كلية التجارة
قسم المحاسبة

دور حوكمة تكنولوجيا المعلومات في الحد من المخاطر المصرفية الإلكترونية

- دراسة ميدانية -

ملخص رسالة مقدمة للحصول على درجة الماجستير في المحاسبة

إعداد

نعمة محمد عبد المنعم عبدالله

مصرفي بالبنك الأهلي المصري

إشراف

أ.د/ سليمان محمد مصطفى

أستاذ المحاسبة المالية
ونائب رئيس جامعة بنها الأسبق
لشئون التعليم والطلاب

د/ محمود محمد عبد الرحيم

مدرس المحاسبة
كلية التجارة - جامعة بنها

الملخـــــص:

لقد أصبح إستخدام البنوك التجارية لتكنولوجيا المعلومات في إتمام معاملاتها أمراً ضرورياً لمواجهة المنافسة بين البنوك وتعظيم الحصة السوقية وبالتالي تعظـيم الربحيـة، ولكن على الرغم من المزايا العديدة التي يحققها إستخدام تكنولوجيا المعلومات في البنـوك التجارية إلا أنه يحيط بها العديد من المخاطر الداخلية والخارجية التي قد تؤثر على الأداء والقدرة التنافسية. مما يتطلب آليات جديدة لتأمين المعلومات وإدارة المخاطر المتعلقة بها، وتعتبر حوكمة تكنولوجيا المعلومات هي إحدى الآليات التي قد يؤدى تطبيقهـا إلـى إدارة مخاطر العمليات المصرفية الإلكترونية في البنوك التجارية، بإعتبارها مجموعـة متكاملـة من الإجراءات والسياسات والعمليات والهياكل التنظيمية المطلوبة للرقابـة الفعالـة علـى العمليات المصرفية الإلكترونية.

ولذلك هدف هذا البحث إلى دراسة دور حوكمة تكنولوجيا المعلومات فـي الحـد من مخاطر العمليات المصرفية الإلكترونية في البنوك التجارية بمـا يضـمن الحـد مـن المخاطر الإلكترونية بهدف تحسين أداء البنوك.

وتوصلت الدراسة إلى أن تطبيق حوكمة تكنولوجيا المعلومات يؤدى إلى الحد من المخاطر المصرفية الإلكترونية، وهو ما يضمن تحقيـق الأهـداف الإسـتراتيجية والنمـو والاستمرارية. كما توصلت الدراسة إلى أن نظام الرقابة الداخلية يؤدى إلى تدعيم حوكمـة تكنولوجيا المعلومات وذلك في ظل إطار COBIT.

ABSTRACT:

The use of information technology by commercial banks in completing their transactions has become necessary to face competition between banks and maximize market share and thus maximize profitability, but despite the many advantages that the use of information technology brings in commercial banks, it is surrounded by many internal and external risks that may affect Performance and competitiveness.

This requires new mechanisms to secure information and manage the risks related to it, and information technology governance is one of the mechanisms that its application may lead to managing the risks of electronic banking operations in commercial banks, considering it as an integrated set of procedures, policies, processes and organizational structures required for effective control of electronic banking operations. Therefore, this research aims to study the role of information technology governance in reducing the risks of electronic banking operations in commercial banks in order to reduce electronic risks in order to improve the performance of banks.

The study found that the application of information technology governance leads to a reduction in electronic banking risks, which ensures the achievement of strategic objectives, growth and continuity. The study also found that the internal control system leads to strengthening the governance of information technology under the framework of COBIT.

أولاً: مقدمة ومشكلة البحث:

يعتبر من أهم التطورات فى البيئة التكنولوجية إعتماد معظم البنوك بشكل عام والبنوك التجارية بشكل خاص على إتمام معاملاتها بإستخدام وسائل تكنولوجيا المعلومات، حيث شهدت الصناعة المصرفية في الآونة الأخيرة تقدماً ملموساً في مجال السماح لعملاء البنوك بإجراء العمليات المصرفية من خلال شبكة الإتصال الإلكترونية، ومن المتوقع أن تنتشر هذه الخدمات بشكل واسع فى الفترة المقبلة خاصة فى ظل التطور المستمر في مجال تكنولوجيا المعلومات في المجال المصرفي.

تتمثل مشكلة البحث في تعرض البنوك التجارية للعديد من المخاطر المرتبطة بالأنشطة المصرفية الإلكترونية التي قد تؤثر على أدائها وقدرتها التنافسية، لذلك تحاول الباحثة دراسة دور حوكمة تكنولوجيا المعلومات فى إدارة هذه المخاطر من خلال تدعيم إجراءات الرقابة الداخلية للعمليات المصرفية الإلكترونية. **وتتلخص مشكلة البحث في محاولة الإجابة على التساؤلات الآتية:**

(١) ماهي مخاطر التي تتعرض لها البنوك التجارية عند إستخدام تكنولوجيا المعلومات في العمليات المصرفية الإلكترونية بالبنوك؟

(٢) هل تقوم آليات حوكمة تكنولوجيا المعلومات بالحد من مخاطر العمليات المصرفية الإلكترونية؟

(٣) ماهو دور حوكمة تكنولوجيا المعلومات فى تدعيم نظام الرقابة الداخلية للعمليات المصرفية الإلكترونية للحد من المخاطر المصرفية بالبنوك التجارية؟

ثانياً: هدف البحث:

يتمثل هدف البحث فى دراسة دور حوكمة تكنولوجيا المعلومات في الحد من مخاطر العمليات المصرفية الإلكترونية في البنوك التجارية بما يضمن الحد من المخاطر الإلكترونية بهدف تحسين أداء البنوك.

أهمية البحث:

تنبع أهمية البحث من حداثة مفهوم حوكمة تكنولوجيا المعلومات، وخاصة في ظل اتجاه كثير من البنوك لإستخدام الوسائل الإلكترونية والتعامل على شبكة الإنترنت ودور الرقابة الداخلية في ذلك، وتوضيح الإجراءات التي تقوم بها البنوك للحد من تلك المخاطر المصرفية الإلكترونية.

فروض البحث:

١. يؤدى استخدام تكنولوجيا المعلومات إلى ظهور العديد من مخاطر العمليات المصرفية الإلكترونية.

٢. يؤدى تطبيق حوكمة تكنولوجيا المعلومات إلى الحد من المخاطر المصرفية الإلكترونية.

٣. يؤدى نظام الرقابة الداخلية إلى تدعيم حوكمة تكنولوجيا المعلومات.

حدود البحث:

١. لن يتناول البحث مقررات لجنة بازل، وكذا دور المراجعة الداخلية في الحد من المخاطر المصرفية الإلكترونية إلا بالقدر الذي يخدم البحث .

٢. لن يتناول البحث دور حوكمة تكنولوجيا المعلومات فى الحد من المخاطر المصرفية التقليدية.

٣. لن يتناول البحث البنوك المتخصصة والبنك المركزي فى الدراسة الميدانية

خطة البحث:

سعياً لتحقيق هدف البحث واختبار فروضه تم تقسيم محتويات البحث كالآتى:

أولاً: الدراسات السابقة.

ثانياً: مخاطر العمليات المصرفية الإلكترونية وإجراءات الحد منها وأثرها على الرقابة الداخلية بالبنوك التجارية.

