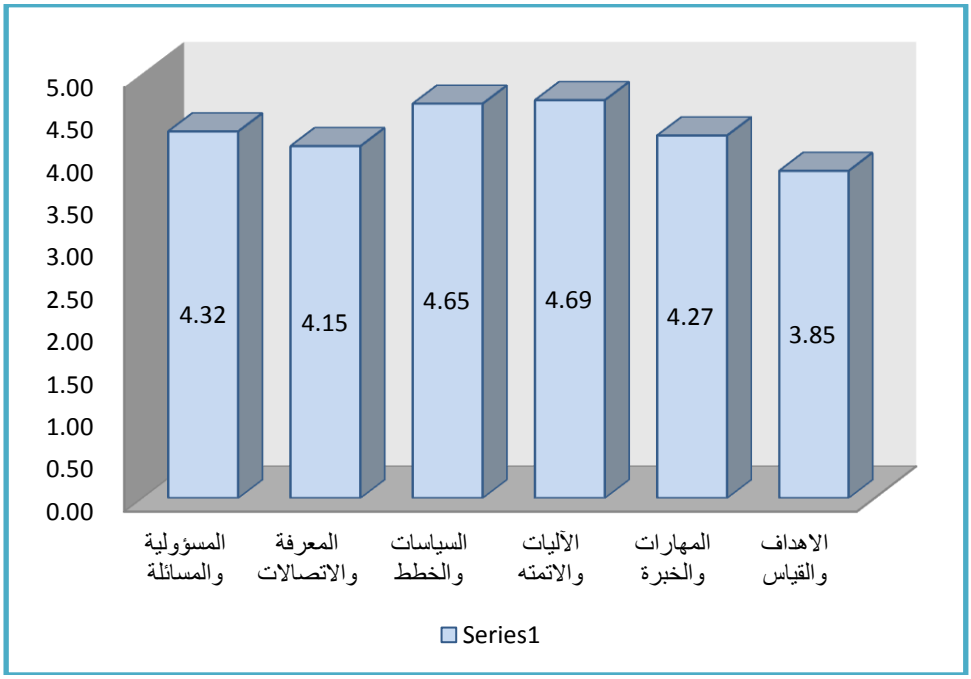
يبين الشكل ٢ التأثير المتفاوت لأبعاد أو عناصر حوكمة تكنولوجيا المعلومات في مستوى مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية. ويتضح من هذا الشكل أن متغير الأدوات والاتمته هو الأكثر تأثيراً في تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية، حيث بلغ متوسط استجابة أفراد العينة للفقرات المتعلقة

بهذا المتغير ٤,٦٩، وهي نسبة عالية مقارنة بالمتغيرات الأخرى. هذه النتيجة تظهر الأهمية البالغة التي يضعها أفراد العينة لإجراءات الحوكمة المتعلقة بالأدوات والاتمته. ويمكن تفسير هذه النتيجة بان إجراءات تتمثل ببرمجيات تمكن الشركة من الكشف عن محاولات اختراق النظام، أو آليات تدقيق مؤتمته لقواعد البيانات لكشف الثغرات في وسائل الرقابة الداخلية يساعد إلى حد كبير في تقليل المخاطر المتأصلة في بنود الكشوفات المالية، كذلك فان وجود نظام برمجيات متكامل لإدارة قاعدة البيانات سيسهم بما لا شك فيه في تسهيل وتأمين انتقال المعلومات داخل النظام مما يؤدي إلى تقليل مخاطر الاختراق أو التلاعب بالمعلومات.

