تقييم أثر أمن المعلومات على أداء المصارف

■ د. ابتسام إبراهيم بوكر الغزيوي *

● تاريخ استلام البحث 2024/04/17م . ● تاريخ قبول البحث 2024/05/25م

■ **المستخلص:**

تهدف هذه الدراسة إلى تقييم أثر أمن المعلومات على أداء المصارف في القطاع المصرفى لعام 2021/2020، لعينة تتكون من 13 مصرفاً، بينما يبلغ مجتمع البحث 32 فرعاً مصرفياً، وقد تم قياس أمن المعلومات من خلال الإجراءات الخاصة بتطبيق معايير أمن المعلومات ومقاييس نظام حماية الخدمات المصرفية الإلكترونية، وسرعة معالجة تهديدات أمن المعلومات، وذلك فى محاولة لمعرفة تأثير تلك المتغيرات المستقلة على مؤشرات الربحية وجودة الأصول.

وتم تحليل أثر أمن المعلومات على الأداء بالمصارف بإستخدام أسلوب تحليل الانحدار المتعدد واختبار كا تربيع (Chi-Square)، وأوضحت النتائج الجوهرية أثر أمن المعلومات على مؤشرات الربحية التي تمثلت في (معدل العائد على الأصول، ومعدل العائد على الملكية ومعدل العائد على رأس المال)، وكذلك على جودة الأصول التي تمثلت فى نسبة مخصصات خسائر القروض.

● **الكلمات المفتاحية:** أمن المعلومات، مخاطر أمن المعلومات، الأداء، المصارف .

■ **Abstract:**

This research aims to assess the impact of information security on the performance of banks in the banking sector for the year 2020/2021، for a sample consisting of 13 banks، while the research community is 32 bank branches، and information security has been measured through the procedures for ap-

*أستاذ مساعد بقسم التجارة الإلكترونية وتحليل البيانات- كلية الاقتصاد والعلوم السياسية بجامعة طرابلس E-mail: ebtesamboker@gmail.com

plying information security standards and banking services protection system standards electronic data، and the speed of processing information security threats، in an attempt to find out the impact of these independent variables on indicators of profitability and asset quality.

The impact of information security on performance in banks was analyzed using the method of multiple regression analysis and the Chi-Square test. As well as on the quality of assets، which was represented in the ratio of provisions for loan losses.

● **Key words:** Information security، information security risks، performance، bank

■ المقدمة

يتطلب الاعتماد المتزايد على التكنولوجيا في تقديم المصارف لخدماتها المصرفية توافر السرية للمعلومات عند تنفيذ أى تعامل إلكتروني لتجنب المخاطر التي يمكن أن تتعرض لها المصارف، لذلك تهتم المصارف بوضع سياسات أمنية لمواجهة تهديدات أمن المعلومات وحماية البيانات والأصول من تسرب البيانات والاحتيال والوصول غير المصرح به لنظام المعلومات.

إن البحث في مجال أمن المعلومات" – فى واقع الأمر لا يمكن أن ينحصر تحت مظلة واحدة، فالباحثون في المجال الأكاديمى يتناولونه باعتباره العلم الذي يبحث فى نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، كذلك المشتغلون فى مجال تقنية المعلومات يتناولونه باعتباره الوسائل والأدوات والإجراءات اللازمة لضمان حماية المعلومات من المخاطر، ومن الناحية القانونية، يعتبره الدارسون بأنه هو مجموعة التشريعات والقوانين لحماية المعلومات من الأفعال غير القانونية التي تستهدف تلك المعلومات وأنظمتها، وقد عرف (2011) Tiwari أمن المعلومات بأنه هو كل ما يتعلق بحماية المعلومات ونظم المعلومات من الوصول غير المصرح به والاستخدام والإفصاح والتعديل، والاطلاع والفحص والتسجيل، وأضاف (2011) Teltumde بأن أمن المعلومات الهامة بها.

ويتضح مما سبق أن أمن المعلومات هو مجموعة الإجراءات والتدابير الوقائية التي تستخدم لحماية المعلومات والأجهزة والبرمجيات، وذلك من خلال توفير الأدوات والوسائل اللازمة للحماية من أي مخاطر، حيث تعتمد حماية المعلومات على العنصر البشرى ووسائل التقنية والسياسات الأمنية.