ثالثاً: دور آليات حوكمة تكنولوجيا المعلومات في الحد من المخاطر المصرفية الإلكترونية.

رابعاً: الدراسة الميدانية.

خامساً: النتائج والتوصيات والتوجهات البحثية المستقبلية.

أولاً: الدراسات السابقة:

تنوعت الجهود البحثية في مجال تكنولوجيا المعلومات، وسوف يتم الاقتصار على الدراسات وثيقة الصلة بموضوع البحث والتى يمكن استعراضها على النحو التالى:

١. **دراسة (جمال موسى، ٢٠١١)**: هدفت الدراسة إلى التعرف على طبيعة الخدمات المصرفية الإلكترونية والمخاطر المصاحبة لها، وكذلك التعرف على متطلبات الرقابة الداخلية لأمن المعلومات والتحقق من مدى توافق أنظمة الرقابة الداخلية فى البنوك محل الدراسة مع متطلبات الرقابة الداخلية لأمن المعلومات المصرفية. وتوصلت الدراسة إلى وجود توافق فى أنظمة الرقابة الداخلية فى البنوك مع متطلبات الرقابة الداخلية لأمن المعلومات المصرفية.

٢. **دراسة (أماني هاشم، ٢٠١٢)** هدفت الدراسة إلى التعرف على المخاطر المصرفية الإلكترونية بأنواعها المختلفة ومعرفة دور لجان المراجعة في الحد من المخاطر المصرفية الإلكترونية كمحاولة للحد من هذه المخاطر. كما إختبرت الدراسة قدرة لجان المراجعة على تخفيض المخاطر المصرفية للبنوك الإلكترونية. وتوصلت الدراسة إلى أن هناك دوراً فعالاً للجان المراجعة في الحد من المخاطر المصرفية.

٣. **دراسة (Enslin, 2012)**: هدفت الدراسة إلى إختبار أثر تطبيق آليات حوكمة تكنولوجيا المعلومات على الأداء المالي للبنوك. وقد قامت الدراسة بقياس الأداء المالي للبنوك قبل وبعد تطبيق آليات حوكمة تكنولوجيا المعلومات. وتوصلت الدراسة إلى هناك إهتمام كبير من جانب البنوك بحوكمة تكنولوجيا المعلومات، وذلك لتبرير الإستثمارات الضخمة التي تنفقها تلك البنوك في تكنولوجيا المعلومات. كما تحقق البنوك التي تقوم بتطبيق نماذج جيدة لحوكمة تكنولوجيا المعلومات عوائد على الإستثمار في تكنولوجيا المعلومات أكبر من منافسيها. وأن هناك تحسن في الأداء المالي للبنوك التي قامت بتطبيق آليات حوكمة تكنولوجيا المعلومات، وذلك بالمقارنة مع البنوك التي لم تطبق هذه الآليات.

٤. دراسة (Spremic, 2012): هدفت الدراسة إلى توضيح مدى تأثير COBIT وبعض الهياكل التنظيمية الأخرى في كرواتيا على مستوى أداء حوكمة تكنولوجيا المعلومات،كما هدفت الدراسة إلى قياس أداء نظم المعلومات وتقييم جودتها وذلك بهدف الفحص المنظم لرقابة تكنولوجيا المعلومات، وتحديد مناطق ومستوى الخطر المرتبطة بتكنولوجيا المعلومات وتقييمها وفحص جودة نظام المعلومات وهي دراسة ميدانية على عينة من البنوك. وتوصلت الدراسة إلى أنه من خلال قيام البنوك بمراجعة نظام المعلومات،فإنه يمكنها بشكل دوري قياس أداء حوكمة تكنولوجيا المعلومات، وذلك بإستخدام COBIT الأمر الذي يساعد في تحسين مستوى تطبيق حوكمة تكنولوجيا المعلومات وتشمل مناطق حوكمة ومراجعة نظم المعلومات المعتمدة على COBIT سياسة إدارة المخاطر بالإضافة إلى المراجعة الداخلية وأمن وصيانة نظم المعلومات وإدارة إستمرارية العملية.

٥. دراسة (منى إبراهيم، ٢٠١٢): هدفت الدراسة إلى وضع إطار محاسبي مقترح لتطوير وتنظيم عملية الإفصاح الإلكتروني في ظل آلية حوكمة تكنولوجيا المعلومات. وتوصلت الدراسة إلى الإفصاح الإلكتروني يدعم خاصية الملاءمة والتوقيت المناسب للمعلومات المحاسبية ويعمل على زيادة الشفافية وتخفيض حالة عدم تماثل المعلومات وذلك عن طريق توصيل كافة المعلومات المحاسبية لجميع المستخدمين في نفس الوقت. كما أن الإفصاح المحاسبي بالأسلوب الورقي ضروريا ولا يمكن الإستغناء عنه وإستبداله بالإفصاح المحاسبي الإلكتروني في الوقت الراهن وخاصة في غياب إطار موحد ملزم ينظم عملية الإفصاح الإلكتروني. كما توصلت الدراسة إلى إن الإفصاح الإلكتروني لايتعارض مع الإطار الفكري لنظرية المحاسبة من حيث الأهداف أو الفروض أو المبادىء المحاسبية المتعارف عليها.

٦. دراسة (سامي غنيمي، ٢٠١٦): هدفت الدراسة إلى محاولة إبراز دور آليات حوكمة تكنولوجيا المعلومات في تحسين جودة المعلومات المحاسبية وزيادة القدرة التنافسية للبنوك التجارية. وتوصلت الدراسة إلى أن الهدف الأساسي من حوكمة تكنولوجيا المعلومات في البنوك هو التأكيد علي توافق أهداف نظام تكنولوجيا المعلومات مع الأهداف الإستراتيجية للبنك. وأن الحوكمة الفعالة لتكنولوجيا المعلومات أصبحت ضرورة حتمية لإضافة قيمة حقيقية للبنك، وتعظيم قيمة إستثماراته في مجال تكنولوجيا المعلومات، وتحقيق أكبر إستفادة ممكنة من خلال إعادة تقييم إجراءات حوكمة الشركات وفقا لمتطلبات تطبيق الحاسبات وتكنولوجيا المعلومات. كما توصلت إلى أن تطبيق آيات حوكمة تكنولوجيا المعلومات يساهم في تفعيل عملية إدارة المخاطر المرتبطة بالأنشطة وتقديم الخدمات الإلكترونية بالبنوك.

٧. دراسة (Rubino and Others, 2018): هدفت هذه الدراسة إلى تحليل تأثير إطار حوكمة تكنولوجيا المعلومات (COBIT) على تحسين نظام الرقابة الداخلية، حيث يوفر (COBIT) بعض المؤشرات للمديرين والمراجعين الداخليين التي تساعدهم في تقييم نظام الرقابة الداخلية، ويقترح الحلول والأدوات التي يمكن أن تساعد المديرين والمراجعين الداخليين لمعالجة تقييم بيئة الرقابة. وتوصلت الدراسة إلى أن إطار COBIT يُمكن البنك من تطبيق نظام الرقابة الداخلية الذي يسمح بالتغلب على قيود لجنة المنظمات الراعية، ويسمح هذا الإطار أيضاً بمعالجة إحتياجات البنك ويؤثر في المقام الأول على إدارة الموارد والهيكل التنظيمي بشكل عام والفصل بين الواجبات والتركيز على التحسين المستمر والإتصال.

