مجلة البحوث المحاسبية

https://abj.journals.ekb.eg/

كلية التجارة – جامعة طنطا

العدد : الرابع

ديسمبر 2023

أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي – دراسة تطبيقية

الدكتور

خالد محمد عثمان احمد

أستاذ مساعد بقسم المحاسبة

كلية التجارة– جامعة المنصورة

kmahmed191@gmail.com

أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي – دراسة تطبيقية

المستخلص:

أدت زيادة الهجمات السيبرانية الى زيادة الاهتمام بإجراءات الأمن السيبراني في البنوك، حيث انها أكثر عرضة من غيرها لهذه الهجمات. لذلك ركزت هذه الدراسة على اختبار أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي للبنوك. ولتحقيق ذلك تم اختبار هذه العلاقة على البنوك التجارية السعودية في الفترة من عام ٢٠١٨ الى عام ٢٠٢٢، اعتمادا على تصميم دليل للإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني الذي يستند على دليل الأمن السيبراني للبنوك الصادر عن هيئة سوق المال السعودية. ولقد خلصت نتائج الدراسة الى عدم وجود علاقة معنوية بين الإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني والأداء المالي في البنوك التجارية السعودية. كما تبين وجود علاقة طردية معنوية بين مقاييس تعقيد عمليات البنك المقاسة بإجمالي الودائع واجمالي الأصول والأداء المالي للبنك، في حين توجد علاقة عكسية غير معنوية بين مقاييس عدد الفروع وعدد العملاء وعدد الصرافات في علاقتها بالأداء المالي للبنك. كما اتضح وجود علاقة طردية معنوية عند اختبار العلاقة المشتركة بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني والأداء المالي للبنك. وقد اوصت الدراسة بضرورة إصدار معيار يتناول متطلبات إجراءات إدارة مخاطر الأمن السيبراني ومعيار آخر لمراجعتها، وادراج دليل للإفصاح عن هذه الإجراءات في القطاع المصرفي ضمن توصيات لجنة بازل، مع إلزام البنوك المركزية بالإفصاح عنها.

الكلمات المفتاحية: تعقيد عمليات البنوك، الإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني،الأداء المالي.

The Impact of the interaction between the complexity of banking operations and the Disclosure of Cybersecurity Risk Management Procedures on Financial Performance - An empirical study

Abstract:

The increase in cyberattacks has led to increase the emphasis on cybersecurity procedures in banks, as they are more vulnerable than others to these attacks. Therefore, I first develop a disclosure framework for cybersecurity risk management practices derived from the Saudi Capital Market Authority's cybersecurity guidelines and investigate whether this disclosure influences banks' financial performance using a sample of Saudi commercial banks over the period from 2018 to 2022. I, then, investigate whether the complexity of banking operations moderate this relationship. While I find insignificant relationship between the disclosure of cybersecurity risk management and the financial performance of Saudi commercial banks, I find a significant positive relationship between the financial performance of these banks and the complexity of banking operations as measured by total deposits and total assets. Also, I find inverse but insignificant relationship between banks' financial performance and the number of branches, the number of customers, and the number of ATMs. Interestingly, I find a significant relationship between the financial performance of Saudi commercial banks and the interaction between the complexity of banking operations, and the disclosure of cybersecurity measures.

The findings of this study have important policy implications and highlight the importance of issuing a standard for cybersecurity risk management procedures along with another standard for their audits, as well as including a disclosure guide for these measures in the banking sector within the recommendations of the Basel Committee, with central banks being obligated to disclose them.

Keywords : Complexity of banking operations, Disclosure of cybersecurity risk management Procedures, Financial Performance.

١/مقدمة:

أصبح من المسلمات، بل والضروريات التي تدعم استقرار واستمرار منشآت الاعمال استخدام الحلول القائمة على تكنولوجيا المعلومات، وبصفة خاصة التكنولوجيا المالية **(FinTech)** لتحقيق مزايا تنافسية نتيجة السرعة والمرونة والدقة في الأداء، وبصفة خاصة بالنسبة للبنوك نتيجة لزيادة ابتكارات وتطوير الخدمات المالية التي تحسن الكفاءة وتقلل التكاليف، بما يحسن تجربة المستخدمين. وقد نتج عن ذلك وتزامن معه زيادة مخاطر الامن السيبراني والجرائم الإلكترونية **(Murinde et.al, 2022)**، حيث تعتبر من أكثر المخاطر أهمية في جميع أنحاء العالم وفق **Allianz Risk Barometer** لعامي ٢٠١٩ و٢٠٢٠. وقد دفع ذلك المعهد الأمريكي للمحاسبين القانونيين لتطوير إطار عمل لتقارير إدارة الامن السيبراني لتعزيز الإفصاح عنه بما يفيد مستخدمي المعلومات المحاسبية**(Cheng et al., 2022)** وتزداد هذه المخاطر نتيجة التوسع في استخدام أنظمة المعلومات الإلكترونية والشبكات **(RSA, 2016)**، واستخدام تقنيات الثورة الصناعية الرابعة، والتي أدت الى زيادة التركيز على المهام التحليلية للمحاسب على حساب المهام الروتينية **(نافع،٢٠٢٢)**، وتطوير البنوك لنماذج جديدة للأعمال لتحسين الخدمات المالية، ومواجهة التحديات السيبرانية المختلفة لحماية العملاء **(Murinde et.al, 2022)** كما تطلب ذلك تخصيص مبالغ إضافية لإدارة المخاطر السيبرانية **(Kejwang, 2022).**

وتتعدد دوافع الهجمات السيبرانية حيث قد تكون عسكرية أو سياسية، الا ان الغالبية منها يكون لدوافع تجارية مثل هجوم **(WannaCry)** عام ٢٠١٧، وهجوم أشباح الشرق الأوسط **(APT34)** عام ٢٠١٩، وهجوم **(Target hack)** عام ٢٠١٣، والهجوم على شركة **(Yahoo)**عامي٢٠١٣و٢٠١٤،والذي نتج عنه تخفيض شركة **Verizon Communications**التي كانت تسعى لشراء **Yahoo** لسعر الصفقة بمقدار ٣٥٠ مليون دولار. إضافة الى انتشار الفيروسات مثل فيروس الفدية، وفيروس الدودة، وفيروس حصان طروادة، وفيروس القنبلة المنطقية **(شحاتة،٢٠٢٢؛Tariq, 2018)**. وتزيد مخاطر الأمن السيبراني في المنشآت المالية، حيث تبين ان ٧٠٪ من الخروقات السيبرانية تستهدف هذه المنشآت **(2021 Data Breach Investigations Report, Cybersecurity in Banking & Financial Institutions", Kaspersky, Cybersecurity in**

Financial Services,). وكذلك ظهور شركات التكنولوجيا الماليـــة مثل **Avant** و **Sofi** و **Adyen** و **Anti Financial**، والتي تقدم خدمات مصرفية اعتمادا على التقنية الالكترونية **(قوجيل وطيبة،٢٠٢٢)**. وتعمل البنوك على زيادة التطور التكنولوجي المستخدم لتحسين تجربة المستخدم وتبسيط العمليات المصرفية من خلال تطوير تقنيات الذكاء الاصطناعي والتحليل الضخم للبيانات واستخدام تقنيات الدفع الإلكتروني والمحفظة الرقمية والتحويل الفوري. وتزداد المخاطر السيبرانية نتيجة تطبيق هذه التقنيات، بما يستلزم ضرورة استخدام إجراءات للحماية من هذه المخاطر، وتقرر الإدارة مستوي الإفصاح المناسب عن هذه الإجراءات، بما يؤثر على الأداء المالي للبنك. وكلما زاد الوعي بإدارة مخاطر الأمن السيبراني زاد الاستثمار فيها، لتأثيره البالغ على الأداء المالي **(Francis et al.,2019)**.

ويعد قطاع البنوك هو الأعلى من حيث الإفصاح عن المخاطر السيبرانية **(موسي وآخرون،٢٠٢٣)**. خاصة البنوك السعودية بعد ان احتلت المملكة المركز الثاني عالمياً من بين ١٩٣ دولة، في المؤشر العالمي للأمن السيبراني الذي يصدره الاتحاد الدولي للاتصالات ووفق تقرير الكتاب السنوي للتنافسية العالمية لعام ٢٠٢٢ الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية، الذي يُعد من أكثر التقارير شمولية في العالم، بفارق بسيط يقدر بـــ٠.٤٦ عن الولايات المتحدة، والمركز الأول عربيا وفى الشرق الأوسط وآسيا، بما جعل البنوك السعودية تمتلك أحدث التقنيات والخدمات المصرفية عبر الإنترنت والتطبيقات المالية الذكية. إضافة الى تمتعها بأداء مالي قوي ومستقر، لوجود تشريعات وإجراءات صارمة للرقابة المالية، بما رفع تصنيفها الائتماني عالميا، وزاد الثقة فيها، وساعد على تحقيق الاستقرار والنمو المالي المستدام. كما تعد البنوك السعودية من أكبر البنوك في منطقة الشرق الأوسط وفقًا لبيانات عام ٢٠٢١، بإجمالي أصول تتجاوز ٨٠٠ مليار دولار، وتتميز بدرجة عالية من السيولة والكفاءة في إدارة المخاطر، إضافة الى تنوع استثماراتها، والتي منها الاستثمار العقاري والأسهم والتمويل الإسلامي. وقد ساعد هذا التنوع على تخفيض الأثر السلبي لتداعيات الازمات المالية العالمية مثل أزمة جائحة كوفيد-١٩، ومحافظتها على مستوى جيد من الأداء المالي.