ونتيجة للمخاطر المرتبطة بالخدمات المصرفية الإلكترونية؛ يتعين على المصارف – فى ضوء قانون المصرف المركزى والجهاز المصرفي والنقد رقم 88 لسنة 2003 والمعدل بالقانون رقم 8 لسنة 2013 – وضع إجراءات، وضوابط والالتزام بالمعايير العالمية لأمن المعلومات للحفاظ على خصوصية البيانات وسرية حسابات العملاء من أي مشاكل تسبب حدوث إختراق لخصوصية البيانات نتيجة عمليات القرصنة، أو الاحتيال، مما يؤثر سلبياً على ثقة العملاء وسمعة المصرف.

وللتأكيد على أكثر الالتزام بالسياسات والضوابط المحددة، والمعايير العالمية لأمن المعلومات، فقد كشفت مؤسسة (Financial Fraud Action UK) – وهي مؤسسة ببريطانيا تستهدف التنسيق مع أنشطة الخدمات المالية للوقاية من عمليات الاحتيال – في عام 2013 قدرت الخسائر بنحو 40.9 مليون دولار نتيجة الاحتيال عبر خدمات الانترنت المصرفي، و 11.6 مليون دولار نتيجة الاحتيال من خلال الخدمات المصرفية عبر الهاتف وهناك أمثلة محلية بالقطاع المصرفى، من أرصدة بطاقات عملاء مصارف بليبيا نتيجة استخدام طرق احتيالية.

● **أولاً: مشكلة البحث.**

في الأونه الأخيرة؛ شهدت الصناعة المصرفية تقدماً ملموساً في تقديم الخدمات المصرفية التقليدية أو المبتكرة من خلال شبكات الاتصال الإلكترونية بما يلبي توقعات العملاء وبشكل يحقق مواكبة التقدم التكنولوجى في هذا المجال، وقد شملت الخدمات المصرفية الإلكترونية النظم التي تسمح للعملاء بالحصول على معلومات عن الخدمات المالية من خلال قنوات الاتصال الإلكترونية ماكينات الصراف الآلى والانترنت المصرفي، والخدمات المصرفية عبر الهاتف المحمول).

ونظراً لزيادة اعتماد الخدمات المصرفية على التكنولوجيا، فإن ذلك يتطلب الالتزام بالضوابط الرقابية للعمليات المصرفية الإلكترونية، والقواعد المنظمة للمصارف بشأن تقديم تلك الخدمات ووضع رقابة فعالة على المخاطر المرتبطة بتقديمها لضمان سرية وأمن المعلومات.

وهناك عدة أساليب لضمان سرية وأمن المعلومات تتمثل في: أساليب إدارية منها: تقليل الإفصاح عن البيانات الهامة والحساسة إلا للمسؤولين، وتغيير أساليب الدخول بشكل مستمر مثل كلمة السر.

وتتحدد مشكلة البحث في محاولة الإجابة على السؤال التالي:

- ما هو أثر أمن المعلومات على أداء المصارف؟

ومن خلال التساؤل الرئيسي برزت تساؤلات فرعية هي:

1 - مامدى مؤشرات الربحية المتمثلة فى معدل نمو العائد على الأصول، ومعدل نمو العائد على الملكية، ومعدل نمو العائد على رأس المال، ومعدل التغير النسبى فى سعر السهم Stock Market Return ؟.

2 - ما مدى جودة الأصول معبراً عنها بمعدل نسبة مخصصات خسائر القروض إلى إجمالي القروض؟.

فرضيات الدراسة:-

- لا يوجد تأثير معنوى - ذو دلالة إحصائية - لأمن المعلومات على ربحية المصارف.
- لا يوجد تأثير معنوى - ذو دلالة إحصائية - لأمن المعلومات على جودة الأصول بالمصارف.

■ **أهداف البحث.**

1 - التعرف على مدى استفادة المصارف الليبية من تطبيق الإجراءات ومعايير أمن المعلومات وتأثير ذلك على أدائها من خلال مؤشرات الربحية وجودة الأصول بالمصارف.