وترى الباحثة أن الدراسات السابقة اقتصرت على معيار كوبيت ولم تتناول باقي آليات حوكمة تكنولوجيا المعلومات ودورها في دعم نظم الرقابة الداخلية لإدارة هذه المخاطر والحد من المخاطر المصرفية الإلكترونية وكذا تحقيق الأهداف الإستراتيجية. وهو ما سوف تتناوله الباحثة فى هذا البحث.

ثانياً: مخاطر العمليات المصرفية الإلكترونية وإجراءات الحد منها وأثرها على الرقابة الداخلية بالبنوك التجارية.

على الرغم من أهمية وفائدة إستخدام تكنولوجيا المعلومات في تقديم الخدمات المصرفية، إلا أن هذا يصاحبه العديد من المخاطر، وبالتالي يرتبط مفهوم المخاطر أساساً بحالة عدم التاكد (وهي حدوث خسائر غير متوقعة وغير مخطط لها)، وترتبط المخاطر أيضا بضعف قنوات الإتصال داخل البنك بين مكوناته وبين البنك والبيئة الخارجية.

وبالرغم من أنّ حالة عدم التأكد هي الحالة التي تواجهها كافة البنوك في ممارستها لأنشطتها، إلا أن هذه الحالة أكثر عمقاً في البنوك التجارية، وبالتالي يجب أخذها في الإعتبار حيث أن إهمالها قد يؤدي إلى خسائر، الأمر الذي جعل المنظمات المهنية تلقي الضوء عليها، وخاصة لجنة بازل للرقابة المصرفية حيث أشارت اللجنة إلى أنه ينبغي قيام البنوك بوضع السياسات والإجراءات التي تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها، وأصدرت اللجنة مبادئ لإدارة هذه المخاطر، ومن بين هذه المخاطر التي تتعرض لها البنوك من جراء العمليات المصرفية الإلكترونية ومواجهة رقابة البنك المركزي لها، ما يلي:

١) **مخاطر التشغيل Risk Operational:**

تنشأ مخاطر التشغيل من الخسائر الناتجة عن العمليات الداخلية غير السليمة وعن الأفراد والنظم، إلى جانب الحوادث الخارجية – عدم التأمين الكافي للنظم أو عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة –، وكذا نتيجة إساءة الإستخدام من قبل العملاء .

وللحد من هذه المخاطر يتطلب الأمر أن تقوم البنوك بالآتي:

- بناء أنظمة كفء ومتكاملة وتوفر البنية التحتية الملائمة بما يكفل السلامة والأمن.
- إتخاذ إجراءات وتدابير للتحقق من صحة هوية العملاء المتعاملين إلكترونياً.

- إستخدام أساليب التأكد من صحة المعاملات والمسئولية في التعاملات الإلكترونية.
- تطبيق الإجراءات المناسبة التي تحدد الواجبات والمهام للأنشطة المصرفية الإلكترونية.
- يجب على البنوك أن تمتلك البنية التحتية للقدرة على الإستمرار في تحسين خدماتها المصرفية الإلكترونية وإرضاء العميل.

٢) مخاطر السمعة Reputational Risk:

تنشأ مخاطر السمعة في حالة توافر رأي عام سلبى تجاه البنك نتيجة عدم القدرة على بناء علاقات طيبة مع العملاء أو ترويج إشاعات سلبية عن البنك أو عدم توفيرها للخدمات المصرفية الإلكترونية بكفاءة أي وفقاً لمعايير الأمان والسرية والدقة والاستجابة الفورية لحاجات ومتطلبات العملاء، أو نتيجة عدم مقدرة البنك على إدارة أنظمة أمان سرية المعلومات الشخصية فى البنك بكفاءة أو حدوث إختراق مؤثر لها، الأمر الذى قد يمتد إلى التأثير على بنوك أخرى.

ولكي تتفادي البنوك مخاطر السمعة يجب أن تسعى للآتي:

- وضع معايير لأنشطتها الإلكترونية، ومراقبتها ومراجعتها بصورة دورية ومنتظمة.
- إرشاد العملاء عن الإجراءات والمخاطر المحتملة وكيفية إستخدامها بالشكل الأمثل.
- حصر دقيق وواضح لجميع التعاملات الإلكترونية مع وجود أنظمة كفيلة بالحفظ والسرية.
- التامة وتخزينها في قواعد البيانات والمعلومات حتى يتسنى الرجوع إليها عند الحاجة.

٣) المخاطر القانونية Legal Risks:

تقع هذه المخاطر في حالة إنتهاك القوانين أو القواعد أو الضوابط المقررة خاصة تلك المتعلقة بمكافحة عمليات غسيل الأموال، أو نتيجة الإساءة في إستخدام البيانات والمعلومات أو نتيجة عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الإلكترونية ومن ذلك عدم وضوح مدى توافر قواعد لحماية المستهلكين في بعض الدول أو لعدم المعرفة القانونية لبعض الإتفاقيات المبرمة بإستخدام وسائل الوساطة الإلكترونية.

وللحد من هذه المخاطر يتوجب على البنوك التأكد من:

- إكمال متطلبات الإفصاح للعملاء وتحديداً التعريف بالأطر القانونية والتشريعية والإشرافية للمعاملات الإلكترونية وما قد ينشأ عنها من حقوق وإلتزامات.
- التأكد من الإجراءات القانونية والقضائية السائدة في المنطقة التي تقدم فيها الخدمات المصرفية الإلكترونية.
- الإفصاح والشفافية عن المعلومات الصحيحة على موقع الإنترنت الخاص بكل بنك حتى يتسنى للعملاء التوصيل إلى هوية البنك المعنى ووضعة التنظيمي والقانوني وكيفية الدخول معه في تعاملات إلكترونية.
- وضع التدابير الكفيلة بالإلتزام بالمتطلبات المتعلقة بخصوصية العملاء في إطار الإلتزامات التشريعية والقانونية السائدة.

٤) المخاطر الإستراتيجية Strategic Risk:

أصل هذه المخاطر في العمليات المصرفية هي الأخطاء أو الخلل الذي قد يحدث عند تبني إستراتيجيات وخطط تقديم هذه العمليات والخدمات وتنفيذها من قبل الإدارة العليا، وذلك في ضوء الحاجة الملحة لتقديم مثل هذه الخدمات وتنفيذها في ظل تزايد الطلب عليها من جهة، وشدة المنافسة المصرفية في هذا الشأن من جهة أخرى.

وبناءً على ما تقدم فإن المخاطر الإستراتيجية للعمليات المصرفية الإلكترونية ترتبط بجزء كبير منها بقضايا التوقيت، فقد تنشأ مخاطر إستراتيجية كبيرة في حالة توجه إدارة المصرف لأخذ زمام الريادة في إستخدام تقنيات حديثة، أو على العكس تماماً قد تنشأ هذه المخاطر في حالة تباطؤ إدارة المصرف في إدخال التكنولوجيا المصرفية الحديثة.