من ناحية اخري يؤدي تعقيد عمليات البنوك الى زيادة المخاطر السيبرانية التي يتعرض لها البنك نتيجة زيادة معدل استهداف البنك من قبل المهاجمين بما يزيد مخاطر الهجمات

السيبرانية ، ويؤثر سلباً على أدائها المالي **(Zaki, & Hassan, 2018)** ، بما يلزم معه العمل على خفض المخاطر السيبرانية الناتجة عن التعقيد لتحسين سمعة البنك من خلال التوسع في الإفصاح عن قيام البنك بالإجراءات اللازمة للحد من هذه المخاطر لتلبية احتياجات الأطراف ذات العلاقة بالإفصاح عن كل المعلومات الهامة وفقا لنظرية الشرعية، كما تقضي نظرية الإشارة بالإفصاح عن المعلومات التي تقدم إشارات إيجابية للمستثمرين، حيث انه لم يتم الإفصاح، فإن ذلك يعطي إشارات سلبية. كما يساعد التوسع في الإفصاح عن هذه المعلومات على تخفيض تكاليف الوكالة.

١/١مشكلة الدراسة: تشكل مخاطر الامن السيبراني تهديداً حقيقياً للاستقرار المالي، وحيث تعد من أهم التحديات التي تواجه المنشآت في الوقت الحالي **(IIA, 2022)**، كونها أكثر المخاطر اثارة للقلق بعد الكوارث الطبيعية، خاصة المخاطر المالية في البنوك **(مخاطر الائتمان، ومخاطر السيولة، ومخاطر أسعار الفائدة، والمخاطر التشغيلية)**، بما يؤثر سلبا على الأداء المالي **(Gweyi ,2018)**، حيث توجد علاقة طردية معنوية بين الإدارة الفعالة للمخاطر المالية والأداء المالي **(Mwaura, 2020)**. وتزيد الهجمات السيبرانية على الأنظمة الرقمية للسيطرة على البيانات الحساسة، بغرض الابتزاز والسرقة. لذلك تزداد مطالبة العملاء بحماية البيانات وتحسين أمن المعلومات، من خلال تطوير إجراءات لإدارة مخاطر الأمن السيبراني – **يستخدم الباحث مصطلح إجراءات الامن السيبراني للتعبير عن إجراءات إدارة مخاطر الامن السيبراني في هذه الدراسة**– لتقليل الآثار السلبية للهجمات **(Tariq, 2018)**، وتحقيق السلامة والأمان واستقرار المجتمع **(Cheng et al., 2022)**. وتزداد أهمية دراسة هذه الإجراءات نتيجة التحول الرقمي والشمول المالي، وزيادة الاهتمام بالأمن السيبراني، رغم عدم صدور معيار للتقرير عنه **(على وصالح، ٢٠٢٢)**.

وتهدف إجراءات الأمن السيبراني الى حماية الأفراد والأنظمة من الاختراقات السيبرانية، وتجنب تعريض المعلومات الحساسة للخطر، وتأمين الأساليب التقنية اللازمة لتحسين عمليات التشغيل وجودة الخدمات المقدمة لتحقيق مزايا تنافسية **(Khanom, 2020; Adiloglu & Gungor, 2019، العيسوي وأبو النصر،٢٠٢٠)**، من خلال تطبيق إرشادات وإجراءات فعالة من أشهرها وأكثرها قبولا معياري **ISO 27001;27002 (Kejwang, 2022)**. إذ

يؤثر تطبيق هذين المعايرين إيجابا على الأداء المالي للمنشآت ويحسن السمعة التجارية (Bokhari & Manzoor ,2022). إضافة الى المعايير المحلية الخاصة بالبنوك ومن أهمها الدليل الاسترشادي للبنوك الصادر عن هيئة سوق المال السعودية، والذي استفاد من المعايير السابقة. وتزداد أهمية تطبيق هذه الإجراءات بسبب التحولات الرقمية بواسطة المحمول والخدمات السحابية والوسائط الاجتماعية ووسائط الإنترنت للرغبة في زيادة ثقة المستهلك وتحسين الأداء المالي (Lee,2021; Kejwang, 2022). إذ تعاني المنشآت التي تتعرض لهجمات سيبرانية من تراجع في الأداء المالي، نتيجة ارتفاع تكاليف معالجة آثار الهجمات الإلكترونية وتكاليف استقطاب والاحتفاظ بالعمالة الماهرة، والخسائر المالية الناتجة عن تعريض البنية التحتية التكنولوجية للمنشأة للخطر، وتكلفة التقاضي او سداد تعويضات او احتمال فقد عملاء، والاضرار بسمعة المنشأة، بما يؤثر سلبا على الأداء المالي (Badawy,2021;IIA,2022;Gatzert&Schubert, 2022; Francis et al.,2019 **شرف،٢٠٢٣؛ أبو موسي، ٢٠٠٤**) لذلك يجب إجراء مزيداً من الأبحاث في هذا المجال لبيان هذه الإجراءات وكيفية الإفصاح عنها (Alrazoq et. al, 2020) ، حيث يؤثر الإفصاح عن إجراءات الأمن السيبراني على رد فعل السوق، لذلك يلزم الامر دراسة أثر هذا الإفصاح على الأداء المالي (**موسي وآخرون،٢٠٢٣**).

ويزيد الإفصاح عن إجراءات الأمن السيبراني من المصداقية والدقة والثقة في البيانات المالية المرتبطة بالأداء، نتيجة زيادة ثقة أصحاب المصالح في هذه البيانات، بما يساعد في جذب عملاء جدد، ويحسن من فعالية التعامل مع المخاطر التشغيلية والمالية، وبصفة خاصة للبنوك. بسبب زيادة تعرضها للهجمات السيبرانية،وكثرة استخدام هذه الإجراءات(**رشوان وقاسم،٢٠٢٢**)، لوجود كم هائل من البيانات والمال المتداول فيها(Kejwang, 2022) ، ويؤكد ذلك استهداف أكثر من نصف بنوك العالم بنوع واحد على الأقل من الهجمات الإلكترونية (Security Intelligence Solutions, 2020). مثل هجوم بنك (Societe Generale Hack) في فرنسا في عام ٢٠١٤، وهجوم (Burma Hack)على بنوك جنوب شرق آسيا عام ٢٠١٦، وهجوم (WannaCry) على البنوك عام ٢٠١٧، وهجوم بنك (Banco de Chile Hack) في تشيلي عام ٢٠١٨. كما يتوقع ان تتجاوز تكلفة الجرائم السيبرانية للمنشآت

المالية حول العالم ١٠ تريليون دولار بحلول عام ٢٠٢٥. لذلك تسعي البنوك لتطبيق وتطوير إجراءات فعالة لإدارة الأمن السيبراني والافصاح عنها لتأثيرها على الأداء المالي (موسي وآخرون،٢٠٢٣; Data Breach Investigations Report, 2021).

وتزداد أهمية دراسة الإفصاح عن إجراءات الامن السيبراني في البنوك، نتيجة امتداد مخاطر الأمن السيبراني لجميع أنشطة البنوك، مثل إجراء المدفوعات واستلامها، والادخار والاستثمار، والاقراض، وإدارة المخاطر والمدخرات، وإدارة العملات النقدية واستخدام خدمات الدفع الإلكتروني، والخدمات الرقمية عبر مواقعها وخدمات الحوسبة السحابية. إضافة الى استخدام التطبيقات البنكية على الهواتف الذكية لتقديم الخدمات المصرفية عبر الهاتف، بما يزيد من مخاطر تسرب البيانات أكثر من الحاسب الآلي (Nechai et al., 2020)، لسهولة اختراق المعلومات الشخصية عبر الشبكات اللاسلكية على تطبيقات الهواتف الذكية (Atkinson et al., 2018)، بما يؤثر سلبا على سمعة البنوك (Bokhari & Manzoor, 2022) إضافة لوجود تداعيات متتالية على أصحاب المصالح وتحملهم خسائر أكبر عند حدوث اختراق سيبراني، بما يؤثر على الأداء المالي في الاجل القصير والطويل. لذلك يجب استخدام إجراءات وتقنيات قوية جدا وفعالة لإدارة مخاطر الأمن السيبراني لتقليل الخسائر المباشرة وغير المباشرة، كما يجب توطين الإجراءات الأمنية لإدارة المخاطر السيبرانية وتقييمها بشكل منتظم للتأكد من فعاليتها واتفاقها مع المعايير الدولية (Cybersecurity in the Financial Sector: Threats & Solutions", Investopedia, Cybersecurity in Banking & Financial Institutions", Kaspersky, Cybersecurity in Financial Services,)

ومن ناحية اخري يؤثر تعقيد عمليات البنوك على الأداء المالي (Nyola et al,2021;Larsen et al, 2019; Audretsch, & Belitski, 2021) ، من خلال زيادة المخاطر السيبرانية التي يتعرض لها البنك، نتيجة زيادة معدلات استهداف البنك من قبل المهاجمين، بما يلزم معه ضرورة التوسع في الإفصاح عن معلومات إجراءات التعامل مع هذه الهجمات، كونها معلومات هامة للأطراف ذوي العلاقة تطبيقا لنظرية الشرعية، حتى لو كانت هذه المعلومات غير جيدة. وتؤكد نظرية الإشارة نفس النتيجة، لأن التوسع

في الإفصاح عن هذه المعلومات يعطي إشارات إيجابية للمستثمرين عن نجاح البنوك في وضع إجراءات فعالة ومناسبة للتعامل مع آثار الهجمات السيبرانية. ومن ناحية اخري يزداد طلب المستثمرين والمحللين على هذه المعلومات لأهميتها في تقييم الاداء وتحديد درجة الاستقرار الاقتصادي للبنوك. وإذا لم يتم الإفصاح من قبل البنك، فستصل هذه المعلومات الى المستثمرين والمحللين الماليين من مصادر اخري في السوق تكون اقل موثوقية، بما يعطي إشارات سلبية (**النقيب، ٢٠٢٠**). كما يجب التوسع في الإفصاح عن إجراءات الأمن السيبراني الناتج عن زيادة المخاطر السيبرانية بسبب تعقيد عمليات البنك، غير ان تعارض المصالح بين الإدارة والملاك وفقا لنظرية الوكالة يؤدي الى عزوف المديرين عن التوسع في الإفصاح للرغبة في تخفيض هذه المخاطر، رغم مزايا التوسع في الإفصاح لتخفيض تكاليف الوكالة. ويري الباحث زيادة هذا التأثير بالنسبة للبنوك السعودية، كونها من اعلى البنوك تطبيقا لإجراءات الامن السيبراني في منطقة الشرق الأوسط.