2 - التعرف على الضوابط الإلكترونية والمتابعة المستمرة للتطورات في النظم الأمنية لضمان فعالية تأمين الخدمات المصرفية الإلكترونية والإجراءات الرقابية اللازمة لحماية العمليات المصرفية من أي تهديدات داخلية أو خارجية.

3 - التعرف على الاختراقات والانتهاكات الأمنية مثل وصول أشخاص غير مصرح لهم إلى التطبيقات وقواعد البيانات الخاصة بالخدمات المصرفية الإلكترونية،

4 - التعرف على العلاقة بين المتغيرات الرئيسية للدراسة من خلال التعرف على تقييم أثر أمن المعلومات على أداء المصارف.

■ أكثر الدراسة:

1 - تكمن أكثر هذه الدراسة في تشخيص واقع أثر أمن البيانات على أداء المصارف كونه موضوعاً من مواضيع الساعة نظراً لزيادة اعتماد الخدمات المصرفية على التكنولوجيا.

2 - إبراز خصوصيات أمن البيانات والتعرف على إجراءات الوقاية والحماية التي يجب أن تكون مكتملة ومستمرة باستمرار الاتصالات .

3 - مساعدة المصارف محل الدراسة على تبني إستراتيجية واضحة لوضع السياسات والضوابط الرقابية اللازمة لحماية العمليات المصرفية من الإختراق.

● ثانياً : الدراسات السابقة

1 - دراسة (2016) (Dunkerley & Tejay) (**بعنوان تطوير نموذج لنجاح أمن نظم المعلومات**)

Developing an Informationfor Model Systems Security Success E- "Government Context"

وهذه الدراسة تهدف إلى فهم أفضل للعناصر التي تشكل نجاح أمن المعلومات بالمنظمة، وتطوير نموذج لضمان حماية المعلومات داخل المنظمة، وقد توصلت الدراسة إلى ضرورة توافر العلاقة التبادلية بين العناصر التالية: (سرية المعلومات، وحماية نظم المعلومات واتباع النظم الإدارية، والاستفادة من الخبرة والمعرفة وفوائد توافر أمن المعلومات)، وذلك

لوضع نموذج لنجاح أمن المعلومات داخل المنظمة وأيضا لفهم العلاقة بين تواجد الأمن بالمنظمة ونظام المعلومات والتكنولوجيا المستخدمة لحماية تلك المعلومات.

2 – دراسة (2016) Kumar & Puri، فقد تناولت الإطار العام لتقييم سياسة أمن المعلومات "Framework for Evaluation and Validation of" "Information Security Policy.

تهدف هذه الدراسة إلى توفير آمان أفضل للبيانات وللنظام، كما أوضحت مختلف التهديدات التى تواجه المعلومات والإستراتيجيات التي يتم التعامل معها من خلال إدارة المخاطر، وتم تحليل سياسات أمن المعلومات لعدد من الجامعات وهي: Birmingham, City, Georgetown, Gndu, Punjabi Rice, Victoria and Virginia لتصميم إطار عام جديد لأمن المعلومات من خلال الأنشطة التي تتمثل في Service Access Control, Back Up System Security Management, Authentication, Cryptography, and Access Control لتوضيح إلى أى مدى تتحقق المرونة والآمان، والسرية، وقد توصلت الدراسة إلى إمكانية تطبيق سياسات أمن المعلومات التي تحتوى على هذه الأنشطة باستخدام البرامج، كما أكدت على ضرورة اتباع هذه الأنشطة لحماية المعلومات من المخاطر التي تواجهها.

3 – دراسة (2015، Smartphone Information (Nunoo" Security Risks إلى ارتباط استخدام الأدوات سهلة النقل مثل "Smartphone" بالتهديدات والمخاطر، ونقاط الضعف

هدفت هذه الدراسة إلى إدراك وملاحظة تهديدات أمن المعلومات الناتجة عن استخدام Smartphone بالمنظمة، ومن نتائج هذه الدراسة التحديات التي تواجه أمن المعلومات. وتوصلت إلى بعض الحلول عند استخدام تلك الأدوات واستخدام نظرية التقنية لمواجهة المخاطر.