٥) المخاطر الإئتمانية Credit Risk:

إستخدام شبكة الإنترنت في البنوك ينتج عنه مجموعة من المخاطر الإئتمانية تتمثل في الآتي:

- في البنوك الصغيرة تحديداً لكي توسع نشاطها وأعمالها بشكل كبير ومتسارع الأمر الذي يؤدي إلى زيادة المخاطر المرتبطة بجودة الأصول ومتطلبات التدقيق الداخلي اللازمة.
- صعوبات في التحقق من هوية العملاء وجدارتهم الإئتمانية مما قد يزيد من احتمالات إخفاق بعض العملاء في سداد إلتزاماتهم وبالتالي زيادة المخاطر الإئتمانية.
- التوسع الجغرافي الذي تتيحه الشبكة في تقديم الخدمات والمنتجات المصرفية قد ينتج عنه مخاطر إئتمانية مرتبطة بمتطلبات معرفة السوق وطبيعة العملاء والتحقق من صحة الضمانات.

٦) مخاطر مصرفية خارجية:

تنشأ هذه المخاطر نتيجة ممارسة البنك لمعاملات مصرفية خارج حدود الدولة، حيث تواجه البنوك متطلبات قانونية وتنظيمية تختلف عما تطبقه على أرضها، فهناك أنشطة مصرفية جديدة وهناك دول تسود فيها ظروف سياسية وإقتصادية وقانونية معينة، ودول بها حالة من عدم التأكد حيال هذه الأنشطة مما قد يؤدي لحدوث سوء فهم مما يعرض البنك لمخاطر قانونية جديدة مثل مخاطر تنازع القوانين الذي سوف يطبق على المعاملات المصرفية بالإضافة لتعرض البنك للعديد من المخاطر السابق ذكرها.

٧) مخاطر مصرفية داخلية:

وهذه المخاطر تحدث نتيجة أعمال سلبية داخل البنك فتتسبب في إنتشار هذه المخاطر ومنها:

- إساءة إستخدام العاملين بالبنك البيانات الشخصية للعملاء.
- الخطأ الشخصي للعاملين بالبنك في تسجيل الحسابات مثل الإضافة في حساب العميل دون أن يضعه بنفسه عن طريق الخطأ الشخصي للموظف .
- إستخدام الإدارة أسلوب المجاملات مثل إعطاء قرض بدون ضمانات كافية.
- إدخال غير مقصود لبيانات غير سليمة بواسطة القائمين على العمل.
- مراجعة وتصحيح غير مناسب للبيانات بعد ترميزها.
- أخطاء في البرامج ونظم التشغيل سواء بقصد أو دون قصد.

٨) المخاطر التي تهدد أمن وسلامة نظم المعلومات في بيئة البنوك الإلكترونية:

لقد ترتب على إستخدام تكنولوجيا المعلومات المعتمدة على الحاسبات الآلية ظهور ما يسمي جرائم الحاسبات، ويقصد بها إستخدام تكنولوجيا المعلومات بشكل مباشر أو غير مباشر في القيام بأنشطة أو تصرفات غير قانونية مثل السرقة أو تحريف البيانات مما يؤدى إلى الإضرار بالمحتوى المعلوماتى للبنك، وترجع أسباب هذه المخاطر لطبيعة هذه البنوك وأنها إلكترونية ومن أمثلة هذه المخاطر ما يلي:

- فشل الأجهزة مثل تعطل أحد أجهزة الحاسب أو أحد أجهزة الإتصال، أو إحدى النهايات الطرفية، أو تدمير أو سرقة أحد الوسائط الممغنطة.
- فشل البرامج مثل وجود أخطاء منطقية في أحد البرامج المتعلقة بحل المشكلة.
- مخاطر التغذية المتعمدة أو غير المتعمدة لقاعدة البيانات ببيانات غير صحيحة.

٩) مخاطر الجرائم الإلكترونية:

الجريمة الإلكترونية هي الجريمة التي لا تعرف الحدود الجغرافية و التي يتم ارتكابها بالحاسب الآلى، عن طريق شبكة الإنترنت بواسطة شخص على دراية فائقة بهما، وقد كان لظهور وسائل الدفع الإلكترونية عاملاً مساهماً في ظهور هذا النوع من الجرائم بحيث تكون معظم عمليات الإحتيال على مستوى الحسابات المصرفية الإلكترونية على اضطرار المستخدم إلى الإفصاح عن كلمة السر ومعلومات سرية من خلال رسائل خبيثة أو بسبب تعرض الحاسوب أو الهاتف الذكي لبرنامج خبيث مصمم لسرقتها.

وترى الباحثة أن الرقابه الداخلية في البنوك يجب أن تكون جزء أساسي من الرقابة المصرفية الشاملة، وأنها تمثل خط الدفاع الأول في منع وصد وتحجيم المخاطر التي يمكن أن تتعرض لها البنوك في أعمالها، ولهذا سوف تقوم الباحثه بتناول دور حوكمة تكنولوجيا المعلومات في دعم نظام الرقابة الداخلية للحد من المخاطر المصرفية الإلكترونية بشيء من التفصيل كما يلي:

ثالثاً: دور آليات حوكمة تكنولوجيا المعلومات في الحد من المخاطر المصرفية الإلكترونية.

إن الغرض من الرقابة على العمليات المصرفية هو الحفاظ على متانة وسلامة الجهاز المصرفي من حيث حماية حقوق المودعين وحماية مصالح البنك بحد ذاته، ونتيجة لتطور أعمال البنوك والنشاطات التي تقوم بها. فقد أصبحت الرقابة على درجة كبيرة من التعقيد كما هو الحال في ميكنة العمل المصرفي وجعله إلكترونياً، مما أصبح يستلزم معها التغيير في أسلوب الرقابة بحيث أصبح يرتكز على المخاطر وكيفية القضاء عليها أو الحد منها مما له تأثيراً كبيراً على أوضاع البنوك.

وتهدف الرقابة الداخلية على العمليات المصرفية الإلكترونية إلى:

١. ضمان فعالية العمليات عن طريق تحقيق أهداف النظام ومنها: ضمان صدق وتمام ودقة المدخلات وضمان دلة وتمام التحديث للملفات الرئيسية.
٢. ضمان الإستخدام الكفء للموارد المملوكة للبنك.

٣. حماية موارد البنك وأصوله من الإختلاس أو الضياع أو سوء الاستعمال.
٤. التأكد من دقة البيانات ووثوقية المعلومات وإمكانية الإعتماد عليها.
٥. تشجيع الإلتزام بالسياسات والقرارات الإدارية.

ويعتبر COBIT الآلية التي تحدد خطة تكنولوجيا المعلومات الإستراتيجية، والحصول على البرامج اللازمة التي تمكن من تنفيذ إستراتيجية تكنولوجيا المعلومات لضمان الخدمة المتواصلة، كما تساعد المراجعين في الرقابة على البنية التحتية لتكنولوجيا المعلومات البنك، فهو إطار عمل لإدارة مخاطر تكنولوجيا المعلومات والمعيار الذي يغطي جميع الأنشطة ذات الصلة لحوكمة تكنولوجيا المعلومات تساعد المديرين على سد الفجوة بين متطلبات الرقابة وتكنولوجيا المعلومات والمخاطر".

