برنامج تدقيق مقترح للنظام المصرفي الالكتروني الشامل القائم على مخاطر الأعمال (بحث تطبيقي)

A proposed audit program for a comprehensive electronic banking system based on business risks (applied research)

Ali Mohaamed Nayyef Al-Ahmedi[1] | **Dr. Ali Mohammed Thijeel AL-Mamouri[2]**

Received 16/5/2023
Accepted 30/5/2023
Published 30/6/2023

Abstract:

The research seeks to identify the comprehensive electronic banking system and the role of the auditor in light of the customer's application of electronic systems that depend on the Internet in providing its services, as a proposed audit program has been prepared in accordance with international auditing controls and standards based on the study of the customer's environment and the analysis of external and internal risks in the light of financial and non-financial indicators, the research reached a set of conclusions, most notably, increasing the dependence of banks on the comprehensive banking system for its ability to provide new and diverse banking services, The researcher suggested several recommendations, the most important of which is the need for management to increase investment in information technology and monitor the financial allocations required to implement the comprehensive system according to a specific plan and schedule and monitor deviations in the application, their causes and ways to address them, with the need for the auditor to adopt an audit program in line with the size of the client's internal and external risks and analyze them to determine the risks that threaten the continuity of the client's activity and the size of the material misrepresentations. The remaining ones that extend to the financial statements.

Keywords: Comprehensive Electronic Banking System , Business Risk Audit, Audit Procedures

المستخلص:

يسعى البحث في التعرف على النظام المصرفي الالكتروني الشامل ودور مراقب الحسابات في ظل تطبيق العميل الانظمة الالكترونية التي تعتمد على الانترنت في تقديم خدماتها، اذ تم أعداد برنامج تدقيق مقترح على وفق الضوابط والمعايير التدقيق الدولية يعتمد على دراسة بيئة العميل وتحليل المخاطر الخارجية والداخلية على ضوء المؤشرات المالية والغير مالية، توصل البحث الى مجموعه من الاستنتاجات أبرزها، زيادة أعتماد المصارف على النظام المصرفي الشامل لقدرتهِ على تقديم الخدمات المصرفية الجديدة والمتنوعه ، مماتطلب من مراقبي الحسابات تطوير أساليب وأجراءات التدقيق بمايتواكب مع حجم التطور في بيئة العميل وعلية أقترح الباحث

1.Postgraduate Student, Rafidain Bank, Ali.Naief1701@pgiafs.uobaghdad.edu.iq. Iraq

2.Assistant Professor, Post Graduate Institute for Accounting and Financial Studies, University Baghdad, ali.mamouri@yahoo.com. Iraq

عدة توصيات أهمها،ضرورة توجة الادارة الى زيادة الاستثمار بتكنلوجيا المعلومات ورصد التخصيصات المالية المطلوبة لتطبيق النظام الشامل وفق خطة وجدول زمني محدد ورصد الانحرافات في التطبيق واسبابها وطرق معالجتها مع ضرورة أعتماد مراقب الحسابات على برنامج تدقيق يتماشى مع حجم مخاطر الداخلية والخارجية للعميل وتحليلها لتحديد المخاطر التي تهدد استمرارية نشاط العميل وحجم التحريفات الجوهرية المتبقية التي تمتد للبيانات المالية.

الكلمات المفتاحية: النظام المصرفي الالكتروني الشامل ،التدقيق وفق مخاطر الاعمال ، اجراءات التدقيق.

المقدمة :

تعتبر المصـارف أحد الركائز المهمة التي يقوم عليها الاقتصـاد في مختلف الدول نتيجة للدور الكبير الذي تقوم به وقد شـهدت في الاونة الاخيرة تطورات تكنولوجية أحدثت تأثيرا كبيرا في القطاع الانشـطة الاقتصـادية ومن بينها القطاع المصـرفي حيث شـرعت المصارف في الاستفادة من تلك التطورات من خلال استخدام تلك التكنولوجيا لتقديم افضل الخدمات في ظل المنافسة الشديدة التي يشـهدها القطاع المصـرفي، وان عملية التطور والعولمة والانفتاح في الاقتصـاد العراقي اعطت سببا للقطاع المصـرفي بأعادة النظر في الانظمة القديمة واسـتخدام انظمة جديدة لمواكبة تلك التطورات، وان التطورات الحاصـلة في بيئة الاعمال المصـرفية أثرت في عمل مراقب الحسـابات وفرضـت عليه تحديات جديدة، إذ اصـبح لمراقب الحسـابات مهام جديدة ومسـؤوليات اكبر في ظل اعتماد المصارف على النظام المصرفي الالكتروني الشامل فالمدقق الخارجي اصبح اليوم مسؤولا عن اعطاء الثقة للاطراف المتعاملة مع المصارف في البيانات المالية وكذلك أعطاء الثقه بسلامة انظمتها الالكترونية ومدى قدرة المصرف على الاستمرار في ظل مخاطر الاعمال المحيطة بالمصرف.

المبحث الأول: منهجية البحث :تتمثل منهجية البحث بالتي:

1-مشـــكلة البحث :ان عدم وجود برنامج تدقيق يعتمد على دراســـة وتحليل المخاطر الخارجية والداخلية للعميل في ظل تطبيق النظام المصرفي الالكتروني الشامل يؤدي الى فشل العميل في تحقيق اهدافة ومخاطر تحريفات جوهرية تمتد الى البيانات المالية.

2-اهداف البحث :يتمثل الهدف الى الاتي:-

1-التعرف على النظام المصرفي الالكتروني الشامل مع تسليط الضوء على طبيعة عمل مراقب الحسابات في ظل تطبيق العميل النظام المصرفي الالكتروني الشامل .

2-تقديم برنامج تدقيق مقترح على ضوء الضوابط والمعايير التدقيق الدولية.

3-أهمية البحث :يسـتمد البحث اهميته من تقديم برنامج تدقيق مقترح للنظام المصـرفي الالكتروني الشـامل وفق ضـوابط ومعايير التدقيق الدولية حيث يتضمن إجراءات تدقيق فعالة يتم تطبيقها للحد من مخاطر فشل العميل في تحقيق اهدافة.

4-فرضيات البحث :يفترض البحث ان تدقيق النظام المصرفي الالكتروني الشامل وفق ماجاء في المعايير الدولية والضوابط الرقابية تمكن المدقق من السيطرة على مخاطر التحريفات الجوهرية المتبقية، وبما يساهم المدقق في تخفيض مسؤوليتهِ أتجاه الشركة محل التدقيق وألاطراف الاخرى ذات العلاقة.

5-مجتمع وعينة البحث: يتمثل مجتمع البحث بالمصـــارف العراقية الحكومية العاملة في العراق التي تتطبق النظام المصـــرفي الالكتروني الشامل وسيتم اخذ مصرف الرفدين عينة للبحث لدراسة متغيرات البحث واستعراض عناصر مشكلته واثبات فرضيته.

6-الحدود المكانية والزمانية :الحدود المكانية: تم تحديد مصرف الرافدين، عينة لتطبيق البحث لامتلاكها البيئة المناسبة.

2- الحدود الزمانية: تتمثل الحدود الزمانية للبحث في السنوات (2020-2021-2022).

7-اسلوب البـــــــحث :سيتم اعتماد المنهج الاستقرائي في تناول مشكلة البحث وعناصرها المختلفة واثبات فرضية البحث وتحقيقاً لاهداف البحث في الجانب النظري، وسيتم اعتماد المنهج الوصفي التحليلي في الجانب التطبيقي للبحث.

المبحث الثاني: الجانب النظري للنظام المصرفي الشامل ، التدقيق وفق مخاطر الاعمال

2-1 تعريف النظام المصرفي الالكتروني الشامل:

تعددت التعاريف الخاصة بالانظمة المصرفية الالكترونية الشاملة من قبل المنظمات المهنية والباحثين ونذكر منها الاتي:

جدول رقم (1) تعريف النظام الشامل

المصدر	التعريف
(Shernish:2011:16)	عبارة عن شبكة من الفروع والتي تمكن العملاء من تشغيل حساباتهم والاستفادة من الخدمات المصرفية من اي فرع من فروع البنك بغض النظر عن المكان الذي يحتفظ فيه الحساب وفي اي وقت.
(Musau,2015:9)	هو البرامج التي تستخدم في القطاع المصرفي لمساعدة المصرف على تنفيذ الخدمات المصرفية لعملائة.
(Shanmugam. et.al,2017:309)	مجموعة من التطبيقات التي تدير العمليات المصرفية الشاملة للبنك وتسهل خطوط الاعمال لتقديم خدمات مصرفية فعالة وسريعة.
(chadima:2017:10)	هو وحدة العمليات المركزية للبنك والتي يستخدمها لتوسيع قنواتها لتوفير مجموعه واسعه من الخدمات لجمهوراها ، مع السماح للبنك بالعمل بسهولة وبساطة اكبر من العمليات الفردية.
(Atlabachew,2018:7)	هو المنصة التي يتم فيها دمج تكنلوجيا المعلومات والاتصالات لتناسب الاحتياجات الاساسية للخدمات المصرفية كالتعامل مع الودائع او القروض.