ويعتقد الباحث بوجود أثر للعلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي للبنوك، حيث يزيد تعقيد العمليات من المخاطر السيبرانية، ومن الإفصاح عن إجراءات الحماية منها، بما يستلزم دراسة هذه العلاقة. غير ان هذا الاعتقاد يتطلب وجود دليل تطبيقي يؤكد ذلك او ينفيه في ظل عدم وجود دراسات سابقة تناولت هذه العلاقة في البنوك السعودية على حد علم الباحث. ويمثل ذلك إضافة علمية.

يتضح بما سبق أن الإفصاح عن إجراءات الامن السيبراني وتعقيد عمليات البنوك يؤثران على الأداء المالي، بما يبرر زيادة الاستثمار في الأمن السيبراني. لذلك يتمثل موضوع هذه الدراسة في أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي – دراسة تطبيقية. وتتمثل تساؤلات الدراسة في أربعة تساؤلات، الأول ما هو أثر اختلاف مستوي الإفصاح عن إجراءات الأمن السيبراني بين البنوك التجارية السعودية؟ والثاني ما هو أثر الإفصاح عن إجراءات الأمن السيبراني على الأداء المالي للبنوك؟ والثالث ما هو أثر تعقيد عمليات البنك على الأداء المالي للبنوك؟ والرابع ما هو أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات الأمن السيبراني على الأداء المالي؟

١/٢-أهداف الدراسة: تتمثل في أربعة اهداف رئيسية، أولهما قياس اختلاف مستوي الإفصاح عن إجراءات الأمن السيبراني بين البنوك السعودية، وثانيهما اختبار العلاقة بين الإفصاح عن إجراءات الأمن السيبراني والأداء المالي للبنوك، وثالثهما اختبار العلاقة بين تعقيد عمليات البنك والأداء المالي للبنوك، اما الرابع فهو اختبار أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات الأمن السيبراني على الأداء المالي. وسيتم التطبيق على البنوك التجارية السعودية لتقديم دليل تطبيقي عملي.

١/٣-أهمية الدراسة: تتمثل الأهمية العلمية للدراسة في أهمية دراسة العلاقات بين الإفصاح عن إجراءات الامن السيبراني والأداء المالي في البنوك، وفق الدليل الاسترشادي للبنوك للأمن السيبراني في السعودية، والتي احتلت المركز الثاني عالمياً في المؤشر العالمي للأمن السيبراني. إضافة الى دراسة أثر تعقيد عمليات البنك على الأداء المالي، ثم اختبار أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات الأمن السيبراني على الأداء المالي. وتمثل دراسة هذه العلاقات أهمية بحثية في الفكر المحاسبي المعاصر، كما تعد الدراسة الحالية استجابة لتوصية دراسات سابقة بزيادة اهتمام الدراسات الأكاديمية التي تهتم بتأثير الإفصاح المحاسبي عن الأمن السيبراني على الأداء المالي (**الأمير،٢٠٢٢**). اما الأهمية العملية فتتمثل في تقديم دليل تطبيقي مبني على بيانات فعلية لاختبار العلاقات السابقة، من خلال تقديم نماذج احصائية لاختبارها في السوق السعودي، بما يساعد متخذي القرارات والجهات المهنية في تحديد مستوي الإفصاح المناسب عن معلومات إجراءات الأمن السيبراني في ظل تعقيد عمليات البنك. وتزداد هذه الأهمية نتيجة ندرة هذه الدراسات في السعودية والمنطقة، حيث انها الدراسة الاولي- في حدود علم الباحث- التي تختبر هذه العلاقات بالاعتماد على بيانات فعلية، وبصفة خاصة اختبار علاقتين على درجة عالية من الأهمية، الأولى أثر تعقيد عمليات البنك على الأداء المالي للبنوك، والثانية أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات الأمن السيبراني على الأداء المالي.

١/٤-منهج الدراسة: تعتمد الدراسة على المنهج الاستقرائي من خلال مراجعة الدراسات السابقة والتقارير السنوية والمواقع الإلكترونية الخاصة بإدارة الامن السيبراني لتناول علاقة الإفصاح عن إجراءات الأمن السيبراني وتعقيد عمليات البنك بالأداء المالي، وبناء الإطار

النظري للبحث واشتقاق الفروض. ويستخدم المنهج الاستنباطي لاقتراح نماذج لاختبار العلاقات السابقة، وفحص التقارير السنوية للبنوك السعودية، والمنهج التحليلي لتحليل بيانات الدراسة التطبيقية واختبار الفروض. وقد تم تجميع البيانات من التقارير المالية المنشورة للبنوك السعودية خلال الفترة من ٢٠١٨ الى ٢٠٢٢، واستخدم الباحث أسلوب الانحدار المتعدد.

١/٥- حدود ونطاق الدراسة:

-لا تتطرق الدراسة الى الأساليب التكنولوجية المستخدمة في الأمن السيبراني.

-تقتصـــــر الدراســـــة على المعايير الأكثر قبولا عالميا لإدارة مخاطر الامن السيبراني وهما**ISO 27001;27002** ودليل الهيئة الوطنية السعودية للأمن السيبراني، وإجراءات الأمن السيبراني وفق الدليل الاسترشادي للبنوك للأمن السيبراني في السعودية. وقد اقتصرت الدراسة التطبيقية على الدليل الأخير، كونها تركز على البنوك السعودية.

-ركزت الدراسة على استخدام العائد على الأصول كمقياس لتقييم الأداء المالي للبنك.

١/٦- فروض الدراسة التطبيقية: تم تحديد الفروض في صورتها العدمية بما يتفق مع أهداف الدراسة كما يلي:

الفرض الأول: لا يختلف مستوي الإفصاح عن إجراءات الأمن السيبراني بين البنوك التجارية السعودية.

الفرض الثاني: لا توجد علاقة معنوية بين الإفصاح عن إجراءات الأمن السيبراني والأداء المالي للبنوك.

الفرض الثالث: لا توجد علاقة معنوية بين تعقيد عمليات البنك وادائه المالي.

الفرض الرابع: لا يوجد تأثير معنوي للعلاقة(التفاعلية) المشتركة بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك.

١/٧-مجتمع وعينة الدراسة: يتمثل مجتمع الدراسة في جميع البنوك السعودية المرخصة من قبل البنك المركزي السعودي والمقيدة في هيئة سوق المال السعودية (تداول) خلال الفترة من عام ٢٠١٨ الى عام ٢٠٢٢ وعددها ١٣ بنك.وتتمثل العينة في البنوك التي توفرت فيها جميع بيانات متغيرات الدراسة، وعدم تغير السنة المالية خلال فترة الدارسة، ووجود تداول نشط على أسهمها. وقد تم استبعاد بنكين نظرا لأنهما حصلا على الترخيص ولم

يزاولا النشاط وهما بنك إس تي سي والبنك السعودي الرقمي. كما استبعد بنك الخليج الدولي – السعودية لعدم توافر بياناته، ليصبح عدد البنوك ١٠ بنوك، وعدد المشاهدات ٥٠مشاهدة. ويتسق حجم هذه العينة مع العديد من الدراسات السابقة في السوق السعودي مثل **(Al-Sheikh& Al-Olyan,2020; Al-Shammary & Al-Samayi,2021)**

٨/١- **تنظيم الدراسة:** يتم تنظيم الجزء المتبقي من الدراسة من خلال التعرض للجوانب التالية:

٢-الامن السيبراني: المفهوم والخصائص والعناصر.

٣-إجراءات إدارة مخاطر الامن السيبراني وأهم ارشاداته.

٤-علاقة إجراءات إدارة مخاطر الامن السيبراني بالأداء المالي.

٥-الإفصاح عن إجراءات إدارة مخاطر الامن السيبراني.

٦-علاقة تعقيد عمليات البنك بالأداء الأداء.

٧-اشتقاق وصياغة الفروض

٨-الدراسة التطبيقية.

٩-النتائج والتوصيات والبحوث المستقبلية.