4 – دراسة Arcurial 2015 أثر اختراق أمن المعلومات على عوائد الأسهم،

هدفت هذه الدراسة لاختيار أثر الإعلان عن الهجمات، وتم جمع 128 بياناً عن الهجمات الإلكترونية لـ 81 شركة باستخدام أسلوب دراسة الحدث لاختبار أثر الإعلان

عن الهجمات الإلكترونية على القيمة السوقية للشركات خلال الفترة من 1995 حتى 2014،، ومن نتائج الدراسة إلى أن الإعلان عن الهجمات عبر الانترنت يؤثر على عوائد الأسهم لتلك الشركات، وأوصت الدراسة بتحديد الاستثمارات فى أمن المعلومات لمواجهة تلك المخاطر التي تؤثر على سمعة الشركات.

■ **الإطار النظري:**

أمن المعلومات : هو حماية جميع أنواع المعلومات ومصادر الأدوات التى تتعامل معها وتعالجها من التجهيزات الحاسوبية وغير الحاسوبية المتصلة بها باتباع إجراءات وقائية محدده تكفل المحافظة عليها وحمايتها من الأخطار التى قد تتعرض لها والتى تتخذ صورا متعددة كاستغلال المعلومات الشخصية لغير الأغراض التى جمعت من أجلها، أو كشف ما يعد منها سريا وما قد ينتج عنه من اطلاع الأشخاص غير المصرح لهم على معلومات ما كان ينبغى لهم الاطلاع عليها، أو اتلافها أو تعرضها للاستعمال غير المشروع سواء بالتغيير أو التعديل (الشوابكة، 2019،ص 164، 187).

مخاطر أمن المعلومات: هي أي عوامل أو ظروف أو أحداث أو نتائج غير مرغوب فيها تمكن من خرق أمن المعلومات وتسبب في خسارة أو ضرر أو انتهاك للمعلومات أو الأصول أو العمليات أو الأشخاص المرتبطين بها(العمري، 2019،ص15).

الأداء: هو مقياس لمدى تحقيق الفرد أو الفريق أو المنظمة للأهداف والمهام والمسؤوليات الموكلة إليهم بمستوى مقبول من الجودة والكفاءة والإبداع والتميز(العمري،2019،ص17)

المصارف: هي مؤسسات مالية تقوم بتقديم خدمات متنوعة للعملاء والمجتمعات مثل تلقي الودائع وإعطاء القروض والاستثمار والتحويل والتحصيل والتأمين والاستشارة وغيرها من الخدمات المالية والمصرفية (العبيدي، 2018،ص50).

■ **الإطار العملي:**

● **أولاً: منهجية البحث**

في ضوء تحقيق أهداف البحث والإجابة على تساؤلات الدراسة تم استخدام المنهج الميداني الذي يجمع بين المنهج الوصفي والتحليلي الذي يهدف إلى وصف الظاهرة المدروسة

للبيانات المطلوبة وطريقة الحصول عليها: تمثلت البيانات المطلوبة في النسب التي يقررها المصرف المركزى الليبي، بالإضافة إلى البيانات الثانوية التي تتمثل في الميزانيات وقوائم الدخل لقياس المتغيرات التابعة .

أما بالنسبة لقياس المتغيرات المستقلة فقد تم الآتي:

أ- إجراء دراسة استطلاعية لتجميع البيانات فيما يتعلق بمقاييس أمن المعلومات لتصميم قائمة الاستقصاء.

ب - إجراء مقابلات شخصية مع مديرى أمن المعلومات بالمصارف محل الدراسة للإجابة على قائمة الاستقصاء والتي تشمل الآتى: (مقاييس نظام حماية الخدمات المصرفية الإلكترونية، والإجراءات الخاصة بتطبيق معايير أمن المعلومات ISO 27001 & PCI-DSS" ومدى الاستجابة لسرعة معاجة تهديدات أمن المعلومات، ومناقشة كيفية معالجة تلك التهديات والمخاطر التى تؤثر على الأداء بإستخدام تقنيات حديثة.