نستنتج من ماذكر اعلاه ان النظام المصرفي الالكتروني الشامل هو نظام يعمل على تكامل و ترابط فروع المصرف بقاعدة بيانات مركزية واحدة لتقديم خدمات مصرفية جديدة ومتنوعة من سحب او ايداع او ادارة للقروض والمدفوعات في الوقت الفعلي اي بغض النظر عن الزمان او المكان.

2-2 التدقيق وفق مخاطر الاعمال

2-2-1 تعريف التدقيق: هو عملية منهجية منظمة يتم فيها تحليل السجلات عن طريق مجموعه من المعايير الدولية المقبولة قبول عام بهدف التأكد من مدى صدق وعدالة البيانات الواردة في السجلات المحاسبية الاساسية وغيرها من مصادر البيانات والتي تتم بواسطة مدقق مستقل.(الحساني وحمدان، 2016، 4)، اما تعريف التدقيق في ظل الانظمة الالكترونية عملية جمع وتقييم المعلومات لتحديد فيما أذا كان أستخدام الحاسوب الالكتروني يساهم في حماية موجودات الوحدات الاقتصادية ويؤكد سلامة بياناتها ويعمل على تحقيق أهدافها بكفاءه وفاعلية. (الحجامي،2015، 186)

مما سبق يتضح أنَّ التدقيق الالكتروني هو منهج يعتمد على استخدام تكنلوجيا المعلومات في جميع مراحل التدقيق لجمع وتقييم أدالة الاثبات لتحديد ما اذا كانت الأنظمة الالكترونية تساهم في حماية موجودات المنشاة، ويؤكد سلامة بيانتها، وتحسن إدارة مخاطرها، ويحقق أهدافها بكفاءة وفعلية.

2-2-2 اهمية عملية التدقيق:ترجع اهمية التدقيق الى أهمية الجهات المستفيدة من نتائج اعمالة، لذلك كلما كبر حجم المنشاة وأتسع نطاق أعملها كلما زاد عدد المستخدمين وأزداد اهميتها،(الشريفي والمعموري،2021، 118)

وتبرز أهمية تدقيق على مستوى الانظمة الالكترونية من خلال الاتي:

1-أتساع مجالات التعامل مع الانظمة الالكترونية من قبل منظمات الاعمال المختلفة مما يصاحبة توليد بيانات محاسبية تختاج الى تدقيق وتوصيل نتائج التدقيق الى الجهات التي يمكن ان تستفاد منها في اتخاذ القرار.

2-الحاجة الى أضفاء المزيد من الثقة الى البيانات التي تنشأ من العمليات الالكترونيةـ خاصة ان تلك العمليات تتم من خلال بيئة تقنية متطورة تحتاج الى وجود جهة مستقلة قادرة على أعطاء راي فني محايد عن مدى موثوقيتها وتوكيدها وامنيتها.

3-التطورات المستمرة في الانظمة الالكترونية المستخدمة من قبل العميل تتطلب بضرورة تطوير مراقب الحسابات اجراءات التدقيق بالشكل الذي يضمن فاعلية تدقيق تلك الانظمة ومدى امكانية الاعتماد عليها من قبل العميل لتشغيل العمليات الخاصة به.(السقا ورشيد،2012، 41)

2-2-3 اهداف عملية التدقيق:تعددت الاهداف الخاصة بالتدقيق منها الاهداف التقليدية مثل التاكد من دقة البيانات المثبته في سجلات المشروع، وإكتشاف ماقد يوجد من غش أو أخطاء واعطاء رأي فني محايد والتأكد من خلو القوائم المالية من الاخطاء الجوهرية مع منع او تقليل الاخطاء وفرص حدوثها. (أبراهيم ويعقوب، 2022، 341-342)

اما فيما يتعلق بالاهداف الغير تقليدية فتتمثل بمراقبة الخطط الموضوعة ومتابعة تنفيذها وتقييم نتائج أعمال المشروع بالنسبة الاهداف المحددة مسبقا وتحقيق أقصى قدر ممكن من الكفاية الانتاجية في جميع نواحي المشروع.(التميمي وأخرون، 2018، 170)

2-2-4 تعريف مخاطر الاعمال:تعددت التعاريف الخاصة بمخاطر الاعمال من قبل الباحثين والكتب والمنظمات ونذكر منها الاتي:

جدول رقم (2) تعريف مخاطر الاعمال

المصدر	التعريف
معيار التدقيق الدولي رقم 315 فقرة (30)	وهي المخاطر التي تنشأ عن احداث او الحالات او الظروف او افعال مهمة والتي يمكن ان تؤثر سلبيا على قدرة الشركة في تحقيق اهدافها او تنفيذ استراتيجيتها او المخاطر النتايجة عن وضع استراتيجيات او اهداف غير مناسبة.
(معهد المحاسبين القانونين (AICPA	هو حدث يمكن ان يؤدي من خلاله الى تخفيض في قيمة حقوق المساهمين سواء كان عن طريق خساره في راس المال او اي شكل اخر من اشكال الخسارة.
(Arens,and Loebbeeke,2004:44)	هي تلك المخاطر التي سيعاني منها مكتب التدقيق و المدقق نتيجة العلاقة مع العميل، حتى وان كان تقرير المدقق صحيحا.
(Arens,Elder &Beasley,2008: 218)	هو كل شي يدفع المنشاة بعيدا عن تحقيق الارباح والى طريق الانهار والفشل.
(سمرة،2013: 16)	هي عدم قدرة المنشاة على تحقيق اهدافها التي تعكس استراتيجيتها نتيجة عوامل داخلية وخارجية والتي تعتبر من العواقب التي تواجة المنشأة والتي تؤثر سلبا في استمراريتها.
(الصيرفي،2021: 70)	هو احتمال تعرض الشركة الى خسائر غير متوقعه او تذبذب العائد المتوقع من الاستثمار معين والاثار الناجمه عن احداث مستقبلية محتملة الوقوع والتي تؤثر على قدرة الشركة في تحقيق اهدافها.

وعلى ضوء ذلك فإن مخاطر الأعمال هي عبارة عن عوامل تؤثر على قدرة المصارف في تحقيق اهدافها وهذه المخاطر اما يمكن التحكم بها نوعاً ما او لايمكن التحكم بها مثل العوامل الخارجية وكذلك هناك بعض المخاطر يمكن تجنبها او التقليل من اثرها من خلال التامين عليها، وان مراقب الحسابات يهتم بالمخاطر التي تؤثر على البيانات المالية ولذلك يجب عليه فهم بيئة الاعمال الخاصة بالعميل ومخاطرها وبعد ذلك يقوم باختيار استراتيجية تخطيط التدقيق المناسبة على ضوء تلك المخاطر.

2-2-5 منهج التدقيق القائم على مخاطر الاعمال :ان التدقيق القائم على مخاطر الاعمال هو منهج حديث والذي يهدف الى توسيع نطاق تركيز مراقب الحسابات من مخاطر التدقيق والتي تشير بوجود انحراف في البيانات المالية الى مخاطر الاعمال والمشار اليها بفشل المصارف في تحقيق اهدافها، وان هذه المخاطر قد لاتؤثر بصوره مباشرة بالقوائم المالية.

حيث يعمل النهج القائم على مخاطر الاعمال على تصفية المخاطر التي من الممكن ان تؤثر على القوائم المالية لتقليل اخطاء اعداد البيانات المالية.

وهناك نقطتان متعلقة بفحص بيئة المنشأة وفق اسلوب التدقيق المستند الى المخاطر:

1-تحديد وفهم العمليات التشغيلية واساليب الرقابة الاستراتيجية الادارية.

2- اختيار عمليات الرقابة على المخاطر ضمن العمليات التشغيلية المهمه، فعلية يجب تحديد حجم مخاطر الاعمال المتبقية والتي يمكن ان تؤثر على دقة وعدالة البيانات مالية.(القضاة، 2018، 7)

وان المعيار التدقيق رقم (200) الفقرة (2) وضح ان الهدف من تدقيق البيانات المالية هو تمكين مراقب الحسابات من أبداء الراي فيما اذ كانت البيانات المالية اعدت من كافة النواحي الجوهرية ووفقا لاطار التقارير المحددة.