٢-الامن السيبراني: المفهوم والخصائص والعناصر: يركز الأمن السيبراني **Cyber security** على تصميم وتطبيق التقنيات والضوابط والممارسات اللازمة لحماية الأنظمة والبرامج وشبكات الحواسيب والبيانات من التعرض للفيروسات والبرامج الإلكترونية الخبيثة، وسد ثغرات نقاط الضعف المباشرة أو غير المباشرة. ويعبر مفهوم الأمن السيبراني لأنظمة المحاسبة عن درجة الحماية والتامين للعمليات المحاسبية من خلال توفير تقنيات وبرمجيات لتأمين الخصوصية ومنع الاختراق السيبراني الداخلي والخارجي للبيانات والأجهزة والبرمجيات والعمليات المحاسبية **(Boss et al., 2022; Janvrin& Wang, 2022)**، لتجنب تعرض المنشأة لخسائر مالية وغير مالية، نتيجة الإضرار بسرية ونزاهة البيانات والمعلومات في الفضاء السيبراني، بما يؤثر على تحقيق أهدافها واستمراريتها **(موسي وآخرون،٢٠٢٣).** وتزيد هذه المخاطر نتيجة توسع المنشآت في استخدام تكنولوجيا المعلومات، وارتفاع تكاليف معالجة آثار الهجمات الإلكترونية والخسائر المالية، والإضرار بالسمعة. كما تطالب القوانين

والعملاء المنشآت بحماية البيانات، ولذلك تسعي المنشآت لتطوير إجراءات للحماية من الهجمات الإلكترونية (Tariq, 2018).

ويتكون الامن السيبراني من سبعة عناصر أساسية هي: ***الأشخاص*** المخولون بإدارة الأمن السيبراني، والتحقق من التهديدات الإلكترونية، وتأمين الرد السريع، و***السُلطة*** الممنوحة للمسؤول للقيام بالتغيرات التنظيمية المطلوبة، و ***دعم الإدارة العليا*** لإدارة الأمن السيبراني لضمان نجاحها، و***المنهجية الفعّالة*** القادرة على إدارة ومواجهة المخاطر الإلكترونية، وتحديد سبل الاستجابة الفعّالة، و***التقنيات المناسبة المُستخدمة*** لمواجهة التهديدات المُكتشفة، و***التوقيت المناسب للتواصل*** من خلال التنسيق بين فريق الأمن السيبراني ومسؤولي الشبكات،ومهندسي الأنظمة، والإدارة، وغيرهم، و***الموازنة المناسبة المخصصة*** **Components of Cyber Security, 2021)**. كما يُصنف الأمن السيبراني إلى عدة أنواع، أشهرها: **أمن الشبكة** لمنع الهجمات على الشبكة وتأمينها. و**أمن التطبيقات** لتصميم برامج مضادة للفيروسات، وجدران الحماية، وتشفير المعلومات وحماية الأجهزة. و**الأمن التشغيلي** لحماية ومعالجة وتخزين ومشاركة البيانات وتحديد الأذونات المسموح بها للمستخدمين. و**الأمن السحابي** لتأمين السحابة الرقمية. و**أمن البنية التحتية** لتأمين الحماية المادية والإمداد بالطاقة والتبريد. و**أمن المعلومات** للحفاظ على سلامتها وخصوصيتها وسريتها وتخزينها ونقلها. و**رفع الوعي الأمني للمستخدم النهائي** وتثقيفه لتجنب إدخال فيروسات. و**التعافي من اثار الهجمات الإلكترونية** وتحديد سياسات التعافي بهدف استمرارية العمل والعودة إلى نفس القدرة التشغيلية السابقة. و**أمن الأجهزة** المتصلة بالأنترنت من خلال مراقبة أي عملية استغلال لها **(Difference Between Cybersecurity & Information Security, 2021)**. ويتميز الامن السيبراني بعدة خصائص، أهمها: الثقة وعدم الثقة، حيث يتم التعامل مع كل البرامج والتقنيات والروابط على أنها غير جديرة بالثقة، ويسمح فقط بمرور الموثوق منها. والحماية من التهديدات الداخلية الناتجة عن انخفاض وعي الموظفين، حيث تبين أنها أخطر التهديدات **(Alqahtani, 2017;Ki-Aries & Faily,2017)** والحماية من التهديدات الخارجية من خلال بناء جدار حماية يعمل على مدار الساعة كمرشح إلكتروني لتصفية المخاطر الرقمية الخارجية، ومعالجة ثغرات النظام. وتحقيق رؤية شاملة على نقاط القوة والضعف والثغرات التكنولوجية المحتملة

التي تؤثر على تقييم الأداء المالي، والعمل على حلها بأسرع وقت، وتقديم مقترحات تمنع تكرارها **(Kejwan ,2022)**.

وتتعدد مخاطر الأمن السيبراني، فمنها المخاطر التكنولوجية والتشغيلية والتنظيمية الناتجة عن اختراق النظام **(Badawy, 2021; Hartmann & Carmenate, 2021)**، ومخاطر الأداء التي تعبر عن فشل الأدوات التقنية في تحقيق أهدافها، ومخاطر الاختراق المادي، والتجسس الموجي **Eavesdropping on Emanations** عن بعد، والمخاطر المرتبطة بالعاملين نتيجة استغلال العلاقات الاجتماعية للوصول غير المرخص به. أما مخاطر المعلومات والاتصالات فتتضمن الهجمات على البيانات، لإحداث اضطراب في العمليات التجارية أو إلحاق خسارة مالية، أو الإضرار بسمعة المنشأة المخترقة **(شحاتة،٢٠٢٢)**. لذلك تحافظ المنشآت على مستوى عالٍ من الأمن السيبراني وتضع التدابير الوقائية لمواجهة الهجمات المحتملة **(Tariq, 2018; Kejwang, 2022)**، من خلال القيام بمجموعة من الإجراءات مثل القيام بهجوم تجريبي متعمد لاكتشاف الثغرات والعمل على إصلاحها، وتصميم إجراءات الاستجابة والتخفيف من آثار التعرض للخطر أو الوصول غير المرخص به، واستخدام الدرع السيبراني كجدار حماية فعال لاكتشاف الثغرات **(Alqahtani, 2017)**.وتتمثل أهم تهديدات الامن السيبراني في: البرمجيات الخبيثة(الفيروسات)، مثل فيروس الفدية الذي يحجب بيانات الضحية ويشفرها، حتى يتم دفع فدية مالية. والبرامج الثنائية أو هجوم الوسيط، وفيها يستغل المهاجم لجوء الضحية إلى مصدر تقني آخر ضعيف الحماية، ويدخل إلى النظام من خلاله كاستغلال شبكة الواي فاي واختراق الأجهزة المشتركة فيها. والتصيد المباشر للمعلومات من خلال مشاركة معلومات حساسة أو سرية. وتعد نسبة عمليات التصيد الاحتيالي للمعلومات ٨٠٪ من الهجمات الإلكترونية، كما تبين ان ٧١٪ من الهجمات يركز على سرقة تفاصيل تسجيل الدخول **(Ukwandu et al.,2022)**. والتسلسل المتقدم طويل الأمد، والذي يتم بشكل خفي وتدريجي، ولا يتم اكتشافه إلا بعد مرور فترة زمنية طويلة، يكون الضرر قد وقع بالفعل . وهجمات رفض الخدمة وفيها يتم تكثيف حركات المرور والرسائل لمستخدمين وهميين، للضغط على الخوادم وتعطيلها أو جعلها بطيئة. وتمثل نسبة هذه الهجمات **25٪ (Ukwandu,et al., 2022)**. وتؤثر كل هذه المخاطر على أمن المعلومات المحاسبية وعلى الأداء المالي، بما يبرر تفعيل

إجراءات الأمن السيبراني، والتي تساعد في حماية البيانات والمعلومات، كما تضمن تطبيق برامج وآليات متطورة للدفاع الإلكتروني بما يضمن استقرار المجتمع(**Cheng et al., 2022**) ولذلك يتطلب الامر دراسة علاقة هذه الإجراءات بتقييم الأداء (**على وصالح، ٢٠٢٢؛ شرف، ٢٠٢٣**)، خاصة في ظل عدم صدور معيار ينظم إعداد تقرير عن إجراءات الأمن السيبراني (**على وصالح، ٢٠٢٢**). وترتبط جميع هذه الإجراءات بالأمن المالي للمعاملات وقرصنة البيانات المالية، والتي ترتبط بأداء وظيفة المحاسبة والدورة المحاسبية، كما تساعد في تقديم حلولٍ مبتكرة عند الهجوم على قواعد البيانات، لحمايتها من التهديدات. لذلك تهتم البنوك بإجراءات إدارة مخاطر الامن السيبراني، وهذا ما سيتم تناوله في الجزئية التالية.

٣- **إجراءات إدارة مخاطر الأمن السيبراني وأهم ارشاداته:** ويقصد بها تحديد الإجراءات الرقابية والتقنيات اللازمة لدعم الفضاء الالكتروني والحماية من التهديدات السيبرانية للحد من أو تلافي حدوث حالات الاحتيال أو انتشارها (**دليل مكافحة الاحتيال المالي في البنوك والمصارف العاملة في المملكة العربية السعودية،٢٠٢٠،شرف،٢٠٢٣، AICPA,2017**)، بهدف تقليل المخاطر المحتملة، وتطوير خطط للطوارئ والاستجابة والتعاون مع الجهات الحكومية المعنية، واتخاذ الإجراءات التصحيحية اللازمة، وتقييم تأثيرها على الأداء المالي (**Kejwang, 2022**)، لضمان استمرارية تطوير استراتيجيات شاملة لحماية السلامة الإلكترونية، بما يفيد في التنبؤ باتجاهات الهجمات المستقبلية، وتنفيذ تدابير استباقية للحماية لتحسين جودة الخدمات التي تؤثر على ثقة العملاء، بما يحسن الأداء المالي. وتزداد أهمية هذه الإجراءات في البنوك بسبب زيادة الطلب على تكنولوجيا المعلومات كمورد اقتصادي لتحقيق ميزة تنافسية، ووجود دفع أموال الكتروني، ومشاركة بيانات حساسة، بما يزيد من التهديدات السيبرانية، والاعتماد على تقنية الخدمات السحابية وضرورة حماية المستخدمين (**رشوان وقاسم، ٢٠٢٢؛ Bokhari, & Manzoor, 2022; Hung et al., 2019; Wu et al., 2021 ;Kejwang, 2022**) لذلك تستثمر البنوك في إجراءات الأمن السيبراني، كما تسعي لتعزيز الإفصاح عنها على مواقعها الالكترونية (**Ukwandu,et al.,2022 ;Cheng et al., 2022,Hsu et al.,2016**).