<u>ويهدف اطار COBIT الى:</u>

١- عمل ربط لمتطلبات البنك وتكنولوجيا المعلومات من خلال تحديد أهداف البنك.
٢- تحديد المصادر الرئيسية لتكنولوجيا المعلومات والعمل على زيادتها.
٣- تحديد أهداف الرقابة الإدارة لأخذها في الاعتبار.
٤- تحديد الأدوار والمسؤليات لتحقيق الأهداف .

ويحدد إطار العمل COBIT هذا مجموعة من العمليات (٣٤ عملية) يعتبر من خلالها إطاراً للرقابة على تكنولوجيا المعلومات، ويصنف إلى أربع أبعاد أساسية على النحو التالي:

البعد الأول: التخطيط والتنظيم: يشمل هذا المفهوم إستخدام التكنولوجيا بصورة مثالية في البنوك، بحيث تساعدهم في تحقيق أهداف هم العامة والخاصة، ويتناول الإستراتيجية والتخطيط المتعلق بمساهمة تكنولوجيا المعلومات في البنوك، والتأكد من أن الأهداف التي تم تحقيقها تتفق مع ماهو مخطط له، ويتضمن هذا البعد عشر عمليات.

البعد الثاني: الامتلاك والتطبيق: يعني تحديد متطلبات التكنولوجيا والحصول عليها ثم تطبيقها من خلال العمليات التي تتم داخل البنك والتحقق من أن تلك العمليات تعمل على تحقيق أهداف البنك، حيث يتم تحديد عمليات تكنولوجيا المعلومات وامتلاكها وتطبيقها ودمجها داخل البنك ويتضمن هذا البعد سبع عمليات.

البعد الثالث: التوصيل والدعم: أي يتم توصيل تكنولوجيا المعلومات داخل أنظمة البنك وتنفذ تطبيقاتها، ويتم دعم العمليات لتستطيع تنفيذ أنظمة تكنولوجيا المعلومات، فيأخذ هذا البعد في الحسبان الخدمات المطلوب توصيلها، وتتمثل تلك الخدمات في: إدارة الأمن، والإستمرارية، وخدمات تدعيم المستخدمين، وإدارة البيانات، والإمكانيات التشغيلية، حيث يتضمن هذا البعد ثلاثة عشر عملية.

البعد الرابع: المراقبة والتقويم: يهدف هذا البعد إلى التأكد من ملاءمة أنظمة تكنولوجيا المعلومات الحالية مع ماخطط له من أجل تحقيق أهداف البنك، ويهدف أيضا إلى الوصول للتقييم المستقل لتحقيق الكفاءة والفعالية لأنظمة تكنولوجيا المعلومات، حيث أن جميع عمليات تكنولوجيا المعلومات تحتاج إلى مراقبة وتقييم بشكل منتظم من خلال المراجعين الداخليين والخارجيين ومراجعي نظم المعلومات وذلك للحصول على الجودة والإلتزام بمتطلبات الرقابة، ويتضمن هذا البعد أربع عمليات.

ويهدف مديرو المعلومات من إستخدام إطار COBIT5 إلى:

١- المحافظة على معلومات عالية الجودة لدعم القدرة على إتخاذ القرارات.

٢- تحقيق الأهداف الإستراتيجية من خلال الإستخدام الأمثل لتكنولوجيا المعلومات.

٣- الإبقاء على المخاطر المرتبطة بتكنولوجيا المعلومات عند مستوى مقبول.

٤- تحسين تكاليف خدمات تكنولوجيا المعلومات.

٥- تحقيق المنفعة من خلال تطبيق تكنولوجيا المعلومات بشكل يمكن الإعتماد عليها.

وحوكمة تكنولوجيا المعلومات تقوم بتطبيق الرقابة الداخلية من خلال آليات مختلفة منها لجان حوكمة تكنولوجيا المعلومات التي يتم تشكيلها مثل لجنة الإشراف على تكنولوجيا المعلومات، أو أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة COBIT الذي يقوم على منح المديرين والمراجعين ومستخدمي تكنولوجي المعلومات مجموعة من المؤشرات والمقاييس والعمليات التي تساعدهم في تعظيم المنفعة من إستخدام تكنولوجيا المعلومات، والعمل على منع الأخطار والتهديدات المحتملة أو إكتشافها وتصحيحها، وهنا يتضح البعد الإشرافي والرقابي لحوكمة تكنولوجيا المعلومات والذي يهتم بكل من:

- دعم وتفعيل الدور الرقابي لمجلس الإدارة على الإدارة التنفيذية المسئولة عن تطبيق تكنولوجيا المعلومات بالبنك.
- وضع الخطط الإستراتيجية لتكنولوجيا المعلومات بما يتفق مع الخطط والأهداف الإستراتيجية والتي يسعى البنك نحو تحقيقها.
- دعم وتفعيل الرقابة الداخلية على العمليات الخاصة بتكنولوجيا المعلومات وإجراءات إدارة المخاطر المرتبطة بها.

ويوجد العديد من أطر حوكمة تكنولوجيا المعلومات ومن أهمها:

(أ) إطار عمل COSO:

أصدرت لجنة Committee of Sponsoring Organizations (COSO) إطار عام الرقابة الداخلية، ويصف هذا الإطار مدخل موحد لتقييم الرقابة الداخلية الذي تصممه الإدارة لتوفير تأمين معقول لتحقيق الأهداف الأساسية للبنك والتي تتمثل في: كفاءة وفعالية العمليات التشغيلية، وإمكانية الإعتماد على التقارير المالية. وأخيراً الإلتزام بالقوانين والتشريعات المطبقة.

ويحتوي إطار العمل على خمسة مكونات رئيسية تؤكد أهداف البنك وهي بيئة الرقابة، تقييم الخطر، أنشطة الرقابة، المعلومات والإتصال، المتابعة. وهذه المكونات تمثل الأساس للرقابة الداخلية السليمة داخل البنك من خلال قيادة موجهة، وقيم مشتركة، وثقافة توكد المساءلة عن الرقابة.

ويري كل من جمعية مراجعة ورقابة نظم المعلومات ومعهد حوكمة تكنولوجيا المعلومات أن إطار (COSO) هو إطار العمل المقبول قبولاً عاما للرقابة الداخلية على مستوى البنك ككل، فإن إطار أهداف الرقابة على المعلومات والتكنولوجيا المرتبطة بها COBIT هو إطار العمل المقبول للرقابة الداخلية لتكنولوجيا المعلومات والذي يتسق مع إطار COSO.

ويعتبر نموذج COBIT الرقابة الداخلية على أنها العملية التي تتضمن السياسات، والإجراءات، والممارسات، والهياكل التنظيمية التي تساند أهداف وعمليات المنشأة كالبنوك.