اما الفقرة (3) اشارت انه بالرغم ان ابداء راي مراقب الحسابات يعزز مصداقية البيانات المالية الا ان مستخدم هذه البيانات لايستطيع الافتراض ان راي مراقب الحسابات هو تأكيد لاستمرارية الشركة، وان هذا الراي لايبين ان الادارة قامت بادارة امور الوحدة الاقتصادية بكفاءة وفاعلية.

ولهذا يجب على مراقب الحسابات الاخذ بنظر الاعتبار تقييم ما اذا كانت التقارير المالية للوحدات الاقتصادية يتم اعدادها وفق معايير المحاسبية ومعايير التدقيق وان عملية تدقيق الحسابات تاخذ بنظر الاعتبارات المخاطر المرتبطة باخطاء البيانات المالية ومخاطر الاعمال المرتبطة بعمليات الوحدات الاقتصادية وباهدافها الاستراتيجية.(Nobes.et,al.2000: 43)

ويمكن النظر الى العلاقة بين مخاطر الاعمال ومخاطر التدقيق على انها علاقة قوية وتعمل بشكل متوازي، فالمدقق القادر على اكتشاف مخاطر الاعمال وتحديدها، سوف ينخفض تلقائيا من خطر التدقيق، ومع ذلك نجد ان الخبرة والموارد والمتغيرات المتعلقة بالزمن تؤثر على عملية التدقيق ومخاطرها، وذلك لان من الصعب على مراقب الحسابات تحديد جميع مخاطر الاعمال الموجودة.(Kutum,2010: 53)

اي ان مراقب الحسابات لايستطيع تحديد جميع مخاطر الاعمال الموجودة في الوحدة الاقتصادية، وبالتالي لاتوجد طريقة للقضاء نهائيا على مخاطر التدقيق، وكذلك يمكن تركيز مراقب الحسابات على المخاطر الهامة والمشاكل الرئيسية التي تؤثر بشكل مباشر على التدقيق ويتم تجاهل المشاكل وقضايا الثانوية، لذا قد تبقى بعض مخاطر التدقيق موجودة، ولذلك تم استخدام منهج مخاطر الاعمال والذي يبدا من عمليات الوحدة الاقتصادية واهدافها وينتهي بالقوائم المالية، ويركز هذا المنهج على توجيه الجهود نحو المخاطر المهمة وغير مسيطر عليها.(Pong.et.al,1997:101)

اما المخاطر المهمة المتبقية والغير مكتشفة فيتم تحديدها من خلال الرؤية الشاملة للوحدات الاقتصادية تحت التدقيق، والتي تشمل بناء نموذج ذهني لعمليات الوحدة والذي يغطي مختلف عناصرها.(Rich.et,al,1997: 101)

كما تم قياس مخاطر الاعمال من قبل كبرى شركات التدقيق من خلال الاتي:

1-التركيز على مخاطر الاعمال بدلاً من مخاطر البيانات المالية.

2-تغيير طبيعة الأختبارات التي يقوم بها مراقب الحسابات من اختبارات كبيرة الحجم بالنسبة للتفاصيل الى اختبارات عالية المستوى للاشراف والرقابة مدعوما باعمال تحليلية عالية الدقة.(العيساوي،2018: 23)

وان الاساس المنطقي لمنهج التدقيق وفق مخاطر الاعمال يشير الى مدى تمكن مراقب الحسابات من تحديد مصادر خطر الاعمال والتأكد من ان العميل لدية انشطة فعالة لمراقبة تلك المخاطر، وعلى الرغم ان لكل وحدة اقتصادية تأخذ مدخل مختلف في تطبيق

اســـتراتيجية التدقيق وفق مخاطر الاعمال الا ان هناك بعض العناصـــر الاســـاســـية تتمثل بالنقاط الاتية:(Schelluch Peler al.2003:108)

أ–فهم انشطة الادارة لتحديد وتقدير وإدارة المخاطر.

ب– فهم مستقل لعمل الوحدة الاقتصادية و للمخاطر التي تواجها.

ت– استخدام المخاطر المحددة لوضع التوقعات بشأن ارصدة الحسابات والعمليات والنتائج المالية.

ث– تقدير درجة جودة نظام الرقابة الداخلية على ادارة المخاطر التي تواجه الوحدة الاقتصادية.

ج–تحديد المخاطر المتبقية وتحديث التوقعات التي تتعلق بالتأكيدات المالية.

ح–جمع المعلومات وادلة الاثبات بقصد ادارة المخاطر المتبقية للتحريفات عن طريق اختبار مباشر للتأكيدات المالية.

المبحث الثالث: الجانب التطبيقي: برنامج مقترح لتدقيق النظام المصرفي الالكتروني الشامل (CORE BANKING)

تم أعداد هذا البرنامج أســـتنادا لما جاء قي الجانب النظري والكتب والمعايير الدولية والقوانين والســـياســـات والاجراءات والتعليمات والضـــوابط الرقابية بموجب مقررات لجنة بازل2 وضـــوابط الحوكمة والادارة المؤســـســـية لتقنية المعلومات والاتصـــالات في القطاع المصـــرفي الصـــادر من البنك المركزي العراقي2019، وبرامج التدقيق ذات العلاقة بتدقيق النظام المصـــرفي الالكتروني الشـــامل، ويعمل هذا البرنامج على كشـــف مخاطر الاعمال المصـــرفية ســـواء كانت مخاطر تقليدية او الالكترونية في ظل تطبيق النظام المصـــرفي الالكتروني الشـــامل، والعمل على تقييمها بالشـــكل الذي يســـاعد المدقق على توجيه تركيزه على الانشـــطة ذات المخاطر العالية وتعديل اجراءات التدقيق بمايتواكب مع حجم مخاطر الاعمال الجوهرية المتبقية والعمل على مواجهتها والتقليل من أثارها، وفيما يلي برنامج تدقيق المقترح:

التسلسل			أجراءات التدقيق
الرئيسي	فرعي	فرعي	
1			التعرف على نشاط العميل
	1-1		التعرف على طبيعة الخدمات التي تقدم من قبل العميل والنظام المستخدم في معالجة عملياته.
	2-1		الاطلاع على السياسات والاجراءات الخاصة بعمل النظام المصرفي الالكتروني الشامل.
	3-1		الاطلاع على الاليات الاساسية الخاصة بمستويات التخويل (تفويض الصلاحية) اعداد تقارير دورية بما في ذلك الاجراءات السريعة التي تتخذها الادارة في مواجهة الحوادث التي تؤثر على الامن والسلامة والسمعة مثل أختراق الغير الغير مشروع للشبكة.
	4-1		الاطلاع على مدى رغبة الادارة في تحمل المخاطر المرتبطة بالعمليات الالكترونية.
	5-1		التعرف على مورد النظام المستخدم والجهة المسؤولة عن صيانة وتحديث النظام.
	6-1		الاطلاع على السياسيات المحاسبية المستخدمة في معالجة العمليات.
	7-1		الاطلاع على طبيعة المنافسة في القطاع الذي يعمل به العميل.
	8-1		التعرف على الخدمات التي تقدم من قبل الاطراف المنافسة الاخرى.
	9-1		التعرف على العملاء والاشخاص المستفيدين من الخدمات المصرفية.
	10-1		الاطلاع على طبيعة الموارد البشرية المستخدمة للنظام ومؤهلاتهم العلمية والمهنية.
2			فحص وتقييم الضوابط الرقابية للنظام المصرفي الالكتروني الشامل لمعرفة مدى الاعتماد عليها:
			ضوابط الرقابية العامة
	1-2		الضوابط التنظيمية:

	2-1-1	أ	التحقق من توفر سياسات واجراءات تتعلق بالرقابة على عمل النظام الالكتروني المستخدم من قبل العميل.
		ب	التحقق من مدى كفاءة وكفاية المهارات والمؤهلات المعينين بالتدقيق الداخلي والتدقيق الخارجي والمستشارين في مجال تقنيات المعلومات والاتصالات.
		ج	التحقق من مدى شمولية الوصف الوظيفي لملاك تقنيات المعلومات والاتصالات والتدقيق الداخلي لتقنيات المعلومات والاتصالات ولامن المعلومات ومدى الالتزام بهِ.
		د	التحقق من مدى كفاية ادارة أمن المعلومات من حيث الهيكل التنظيمي ومدى توظيف الموارد المختلفة بما في ذلك العنصر البشري.
		هـ	التحقق من الفصل الملائم بين الوظائف (مثل الفصل بين شخص مشغل النظام عن الشخص المسموح له بادخال البيانات الى النظام).
		و	التحقق من أستمرار عمليات الفصل مابين الموظف المسؤول عن ادخال البيانات وبين المسؤولين عن التحقق من مصداقيتها.
		ز	التحقق من الاختبار الدوري للنظام المصرفي الالكتروني الشامل للتاكد من عدم التجاور او الالتفاف على الفصل بين الوظائف.
		ح	التأكد من وجود معايير لقياس جودة وفاعلية النظام المصرفي الشامل لدى ادارة المصرف مثل مستوى رضا العملاء او الموظفين عن خدمات النظام، ومدى فاعلية النظام في تحقيق أهداف المصرف.
		ط	التحقق من مستوى رضا الزبائن على ادارة الخاصة بتقنيات المعلومات والاتصالات والخدمات والمنتجات والدعم الفني المقدم.
		ي	التأكد من مدى الامتثال لضوابط وتعليمات الصادرة من البنك المركزي بخصوص تبني وتطبيق الانظمة الالكترونية الشاملة.
		ك	التحقق من مدى امتثال مجلس الادارة والادارة التنفيذية للمصرف لضوابط حوكمة تقنيات المعلومات والاتصالات.
		ل	التحقق من وجود سياسات فعاله لتدريب وتاهيل الموارد البشرية مع كفاءة البرامج التدريبية لموظفي المصرف وزبائنهِ من ناحية نشر الوعي بالممارسات السليمة لامن المعلومات وحمايتها.
		م	التحقق من وجود ضوابط تعمل على توفير البدلاء لمستخدمي ومبرمجي الانظمة في حال التمتع باجازة.
		ن	التحقق من وجود دليل توثيق لطبيعة عمل النظام الشامل يتم اللجوء الية عند الحاجة.
		س	التحقق من وجود خطة طوارئ لمواجهة الكوارث وتوقف النظام.
		ع	التحقق من توفير مصدر بديل للطاقة لحماية البيانات من الفقدان.
		ف	التأكد من قيام الادارة بالاهتمام المطلوب للمخاطر وتحليلها قبل تنفيذ الانشطة الالكترونية المصرفية.
		ص	التحقق من وجود تحديد واضح لمسؤوليات الادارة والعاملين فيما يخص الاشراف على وضع سياسات الامان للمصرف.
		ق	التحقق من مدى سلامة اجراءات التوثيق والمتابعة للعمليات المصرفية الالكترونية المنجزة خلال النظام.
			ضوابط صيانة وتطوير النظام الشامل
		أ	التحقق من سلامة تطبيق وتوثيق النظام المصرفي الشامل والقيام باختبار الانظمة الجديدة او المعدلة.
			التحقق من طبيعة التغييرات على الانظمة التطبيقية للنظام الشامل.
	2-1-2	ب	التحقق من وجود عقد او بند من ضمن عقد تطبيق النظام المصرفي الشامل للصيانة او التحديث الدورية للنظام.
		ج	التحقق من دوران للموظفين المسؤولين عن تشغيل وصيانة النظام الشامل.

		د	التحقق من فحص كافة البرامج المستحدثه والمضافة من قبل اشخاص مفوضين بالفحص غير
		هـ	الاشخاص الذين قاموا بالتعديل.
			التحقق من وجود تعليمات وصلاحيات للموافقة على استحداث وتعديل الانظمة والبرامج.
		ح	التحقق من وجود فصل مابين الاشخاص المسؤولين على تطوير النظام والاشخاص المسؤولين عن
		ط	ادارة النظام.
			ضوابط تشغيل الحاسوب
			التحقق من ان الانظمة يتم استخدامها لأغراض المرخصة فقط.
		أ	التحقق من الوصول الى عمليات الحاسوب مقيد بالاشخاص المخولين فقط.
		ب	التحقق من ان الاخطاء عمليات المعالجة قد تم اكتشافها وتصحيحها.
	2-1-3	ج	ضوابط برامج النظام الشامل
			التحقق من الموافقة والمصادقة والاختبار والتطبيق والتوثيق للبرامج الانظمة الالكترونية الجديدة،
		أ	وطبيعة التعديلات على برامج الانظمة الحالية.
			التحقق من تقييد الوصول الى برمجيات الانظمة الشاملة للاشخاص المخولين فقط.
		ب	الضوابط الرقابية على الوصول
	2-1-4		التحقق من وجود أجراءات لتشفير البيانات واستخدام رقم اوكلمة السر للوصول الى بيانات النظام.
		أ	التحقق من وجود اجراءات لفحص اختراق البيانات في النظام الشامل.
			التحقق من تبويب البيانات حسب حساسيتها واهميتها.
		ب	التحقق وضع اجهزة الحاسوب التي تحتوي على النظام في اماكن امنه ومناسبه، وعدم السماح الدخول
		ج	اليها الى من قبل الاشخاص المخولين بموجب تفويض رسمي.
	2-1-5	د	التحقق من استخدام الخصائص الفزيائية كالبصمة للوصول الى اجهزة الحاسوب.
			التحقق من وجود سجل لتسجيل الزوار والتوقيع من قبل الاشخاص الداخلين والخارجين من الاماكن
		هـ	الخاصة بالاجهزة التي تحتوي على خوادم النظام.
		و	الضوابط الرقابية على حماية وأمن ملفات النظام
			التحقق من أنشاء نسخ أحتياطي للبيانات والبرامج وحفظها في مواقع مناسبة وامنة.
			التحقق من الفحص الدوري للنسخ الاحتياطي للبرامج والبيانات.
		أ	التحقق من وجود تأمين على النظام المصرفي الالكتروني الشامل من مخاطر التخريب اوالسرقة او
		ب	الحريق والكوارث وغيرها من المخاطر.
		ج	التحقق من توفر وسائل الحماية اللازمة على ملفات النظام من التعرض الى الفايروسات من خلال
			وجود برامج مضادة لها لمكافحة الفايروسات على الخوادم ومحطات العمل مع العمل على تحديث تلك
		د	البرامج بشكل منتظم وانشاء جدول الفحص التلقائي للفايروسات والعمل على معالجتها.
	2-1-6		التحقق من وضع خطة لمواجهة الكوارث كعقد اتفاق مع مورد النظام بتزويد المصرف مواقع بديلة في
			حال توقف النظام او في حالات الطؤارئ مع العمل على اختبار تلك المواقع وتجريبها والتاكد من
			سلامتها.
		هـ	التحقق من وجود مصدر للطاقة احتياطي لتجنب فقدان البيانات او الاخطاء عند انقطاع مصدر
			الطاقة.
			التحقق من توفر انظمة الحماية والاخماد الالي للحرائق في قاعدة بيانات المركزية للنظام.
		و	التحقق من اعتماد المعايير والمواصفات القياسية العالمية لحماية مركز البيانات.
			الضوابط التطبيقية على النظام الشامل
		ز	الضوابط الرقابية على مدخلات النظام الشامل
		ح	التحقق من جميع المعاملات تم المصادقة عليها بالشكل المناسب قبل معالجتها من قبل النظام.
			التحقق من فحص ضوابط ادخال البيانات على البرامج الحساسة مثل وجود (Maker,Checker)
			التحقق من سلامة ودقة تحويل البيانات بالصيغة القابلة للقراءة بواسطة الحاسوب.