- **ثانياً مجتمع وعينة الدراسة** : يشمل مجتمع البحث المصارف العاملة في الدولة الليبية

والمسجلة لدى المصرف المركزي الليبي خلال عام 2021/2020، ويبلغ عددها 32 مصرفاً، وتم اختيار عينة تتكون من 16 مصرفاً ولكن تمت الإجابة على قائمة الاستقصاء المستخدمة لقياس المتغير المستقل من قبل 13 مصرفاً، وبذلك يمثل عدد مفردات العينة 40 ٪ من عدد مفردات مجتمع الدراسة.

- **الأساليب الإحصائية المستخدمة في الدراسة.**

ج. المتغيرات المستخدمة وطريقة قياسها: يمكن توضيح المتغيرات التابعة (Dependent Variables) المستخدمة في الدراسة كما يلي:

جدول :(1) المتغيرات التابعة وطريقة قياسها

الرمز	المتغير	طريقة قياسه
ROA	معدل العائد على الأصول	صافي الأرباح / الأصول
ROE	معدل العائد على حقوق الملكية	صافي الأرباح / حقوق الملكية
ROC	معدل العائد على رأس المال	ضافي الأرباح / رأس المال المدفوع
SMR	معدل التغير النسبي في السعر	السعر$_{ن}$ – السعرن $_{ن-1}$ / السعرن $_{ن-1}$
NPL	جودة الأصول	مخصصات خسائر القروض إلى إجمالي القروض

ويمكن توضيح المتغيرات المستقلة (Independent Variables) كما يلي: (Salah & Hinson, 2009)

- تحديد السياسات والأهداف لتطبيق نظام إدارة أمن المعلومات من خلال جمع المعلومات وتحليلها، ووضع خطة محددة إستراتيجية لتحقيق الأهداف.
- مدى تطبيق نظام إدارة أمن المعلومات (ISMS) على كل المجالات المعرضة للمخاطر.
- خطة لمعالجة المخاطر.
- وضع معايير لإدارة المخاطر، وإعداد التقارير الخاصة بها.
- إجراءات معالجة المخاطر (إدارة التغير).
- إجراءات المتابعة والرقابة ووضع مؤشرات أداء لقياسها .
- تحديد المسؤوليات وإجراءات المحاسبة الداخلية والمسؤولية الإدارية من خلال مصفوفة المسؤوليات والأنشطة والواجبات لكل فرد.
- طرق وإجراءات الحماية والوقاية من مخاطر أمن المعلومات.

ويتم الحصول على البيانات الخاصة بكل بند من البنود السابقة من خلال تحديد مستوى التطبيق التالي:

- هل صممت كفكرة مبدئية (تم تجربتها)؟
- هل التصميم محدد وموزع على كافة الأنشطة؟
- هل تم إجراء تمهيدى؟
- هل تم تطبيقه بالفعل؟

ب. الإجراءات الخاصة بمعيار "Payment Card Industry Data (Security Standard" PCI-DSS) وتشمل متطلبات إدارة الأمن والسياسات والإجراءات وحماية الشبكات وتصميم البرمجيات والتدابير LLC، الوقائية لحماية البيانات PCI Security Standards Council LG الخاصة بمعيار (PCI-DSS) مطبقة أم لا؟.

ج- مقاييس نظام حماية الخدمات المصرفية الإلكترونية كالخدمات المصرفية عبر الانترنت وتتمثل في: الأجهزة التى تمنع الدخول غير المصرح به لموقع المصرف باستخدام جدار الحماية Firewall وتشفير عملية نقل البيانات الخاصة بالعملاء ورصد التهديدات وكلمات المرور لحماية الحسابات والتغيير الدورى لها. ويتم الحصول على البيانات من خلال تحديد إذا كانت تلك الإجراءات مطبقة أم لا؟.

د. مدى سرعة الاستجابة لمعالجة تهديدات أمن المعلومات والتي تتمثل في: (الوصول غير المصرح به وسرقة البيانات وهجمات عبر الانترنت، والتصيد الاحتيالي، "Phishing، ورسائل إلكترونية غير مرغوب بها قد تحتوى على فيرس Spam وسرقة الهوية identity Theft"، والبرامج الخبيثة "Malware"، وبرامج التجسس "Spyware" التي تقوم بجمع معلومات عن المستخدمين دون الحصول على موافقتهم وعيوب في تصميم البرامج واختراق خصوصية البيانات بسبب عمليات القرصنة piracy أو الاحتيال). ويتم الحصول على البيانات من خلال تحديد مدى سرعة الاستجابة للمعالجة كالآتى: (في الوقت الحالي بعد أسبوع - أكثر من أسبوع).