ولقد اهتمت جهات متعددة بإصدار إرشادات لإدارة مخاطر الأمن السيبراني. ويركز الباحث بالنسبة لهذه الارشادات على **ISO 27001;27002**، كونهما أكثر المعايير استخداما وقبولا على المستوي العالمي **(Malatji, 2023)**، ودليل الهيئة الوطنية السعودية للأمن السيبراني، والدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية، ودليل الأمن السيبراني للبنوك الصادر عن هيئة سوق المال السعودية كونها من أفضل الارشادات المقدمة عربيا **(انديجاني وفلمان، ٢٠٢١؛ الجهني وآخرون،٢٠٢٠)**. ولقد استفادت الارشادات المحلية السعودية من الارشادات الدولية.

– معيار **ISO/IEC 27001**: يعد إطاراً مؤسسياً دولياً شاملاً يوفر المتطلبات الأساسية لإدارة مخاطر الأمن السيبراني، من خلال تحديد المخاطر المحتملة التي تواجه الأشخاص والعمليات وأنظمة تكنولوجيا المعلومات، وتوفير إجراءات وإرشادات بغرض تقييم وتقليل هذه المخاطر **(Bokhari & Manzoor,2022; Peng et al.,2019 ,Dao et al.,2017)** وتتضمن هذه الإجراءات تحديد نطاق نظام إدارة مخاطر الأمن السيبراني، وتطوير التدابير الأمنية اللازمة لتجنبها أو التخفيف منها وتقييم فعاليتها. وتتم مراجعة هذا التقييم على فترات دورية مخططة لضمان استمرار ملاءمتها وكفايتها أو عند حدوث تغييرات كبيرة، ومقارنة النتائج بالمعايير المحددة مسبقا، لتحسين إدارة أمن المعلومات الداخلية والخارجية. وتقع مسئولية إعداد هذه الإجراءات على الإدارة وفق اتجاهاتها الاستراتيجية وعملياتها التشغيلية، والموارد اللازمة للتطبيق، والموازنة بين السلطة والمسئولية، وتحديد الأشخاص المؤهلين ووسائل الاتصالات اللازمة، وفترة التنفيذ، والافصاح عن هذه الإجراءات، ويضاف الى ذلك تحديد الإجراءات التصحيحية لمواجهة أي اختراق سيبراني والتعامل مع اثاره، وإزالة أسباب تكرره، والعمل على تحسين ملاءمة وكفاية وفعالية هذه الإجراءات **(ISO 27001, 2022)** ، وتحسين معرفة الفريق التشغيلي بالمشاكل السيبرانية **(Nechai et al., 2020)**، وتحديد إجراءات التعامل مع الحسابات المجمدة، والمحافظة على الأمان المادي للأجهزة والأنظمة والشبكات **(Calder, 2017; Bokhari & Manzoor , 2022)**، وتعزيز الكفاءة التنظيمية، وجذب موظفين متميزين وتعزيز ثقة العملاء، وتحسين العلامة التجارية

(Mukundan & Sai, 2014). ويصلح تطبيق هذا المعيار لجميع أنواع المنشآت الصناعية والخدمية والمالية **(Bokhari, & Manzoor, 2022)**.

-معيار **ISO/IEC 27002** يعد مرجعاً توجيهياً يوفر إرشادات وممارسات محددة لتوحيد مفاهيم وإجراءات الأمن السيبراني وتنفيذ وتطبيق الممارسات الأمنية الصحيحة، مثل سياسات إدارة الوصول والتحكم، وحماية البيانات، وإدارة التحديثات والتغييرات الأمنية، وتنظيم أنشطة المراقبة والتدقيق. ويستخدم المعياران معًا لتحسين نظام إدارة الأمن السيبراني وتحسين فعالية إجراءاته وتقييمها وتحديثها بشكل دوري.

- **دليل الهيئة الوطنية السعودية للأمن السيبراني، ٢٠١٨:** حدد الدليل الضوابط الأساسية لإدارة مخاطر الأمن السيبراني في خمسة مكونات هي **حوكمة الأمن السيبراني Cybersecurity Governance**، **وتعزيز الأمن السيبراني Cybersecurity Defense**، **وصمود الأمن السيبراني Cybersecurity Resilience**، **والأمن السيبراني المرتبط بالأطراف الخارجية والحوسبة السحابية Third-Party & Cloud Computing Cybersecurity**، **والأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity**. ويحتوي كل مكون على مجموعة فرعية من العناصر**(الهيئة الوطنية السعودية للأمن السيبراني، ٢٠١٨)**.

- **الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية، ٢٠٢٠:** تضمن الدليل أربعة محاور هي: محور حوكمة الأمن السيبراني، والذي تضمن **(القيادة والمسئوليات وحوكمة وأمن البيانات والاستراتيجية والسياسات والتدريب والتوعية والأمن السيبراني المرتبط بالموارد البشرية)**. ومحور إدارة مخاطر الأمن السيبراني والمراجعة والتدقيق. ومحور ضوابط الأمن السيبراني للعمليات التشغيلية، والذي تضمن ١٦ مكون **(هيكلة الأمن السيبراني، أمن البنية التحتية، إدارة التغير وإدارة المشاريع، إدارة هويات الدخول والصلاحيات، إدارة الأصول المعلوماتية والتقنية، الاتلاف الأمني، إدارة حوادث الأمن السيبراني، إدارة سجلات أحداث الأمن، إدارة تهديدات الأمن السيبراني، حماية التطبيقات، التشفير، إدارة الثغرات، خدمات التداول الالكتروني، والأمن المادي، إدارة استمرارية الأعمال، استخدام الأجهزة الشخصية)**. ومحور أمن الأطراف الخارجية والموردين، والذي

تضمن ثلاثة مكونات (**إدارة العقود والموردين، والاسناد الخارجي، والحوسبة السحابية**). ويتضمن كل مكون فرعي منها تحديد الهدف والضوابط الإجرائية الأساسية اللازمة لتنفيذها.

- **دليل الأمن السيبراني للبنوك والصادر عن هيئة سوق المال السعودية:** ويتضمن الدليل ٧٧ ارشاداً واجراءً (يوضح الملحق رقم (١) تفاصيل هذا الدليل)، والتي تستخدم لحماية بيانات البنوك من التهديدات السيبرانية. وينقسم الدليل الى ست مجموعات فرعية هي: تعريف بالتهديدات السيبرانية والتحديات التي تواجهها البنوك، وكيفية التعامل معها، ومتطلبات الأمن السيبراني الأساسية للبنوك، ومتطلبات الأمان الإداري للبنوك، وإجراءات الاستجابة لحوادث الأمن السيبراني، ومتطلبات التدريب والتوعية الأمنية للموظفين في البنوك، ومتطلبات التدقيق والمراجعة الأمنية الدورية للبنوك. وسوف تركز هذه الدراسة على الإفصاح عن إجراءات الامن السيبراني وفقا لهذا الدليل عند القيام بالدراسة التطبيقية. وتؤثر جميع هذه الإجراءات على الأداء المالي للبنوك. لذلك تركز الجزئية التالية على هذه العلاقة.

٤- علاقة إجراءات إدارة مخاطر الأمن السيبراني بالأداء المالي: يعبر الأداء المالي عن كفاءة الإدارة في استخدام وإدارة الأصول المتاحة، بما يُرشد التكاليف ويحسن استغلال الموارد، ويعظم العوائد، ويزيد حجم المعاملات وعدد العملاء، ويساعد أصحاب المصالح على اتخاذ قراراتهم الاقتصادية الرشيدة، والحكم على كفاءة وفعالية الإدارة، من خلال الاستغلال الأمثل للموارد والفرص المتاحة، وحماية أصولها من المخاطر السيبرانية، ووضع سيناريوهات واجراءات واضحة للتعامل مع الظروف الطارئة (**موسي وآخرون،٢٠٢٣؛ Mulyana & Adidarma, 2020**) وتتعدد مقاييس تقييم الأداء المالي، حيث تبين أن أكثرها استخداما من بين المقاييس المحاسبية معدل العائد على الأصول بنسبة ٤٦٪، و٥٤٪ لبقية المقاييس الأخرى (**Al-Matari et al., 2014**)، واستخدمه العديد من الدراسات مثل (**Pedron et al.,2021; Wulandari et al.,2019;Kouaib & Amara,2022**). كما يعتمد تحسن الأداء المالي للمنشآت على قدرتها على التوافق مع التغيرات البيئية والتكنولوجية المحيطة (**Liu et al., 2022**). وتعد إجراءات الأمن السيبراني أحد اهم هذه التغيرات، بشرط توافر مقومات نجاحها، والتي تتمثل في الفهم الشامل، وتبرير استثماراتها، وبرامج إدارة ثغرات الأمن السيبراني وإدارة الحوادث، ومراقبة الشبكة. ويتم ذلك وفق

جداول زمنية للتطبيق (Abdulrahim ,2019) . وتضمن هذه الاجراءات تحسين كفاءة وفعالية تقنيات الأمن السيبراني، وتعزيز الوعي بثقافته لدي الموظفين (**انديجاني وفلمان**، ٢٠٢١، Alqahtani, 2017)، من خلال تحديد أفضل الإجراءات الوقائية والتصحيحية لتحقيق التحسين المستمر، واعتماد منهجية مرنة للتعامل مع المخاطر السيبرانية (**على وصالح**،٢٠٢٢)، وتطوير إجراءات الاستجابة لضمان السرعة عند وقوعها.