أما المتغير الثاني من حيث التأثير في مخاطر التدقيق فكان متغير السياسات والخطط، حيث بلغ متوسط استجابة أفراد العينة للفقرات المتعلقة بهذا المتغير ٤,٦٥ مما يشير للأهمية التي تتمتع بها الإجراءات المتعلقة بالسياسات والخطط ذات الصلة بتكنولوجيا المعلومات المتبعة داخل المنظمة في تقليل مخاطر التدقيق. وترجع هذه النتيجة إلى أن تصميم إجراءات تقويم دورية لفاعلية وسائل الرقابة على انتقال البيانات في مراحلها المختلفة المدخلات، المعالجة والمخرجات الكترونيا أو يدوياً ، فضلاً عن الإجراءات التدقيقية المتعلقة بالكشف عن الدخول غير المصرح للنظام تسهم في تقليل حالات التلاعب في البيانات أو إدخال بيانات مزيفة مما يقلل من مخاطر تدقيق هذه البيانات. أما المتغير الثالث من حيث الأهمية فقد كان متغير المسؤولية والمساءلة، فقد بلغ متوسط استجابة أفراد العينة للفقرات المتعلقة به ٤,٣٢، مما يشير إلى اهتمام أفراد العينة بالإجراءات المتعلقة بالمسؤولية والمساءلة وأثرها في تقليل مخاطر التدقيق. هذه النتيجة تشير إلى أن إعداد المنظمة لتوصيف صريح للمسؤوليات والصلاحيات المتعلقة بأنشطة تكنولوجيا المعلومات، ووجود دليل للسلوك المهني النزيه، وكذلك وجود تقارير للاختراقات والسلوكيات المشكوك فيها يسهم في خلق بيئة تدعم السلوكيات النزيهة داخل المنظمة مما ينعكس إيجابا على مستوى الثقة في النظام المطبق ككل.

الشكل رقم ٣

(التأثير المتفاوت لأبعاد حوكمة تكنولوجيا المعلومات على مخاطر التدقيق)



أما متغير المهارات والخبرة فقد جاء بالترتيب الرابع من حيث الأهمية، إذ بلغ متوسط استجابة أفراد العينة للفقرات المتعلقة به ٤,٢٧، مما يشير إلى وجود تأثير نسبي لهذا المتغير في تقليل مخاطر التدقيق. ويرجع السبب في هذه النتيجة إلى الاهتمام بالكوادر البشرية التي تدير النظام من خلال وضع معايير توظيف مناسبة يراعى بها الخبرة والنزاهة والأمانة، التقويم المستمر لامتثال الموظفين بمعايير امن المعلومات المتبع في الشركة، إضافة

للتدريب المستمر يقود إلى تقليل حالات الخطأ المتعمد أو غير المتعمد، ومن ثم يؤدي إلى تقليل مخاطر تدقيق النظام. أما متغير المعرفة والاتصالات فقد جاء بالترتيب الخامس وبمتوسط استجابة مقداره ٤,١٥ لفقرات الاستبانة المتعلقة بهذا المتغير. وهذه النتيجة تبرز اهتمام جيد من قبل أفراد العينة بهذا المتغير وأثره على مخاطر التدقيق، ويرجع السبب في ذلك إلى أن وجود نظام فاعل للتقارير بين الإدارة وقسم تكنولوجيا المعلومات يعد عنصراً مهماً في نجاح جهود المنظمة في استثمار التقنيات المتاحة لديها في تحقيق أهدافها وتوفير قيمة مضافة للاستثمار في تكنولوجيا المعلومات. وذلك يؤثر إيجابا في مستوى مخاطر التدقيق المتأصلة في بعض بنود الكشوفات المالية للمنظمة.

وأخيرا نجد أن متغير الأهداف والقياس قد جاء سادساً من حيث الأهمية في التأثير في مستوى مخاطر التدقيق في النظم المحاسبية الالكترونية.إذ بلغ متوسط استجابة أفراد العينة للفقرات المتعلقة بهذا المتغير ٣,٨٥، وهي نسبة قليلة مقارنة بالمتغيرات الأخرى. ويرجع السبب في ذلك إلى الانخفاض النسبي في فاعلية إجراءات الحوكمة المتعلقة بوضع الأهداف وقياسها في تقليل مخاطر التدقيق. مع ذلك نجد أن إجراءات الحوكمة المتعلقة بتحديد أهداف تكنولوجيا المعلومات، تطوير الخطط التشغيلية للمنظمة، وكذلك وجود آلية فاعلة لربط أداء تكنولوجيا المعلومات بأهداف المنظمة قد تسهم في زيادة فاعلية أساليب الرقابة الداخلية في النظم المحاسبية الالكترونية من التقويم المستمر للتكنولوجيا المتبعة داخل المنظمة.

بناء على ما تقدم يمكن القول أن وجود نظام فاعل للرقابة الداخلية في المنظمات التي تعتمد نظم معلومات محاسبية الكترونية عالية التقنية كالمصارف أو غيرها من المنظمات مع وجود آليات لحوكمة تكنولوجيا المعلومات بالاستناد إلى إطار عمل COBIT للرقابة الداخلية يؤدي إلى تحقيق المزايا الآتية:

١. تحسين كفاءة الأداء تكنولوجيا المعلومات المطبقة في المنظمة من خلال تحسين امن المعلومات التي الناتجة عن النظام المحاسبي في كل مرحلة من مراحله.