(ب) قانون SOX:

"هو اختصار لـ Sarbanes-Oxley Act ولقد صدر هذا القانون بعد إزدياد الممارسات غير السليمة في الولايات المتحدة الأمريكية، بما في ذلك شركة انرون وشركة ورلدكوم، وصدر هذا القانون عام ٢٠٠٢ وعرض العلاقة ما بين قانون Sarbanes-Oxley وخدمات تكنولوجيا المعلومات المطبقة داخل البنك،ونظرا لأن معظم أعمال ومعاملات البنوك يتم تشغيلها إلكترونياً، فإن نظم تكنولوجيا المعلومات أصبحت جزءاً مكملاً لنظم الرقابة الداخلية، هذا أدى إلى زيادة مسئولية الإدارة العليا عن فعالية وكفاءة خدمات تكنولوجيا المعلومات المطبقة داخل البنك، والغرض من ذلك حماية المستثمرين عن طريق تحسين دقة وموثوقية نظام الإفصاح".

"وهناك من تناول إرشادات أهداف رقابة تكنولوجيا المعلومات للإلتزام بقانون ساربينس أوكسلي"IT Control Objective For Sarbanes- Oxley Act" والصادر عن معهد حوكمة تكنولوجيا المعلومات عام ٢٠٠٤ والتي أوضحت أهداف الرقابة تكنولوجيا المعلومات والتي يجب أخذها في الاعتبار عند تقرير الرقابة الداخلية للإلتزام بما هو مطلوب في قانون Sarbanes- Oxley Act وتتضمن حيازة لنظم ولبيئة والبنية التحتية لتكنولوجيا المعلومات وضمان أمن النظم".

ومن الضروري تبني ممارسات جيدة للحوكمة وخاصة حوكمة تكنولوجيا المعلومات (ITG) لمواجهة تعدد مخاطر تكنولوجيا المعلومات والتي تهدف إلى وجود تنسيق بين إستخدام تكنولوجيا المعلومات والأهداف الإستراتيجية للمنشأة من خلال تكوين أو إنشاء نظم رقابة فعالة لتكنولوجيا المعلومات، وعليه فإن العلاقة بين تكنولوجيا المعلومات والحوكمة علاقة سببية متبادلة، أو بمعني أخر أنهما يغذيان بعضهما البعض، أي أن وجود أحدهما يتطلب وجود الأخر. ومن ثم فإن تطبيق حوكمة تكنولوجيا المعلومات (ITG) أصبح ضرورة حتمية تناسب طبيعة نشاط البنوك.

وحوكمة تكنولوجيا المعلومات ليست مجرد مجموعة من الأنشطة غير المتناسقة، والتي يتم ممارستها بصورة عشوائية، بل تعتمد على مجموعة من المقومات والأسس، ومن ثم فإن حوكمة تكنولوجيا المعلومات يجب أن تساند وتعضد استراتيجيات تلك البنوك وأهدافها الموضوعة.

ولأن خطر تكنولوجيا المعلومات في الماضي يمكن أن يسبب مشاكل فنية بسيطة، إلا أنه اليوم أصبح يؤثر على الموقع التنافسي والأهداف الإستراتيجية للبنك، لذا يجب تحديد المخاطر التي تعوق تحقيق أهداف البنك، وهذه المخاطر قد تكون تهديدات في حالة حدوثها وبالتالي تؤثر على البنك بشكل سلبي، لذلك فإن حوكمة تكنولوجيا المعلومات تعمل على تدعيم نظام الرقابة الداخلية من خلال تحديد المخاطر والعمل على معالجتها وذلك من خلال تفعيل معايير حوكمة تكنولوجيا المعلومات COBIT، COSO، SOX.

ويتمثل دور آليات حوكمة تكنولوجيا المعلومات في الحد من المخاطر التي تواجه أمن المعلومات في البنوك في ظل نظام العمليات المصرفية الإلكترونية، وبالتالي الحد من المخاطر المصرفية الإلكترونية الذي يعد من أهم المخاطر التي تهدد وتؤثر على أمن المعلومات.

ويمكن تحقيق الإتساق بين أهداف البنوك ومتطلبات أمن المعلومات في ظل العمليات المصرفية الإلكترونية وذلك من خلال:

١. تخفيض وقت وجهد وتكاليف تحليل وتصنيف البيانات اللازمة لإستخراج المعلومات والحد من مخاطر إستخدام تكنولوجيا المعلومات في إستخراج هذه المعلومات.
٢. إدارة مخاطر تكنولوجيا المعلومات وزيادة أمن المعلومات مما يساعد في الحد من المخاطر المصرفية الإلكترونية.
٣. الحد من تسريب المعلومات الخاصة بالعملاء وبالتالي زيادة ثقة المتعاملين مع البنوك.
٤. تمكن البنوك من الإستغلال الأمثل في تكنولوجيا المعلومات في العمليات المصرفية الإلكترونية.
٥. توفير أدوات حماية البيانات والمعلومات مما يزيد من مصداقيتها وبالتالي تحد من التلاعب في المخاطر المصرفية الإلكترونية.
٦. الفصل بين الوظائف مما يؤدي إلى تحقيق الرقابة الداخلية وزيادة قدرتها على تقييم ومتابعة الأداء وإكتشاف المخاطر الإلكترونية.

رابعاً: الدراسة الميدانية:

تناولت الباحثة الدراسة الميدانية من حيث الهدف من الدراسة وفروضها وأسلوب جمع البيانات من عينة الدراسة بالتطبيق على قطاع البنوك، والتى شملت أربعة فئات هم:

- أعضاء مجلس الإدارة بالبنوك المصرية.
- مسئولى إدارة تكنولوجيا المعلومات، ومسئولى الرقابة الداخلية بالبنوك المصرية.
- مسئولى لجنة إدارة المخاطر بالبنوك المصرية.

وقامت الباحثة بتوزيع قوائم الإستقصاء (١٠٠ قائمة) من خلال المقابلة الشخصية والتسليم باليد أو إرسالها وإستلامهاعن طريق البريد الإلكترونى أو عن طريق إعداد نموذج لقائمة الإستقصاء من خلال نماذج جوجل.ولقد استعانت الباحثة عند تحليل نتائج الردود على أسئلة قوائم الاستقصاء ببرنامج (SPSS)، وذلك لاختبار فروض البحث. واعتمد تحليل نتائج الدراسة على ثلاث مراحل بدأت بالتحقق من صلاحية البيانات للتحليل الإحصائى، ثم عرض الإحصاء الوصفي لمتغيرات الدراسة وانتهاء بتقدير نماذجها واختبار الفروض من خلال تحليل الإرتباط والإنحدار.

خامساً: النتائج والتوصيات والتوجهات البحثية المستقبلية:

استهدفت الدراسة الميدانية ربط الجوانب النظرية بالجوانب العملية، واستكمالاً للفائدة المرجوه من البحث، وبعد إجراء التحليل الإحصائي للبيانات وإختبار صحة الفروض انتهت الدراسة الميدانية إلى الآتي:

١- **ثبوت صحة الفرض الأول:** يؤدى استخدام تكنولوجيا المعلومات إلى ظهور العديد من مخاطر العمليات المصرفية الإلكترونية.

٢- **ثبوت صحة الفرض الثاني:** يؤدى تطبيق حوكمة تكنولوجيا المعلومات إلى الحد من المخاطر المصرفية الإلكترونية.

٣- **ثبوت صحة الفرض الثالث:** يؤدى نظام الرقابة الداخلية إلى تدعيم حوكمة تكنولوجيا المعلومات.