كما تبين وجود علاقة معنوية بين اجراءات الامن السيبراني وتقييم الأداء المالي للحصول على شهادة ISMS ISO 27001 نتيجة تطبيق اجراءاته (Wu et al.,2021;Hsu et al.,2016;Nechai et al.,2020 Bokhari&Manzoor,2022;Velasco et al.,2018) من خلال تخفيض النفقات الزائدة (Han et al., 2017) وتحقيق مزايا تسعيرية، بما يؤثر بشكل إيجابي على سمعة المنشأة (Kamdjoug et al.,2018; Bokhari & Manzoor, 2022; Tewamba et al.,2019) ويحسن الإفصاح عن إجراءات الأمن السيبراني من كفاءة قرارات الاستثمار والذي ينعكس إيجابا على الأداء المالي(**على وصالح**،٢٠٢٢)، من خلال تحسين تصورات وانطباعات الأطراف ذوي المصلحة عن قيام المنشاة بمسئولياتها الاجتماعية في الحماية السيبرانية، كما يعزز رضا العاملين، ويعزز التتبع الإيجابي من الخبراء الماليين، بما يساعد في جذب عملاء جدد، وتحسين العلامة التجارية، والقيمة السوقية (Tien et al., 2020). ويساعد ذلك في تبرير تكاليف الاستثمار في تقنيات الأمن السيبراني (Kamdjoug et al., 2018; Ki-Aries & Faily, 2017; Tewamba et al., 2019) ، رغم صعوبة هذا التبرير لأن المنافع تكون غير واضحة كما أن هذه التكاليف تعتبر ثابتة اختيارية قد تتجنبها الإدارة للرغبة في تحسين الدخل تحت مبرر أن "لا شيء يحدث" (Menon & Siponen, 2020) ، حيث يفضل المديرون التنفيذيون الأساليب العلاجية وليس الوقائية بما يزيد من تكلفة الأضرار (Bokhari & Manzoor,2022). كما تضر انطباعات انخفاض إجراءات الأمن السيبراني بسمعة المنشأة، نتيجة ارتفاع معدلات الهجمات الإلكترونية، والفشل في تلبية احتياجات أصحاب المصلحة، بما يهدد استمرا المنشأة في دنيا الاعمال (Fombrun et al., 2015)

ويتم تقييم إجراءات الأمن السيبراني والتقنيات المرتبطة بها بعدة طرق، مثل: التدقيق الداخلي والخارجي، من خلال تقييم دوري لتطبيقها داخل البنك بواسطة فريقين متخصصين الاول

داخلي والثاني خارجي، بغرض تحديد نقاط الضعف واقتراح توصيات التحسين. كما يتم اجراء اختبار فني أمني منتظم للإجراءات السيبرانية لتحديد الثغرات والمخاطر المحتملة، من خلال المختبرات الأمنية المتخصصة للبرمجيات والأجهزة والشبكات والتطبيقات داخل البنك والتأكد من الامتثال للإجراءات المخططة ومن فعاليتها، ومراجعة السجلات الأمنية، للتحقق من تسجيل كافة الأنشطة والوصول إلى الأنظمة والبيانات، واكتشاف أي أنشطة غير مصرح بها، والرصد المستمر لنشاط الشبكة وإعلام الموظفين بها في أسرع وقت ممكن. وتطبيق مصادقة متعددة العوامل عن طريق الالتزام بأكثر من طريقة للتحقق من هوية المستخدمين، مثال ذلك كلمة المرور وبصمة الأصبع أو المسح الضوئي للوجه، واستخدام التشفير لحماية البيانات الحساسة، وتحديث البرامج، وتدريب موظفي البنك على أفضل الممارسات، مثل تقنية blockchain. وتقييم الوعي الأمني لهم، وتجزئة الشبكة إلى أجزاء أصغر لمنع انتشار البرامج الضارة وتقليل تأثير الاختراق، ووضع خطة استجابة لحالات الطوارئ، لتخفيض الخسائر المالية، والتغذية العكسية لمعرفة طرق الاختراق الجديدة **(Selimoğlu & Saldı, 2023; Greiner,et al.,2022; Lois et al., 2020 NIST,2021; ISACA,2021)** ويجب التأكيد على أن هذا التقييم والتطوير لإجراءات الأمن السيبراني عملية مستمرة في البنوك لتحقيق التحسين والتطوير المستمر لهذه الإجراءات.

وتستثمر البنوك في التقنيات الحديثة مثل تقنيات الكشف والحماية الذاتية الآلية من الاختراق والبرامج الخبيثة التي تمنع الوصول إلى شبكات الحاسب، مع استخدام بروتوكولات التشفير القوية والتوقيع الرقمي وأنظمة إدارة المفاتيح والتحقق من هوية المستخدمين عن طريق التعرف البيومتري لمعلومات البصمات والتعرف على الوجه وتقنيات الحوسبة السحابية الآمنة، وزيادة السرعة والكفاءة في الوصول إلى البيانات والتطبيقات. كما تستخدم تقنيات الذكاء الاصطناعي لمعرفة الأنماط غير العادية في السلوك الإلكتروني والتعامل معه بشكل فوري، لرصد أي نشاط غير مصرح به، وتقنيات تحليل السجلات والأحداث **(Logs & Events)**. ويجب وجود تكامل تقني بين البرامج المحاسبية والتطبيقات اللازمة لإدارة

مخاطر الأمن السيبراني الفعال لتقليل عمليات الاختراق وزيادة الموثوقية عند عرض القوائم المالية (Janvrin & Wang, 2022)، وتحقيق الاتساق التنظيمي والإجرائي بين الموظفين في إدارة أمن المعلومات (Achar, 2018)، والتعامل الصحيح مع المخاطر المكتشفة، وانشاء تقنيات الاستجابة للتهديدات لتعزيز ثقة العملاء، وتنفيذ الإجراءات الوقائية بعد موافقة العملاء (Jegede & Olowookere,2016). ويتم كل ذلك وفق إطار شامل. ولقد تبين وجود علاقة معنوية بين الاستثمار في هذه التقنيات وتحسن الأداء المالي للبنوك (Yang & Wang,2020; Javaid, 2020; Adetiloye, 2019). كونها تساعد في منع الاختراق، وتأمين البيانات المحاسبية، وزيادة وعي العاملين، وتعزيز الأمن المعلوماتي(Cram ,et al.,2022; Zhang,2022; Kumar,2021). كما تقلل هذه التقنيات من تكاليف الاختراقات، وتحسن من جودة الخدمات المصرفية وتوفر بيئة آمنة للعملاء، بما يحسن من سمعة البنك ويزيد الإيرادات (Beshir & Bashir,2018; Mutungi,2021;Alghamdi,2021;Zhang,2022;Kumar,2021;Abdel-Megeed,2021; Bokhari, & Manzoor, 2022). كما تحدث البنوك هذه التقنيات والأنظمة بشكل دوري، بما يحقق التوازن بين تكاليف الاستثمار والحفاظ على الأمن والأداء المالي (Official Annual Cybercrime Report, 2019). من خلال تخصيص مبالغ إضافية لإدارة المخاطر أو الاحتفاظ بها أو تحملها أو نقل عبئها وذلك عند وقوعها، بما يحمي مصالح العملاء (Kejwang, 2022). اذ تبين عدم قدرة أكبر المنشآت المالية على القضاء التام على التهديدات السيبرانية (Hausken,2020). لذلك يستخدم التأمين لتخفيف تأثيرها على الأداء المالي، من خلال اصدار شركات التأمين منتجات جديدة تتناسب مع مخاطر الأمن السيبراني (Osiemo,2016).

ولإنجاح هذه الإجراءات يجب القيام بعدة مهام، منها مهمة إدارة وتحديد الهوية، لتطوير الفهم التنظيمي للمخاطر، ومهمة الحماية لتشغيل الضمانات المناسبة لتوفير خدمات البنية التحتية وتقييد أو احتواء الاختراقات السيبرانية والوعي والتدريب، وإجراءات أمن وحماية البيانات (Security Intelligence Solutions,2020،Wu,et al.,2020) . يضاف الى ذلك مهمة تحديد الأولويات وفقًا لاستراتيجية إدارة المخاطر واحتياجات العمل. ومهمة الكشف عن الأحداث

الشاذة، ومهمة تنفيذ أنشطة الاستجابة، ومهمة استرداد القدرات المتضررة والعودة إلى العمليات العادية، ومهمة المراجعة المستقلة للسجلات (**الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية، هيئة السوق المالية; Wu et al.,2020**).