٢. تحسين كفاءة الاستثمار في تكنولوجيا المعلومات في المنظمة وتجنب الإنفاق غير الضروري في هذا المجال.

٣. زيادة ثقة مستخدمي المعلومات والمتعاملين الآخرين بمعلومات المنظمة من خلال وجود آلية رقابة فاعلة على عمل النظام المحاسبي المطبق سواء من الجوانب التقنية أو توافر الكوادر المؤهلة للتعامل مع النظام.

٤. تقليل الجهد والوقت المبذول من قبل المدقق الخارجي نتيجة لوجود نظام رقابة داخلية فعال وانخفاض مستوى مخاطر التدقيق وبما يضمن تقليل تكاليف التدقيق المقترنة بها.

٥. تحسين جودة التدقيق الخارجي والذي يعد نتيجة مباشرة لانخفاض مخاطر التدقيق وتحسين امن المعلومات المعلنة في الكشوفات المالية.

المبحث الرابع
(الاستنتاجات والتوصيات)

الاستنتاجات

توصل البحث إلى مجموعة من الاستنتاجات نلخص أبرزها بالنقاط الآتية:

١. يسهم تبني آليات حوكمة تكنولوجيا المعلومات في الحد من التلاعب المالي في ظل النظم المحاسبية الالكترونية.
٢. يؤدي تطبيق آليات حوكمة تكنولوجيا المعلومات في ظل إطار COBIT للرقابة الداخلية إلى تعزيز نظام الرقابة الداخلية في النظم المحاسبية الالكترونية.
٣. يوفر تبني إطار عمل COBIT للرقابة الداخلية تقليل مخاطر امن المعلومات في ظل نظم المعلومات المحاسبية الالكترونية.
٤. يؤدي تطبيق إطار COBIT إلى زيادة ثقة مستخدمي المعلومات المحاسبية نتيجة لتكثيف وسائل الرقابة على تكنولوجيا المعلومات المطبقة في الشركة.
٥. أن توفير بيئة مناسبة للرقابة الداخلية في ظل نظم المعلومات المحاسبية الالكترونية من خلال تطبيق آليات حوكمة تكنولوجيا المعلومات يساهم في تحسين جودة التدقيق الخارجي ويؤثر في تقليل تكاليف التدقيق.
٦. بينت نتائج التحليل الإحصائي لاستجابات أفراد العينة إلى وجود علاقة موجبة و ذات دلالة إحصائيا بين تعزيز حوكمة تكنولوجيا المعلومات وتقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية.
٧. أظهرت النتائج الميدانية وجود علاقة موجبة و ذات دلالة إحصائيا بين مكونات حوكمة تكنولوجيا المعلومات المتثلمة بمتغيرات (المسؤولية والمساءلة، المعرفة والاتصالات،السياسات والخطط ، الآليات والاتمته، المهارات والخبرة ، الأهداف والقياس) وتقليل مخاطر تدقيق نظم المعلومات الالكترونية.
٨. أظهرت نتائج اختبار فرضيات البحث وجود تفاوت في تأثير إجراءات حوكمة تكنولوجيا المعلومات مخاطر التدقيق على مستوى المتغيرات الفرعية، حيث كان التأثير الأكبر لمتغير الآليات والاتمته، ومن ثم متغيرات السياسات والخطط، المسؤولية والمساءلة، المهارات والخبرة، والمعرفة والاتصالات على التوالي، في حين جاء تأثير متغير الأهداف والقياس الأقل من بين المتغيرات الأخرى.