4. الأسلوب الإحصائى المستخدم لاختبار الفروض: يعتمد الباحث - في اختبار كل من

الفرض الأول والثانى – على أسلوب الانحدار المتعدد، واختبار كا تربيع Chi square على النحو التالي:

- أسلوب تحليل الانحدار المتعدد لاختبار جوهرية تأثير أمن المعلومات على مؤشرات الربحية، وجودة الأصول.

- **سابعاً: نتائج الدراسة الميدانية.**

يبدأ الجزء الميدانى من البحث بمحاولة استكشاف خصائص المتغيرات محل البحث، حيث تلخص الجداول التالية الإحصاءات الوصفية لهذه البيانات، وذلك كما يلى:

جدول :(2): الإحصاءات الوصفية للمتغيرات التابعة

	الحد الأدنى	الحد الأقصى	الوسط الحسابي	الانحراف المعياري
ROA	-0.0818	0.0285	0.007661	0.0184251
ROE	-1.4040	0.5022	0.057149	0.3127977
ROC	-0.4926	0.9267	0.212684	0.2609193
SMR	-0.7529	1.1514	0.043934	0.468983
NPL	0.0000	0.8000	0.168293	0.20839.7

جدول (3) : الإحصاءات الوصفية للمتغيرات المستقلة

	الحد الأدنى	الحد الأقصى	الوسط الحسابي	الانحراف المعياري
PCL	0.0000	1.0000	0.633660	0.3867228
ISO	0.000	5.000	3.76315	1.6999115
M	0.5630	1.0000	0.771000	0.1432951
ET	2.4348	5.0000	3.985379	0.7948313

- **المصدر: نتائج معالجة البيانات**

ويوضح الجدول التالى تأثير كل من الإجراءات الخاصة بتطبيق معيار أمن معلومات ISO 27001، ومقاييس نظام حماية الخدمات المصرفية الإلكترونية، مدى الاستجابة لسرعة معالجة تهديدات أمن المعلومات على أداء المصارف محل الدراسة.

جدول رقم (4) تحليل أثر أمن المعلومات على أداء المصارف باستخدام أسلوب تحليل الانحدار المتعدد

المتغير التابع	B_{ET}	B_M	B_{ISO}	F	R^T
ROA	0.003 6.474 ***	-	-	41.916 0.000 ***	0.777 0.00684
ROE	---	0.172 6.295 ***	-	39.621	0.768 0.07699
ROC	-	-	0.063 3.831 ***	14.674 0.002 ***	0.550 0.25676
SMR	-	-	-	-	-
NPL	-	-	-	-	-

تشير القيم - أسفل معاملات الانحدار - إلى قيم، حيث * تشير إلى مستوى المعنوية 10 ٪ بينما تشير إلى مستوى المعنوية 0 ٪ وتشير ... إلى مستوى المعنوية، كما تشير القيم بين القوسين - أسفل معامل التحديد R2 - إلى الخطأ المعياري والقيم - أسفل F - إلى مستوى المعنوية.

تشير النتائج من القيم الواردة بالجدول السابق إلى الآتي:

1. استجابة المصارف لسرعة معالجة تهديدات أمن المعلومات (ET) تؤثر على معدل العائد على الأصول (ROA) بقدره تفسيرية تبلغ 77.7 ٪ عند مستوى معنوية 1 ٪.

2. نظام حماية الخدمات المصرفية الإلكترونية (M) يؤثر على معدل العائد على الملكية (ROE) بقدره تفسيرية تبلغ 76.8 ٪ عند مستوى معنوية 1٪.