		أ	التحقق من الحصول على الموافقة من الجهات المخولة قبل ادخال البيانات الى النظام.
			التحقق من وجود برنامج للتخلص من اخطاء المدخلات.
			التحقق من الاخطاء والارصدة الغير متصلة بقاعدة البيانات.
		ب	<u>الضوابط الرقابية على عملية المعالجة</u>
		ج	التحقق من مدى سلامة برامج النظام في معالجة البيانات ومدى مصداقية المدخلات والمخرجات.
	2-2	د	التأكد من عدم ضياع المعاملات او اضافتها او تكرارها او التغير عليها بالشكل الغير مناسب.
	2-2-	هـ	التاكد من اخطاء المعالجة تم اكتشافها وتصحيحها في الوقت المناسب.
	1		<u>الضوابط الرقابية على المخرجات</u>
		أ	التحقق من وجود ضوابط للحفظ الامن للوثائق الحساسة المستخرجة من برامج النظام.
			التحقق من ان المخرجات تم تقديمها الى الاشخاص الملائمين وفي الوقت المناسب.
		ب	التحقق من الوصول الى المخرجات مقيد بالاشخاص المخولين فقط.
		ج	
			<u>فهم أستراتيجية الادارة وأجراءاتها في الحد من المخاطر :</u>
		أ	التاكد من وجود تقييم لمخاطر النظام المصـــرفي الشـــامل ورفع تقارير دورية عن تلك المخاطر الى
		ب	المستويات الادارية المناسبة.
	2-2-	ج	الاطلاع على استراتيجية الادارة لمواجهة مخاطر استخدام النظام المصرفي الالكتروني الشامل.
	2		الاطلاع على الاسس والسياسات المتبعة من قبل الادارة في تحديد المخاطر.
3			التأكد من أعتماد مجلس ادارة المصـرف على السـياسـة والاسـتراتيجية المناسـبة لكل نوع من انواع
			المخاطر.
			التحقق من قيام الادارة باجراءات سليمة لمواجهة مخاطر المرتبطة بالامان والمصادقية واتاحة الخدمات
			المصرفية الالكترونية، والتأكد من ان المجهز النظام يتبع نفس الاجراءات.
	2-2-		التأكد من توفر دليل استرشادي بالاجراءات المعتمدة لادارة المخاطر المصرفية.
	3		الاطلاع على طبيعة المخاطر ودرجة تاثيرها من خلال التقارير الصادرة من قبل قسم ادارة المخاطر.
			التحقق من قيام الادارة بمراجعة السـياسـات والاجراءات والعمل على تحديثها لمواكبة المخاطر الجديدة
			التي تواجة النظام والعمل على تقديم توصيات لمجلس الادارة بها.
			التحقق من وجود الانظمة الكافية للرقابة على العميات المصرفية الالكترونية وقواعد البيانات.
			الاختبار والفحص الدوري لاجراءات الامن ولضـوابطة، مع العمل على متابعة التحديثات في مجال امن
			الخدمات المصـرفية وتحديث الضـوابط الرقابية بما يتلائم مع طبيعة التحديث في الخدمات المصـرفية
	1-3		الالكترونية.
	2-3		تحديد مخاطر الاعمال في ظل تطبيق النظام المصرفي الالكتروني الشامل :
	3-3		<u>مخاطر البيئة الخارجية:</u>
	4-3		التأكد من أن المصـرف يتفهم بالشـكل الكامل كافة المخاطر المرتبطة بدخول المصـرف بعقد اتفاق مع
			جهات خارجية لتجهيز النظام المصرفي والتطبيقات الخاصة بالعمليات الالكترونية.
	5-3		التأكد من مدى وجود سياسات الاستعانة بالغير وكفائتها (التعهد او الاسناد الى الاطراف الخارجية).
			التحقق من مدى كفاية التوثيق للتعاقدات الخارجية والداخلية ومتابعتها من حيث تفصـــيل الخدمات
4	6-3		المقدمة والمسؤوليات اتجائها.
	7-3		التحقق من التحديد الواضح والصريح لنطاق ومسؤوليات الاطراف الخارجية فيما يخص تطبيق النظام
		1-1-4	المصرفي الالكتروني الشامل بموجب العقد المبرم.
	8-3		التحقق من ادارة نظم تقنية المعلومات والاتصالات وبرامجها بشكل فعال ، بحيث يتم استبدال الانظمة
	9-3	2-1-4	القديمة والغير مدعومة والتي تزيد من تعرضـــها للمخاطر الامنية الى الانظمة الجديدة والمحدثه في
	10-3		الوقت المناسب.

		3-1-4	التحقق من قيام العميل باخذ العناية الفائقة لتاريخ انتهاء دعم المنتج (Eos)، وذلك لتوقف مزودي الخدمة على تقديم التصحيحات اللازمة للثغرات الحاصلة والمكتشفة بعد تاريخ انتهاء دعم المنتج.
		4-1-4	التحقق من خضوع النظام المصرفي الالكتروني الشامل المجهزة من قبل الاطراف الخارجية الى سياسات ادارة المخاطر والامان والتي تفي بالمعايير الخاصة بالمصرف.
		5-1-4	التحقق من أجراءات المراجعة الدورية المستقلة للانشطة التي تم تنفيذها من قبل المجهز الخارجي ومدى توافقها مع النطاق المطلوب والذي تم الاتفاق علية مسبقا.
	1-4	6-1-4	التاكد من منع المتعاقدين والمزودين لخدمات النظام من الحصول على امتيازات الوصول الى الانظمة من دون توفر عملية اشراف ورقابة عالية.
		7-1-4	التحقق من تثبيت اجهزة حماية الشبكات (الجدار الناري) لزيادة صعوبة الاختراق و انظمة كشف التسلل ومنعه، في المراحل الاولى من البنية التحتية لتقنية المعلومات لحمايط محيط الشبكة والنظام من الوصول الغير مصرح به.
		8-1-4	التحقق من وجود اختبار بشكل دوري للجدار الناري للنظام المصرفي الشامل ومدى قدرتة على صد الهجمات الخارجية.
		9-1-4	التأكد من اجراء اخبارات تقييم الضعف (VA) بشكل دوري للكشف عن نقاط الضعف في النظام والثغرات الامنية في بيئة تقنيات المعلومات والاتصالات والعمل على معالجتها.
		10-1-4	التحقق من توفر خطة طورئ في مجال الخدمات المصرفية الالكترونية المجهزة من قبل الاطراف الخارجية في حال توقفها او الهجوم عليها.
		11-1-4	التحقق من وجود خطة بديله في حال عدم امكانية تجديد رخصة تطبيق النظام الشامل سواء كان بسبب عقوبات دولية او عجز مالي.
		12-1-4	التحقق من وجود خط بديل للانترنت في حال توقفه سواء كانت بقرار حكومي او من المصدر.
			التحقق من وجود خط بديل في حال توقف النظام وانقطاع الخدمة من قبل المجهز كحصول كوارث طبيعية في بلد المجهز.
			<u>مخاطر العمليات التشغيلية</u>
		13-1-4	التحقق من وجود سياسات واجراءات فعاله في الكشف عن اوجهة الضعف او القصور في العمليات التشغلية للنظام المصرفي الشامل.
		14-1-4	التأكد من قيام المصرف باعداد تقارير دورية عن حجم المخاطر التشغلية عند تطبيق النظام.
			التحقق من وجود اجراءات لتخفيض من حجم المخاطر التشغيلية من خلال التأمين عليها.
		15-1-4	التحقق من تحليل الطاقة الاستيعابية للنظام المصرفي الالكتروني الشامل ومدى مواكبته لحجم
		16-1-4	العمليات المصرفية الالكترونية والتطور الحاصل في الخدمات.
			التحقق من وضع تقديرات للطاقة اللازمة لمعالجة المعاملات الالكترونية وانها تخضع لاخبارات الجهد بشكل دوري.
		1-2-4	التحقق من مدى كفاءة وكفاية خطط استمرارية العمل، بما في ذلك توافرية موارد تقنية المعلومات والاتصالات والعنصر البشري وتنظم الخطط ضمن اطار الامثال لضوابط البنك المركزي بهذا الشأن مع
		2-2-4	فحص مستوى التوافرية لاجهزة الكمبيوتر ولعناصر الشبكات ومدى ملائمتها مع خطط استمرارية
		3-2-4	العمل.
		4-2-4	التحقق من وجود اجراءات فعاله لاستمرارية النشاط وعدم توقفه من خلال وضع خطة طوارئ للتعافي من الكوارث وضمان تحديثها بشكل دوري وفق الظروف المتغيرة والمتطلبات التشغيلية للصرف.
		5-2-4	التأكد من وضع خطة تعافي من الكوارث تستند الى اسوء السيناريوهات تعطل الخدمات مع وضع الحلول والبدائل لمواجهة تلك الكوارث لضمان استمرارية تقديم الخدمات المصرفية وعدم توقفها.
		6-2-4	التحقق من اجراء عمليات التعافي من الكوارث في موقع جغرافي منفصل عن الموقع الاساسي حتى
	2-4		يتمكن من استعادة النظام واستئناف الاعمال المصرفية في حال حدوث اي عطل في الموقع الاساس.