التوصيات

بناء على ما توصل إليه البحث من نتائج يوصي الباحث بما يأتي:

١. ضرورة تبني الشركات العراقية التي تعمل بيئة نظم المعلومات المحاسبية الالكترونية وخصوصاً المصارف العراقية الأهلية لإطار COBIT للرقابة الداخلية بما يضمن للشركات قدر كاف من الثقة بالنظام المحاسبي المطبق وتحسين امن المعلومات داخل النظام.
٢. يوصي الباحث بضرورة تأسيس هيئة عراقية مستقلة للرقابة الداخلية تهتم بإصدار تعليمات ملزمة للشركات باعتماد معايير حوكمة تتناسب مع احتياجات الشركات باختلاف طبيعة نشاطها ومستوى التعقيد في تكنولوجيا المعلومات المعتمدة فيها.
٣. ضرورة اعتماد الشركات العراقية لقواعد صارمة في اختيار الموظفين العاملين في إدارة تكنولوجيا المعلومات بالشكل الذي يضمن للشركة توفير كوادر مؤهلة علمياً وسلوكياً للعمل في هذا المجال.
٤. ضرورة العمل على وجود وسائل فاعلة للتقويم المستمر لآليات الرقابة على تكنولوجيا المعلومات المطبقة في الشركات، وذلك نتيجة للتطور المستمر في وسائل اختراق النظم الالكترونية أو محاولة التلاعب في معلوماتها.
٥. يوصي الباحث بضرورة عمل دراسات مستقبلية في مجال تقويم فاعلية نظام الرقابة الداخلية باعتماد إطاري عمل COBIT و COSO للرقابة الداخلية. فضلاً عن دراسة مجالات أخرى كتقويم أداء تكنولوجيا المعلومات في المنظمة وعلاقته بتحقيق أهدافها.

المصادر

المصادر العربية

١. ابو حجر، سامح، و عابدين، امينة، ٢٠١٤،" دور آليات حوكمة تكنولوجيا المعلومات في تخفيض مخاطر أمن المعلومات للحد من التلاعب المالي الإلكتروني في الوحدات الحكومية في ظل نظام الحكومة الإلكترونية"، المؤتمر السنوي الخامس لقسم المحاسبة كلية التجارة – جامعة القاهرة.

٢. ألركابي، ناجي شايب كايم، دور الرقابة الداخلية في تخفيض تهديدات نظام المعلومات المحاسبي المؤتمت لتحقيق قيمة للمنظمة والزبون، أطروحة دكتوراه، كلية الإدارة والاقتصاد – جامعة بغداد، ٢٠٠٨.

٣. حمدان علاّم محمد ، عناوسه محمد سلامة، والعتيبي محمود حسني. (٢٠١٢).أثر هيكل الملكي في مستوى الإستثمار في تكنولوجيا المعلومات وأثرها في أداء المصارف الأردنية: دراسة تحليلية للفترة ٢٠٠٨-٢٠٠٣ . مجلة الجامعة الإسلامية: الدراسات الاقتصادية والإدارية، المجلد (٢٠)، العدد (٢)، ص. ٣٨١-٤١٦.

٤. خليل، محمد (٢٠٠٥) "دور حوكمة الشركات في تحقيق جودة المعلومات المحاسبية وانعكاساتها على سوق الأوراق المالية- دراسة نظرية تطبيقية"، مجلة الدراسات البحوث التجارية، السنة الخامسة والعشرون، العدد الأول جامعة الزقازيق.

المصادر الأجنبية

5. Abu-Musa, A., (2009),"Exploring the importance and implementation of COBIT processes in Saudi organizations", Information Management & Computer Security, Vol. 17 Iss 2 pp. 73 – 95
6. Alfaraj M. Hussain, and Qin S,, (2011),"Operationalising CMMI: integrating CMMI and CoBIT perspective", Journal of Engineering, Design and Technology, Vol. 9 Iss 3 pp. 323 – 335.
7. Arens A, Elder RJ, Beasley (2012) "Auditing and Assurance Services: An Integrated Approach" 14th edition. Pearson Prentice Hall.
8. De Haes, S., & Van Grembergen, W. (2015) "Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5" Second Edition, Springer International Publishing Switzerland.
9. Fazlida, M.R. ,and Said, J. , (2015) " Information Security: Risk, Governance and Implementation Setback", Procedia Economics and Finance, Vol. 28, pp. 243–248.
10. Hardy, G. 2006, "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges", Information Security Technical Report, vol. 11, no. 1, pp. 55-61.
11. Haseley, S. & Brucker, J. 2012. Assessing IT Governance: Considerations for Internal Audit. Journal of the Association of Heathcare Internal Auditors, 31(2): 54-58
12. Iliescu F M. (2010), Auditing IT Governance. Informatica Economică. 14(1): 93-102.
13. ISACA. (2007). COBIT 4.1 . Retrieved from www.isaca.org
14. ISACA. (2012). COBIT 5 . Retrieved from www.isaca.org
15. Messier, W.F.; Glover, S.M.; Prawitt, D.F. (2008) Auditing and Assurance Services A Systematic Approach, 6th Ed., McGraw Hill Irwin, New York
16. Mirela, G. (2010). Audit Methodology for IT Governance. Informatica Economică, 14(1), pp 32-42.
17. Moeller, R., (2013) " Executive's Guide to IT Governance Improving Systems Processes with Service Management, COBIT, and ITIL" John Wiley & Sons, Inc.