وبناء على ما توصلت إليه الباحثة من نتائج، يُمكن أن تُبدى التوصيات التالية:

(١) تقوية شبكة المعلومات المصرفية الإلكترونية في البنوك، وذلك من خلال وضع قوانين وتشريعات تحكم التعامل المصرفي الإلكتروني، وخاصة فيما يتعلق بين البنوك والعملاء وتحديد مسئولياتهم وواجبات كل طرف.

(٢) العمل على تنمية وتطوير البنوك والعاملين بها واعدادها للتطور التكنولوجي والمصرفي وذلك بعقد دورات تدريبية مكثفة – داخلية وخارجية – بهدف توعيتهم بأهمية التوسع في العمليات المصرفيّة الإلكترونية .

(٣) ضرورة مواكبة التطورات التكنولوجية في مجال تكنولوجيا المعلومات ومعالجة جوانب الضعف في التكنولوجيا المصاحبة لتقديم الخدمة في البنوك وذلك من خلال نشر ثقافة العمل المصرفي، وزيادة التخصصات المحدودة لتطوير التكنولوجيا في البنك.

(٤) معالجة جوانب الضعف في المكونات المادية المصاحبة لتقديم الخدمة في البنوك وذلك من خلال توفير حاسبات حديثة وتطوير المكونات المادية المتوافرة في البنوك.

(٥) ضرورة تبني البنوك التي تستخدم تكنولوجيا المعلومات في البنوك لإطار COBIT للرقابة الداخلية بما يضمن قدر كاف من الثقة وتحسين أمن المعلومات داخل البنك.

التوجهات البحثية المستقبلية:

في ضوء النتائج التي توصلت إليها الباحثة، ترى أن هناك مجالات عديدة تمثل أساساً لأبحاث مستقبلية، ومنها على سبيل المثال:

(١) دور الإسناد الخارجي لتكنولوجيا المعلومات في الحد من المخاطر المصرفية الإلكترونية.

(٢) إطار مقترح لحوكمة تكنولوجيا المعلومات لتحسين الأداء المالي والسوقي للبنوك.

(٣) قياس أثر الخصائص التشغيلية للبنوك على شكل العلاقة بين حوكمة تكنولوجيا المعلومات والمخاطر الإلكترونية المصرفية.

(٤) مدخل تحليلي لدور مراقب الحسابات في إضفاء الثقة على نظم تكنولوجيا المعلومات بهدف تخفيض المخاطر المصرفية الإلكترونية

قائمة المراجع:

(١) الكتب:

- د/ أحمد محمد غنيم، "إدارة البنوك: تقليدية الماضي وإلكترونية المستقبل"، المكتبة العصرية للنشر والتوزيع، القاهرة، ٢٠٠٧، ص ٩١.
- د/ شعبان محمد فرج،"العمليات المصرفية وإدارة المخاطر"، كلية العلوم الإقتصادية والتجارية، جامعة البويرة، الجزائر، ٢٠١٤، ص ٧٩.
- د/ محمد السيد سرايا، د/عبد الوهاب نصر علي،د/ شحاته السيد شحاته، "أساسيات الرقابة والمراجعة الداخلية الحديثة"، الدار الجامعية، جامعة الأسكندرية ،٢٠١٢، ص٣٠.
- د/ محمود محمد عبدالرحيم، "نظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات"، بدون ناشر، بدون سنة نشر.
- د/ منير محمد الجنبيهي، د/ ممدوح محمد الجنبيهي، "جرائم الإنترنت و الحاسب الآلي ووسائل مكافحتهما"، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص ١٣.

(٢) الدوريات العلمية:

- د/ أحمد عبدالسلام أبو موسى، "الربط بين حوكمة تكنولوجيا المعلومات وتفعيل حوكمة الشركات: نموذج مقترح من سياق المحاسبة الإدارية"، المجلة العلمية للتجارة والتمويل، كلية التجارة، جامعة طنطا، المجلد الأول، العدد الثاني، ٢٠٠٥، ص ٨٠ .
- د/ أمال محمد محمد عوض، دور آليات الحوكمة في تعزيز حوكمة تكنولوجيا المعلومات وضبط مخاطر الأنشطة الالكترونية للمنشآت، "مجلة الدراسات المالية والتجارية"، كلية التجارة، جامعة بني سويف، العدد الأول، ٢٠٠٨، ص ٢٠٠.
- أ/ أمان عبدالعال محمد، الدور الحوكمي لتكنولوجيا المعلومات المحاسبية في تخفيض مخاطر الرهن العقاري، "المجلة العلمية للدراسات التجارية والبيئية"، كلية التجارة، جامعة قناة السويس، المجلد السادس، العدد الأول، ٢٠١٥، ص ٣٨٢.

- د/ أماني هاشم السيد حسن هاشم، "تفعيل دور لجان المراجعة في الحد من المخاطر المصرفية الإلكترونية"، **مجلة التجارة والتمويل**، كلية التجارة، جامعة طنطا،المجلد السادس عشر، العدد الثاني، يوليو ٢٠١٢، ص ص ٣٠١- ٣٦٧.
- د/ إيهاب محمد كامل عاشور،" تفعيل دور الرقابة الداخلية للحد من المخاطر المصرفية الإلكترونية في ظل إشتراطات لجنة بازل ٣ دراسة ميدانية"، **مجلة البحوث المالية والتجارية**، كلية التجارة، جامعة بورسعيد، المجلد الرابع عشر، العدد الثاني، الجزء الأول، ٢٠١٣، ص ص ١-٣٠.
- د/ جمال أحمد حسن موسى، "متطلبات الرقابة الداخلية لأمن المعلومات ومخاطر الخدمات المصرفية الإلكترونية: دراسة ميدانية في البنوك التجارية المصرية "، **مجلة الدراسات المالية والتجارية**، كلية التجارة، جامعة بني سويف، العدد الاول، ٢٠١١، ص ٢٧٣.
- د/ حمزة فائق وهيب الزبيدي،" تطور الصيرفة الإلكترونية وأثر الرقابة الداخلية على العمليات المصرفية الإلكترونية"، **مجلة كلية التراث**، المعهد العالى للدراسات المحاسبية، جامعة بغداد، العدد العشرون، ٢٠١٦، ص ٣٦٩.
- د/ زياد عبد الحليم الذيبة، حاكمية تكنولوجيا المعلومات، "**مجلة الدراسات المالية والمصرفية**"، مجلد التاسع عشر، العددين الثالث والرابع، السنة التاسعة عشر، كانون الأول، ديسمبر ٢٠١١، ص٥١.
- د/ سامي محمد أحمد غنيمي، "دور حوكمة تكنولوجيا المعلومات في تحسين جودة الأداء المالي وزيادة القدرة التنافسية بالبنوك المصرية: دراسة ميدانية، **مجلة البحوث المحاسبية**، كلية التجارة، جامعة طنطا، العدد الأول، أكتوبر، ٢٠١٦، ص ص ١-٥٠.
- د/ سوسن عبدالفتاح محمد أبو الجود،" الرقابة الداخلية لإدارة المخاطر بالبنوك الإلكترونية وفقا للإطار المتكامل الصادر عن لجنة **COSO**"، **مجلة الدراسات والبحوث التجارية**، كلية التجارة، جامعة بنها، السنة ٢٧، العدد الأول، الجزء الثاني، يناير ٢٠٠٧، ص ٩٣.