		7-2-4	التحقق من وجود خطط لاسترداد النظام او المعاملات المصرفية الالكترونية في حال تعرضها الى حوادث غير متوقعه مثل الهجوم الداخلي او الخارجي.
		8-2-4	التحقق من وجود فرق متخصصة قادرة على الاستجابة الى حالات الطوارئ وان تكون حاصلة على التدريب الكافي لتحليل النظام واكتشاف الحوادث والعمل على الاستجابة لها.
		9-2-4	التحقق من وجود لجنة لادارة المشاكل والتي تهدف الى تحديد السبب الجذري للمشكلة للقضاء عليها ومنع تكرارها في المستقبل.
		10-2-4	التحقق من تطوير الاستراتيجية الخاصة بالنسخ الاحتياطي للبيانات المهمة مع اجراء الاختبارات الدورية اليها للتاكد من فاعليتها في استرداد البيانات باسرع وقت.
		11-2-4	التحقق من تشفير الاقراص والاشرطة الخاصة بالنسخ الاحتياطي بما في ذلك وحدات التخزين المتنقلة USB والتي تحتوي على بيانات سرية وحساسة قبل نقلها الى خارج موقع التخزين.
		12-2-4	التحقق من توفر اجراءات الحماية المادية للمحيط الخارجي لمركز البيانات من خلال استخدام نظم الرقابة المادية والبشرية كاستخدام حراس الامن والحواجز التي تقيد من الوصل لقاعدة بيانات النظام.
		13-2-4	التحقق من مدى توفر متطلبات الامن المادي والبيئي لغرف الخاصة بقواعد البيانات المركزية، بناءا على معايير التقييم مثل مدى ملائمة الموقع ودرجة الحرارة والرطوبة المناسبة، مكان الغرفة، وجود اجهزة اطفاء الحرائق، اجهزة الانذار، وكاميرات مراقبة وسجل لتسجيل الزوار مع حصر الدخول الى غرف قاعدة البيانات الا من قبل الاشخاص المخولين فقط.
		14-2-4	التأكد من وجود قواعد بيانات خاصة بالتحقق التي تسمح للمستفيدين الوصول الى حساباتهم المصرفية.
		15-2-4	التحقق من وجود نظم محمية وحساسة لاكتشاف التلاعب والفساد الاداري ويجب ان تدون تلك النتائج.
		16-2-4	التحقق من توفر مخول اصولي ومن قبل مصدر الكتروني متحقق منه في حال حذف اوتغيير لفرد اووكيل مشمول بقاعدة بيانات التحقق.
		17-2-4	التأكد من ان جلسات التحقق الخاصة بالعمليات المصرفية الالكترونية في أمان خلال مدة الجلسة، وفي حال وجود خلل أمني يجب أعادة جلسة التحقق.
		18-2-4	التأكد من ان جميع المعملات الالكترونية قد تم التحقق الايجابي منها مع ادامة عملية المراقبة على القناة التي تم التحقق من خلالها.
		19-2-4	التحقق من توفر الاجراءات الرقابية المناسبة لحماية مصداقية البيانات الخاصة بالعمليات المصرفية الالكترونية والمعلومات والسجلات، اي ان اي تعديل على العمليات المصرفية دون توفر التخويل المناسب يؤدي الى فشل مصداقية البيانات وبالتالي تعرض المصرف الى مخاطر مالية وقانونية ومخاطر سمعة.
		20-2-4	التحقق من وجود برنامج تدريبي شامل بالوعي بامن المعلومات والاتصالات والتدابير الفردية الواجب اتخاذها من قبل الموظف لحماية اصول النظام.
		21-2-4	التحقق من اخذ التدابير المناسبة لحماية بيانات العميل السرية والحساسة وان يتم التصديق على الزبون بالشكل الصحيح قبل الوصول الى تنفيذ المعاملات الالكترونية عبر الانترنت.
		22-2-4	التحقق من توفر الاجراءات المناسبة لفحص التعديلات على النظام وتحليل المخاطر والاثار المترتبة على التغيير في البيئة التجريبية قبل نشرها في بيئة الانتاج.
		23-2-4	التحقق من عمل نسخ احتياطي للانظمة والبرامج المتأثره قبل اجراء التعديل عليها ونشرها في بيئة الانتاج الفعلي.
			مخاطر مالية
			التحقق من استخدام المصرف تكنولوجيا متطورة في قياس وتقييم وادارة مخاطر الخاصة بالائتمان.
			التأكد من سلامة وفاعلية اجراءات منح القروض وتتوافق مع القوانين والسياسات الخاصة بالمصرف.
			التحقق من وضع اسس وقواعد سليمة للموافقة على الائتمانات الجديدة او اعادة تمويل الائتمانات السابقة.

		24-2-4	المراجعة الدورية للسياسات الخاصة بمنح القروض ومقارنتها مع الاجراءات الفعليه للنظام عند منح القرض.
		25-2-4	التحقق من الفصل الملائم مابين الشخص الذي يعمل على تقديم معامله القرض عن الشخص المخول بالموافقه على المنح.
		26-2-4	التحقق من الفصل الملائم مابين الجهات المسؤوله عن منح الائتمان والجهات المسؤوله عن المتابعة والتحصيل.
		1-3-4	التحقق من وجود تقارير دورية من قبل النظام المصرفي الالكتروني الشامل عن القروض المتعثره ومدة التأخير.
		2-3-4	التحقق من أعداد النظام أنذار مبكر لهبوط جودة الائتمان وتحديد وتقييم القروض الغير منتجة او المتعثرة.
		3-3-4	التحقق من سلامة اجراءات فرض الغرامات التأخيرية عن القروض المتعثره.
		4-3-4	التحقق من سلامة اجراءات الاستعلام عن الزبون في حال لدية تعثر في تسديد الديون السابقة اولدية قروض من مصارف اخرى.
		5-3-4	التاكد من وجود حدود ائتمانية محددة من قبل المصرف والعمل على التحقق من عدم تجاوزها من قبل النظام.
	3-4		التأكد من سلامة وفاعلية أجراءات الحصول على الضمانات قبل منح الائتمان.
		6-3-4	التحقق من سلامة اجراءات التقييم الدوري للضمانات المقدمة لمنح القرض والتاكد من مدى صلاحيتها قانونيا.
		7-3-4	التحقق من توفر الاجراءات المناسبة من قبل النظام الشامل للسيطرة على مخاطر السيولة.
		8-3-4	التحقق من اعداد النظام التقارير الدورية عن وضع السيولة بالمصرف واي تغيير مادي يطرأ على مركز السيولة الحالي او المرتقب.
		9-3-4	التحقق من قيام المؤسسة بابلاغ الزبون حامل البطاقة الالكترونية من خلال التنبيهات في حال تجاوز المبلغ المسحوب المبلغ المسموح به مع نزويدة بالمعلومات عن مصدر وقيمة المعاملة.
		10-3-4	التحقق من قيام النظام باعداد تقارير دورية بتركيز الائتماني لاكبر 5 مودعين ومدى نسبة من اجمالي الايداعات.
		11-3-4	التحقق من وجود سياسات واجرات فعاله من قبل المصرف لمواجهة مخاطر عدم القدرة على تسديد التزاماتها نتيجة سحب الزبائن ايداعاتهم بنفس الوقت.
		12-3-4	التأكد من توفر لجان مؤهلة قادرة على متابعة مراحل تنفيذ النظام الشامل والاحداث المهمة التي سيتم الوصول اليها وفق جدول زمني محدد وخطة تنفيذ للمشروع واضحة ومحدده مسبقا.
		13-3-4	التأكد من توثيق الخطط بشكل واضح لجميع مشاريع تقنيات المعلومات والاتصالات مع التحديد الواضح لمخرجات التي يجب تحقيقها في كل مرحلة من مراحل تنفيذ المشروع.
		14-3-4	التحقق من اعداد النظام تقارير دورية عن معدل العائد على الاصول ومعدل تكلفة الالتزامات.
		15-3-4	التحقق من وجود سياسات مصرفية خاصة بتغير اسعار صرف وخاصة في ظل الحوالات المالية للعملات الاجنبية في ظل تقلب الاسعار.
		16-3-4	التأكد من وجود الاشراف الفعال على الموظفين اصحاب صلاحيات التخويل المرتفعه من خلال تسجيل جميع نشاطاتهم ومراجعتها.
			<u>مخاطر القانونية وسمعة المصرف</u>
		17-3-4	التحقق من العرض الواضح والصريح للمعلومات المناسبة على الموقع الرسمي للمصرف على الانترنت، لمساعدة العملاء على الاستنتاج حول هوية ومركز القانوني للمصرف قبل الشروع باجراء العمليات المصرفية الالكترونية.
		18-3-4	
		19-3-4	