18. Pramod, V., Li, J., and Gao, P., (2012),"A framework for preventing money laundering in banks", Information Management & Computer Security, Vol. 20 Iss 3 pp. 170 – 183.
19. Rubino, M. ,and Vitolla, F. , (2014a) "Corporate governance and the information system: how a framework for IT governance supports ERM", Corporate Governance, Vol. 14 Iss 3 pp. 320 - 338
20. Rubino, M. ,and Vitolla, F. , (2014b) "Internal control over financial reporting: opportunities using the COBIT framework", Managerial Auditing Journal, Vol. 29 Iss: 8, pp.736 – 771
21. Sigler, K. E., and Rainey, J.L., (2016) " Securing an IT Organization through Governance, Risk Management, and Audit (Internal Audit and IT Audit)" Taylor & Francis Group, LLC
22. Tuttle, B., Vandervelde, S. D.,(2007) "An Empirical Examination of CobiT as an Internal Control Framework for Information Technology' 'International Journal of Accounting Information Systems, 8(4), 240–263.
23. Van Grembergen, W., & De Haes, S. (2009). Enterprise governance of IT: Achieving strategic alignment and value . New York: Springer.
24. Van Grembergen, W., 2002, Introduction to the minitrack IT Governance and its Mechanisms, Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS).
25. Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. Computers & Security, 24(2), 99-104.
26. Walker, A; McBride, TM; Basson, G; Oakley, R, (2012),"ISO/IEC 15504 measurement applied to COBIT process maturity", Benchmarking: An International Journal, Vol. 19 Iss 2 pp. 159 – 176

الملحق رقم (١)
الاستبانة

حضرة الأساتذة الكرام :
تحية طيبة

الاستمارة التي بين يديك هي جزء من متطلبات البحث الموسوم (دور حوكمة تكنولوجيا المعلومات في تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية في ظل إطار عمل COBIT للرقابة الداخلية) وتهدف هذه الاستبانة من خلال ما تحويه من أسئلة إلى التعرف على أرائكم حول مدى تأثير تعزيز آليات وإجراءات حوكمة تكنولوجيا المعلومات على تقويم المدقق الخارجي لمستوى مخاطر التدقيق في بيئة نظم المعلومات المحاسبية الالكترونية.

الجزء الأول : المعلومات الشخصية.

القسم الأول: معلومات عامة. يرجى اختيار الإجابة المناسبة بوضع إشارة X في المكان المناسب:

مدير فرع	محاسب	مدقق

		الإجابة
المؤهل العلمي	١ –دكتوراه	
	٢ –ماجستير	
	٣ –بكالوريوس	
	٤ – دبلوم	
	٥- أخرى؛ يرجى ذكره	
سنوات الخبرة العملية	١ – أقل من ٥ سنوات	
	٢ – من ٥ سنوات إلى أقل من ١٠ سنوات	
	٣ – من ١٠ سنوات إلى أقل من ٢٠ سنة	
	٤ – من ٢٠ سنة فأكثر.	

القسم الثاني: الاستبانة.

تتكون هذه الإستبانة من ستة محاور بما يتفق مع فرضيات الدراسة وأهدافها؛ راجياً من حضرتكم إبداء أرائكم بكل موضوعية وأمانة حتى تحقق الدراسة أهدافها.