ويوضح الجدول التالى أثر أمن المعلومات على أداء المصارف باستخدام اختبار. Chi-Square كما يلي:

جدول رقم (5) تحليل أثر أمن المعلومات على أداء المصارف باستخدام اختبار Chi-square

المتغير المستقبل / المتغير التابع	PCL	ISO	M	ET
ROC	7.73 0.866	1.942 0.507	1.430 0.242	1.430 0.242
ROE	7.753 0.866	1.942 0.508	1.430 0.242	1.430 0.242
ROC	7.753 0.866	1.942 0.508	1.430 0.242	1.430 0.242
RMR	-	1.020 0.323	72.000 0.230	72.000 0.230
NPL	1.407 ***(0.000)	1.857 0.932	31.571 0.538	31.571 0.538

تشير القيم أسفل المتغيرات المستقلة إلى قيم z بينما تشير القيم بين القوسين – أسفل قيم Z – إلى مستوى المعنوية، وتشير ... إلى مستوى المعنوية 1 ٪.

يتضح من القيم الواردة بالجدول السابق أن:

1 – وجود تأثير معنوي للإجراءات الخاصة بتطبيق معيار PCI-DSS (PCI) على جودة الأصول (NPL).

2 – لا يوجد تأثير للمتغيرات المستقلة على الإجراءات الخاصة بتطبيق معيار أمن المعلومات ISO 27001 ومدى سرعة معالجة تهديدات أمن المعلومات، ونظام حماية الخدمات المصرفية (الإلكترونية على أي من المتغيرات التابعة التالية: معدل العائد على الأصول ومعدل العائد على الملكية ومعدل العائد على رأس المال ومعدل التغير النسبي في السعر وجودة الأصول).

■ **النتائج**

1 - يتم رفض فرض العدم وقبول الفرض البديل، حيث يوجد تأثير معنوى للاستجابة لسرعة معالجة تهديدات أمن المعلومات على معدل العائد على الأصول، ونظام حماية الخدمات المصرفية الالكترونية على معدل العائد على الملكية والإجراءات الخاصة بتطبيق معيار أمن المعلومات ISC 27001 على معدل العائد على رأس المال.

2 - يتم رفض فرض العدم و قبول الفرض البديل، حيث يوجد تأثير معنوى للإجراءات الخاصة بتطبيق معيار PCI-DSS لحماية كروت الائتمان على جودة الأصول من خلال خفض نسبة مخصصات خسائر القروض.

3 - . تتأثر ربحية المصرف بسياسة أمن المعلومات من خلال وضع إطار عام لنظام إدارة أمن المعلومات.

4 - تقييم مخاطر أمن المعلومات باستخدام نظام تشفير لنقل البيانات من خلال الشبكات العامة، وحماية خصوصية البيانات المتبادلة بين الموقع والمستخدمين.

5 - اتخاذ القرارات الرشيدة لحماية بيانات العملاء والإجراءات الخاصة بحماية كروت الائتمان تؤدي إلى خفض نسبة مخصصات خسائر القروض، وبالتالي تؤثر على جودة الأصول بالمصارف محل الدراسة.

■ **التوصيات**

1. الاستثمار في تدريب العاملين بإدارة أمن المعلومات لمعرفة واستخدام وسائل الحماية ضد مخاطر أمن المعلومات، ومواكبة أحدث الاتجاهات في مجال الابتكار المصرفى وتأمين بيانات العملاء.

2. رفع الوعي المجتمعي وكذلك عملاء المصارف بتقنيات الحماية للخدمات المصرفية الإلكترونية الخدمات (المصرفية عبر الانترنت - المصرفية عبر الهاتف المحمول).

3. تحقيق التوازن الجيد بين إضافة عوامل الآمان على القنوات التقنية المصرفية

للحفاظ على أموال وبيانات العملاء وإتاحة الخدمات على مدار اليوم للحماية من عمليات الاختراق وتقديم خدمات جديدة تلبي احتياجات العملاء والحفاظ على التوازن بين الابتكار والتطوير وتأمين بيانات العملاء.

4. إصدار قانون لحماية البيانات الخاصة من أجل تدعيم خصوصية بيانات العملاء والحفاظ على سريتها.

5. حرص المصارف على الالتزام بالمتطلبات الرقابية منها معايير بازل الجديدة حيث يؤثر على استثمارات المصارف فى مجالات التكنولوجيا للعمل على تلبيه المتطلبات التكنولوجية وتوفير قدرات إدارة المخاطر بشكل أفضل.

6. توفير السبل والحلول للتوصل إلى رؤية واضحة للمخاطر لمواجهة الضغوط المتزايدة، ولتحقيق ميزة تنافسية داخل السوق الليبي.