كما تؤثر جودة لجنة المراجعة الداخلية على علاقة إجراءات الأمن السيبراني بالأداء المالي (**شحاتة،٢٠٢٢**)، **حيث انها** آلية فعالة للرقابة اللاحقة التي تتضمن تفاصيل هذه الإجراءات داخل المنشأة (**أبو الخير وطه،٢٠٢٣**). كما تطور اللجنة إجراءات وقائية لهذه المخاطر (**أبو الخير،٢٠٢٢**)، من خلال دعم دور لجنة المراجعة الداخلية الاستشاري والتوكيدي لفعالية إجراءات الأمن السيبراني بما يحقق قيمة مضافة. ويمكن الاستعانة بتقنيات الذكاء الاصطناعي وسلسة الكتل **blockchain** والمنهجية الرشيقة **Agile Approach** لزيادة فعالية اللجنة، وتطوير أدائها لمواجهة مخاطر الأمن السيبراني (**شحاتة،٢٠٢٢، محروس وصالح،٢٠٢٢**). لذلك يستخدم الباحث فعالية لجنة المراجعة الداخلية كمتغير رقابي. وتقاس هذه الفعالية بعدة مقاييس أهمها توافر الخبرة المالية لدي اللجنة، حيث توجد علاقة معنوية بينها وفعالية الرقابة الداخلية (**عبد الفتاح،٢٠٢١**). كما يؤثر حجم لجنة المراجعة وعدد اجتماعاتها على فعاليتها (**Habbash & Alagla,2015**). كما يعد الاشتراك في أكثر من شركة مؤشراً على جودة وفعالية لجنة المراجعة الداخلية(**Daryaei et al.,2022**) . لذلك يستخدم الباحث هذه المؤشرات للتعبير عن فعالية لجنة المراجعة الداخلية.

يخلص الباحث بما سبق إلى زيادة حاجة البنوك لتفعيل وتعزيز وتحديث إجراءات الأمن السيبراني بشكل دوري منتظم، لحماية الأنظمة والبيانات وتقليل خطر الهجمات الإلكترونية واستخدام برامج قوية لمكافحة الفيروسات، وزيادة الإنفاق على التدريب، وتشفير البيانات، للحماية من الخسائر المباشرة وغير المباشرة الناتجة عن التأثر السلبي على ثقة العملاء. ونتيجة لذلك، تلتزم البنوك بتدبير استثمارات كافية لتطوير هذه الإجراءات، وتحقيق التوافق مع المتطلبات القانونية والتوقعات الاجتماعية، بما يحمي مصالح جميع الأطراف، ويؤدي ذلك الى تحسين الأداء المالي للبنك.

ولقد تعددت الدراسات السابقة التي تناولت علاقة إجراءات إدارة مخاطر الأمن السيبراني بالأداء المالي، ومن أهمها: **دراسة (أبو موسي،٢٠٠٤)** التي تعد من الدراسات الرائدة في

هذا المجال في المنطقة العربية، حيث ركزت على اختبار المخاطر الرئيسية التي تهدد أمن نظم المعلومات المحاسبية الالكترونية في السعودية، وخلصت إلى ان اهم المخاطر هي ادخال بيانات غير صحيحة، وإدخال فيروسات، والدخول للنظام من اشخاص غير مخولين، وتدمير البيانات ومخرجات النظام المحاسبي أو تحويل المخرجات لأشخاص غير مسموح لهم بالاطلاع عليها. وقد اوصت بتدعيم ضوابط الرقابة ورفع الوعي، واستطلاع اراء المراجعين الخارجيين والداخليين حول المخاطر الالكترونية. وقد مثلت هذه التوصية أساس لكثير من الدراسات اللاحقة مثل **دراسة (على،٢٠٢٣)** والتي اقترحت منهجاً إجرائياً لقياس استجابة المراجع الخارجي للمخاطر السيبرانية في المنشآت عالية التكنولوجيا، لوجود تأثير طردي معنوي لهذه المخاطر على أعمال المراجع الخارجي. **ودراسة (نافع،٢٠٢٢)** والتي خلصت الى ان تقنيات الثورة الصناعية الرابعة قد حسنت من جودة التقارير المالية من خلال تحسين الموثوقية والملاءمة. **ودراسة (شحاتة،٢٠٢٢)** والتي خلصت الى وجود دور استشاري وتوكيدي للمراجعة الداخلية في قضايا الأمن السيبراني، ويزيد ذلك من فعالية إجراءاته بما يحقق قيمة مضافة، حيث اوصت باستخدام الذكاء الاصطناعي وسلسة الكتل **blockchain** لزيادة فعالية المراجعة الداخلية. ودراسة **(محروس وصالح،٢٠٢٢)** التي اوصت باستخدام المنهجية الرشيقة **Agile Approach** لتطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني، وتبني معايير إدارة الأمن السيبراني الدولية.

٥- **الإفصاح عن إجراءات إدارة مخاطر الامن السيبراني:** يمثل الافصاح عن إجراءات الأمن السيبراني في التقارير المالية للبنوك أهمية كبيرة، للتعبير عن الامتثال للمتطلبات القانونية والتنظيمية للبنك المركزي والجهات الرقابية فيما يخص الأمن السيبراني، مثل قوانين حماية البيانات وقوانين مكافحة غسل الأموال وتمويل الإرهاب، وتقديم تفاصيل حول الإجراءات التي يتخذها البنك لحماية المعلومات الرقمية، وحماية العملاء. كما يبين بشكل موثوق فيه قيام المنشاة بمسئولياتها الاجتماعية في الحماية السيبرانية، مع توصل معلومات إجراءات الامن السيبراني التي قام بها الى المستخدمين وأصحاب المصلحة **(Tien et al., 2020)**، بما يمكن هذه الأطراف من تقييم قدرة المنشأة على معالجة التهديدات

السيبرانية وحماية المعلومات الحساسة، بما يعزز الثقة وبناء السمعة الطيبة، كما يشير الى جدية البنك في حماية المعلومات الحساسة مثل معلومات الحسابات المصرفية والمعاملات المالية **(Fombrun et al., 2015)**. وعلى العكس تؤدي إجراءات الأمن السيبراني الضعيفة إلى تراجع ثقة العملاء، وتراجع العوائد المالية للبنوك **(Kovalčíková & Kotlán, 2019)**. ويبرر ذلك زيادة الاستثمار في دعم الإجراءات والتقنيات السيبرانية **(Yang & Wang,2020; Javaid, 2020; Adetiloye, 2019)**. كما يساعد الافصاح عن إجراءات الأمن السيبراني في تحسين العمليات الداخلية وتعزيز الوعي بأمن المعلومات لدي المستخدمين، حيث يمثل انخفاض الوعي التكنولوجي للمستخدم العائق الرئيسي لتطبيق إدارة فعالة لمخاطر الأمن السيبراني **(Panda & Bower,2020; Governance, I. T. ,2021**؛ **على وصالح،٢٠٢٢؛ دليل مكافحة الاحتيال المالي في البنوك والمصارف العاملة في المملكة العربية السعودية،٢٠٢٠)**. كما يعزز الافصاح عن إجراءات الأمن السيبراني للبنوك من الحوكمة المؤسسية ويساهم في إدارة المخاطر بشكل فعال، مع المساعدة في استقرار القطاع المصرفي **(الأمير،٢٠٢٢، Kovalčíková & Kotlán, 2019)**. لذلك تفصح ٨٧ % من المنشآت الهولندية اختياريا في تقريرها السنوي عن معلومات الأمن السيبراني **(Eijkelenboom & Nieuwesteeg, 2021)**

ولقد تناولت عدة دراسات الإفصاح عن إجراءات الامن السيبراني، ومن أهمها: **دراسة (شرف،٢٠٢٣)** والتي ركزت على قياس تأثير الافصاح عن هذه الإجراءات على قرارات المستثمرين المصريين غير المحترفين، حيث خلصت لوجود تأثير معنوي لهذا الإفصاح لتقديمه إشارات قوية تزيد من ثقة المستثمرين تجاه المنشآت. ويختلف هذا التأثير باختلاف جنس المستثمر وعمره وتأهيله العلمي. وقد اوصت بضرورة وجود إدارة خاصة لمخاطر الأمن السيبراني، مع حث هيئة الرقابة المالية على تعزيز وتطوير الإفصاح عن ممارسات الأمن السيبراني. كما خلصت دراسة **(موسي وآخرون،٢٠٢٣)** الى نتيجة مشابهة، حيث تبين وجود علاقة معنوية بين الإفصاح عن المخاطر السيبرانية وأداء المنشاة المالي. لذلك أوصت بالتوسع في الافصاح عنها، كما طالبت بإصدار معيار محاسبي لتنظيم القياس

والافصاح عن المخاطر السيبرانية، وآثارها على التقارير المالية. وركزت **دراسة (على وصالح،٢٠٢٢)** على اختبار أثر الإفصاح عن تقرير إجراءات الأمن السيبراني على قرار الاستثمار بالأسهم المصرية، حيث خلصت لوجود تأثير معنوي لهذا الإفصاح نتيجة لزيادة الثقة في الحماية من الهجمات الالكترونية، وارسال إشارات إيجابية للمستثمرين وأصحاب المصالح عن أداء المنشآت، بما يحسن من كفاءة قرارات الاستثمار، وينعكس إيجابا على الأداء المالي. كما خلصت الى وجود تأثير معنوي لمستوي الخبرة والتأهيل العلمي للمستثمر على مستوي وعيه بمحتويات تقرير إدارة مخاطر الأمن السيبراني. وقد اوصت بإصدار إرشادات حول تقرير مخاطر الأمن السيبراني، وزيادة الوعي بأهميته واهتمام الجامعات بتدريسه. اما **دراسة (Boss et al.,2022)** فركزت على تأثير الإفصاح عن مخاطر الأمن السيبراني على المراجعين والجهات الضريبية، وتقييم تكاليف الاختراقات السيبرانية. كما ركزت **دراسة (الأمير،٢٠٢٢)** على دراسة دور التحول الرقمي المصرفي في تطوير الإفصاح عن إجراءات الأمن السيبراني، حيث انها تعطي إشارات إيجابية لأصحاب المصالح. إذ يمثل التحول الرقمي في البنوك تحدياً لقدرة البنوك على التكيف مع متطلباته، مثل المحافظة على سرية المعلومة والافصاح عن مخاطر الأمن السيبراني، كما انه في نفس الوقت يمثل فرصة للتنافس في بيئة رقمية. وقد اوصت الدراسة بزيادة اهتمام الدراسات الأكاديمية بتأثير الإفصاح المحاسبي عن الأمن السيبراني. وقد ركزت دراسة **(الرشيدي وعباس،٢٠١٩)** على أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول لمنشآت تكنولوجيا المعلومات المصرية مقارنة بالمنشآت الامريكية، حيث خلصت إلى وجود فروق معنوية في مستوي الإفصاح بين المجموعتين بما يؤثر سلبا على أسعار الأسهم وحجم التداول ومن ثم الأداء المالي. كما تبين وجود آثار إيجابية للإفصاح عن إدارة مخاطر الأمن السيبراني على أسعار الأسهم. وقد اوصت بضرورة اصدار البورصة والبنك المركزي والهيئة العامة للرقابة المالية إرشادات ملزمة لدعم الإفصاح عن مخاطر الأمن السيبراني، وانشاء لجنة متخصصة له.