#	الفقرات هل ترى أن وجود المتطلبات ادناة تساعد في تقليل مخاطر تدقيق نظم المعلومات المحاسبية الالكترونية:	لا اتفق تماماً ١	لا اتفق ٢	محايد ٣	اتفق ٤	اتفق تماماً ٥
١	**المحور الأول: إجراءات تتعلق بالمسؤولية والمساءلة**					
١.	وجود تحديد وتوصيف واضح للأشخاص المسؤولين عن مختلف أنشطة تكنولوجيا المعلومات					
٢.	وجود دليل مكتوب للسياسات المتبعة داخل المصرف يصف بوضوح أنماط السلوك النزيهة وأنماط السلوك المشبوهة، يوزع على المتعاملين مع المعلومات الالكترونية.					
٣.	وجوب إعداد تقارير بالسلوكيات غير النزيهة ذات الأهمية نسبياً وتسجيلها في سجل خاص مع بيان الإجراءات التصحيحية التي تمت بصددها					
٢	**المحور الثاني: إجراءات تتعلق بالمعرفة والاتصالات**					
٤.	وجود قنوات اتصال ثابتة للإدارة العليا مع المدراء التنفيذيين لكي تضمن الإدارة تنفيذ استراتيجيات البنك وأهدافه					
٥.	وجود تقارير معدة من خبير المعلومات تقدم للإدارة تبين الاحتياجات التجارية الحالية والمستقبلية إضافة إلى الحلول المناسبة لمشاكل تكنولوجيا المعلومات					
٦.	وجود تقارير دورية حول مدى توافق تكنولوجيا المعلومات مع إستراتيجية المنظمة والمخاطر المتوقعة وتحدد القيمة المضافة للاستثمار في مجال تكنولوجيا المعلومات					
٣	**المحور الثالث: إجراءات تتعلق بالسياسات والخطط**					
٧.	وجود تقارير تقويم دورية في قسم تكنولوجيا المعلومات لفاعلية إجراءات الرقابة المتعلقة بمصادر البيانات، إدخال البيانات، معالجة البيانات، انتقال البيانات والرقابة على المخرجات.					
٨.	وجود إجراءات رقابة صارمة على انتقال البيانات يدويا والمتعلقة					

	بالمعلومات السرية والحساسة للبنك.					
٩.	يتم تقديم تقارير من قسم تكنولوجيا المعلومات إلى الإدارة بشكل دوري يحدد فيه سجل للحالات التدقيقية التي تكشف أنشطة الدخول غير المرخص للشبكة.					
٤	**المحور الرابع: إجراءات تتعلق بالآليات والأتمتة**					
١٠.	وجود آليات لدى البنك توفر حلول الكترونية تتمثل ببرمجيات تمكن البنك من الكشف وتقويم أي تغييرات أو دخول غير مصرح للنظام ضمن كامل البني التحتية لتكنولوجيا المعلومات وتقدم تصحيحات فورية وفعالة					
١١.	وجود آليات تدقيق نشاط قاعدة البيانات في المصرف يمكنها أوتوماتيكيا متابعة الأنشطة واكتشاف الثغرات في وسائل الرقابة					
١٢.	وجود نظام برمجيات متكامل داخل البنك يدير قاعدة بيانات موحدة يسمح للأقسام والمهام داخل البنك من مشاركة المعلومات وتوصيلها بسهولة وامن					
٥	**المحور الخامس: إجراءات تتعلق بالمهارات والخبرة**					
١٣.	وجود معايير صارمة للتوظيف في مجال تكنولوجيا المعلومات بما في ذلك الخلفية الأكاديمية، النزاهة و السرية					
١٤.	وجود مراجعة مستمرة من قبل الإدارة لأداء موظفي قسم تكنولوجيا المعلومات لغرض التأكد من فهمهم وامتثالهم لسياسات امن نظام المعلومات المطبق في البنك					
١٥.	تنفيذ برامج تدريب مستمرة للمستخدمين لغرض تحسين مهاراتهم و معرفتهم بتطورات الحاصلة في تكنولوجيا المعلومات وتوفير الفرص للأفراد للارتقاء الوظيفي					
٦	**المحور السادس:إجراءات تتعلق بوضع الأهداف والقياس**					
١٦.	وجود إستراتيجية للبنك تتضمن تحديد واضح لأهداف قسم تكنولوجيا المعلومات لكل سنة تقويمية، كما تتضمن إستراتيجية قسم تكنولوجيا المعلومات اعتماد خطة عمل البنك كأولوية لمشاريعها وأنشطتها.					
١٧.	وجود ورش عمل سنوية لمدراء الفروع يحدد فيها استراتيجية البنك للسنة القادمة ويتم فيها حث المدراء على تطوير الخطط التشغيلية للسنة القادمة					
١٨.	وجود آلية لتحديد فاعلية وكفاءة الأداء باستخدام نظام قياس يربط أداء تكنولوجيا المعلومات بأهداف المنظمة كبطاقة الأداء المتوازن					