- د/ شريف مصباح أبو كرش، المصارف والبطاقات الإلكترونية: الفرص والتحديات، "مجلة الدراسات المالية والمصرفية"، الأكاديمية العربية للعلوم المصرفية، الأردن، السنة الثانية والعشرون، المجلد الثاني والعشرون، العدد الثالث، ٢٠١٤.
- د/ محمود العتيبي، تقييم مستوى حاكمية تكنولوجيا المعلومات في جامعة الطائف باستخدام مقياس كوبيت، كلية العلوم الإدارية، مجلة جامعة الطائف، الأردن، العدد الأول، المجلد الواحد وأربعون، ٢٠١٤، ص٩٧.
- د/ نادر شعبان السواح، "دراسة وتقييم أطر إدارة المخاطر المصرفية لأنشطة المراجعة الداخلية لتعظيم دور إدارة المخاطر في بيئة تكنولوجيا المعلومات"، مؤتمر بعنوان: دور المحاسبة والمراجعة في إدارة المخاطر المعاصرة، مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، عدد خاص (الجزء الأول)، ٢٠١٤، ص ص ٣٥٧- ٣٨٤.
- د/ نجلاء إبراهيم يحي عبدالرحمن، "دور حوكمة تكنولوجيا المعلومات في ضبط مخاطر المنشأة في القطاع المصرفي السعودي"، مجلة الفكر المحاسبي، كلية التجارة، جامعة عين شمس، عدد خاص- الجزء الأول، السنة السابعة عشر، أكتوبر ٢٠١٣، ص ص ٢٢١-٢٣٣.

(٣) رسائل الماجستير والدكتوراة:

- أ/ أيمن عمر فتح الله أبوشديدة، حوكمة تكنولوجيا المعلومات وأثرها على فجوة التوقعات في نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية، "رسالة ماجستير في المحاسبة غير منشورة"، كلية التجارة، جامعة طنطا، ٢٠١٦، ص ٤٩-٦١
- أ/ جازية حسيني، إدارة مخاطر العمليات المصرفية الإلكترونية، "رسالة دكتوراة في الإقتصاد"، كلية العلوم الإقتصادية والتجارية وعلوم التسيير، جامعة حسيبه بن بوعلي بالشلف، الجزائر، ٢٠١٨.ص ٦٨.
- أ/ حنان زكريا محمد سليمان، أثر حوكمة تكنولوجيا المعلومات على جودة التقارير المالية: دراسة ميدانية، "رسالة ماجستير في المحاسبة غير منشورة"، كلية التجارة، جامعة بنها، ٢٠١٩، ص ٨.

- أ/ رانيا عبدالحليم رضا عبدالعال، "تقييم خطة البنك المركزي المصري في تحسين أداء الجهاز المصرفي خلال الفترة ٢٠٠٠ - ٢٠٠٨: دراسة مقارنة"، **رسالة دكتوراة في الإقتصاد غير منشورة** ، كلية التجارة ، جامعة عين شمس، ٢٠١١، ص ٢١.
- أ/ شادي سلامة الحولي، إدارة مخاطر العمليات المصرفية الإلكترونية وفق مقررات لجنة بازل: دراسة تطبيقية، **"رسالة ماجستير في المحاسبة"**، كلية التجارة، جامعة غزة، ٢٠١٥.
- أ/ سمير أحمد ابداح، العوامل المؤثرة على الرقابة الداخلية في ظل حاكمية تكنولوجيا المعلومات في البنوك التجارية: دراسة ميدانية، **"رسالة ماجستير في المحاسبة"**، كلية الإقتصاد والعلوم الإدارية، جامعة اليرموك، الأردن، ٢٠١٢.
- أ/ محمد عبدالله فرج السعداوي، "تفعيل أثر تطبيق حوكمة نظم المعلومات في الحد من مخاطر المعلومات: دراسة ميدانية"، **"رسالة ماجستير في المحاسبة غير منشورة"**، كلية التجارة، جامعة عين شمس، ٢٠١٧، ص ١١٧.
- أ/ منى مغربى محمد إبراهيم،" إطار محاسبي مقترح لتطوير الإفصاح الإلكتروني في ضوء حوكمة تكنولوجيا المعلومات "، **رسالة دكتوراة في المحاسبة غير منشورة**، كلية التجارة: جامعة بنها، ٢٠١٢، ص ص ١-٤٠٢.
- أ/ نهى محمد إبراهيم النحال، تفعيل الدور الرقابي فى الحد من المخالفات المصرفية في بنوك القطاع العام :دراسة حالة البنك الأهلي المصري، **"رسالة ماجستير في الإدارة"**، كلية الإقتصاد والعلوم السياسية، جامعة القاهرة، ٢٠١٥.

(٤) **المؤتمرات:**

- أ/ سامح رفعت أبو حجر، أ/ أمنية محمد عبدالعزيز عابدين، "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**، بعنوان المحاسبة في مواجهة التغيرات الاقتصادية والسياسية المعاصرة ، كلية التجارة، جامعة القاهرة، ٢٠١٤، ص ٢٠.

(٥) المراجع باللغة الأجنبية:

- Derek Oliver & John Lainhart, " **Delivering Business Benefits with COBIT: An Introduction to COBIT 5**, Vol. 4, Sep., 2011, P.P.1–4. Available at: http://www.isaca.org/ Retrieved at: 25/ 11/ 2018.
- Hollis, A, Collins, W, and Kinney, W, R."The Discovery and Reporting of Internal Control Deficiencies Prior to SOX–Mandated Audits". **Journal of Accounting and Economics, Retrieved January**, 2010 From: http://Papers.ssrn.com.
- IT Governance Institute " **IT Control Objectives for Sarbanes-Oxley**", IT Governance Institute, USA, 2004, P.27
- Kenneth E. King, "Examine the Relationship Between Information Technology Governance, Control Objectives for Information and Related Technologies, ISO 27001/27002, and Risk Management", **Phd Thesis**, Capella University, February 2017, PP.1-79.
- Mario Spremic, "Measuring IT Governance Performance: A Research on COBIT -Based Regulation Framework Usage", **Journal Of Mathematics and Computers In Simulation**, Vol.6, Issue1, 2012, PP.17-25
- Michele Rubino & Others, "The Impact of An IT Governance Framework on the Internal Control Environment", **Records Management Journal**, Vol.27, No.1, 2018, P.P.19- 35.
- Rosslin john Robles, and Other, ' SOX and Its Effects On IT Security Governance,' **International Journal of Smart Home**,Vol.3,No.1 ,January,2009,PP.81-88.
- Scott D.Vandervelde, " An Empirical Examination of COBIT as an Internal Control Framework for Information Technology",**International Journal of Accounting Information Systems**, 2007, PP. 240-263.
- Tijana Radojevic and Dalibor Radovanovic," Managing Risks of Electronic Banking", **International Scientific Conference**, Gabrovo, Belgrade, Serbia, Novermber 2010, P. 108.
- Weidenmier, L. Marcia, and Ramamoorti, Sridhar, "Reseach Opportunities in Information Technology and International Auditing", **Journal of Information Systems** , Vol. 20, No. 1, 2006, PP. 205-219.