7. مواكبة المصارف للقواعد الموضوعة من الجهات المنظمة للعمل المصرفي بجانب التطوير المستمر لأنظمة المعلومات لديها.

8. القيام ببحوث مستقبلية فى مجال دراسة أثر الاستثمار في أمن المعلومات على أداء الشركات وأثر تهديدات أمن المعلومات على عوائد الأسهم وأثر الدوافع للقيام بتهديدات لأمن المعلومات على أداء المصارف، وأثر مخاطر أمن المعلومات على أداء المصارف.

■ المراجع

● المراجع العربية:

- العبيدي، رائد عبد الخالق والمشهداني، خالد أحمد. (2018). إدارة المؤسسات المالية والمصرفية. الفيوم: دار الفلاح للبحث العلمي وتحقيق التراث.

- العمري، عبد الله بن عبد الرحمن. (2019). أمن المعلومات: مفهومه وأهميته ومجالاته وتحدياته. الرياض: دار الفكر العربي.

- الشوابكة، عدنان عواد(2019،دور إجراءات الأمن المعلوماتي في الحد من مخاطرأمن المعلومات في جامعة الطائف،مجلة دراسات وأبحاث مج 11عدد4 ص 164-187.

- العمري، عبد الله بن عبد الرحمن. (2019). أسس الأداء الوظيفي. الرياض: دار الفكر العربي.
- المركز القومى للمعلومات - الإدارة الفنية. (2016) مقدمة» عن سياسات ومعايير أمن المعلومات، » قسم الجودة والتطوير - وحدة المعايير، الإصدار الأول.
- عبد الجابر يوسف (2018) مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية فى الشركات الصناعية الاردنية» رسالة ماجستير ؛ كلية الأعمال - جامعة الشرق الأوسط.

● **المراجع الأجنبية:**

Ahmad, M., Rosalim, R., Yu Beng, L. & Fun, T. (2010) "Security Issues on Banking System, " International Journal of Computer Science and Information Technologies, Vol. 1 (ε.

Alber, N. (7.1) "Size Effect, Seasonality, Attitude to Risk and Business Banks, "Interntional Performance of Egyptian Research, Vol.v, No.1

Altamimi, T. (2011) "Information Security Risks for Internet Banking in Saudi Arabia, " a study submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Systems at the university of Sheffield.

Ambhire, V., & Teltumde, P. (11) "Information Security in Banking and Financial Industry, " International Journal of Computational Engineering & Management, Vol. Retrieved from http://www.ijcem.org 10

Arcuri, M., Brogi, M., & Gandolfi, G. (2014) "The Effect of Information Security Breaches on Stock Returns: Is the Cyber

www Bonnette, C. (..) "Assessing Threats to Information Security in Financial Institutions, " GSEC Certification Practical Assignment, Version 1.{b Option 1 Retrieved from http://sans.org

El-Bannany, M. (..) "Investment in Information Technology Systems and other Determinants of Bank Performance in the UK and Egypt, " Unpublished PhD Thesis, The Business School, Liverpool John Moore University

Emmanuel, A. (Y.11) "The Effect of Internet Banking on the Ghanaian Banking Industry A Case of CAL Bank, UNI Bank and PRUDENTIAL Bank, " A Thesis Submitted to the Institute of Distance Learning, Kwame Nkrumah University of Science and Technology in partial fulfillment of the requirement for the degree of commonwealth executive master of business administration, P.1.

Feruza, S., & Kim, T. (..) "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. " International Journal of Multimedia and Ubiquitous Engineering Y (Y).

- French, A. (Y1Y) "A Case Study on E-Banking Security-When Security Becomes Too Sophisticated for the User to Access Their Information," Journal of Internet Banking and Commerce 1Y).

Y) - Gayed, N., & Gayed, P., & Alber, N. (Y..) "Using the Marketing Approach to Evaluate Banking Performance: The Case of Egypt". Retrieved from http://ssrn.com/abstract=1014.AV Glaessner, T., Kellermann, T. & Mcnevin, V. (Y..Y). "Electronic Security: Risk Mitigation in Financial Transactions Public Policy