		4-4	التحقق من وجود معايير وسياسات سرية الزبون المصرفي والتي تأخذ بنظر الاعتبار كل الانظمة والقوانين السرية معلومات الزبون عندما تقدم الخدمات والمنتجات له عبر العمليات المصرفية الالكترونية.
			4-3-20
			التأكد من جعل زبائن المصرف على وعي كافي بسياسة المصرف في مجال السرية والقضايا ذات العلاقة بتقديم الخدمات من خلال العمليات الالكترونية.
			4-3-21
			4-3-22
			التأكد من وضع الاجراءات المناسبة لحماية الزبائن الذين يستخدمون الانترنت في انجاز معاملاتهم مع تثقيف الزبائن بشان الاجراءات الامنية التي وضعتها المؤسسة لحماية زبائنها.
			4-2-23
			التحقق من فاعلية اجراءات الاتصال وابلاغ الزبائن بالحوادث المهمة والطرق التي تم التعامل معها لتحسين قضايا العلاقات العامة مع الزبائن وتجنب الاراء السلبية.
			التحقق من عدم أستخدام معلومات الزبون في مجالات تتعدى مامسموح به او مامخول به من قبل الزبون.
			4-4-1
			التحقق من عدم مشاركة المصرف معلومات الخاصة بالزبائن والذي لم يسمحوا للمصرف بمشاركة معلوماتهم الى الاطراف الخارجية الاخرى كاستخدامها للتسويق من خلال معرفة رغباتهم وحاجاتهم ومركزهم المالي.
			4-4-2
			التحقق من تشخيص وتحديد الحادث او الازمة حال وقوعها وتقدير المادي لها للسيطره على المخاطر الخاصة بالسمعة والناتجة عن توقف تقديم الخدمات.
			4-4-3
			التحقق من تنفيذ التدابير المناسبة لمعالجة مخاطر سرقة البيانات وفقدان البيانات او تسريبها من اجهزة (البيانات الموجود في الحاسوب المحمول او الشخصي او البيانات في وحدات التخزين المحمولة) او من مركز الاتصالات او مواقع خدمة الزبائن والتي تطلب حماية تلك المعلومات في جميع اجهزة نقاط النهاية مع التشفير المتين يمنع من تسريبها.
			4-4-4
			4-4-5
			التحقق من فرض الرقابة القوية على كلمات المرور للوصول الى التطبيقات من قبل الزبائن من خلال تغيير كلمة المرور عند التسجيل لاول مرة وتعقيد كلمة المرور والحد الادنى لطول كلمة المرور فضلا عن مدة صلاحية الوصول في الجلسة والواحدة.
			4-4-6
			التحقق من متابعة واستخدام اخر التحديثات التقنية في مجال التعرف على المستخدمين ومنحهم صلاحية الوصول او التفويض لاتمام العمليات المصرفية الالكترونية من خلال استخدام الاساليب البديلة لكلمات المرور كبصمة العين او بصمة الاصبع.
			4-4-7
			التحقق من تنفيذ المصادقة الثنائية عند تسجيل الدخول الى الانظمة الالكترونية عبر الانترنت مع توقيع المعاملة لتأمين عملية تصديق العملاء ولضمان عدم دخول الاشخاص الغير مفوضين لانجاز المعاملات.
			4-4-8
			4-4-9
			التحقق من عدم استخدام مواقع الانترنت الغير امنه كوسائل التواصل الاجتماعي ومواقع التخزين عبر الانترنت او من خلال رسائل البريد الالكتروني للتواصل وتخزين البيانات السرية.
			التحقق من اخذ التدابير المناسبة عند تبادل المعلومات السرية بين المؤسسة والاطراف الخارجية من خلال ارسال المعلومات عبر القنوات المشفرة وارسال مفاتيح التشفير عبر قنوات منفصلة الى المستلم المستهدف.
			4-4-10
			التحقق من توقيع اتفاق مابين العميل والجهة المنفذه للنظام الالكتروني فيما يخص المحافظة على امن وسرية المعلومات والبيانات.
			4-4-11
			التحقق من وجود استراتيجية فعالة لمواجهة مخاوف الاعلامية والسوقية التي قد تنشأ في حال الهجوم على النظام او حصول حوادث مربكة اوالاخلال المادي بالامان.
			التحقق من تزويد الزبائن المستخدمين لخدمات الانترنت لانجاز معاملاتهم الالكترونية بالتاكيدات بان الوصول الى الانترنت واجراء العمليات عبر موقع الرسمي مؤمن وموثق بصورة كافية.
			4-4-12
			التحقق من استخدام ادوات الرقابة التي تمكن من اكتشاف التغيرات في قواعد البيانات او ملفات النظام، لتسهيل التعرف على التغييرات الغير مصرح بها.
			4-4-13

		14-4-4	التحقق من وجود اجراءات فعاله لاخبار السلطات الرقابية في حال حصول حوادث مربكه او هجوم على النظام او اخلال المادي للامان.
		15-4-4	التحقق من وجود سياسة واضحة ومناسبة لاخبار الاطراف الخارجية ذات العلاقة بما فيهم الزبائن بالوقت المناسب في حال حدوث ارباك مادي بعمل النظام المصرفي الشامل واسبابة والتطورات الحاصلة في استئناف عمل النشاط.
		16-4-4	التحقق من جمع البيانات الخاصة بحوادث المتربطة بالعمليات المصرفية الالكترونية للنظام والاحتفاظ بها لتسهيل عملية المراجعه اللاحقة لها، وكذلك للمساعدة على الملاحقة القانونية للمهاجمين.
		17-4-4	التحقق من المعلومات الاساسية للمصرف لايمكن مشاهدتها او استعمالها من غير الاشخاص المخولين، فالافصاح الغير مخول للبيانات ينتج عنه مخاطر قانونية ومخاطر سمعه عالية.
		18-4-4	التحقق من عدم الافصاح عن اي بيانات مصرفية اوسجلات الا الى الوكلاء والافراد المخولين والنظم التي تم التحقق منها.
		19-4-4	التحقق من فاعلية اجراءات اقفال الدخول الى البيانات الخاصة والمقيدة والعمل على بذل الجهود المتواصلة لضمان عدم القدرة على التلاعب بها.
		20-4-4	التحقق من ان العميل لديه السلطة التعاقدية والوسائل اللازمة لازالة البيانات المخزنة في انظمة مزود الخدمة والنسخ الاحتياطية الخاصة بالبيانات في حال انتهاء العقد مع مزود الخدمة.
		21-4-4	التأكد من وضع المؤسسة انظمة كشف الاحتيال المرتبطة بالاهداف السلوكية للزبون او مايعادلها لمساعدة المؤسسة على كشف العمليات التي تظهر انحرافا كبيرا عن سلوك الفرد المعتاد في استخدام البطاقة الالكترونية.
			<u>تحليل وتقييم مخاطر الاعمال المحددة</u>
		22-4-4	تحليل وتقييم مخاطر الاعمال الخارجية في ظل تطبيق النظام المصرفي الالكتروني الشاملة ومدى تأثيرة على البيانات المالية.
		23-4-4	تحليل وتقييم مخاطر الاعمال الداخلية في ظل تطبيق النظام المصرفي الالكتروني الشامل ومدى تأثيرها على البيانات المالية.
		24-4-4	تحديد وتقييم مخاطر الاعمال المتبقية والغير مسيطر عليها، والتي تعتبر الاساس في توجية اهتمام المدقق نحو الامور الهامة والجوهرية عند أجراء عملية التدقيق.
		25-4-4	تطوير برنامج التدقيق على ضوء مخاطر الاعمال المتبقية والعمل على جمع المعلومات وادلة الاثبات الملائمة لعملية التدقيق.
		26-4-4	وضع التوقعات النهائية بخصوص التحريفات الجوهرية التي تؤثر على البيانات المالية واستمرارية العميل على ضوء مخاطر الاعمال المتبقية وادلة الاثبات المتحصل عليها اثناء عملية تقييم المخاطر.
5			عمل الاختبارات المباشرة على البنود الاكثر عرضة للتحريفات الجوهرية بمايتلائم مع مخاطر الاعمال المحددة.
			تعديل اجراءات التدقيق بمايتلائم مع حجم مخاطر الاعمال المحددة والمتبقية في ظل التحول نحو الانظمة الالكترونية الشاملة.
			تركيز جهود التدقيق نحو المواقع التي تحتوي على اخطاء جوهرية اعتماداً على نتائج تحليل المخاطر.
6			

	1-5 2-5 3-5 1-6 2-6 3-6 4-6		

المبحث الرابع: الاستنتاجات والتوصيات

اولاً: الاستنتاجات

1- يساهم النظام المصرفي الالكتروني الشامل في زيادة فاعلية المصرف على تقديم الخدمات المصرفية الجديدة والمتنوعه مع العمل على تكامل وترابط فروع المصرف بقاعدة بيانات مركزية والتي يمكن من خلالها تقديم الخدمات المصرفية في الوقت الفعلي بغض النظر عن الزمان والمكان.

2- ان استخدام تكنولوجيا المعلومات في جميع مراحل التدقيق يساهم في جمع وتقييم ادلة الاثبات لتحديد ماذا كانت الانظمة الالكترونية تساهم في حماية موجودات المنشاة، ويؤكد سلامة بياناتها، ويحقق اهدافها بكفاءة وفاعلية.

3- ان قيام مراقب الحسابات بدراسة وتحليل بيئة العميل والمخاطر التي تحيط به سواء كانت خارجية او داخلية وفق المؤشرات المالية والغير مالية، يساهم في حصول المدقق على المعلومات الملائمة حول نقاط الضعف والقوة لدى العميل مع أعطاء تصورا شاملا عن بيئة العميل والاهداف المحققة من تطبيق النظام الشامل، مما يساعد المدقق على معرفة مدى قدرة العميل على الاستمرار في مزاولة نشاطة في المستقبل وحجم التحريفات الجوهرية التي تتعرض اليها البيانات المالية.

4- ان استخدام المدقق الخارجي برنامج التدقيق المقترح يساهم على معرفة مخاطر الاعمال الجوهرية وتقييم الضوابط الرقابية على تلك المخطر لتحديد حجم مخاطر الاعمال المتبقية لمساعدة المدقق على تعديل أجراءات التدقيق بمايتلائم مع حجم المخاطر المتبقية و توجيه تركيزه نحو البنود الاكثر عرضة للتحريفات الجوهرية.

ثانياً: التوصيات

1- ضرورة توجة الادارة الى زيادة الاستثمار بتكنولوجيا المعلومات ورصد التخصيصات المالية المطلوبة لتطبيق النظام الشامل على جميع فروع المصرف وفق خطة وجدول زمني محدد ورصد الانحرافات في التطبيق واسبابها وطرق معالجتها، نظرا لما يوفره النظام الشامل من تقديم خدمات مصرفية جديدة ومتنوعه بغض النظر عن الزمان والمكان وبكلفة اقل.

2- ضرورة أعتماد مراقب الحسابات على تكنولوجيا المعلومات في عملية تدقيق الانظمة الالكترونية الشاملة لتحقيق الدقة والسرعة والموثوقية في العمل التدقيقي من جهة ومواكبة التطورات السريعة في المهنة من جهة اخرى.

3- ينبغي اعتماد مراقب الحسابات اسلوب تدقيق يتماشى مع حجم مخاطر الاعمال الداخلية والخارجية للعميل وتحليلها لتحديد المخاطر التي تهدد استمرارية نشاط العميل وحجم التحريفات الجوهرية المتبقية التي تمتد للبيانات المالية للتحسين من جودة التدقيق.

4- ضرورة توجه مراقب الحسابات بالتدقيق المستند الى مخاطر الاعمال في ظل استخدام العميل الانظمة المصرفية الذي تعتمد على الانترنت في تقديم خدماته.

المصادر

القوانين والتعليمات

1- معيار التدقيق الدولي رقم (315) والخاص بفهم ومعرفة المنشأة والبيئة التي تعمل بها وتحديد وتقدير مخاطر وجود التحريفات الجوهرية.

2- المعهد الامريكي للمحاسبين القانونين (AICPA)

3- معيار التدقيق الدولي رقم (200) والخاص بالهدف من مراجعة القوائم المالية والمبادئ العامة التي تحكمها.

الكتب العربية

1- الصيرفي ، محمد الصيرفي ، ادارة العمليات المصرفية: العادية ، غير العادية ، الالكترونية) ، دار الفجر للنشر والتوزيع ، القاهرة ، مصر ، 2016.

الرسائل والاطاريح العربية

1- سمرة، ياسر السيد عبد العزيز، نموذج مقترح لقياس اتعاب المراجعة في ظل بيئة مخاطر الاعمال وزيادة المسؤلية الاجتماعية للشركات المقيدة في البورصة المصرية،كلية التجارة، جامعة دمياط ، 2013.

2- العيساوي، كرار جاسم نجم، التدقيق المستند على مخاطر الاعمال واثره على استمرارية النشاط، المعهد العالي للدراسات المحاسبية والمالية، جامعة بغداد، 2018

الدوريات والنشرات والمجلات العربية:

1- الحساني، وعد هادي عبد، حمدان، خولة حسين، تدقيق المبادرة الزراعية ودوره في تحقيق التنمية المستدامة، بحث مستل من اطروحه، مجلة دراسات محاسبية ومالية، عدد خاص، المؤتمر الوطني الاول لطلبة الدراسات العليا، 2016.

2- الحجامي، ستار جابر خلاوي، مخاطر التدقيق في ظل بيئة تكنولوجيا المعلومات، مجلة دراسات محاسبية ومالية، المجلد العاشر، العدد31، الفصل الثاني، 2015.

3- يعقوب، فيحاء عبدالله، ابراهيم، محمد خليل، تأثير مخاطر مراكز العملات الاجنبية في اجراءات التدقيق، مجلة دراسات محاسبية ومالية، المجلد 17، العدد 60، 2022.

4- المعموري، علي محمد ثجيل، الشريفي، احمد عبد الامير، تقييم المدقق للتحريفات المكتشفة وأنعكاسها على اجراءات الادارة(بحث تطبيقي في شركة العامة لتصنيع الحبوب)، مجلة دراسات محاسبية ومالية، المجلد 16، العدد 54، 2021.

5- السقا، رشيد، زياد هاشم، ناظم حسن، متطلبات تدقيق عمليات التجارة الالكترونية في ضوء معايير التدقيق، مجلة دراسات محاسبية ومالية، المجلد7، العدد20، الفصل الثال، 2012.

6- التميمي ، البازي ، التميمي، مهند محمد جاسم، علي محمد، حيدر كاظم، مدى قدرة مراقب الحسابات المستقل على تدقيق تطبيق متطلبات التجارة الالكترونية، مجلة دراسات محاسبية ومالية، المجلد الثالث، العدد44، الفصل الثالث، 2018.

7- خلف، صلاح نوري، علي، نافع حسن، دور التدقيق الخارجي في ادارة المخاطر المصرفية (أطار مقترح أنموذجي أختبارات الرقابة وتقييم المخاطر المصرفية)، مجلة دراسات محاسبية ومالية، المجلد 13، العدد43، الفصل الثاني، 2018.

FOREIGN REFERNCES

1- Arens, A, and, Loebbacke, J, Auditing and Assurance Services: an Integrated Approach, 8ed: USA: Prentice Hall International,Inc,p:44: 2004.
2- Arens, A.A, Elder,R.J and Beasley,M.S, Auditing and Assurance Services: An Intergrated Approach,12th Edition: 2008.
3- Nobes, C.W. and Parker, R., Comparative International Accounting, Prentice-Hall, Sixth Edition, 2000.
4- Pong, C. & Turley, S , "Audit firms and the audit market", in Sherer, M. & Turley, S (editors). Current Issues in Auditing, 3rd edition, London, 1997.
5- Kutum, I, The Application of Business Risk Audit Methodology within Non- Big 4 Firms, Submitted for the Degree of Doctor of Philosophy in Accountancy, Division of Accounting & Finance, Stirling Management School, University of Stirling, 2010.
6- Rich, J. Solomon, I. and Trotman K, multi-auditor judgment and decision making reseach: a decade later, journal of accounting literature,1997.
7- Peler Schelluch and Topple, Seephen and Rittenberg, Larry and Schwieger, Bradle, assurance and auditing: concepts for a changing environment, 1 st ed, Australian,2003.
8- 12- Shernish, Rajin (analytical study on core banking witw reference to state bank of india), Birla institute of technology international center rak,UAE, june, 2011.
9- Musau Harris Ngui,(Factors Influencing Implementation of Core Banking System Projects by Commercial Banks In Kenya:the case of nic bank Kenya limited), A research project report submitted in partial fulfilment of the requirements of the award of the degree of Master of Project Planning and Management of the University of Nairobi, 2015.
10- Bala Shanmugam, Lokesh Gupta, Naftis Alam,(Islamic Finance: A Paractical Perspective), Springer International Publishing: 2018.
11- Chadima Antonin,(core banking system),University of Economics in Prague Faculty of Information and Statistics, 2017.