كما ركزت عدة دراسات على علاقة إدارة مخاطر الأمن السيبراني بالأداء المالي في البنوك، والتي من أهمها: **دراسة (رشوان، قاسم،٢٠٢٢)** والتي ركزت على أثر إدارة مخاطر الأمن

السيبراني على دعم وتعزيز الاستقرار والشمول المالي في البنوك الفلسطينية. وقد خلصت إلى وجود أثر معنوي لإدارة مخاطر الأمن السيبراني على دعم وتعزيز الاستقرار والشمول المالي في البنوك، حيث تبين اعتماد البنوك على المعايير الدولية لإدارة الأمن السيبراني. وقد أوصت باستخدام نماذج فعالة لإدارة المخاطر السيبرانية التي تهدد الاستقرار المالي، وزيادة التوعية بأهمية الاستقرار والشمول المالي لها لزيادة رفاهية العملاء والمجتمع من خلال تخفيض تكلفة الخدمات وتحسين الأداء المالي. بينما ركزت **دراسة (Gatzert & Schubert, 2022)** على أثر الوعي بالمخاطر السيبرانية على الأداء المالي في البنوك الامريكية، من خلال تطبيق خوارزمية التنقيب عن النصوص المرتبطة بتطوير درجة الوعي لإدارة المخاطر السيبرانية في التقارير السنوية. وقد خلصت إلى أن زيادة الوعي بهذه المخاطر يدعم تطبيق إجراءات الامن السيبراني، ويؤثر إيجابا على الأداء المالي، حيث تبين وجود علاقة معنوية طردية بين تطبيق هذه الإجراءات وأداء المنشأة. وتتفق **دراسة(Kovalčíková & Kotlán, 2019)** مع الدراسة السابقة على أهمية الوعي الأمني لدى الموظفين والعملاء. حيث خلصت إلى وجود أثر معنوي لإجراءات الأمن السيبراني على الأداء المالي للبنوك الاوربية، كما تبين وجود أثر إيجابي معنوي لمتغيرات حجم البنك وتنوع أنشطته. وقد اوصت بتطبيق تقنيات التشفير والتعرف على الأنماط والتعلم الآلي والذكاء الاصطناعي، لتقليل تعرض البنوك للهجمات السيبرانية، مع ضرورة التنسيق بين البنوك والمؤسسات الحكومية والدولية لتعزيز تبادل المعلومات حول إجراءات الأمن السيبراني، وتشجيع الاستثمار فيها لتحسين الأداء المالي. في حين ركزت **دراسة (قوجيل وطيبة،٢٠٢٢)** على مخاطر استخدام تقنيات التكنولوجيا المالية في البنوك مثل سلسة الكتل والعقود الذكية والعملات المشفرة والذكاء الاصطناعي نتيجة زيادة التداخل بين العميل والبنك، حيث يستطيع العميل القيام بأنشطة متعددة دون الذهاب للبنك. كما تناولت إجراءات إدارة مخاطر التكنولوجيا المالية في البنوك وفقا لتوصيات بنك نيقارا الماليزي وإدارة الخدمات المالية في نيويورك ومجموعة البنك الدولي وتوصيات مجلس الاستقرار المالي. وقد اوصت بتطوير الإفصاح عن مخاطر التكنولوجيا المالية وخسائر الهجمات السيبرانية، وادراج علاقة إجراءات الأمن السيبراني بالأداء ضمن توصيات اللجان المصرفية الدولية مثل بازل، وانشاء مراكز بحثية مصرفية خاصة بإدارة مخاطر الأمن السيبراني. بينما تناولت **دراسة**

(Kasanga, 2021) تأثير تقنيات المرونة الإلكترونية –ويقصد بها القدرة على مواصلة الأنشطة في جميع الظروف قبل وأثناء وبعد الهجمات السيبرانية (Hollnagel, 2017) – على مواجهة الجرائم الإلكترونية في البنوك الكينية. وقد خلصت إلى وجود تأثير مباشر لتقنيات المرونة المالية في البنوك مثل تقييد الامتيازات، وتنسيق الحماية، والمراقبة التحليلية، والتمثيل الديناميكي على إجراءات إدارة الأمن السيبراني، بما يؤثر إيجابا على أداء البنوك. واقد وصت بتطبيق تقنية الخداع الالكتروني في البنوك لتأخير تأثير الهجوم، وإرباك وتضليل المخترقين واستخدام التحليلات الجنائية لتقييم الضرر الناجم عن الهجمات الإلكترونية. كما خلصت مجموعة من الدراسات (Mutungi,2021;Abdel- Javaid, 2020; Megeed,2021;Al-Masri & Qasim,2021; Kumar,2021; Zhang,2022; Yang & Adetiloye, 2019 ;Alramahi, 2021; Alghamdi,2021; Wang,2020) الى وجود علاقة إيجابية بين إجراءات الأمن السيبراني والأداء المالي للبنوك، حيث تحقق البنوك التي تستثمر في تقنيات الأمن السيبراني أداءً مالياً أفضل. كما تحسن الإجراءات الفعالة للأمن السيبراني من جودة الخدمات المصرفية، وتقلل التكاليف، وتحسن استخدام التقنيات الحديثة للأمن السيبراني من سلوك العملاء، وتوفر بيئة آمنة لهم وتزيد الثقة في البنوك. وقد اوصت هذه الدراسات بتعزيز التوعية بالأمن السيبراني وتشجيع الاستثمار في تقنياته الحديثة، وتبني أنسب إجراءاته للبنوك وفق إطار رقابة فعال، بما يحسن أدائها المالي ويزيد مقدرتها على المنافسة مع زيادة ثقة العملاء فيها.

يخلص الباحث بما سبق الى وجود علاقة بين الإفصاح عن إجراءات الامن السيبراني والأداء المالي للبنك. ويعتقد الباحث ان تعقيد عمليات البنك يؤثر في هذه العلاقة، لذلك تركز الجزئية التالية على هذه العلاقة.

٦-علاقة تعقيد عمليات البنك بالأداء المالي: يقصد بتعقيد عمليات البنك قيام البنك بالعديد من العمليات المختلفة المعقدة والمتشابكة، والتي تتطلب أنظمة وإجراءات معقدة لإدارة هذه العمليات بكفاءة وفعالية (**عبد الباقي وآخرون،٢٠٢١**). ويؤدي تعقيد عمليات البنوك الى زيادة المخاطر التي تتعرض لها البنوك، بما يؤثر سلباً على أدائها المالي (**Zaki, & Al-Issa,2016; Hassan, 2018; Almutairi,2016**) ، خاصة المخاطر السيبرانية والتي تتزايد بشكل كبير نتيجة زيادة الهجمات السيبرانية، بما يؤثر على الأداء المالي له.

إذ يري الباحث ان زيادة تعقيد عمليات البنك تؤدي الى زيادة معدل استهداف البنك من قبل المهاجمين بما يزيد مخاطر الهجمات السيبرانية، ويزيد من الإجراءات الواجب اتخاذها للحد من هذه المخاطر، ويصاحب ذلك زيادة الإفصاح عن إجراءات الامن السيبراني للتعامل مع هذه الهجمات، حيث ان هذه المعلومات هامة وجوهرية، وفقا لنظرية الشرعية. ويتفق هذا المنطق مع ما تقضي به نظرية الإشارة، حيث تتوسع البنوك في الإفصاح الاختياري عن معلومات إجراءات الامن السيبراني، سواء كانت هذه المعلومات جيدة او غير جيدة، لتحسين قيمة الشركة **(Haji & Mohd Ghazali, 2012)**، لأن ذلك يعطي رسالة طمأنة للسوق وللمستثمرين، حيث تعطي إشارات إيجابية للمستثمرين عن نجاح البنوك في التعامل مع آثار الهجمات السيبرانية ووضع الإجراءات المناسبة للتعامل معها. إضافة الى ذلك يزداد طلب المستثمرين والمحللين على معلومات إجراءات الامن السيبراني لأهميتها في تقييم الاداء. وإذا لم يتم الإفصاح من قبل البنك، فإن ذلك يعطي إشارات سلبية، كما انه لن يمنع وصول المعلومات الى السوق، حيث ستصل هذه المعلومات من مصادر اخري في السوق تكون اقل موثوقية، بما يعمق التأثير السلبي لها **(النقيب،٢٠٢٠)**. وتعمل البنوك على خفض المخاطر الناتجة عن التعقيد والعمل على تحسين سمعة البنك من خلال التوسع في الإفصاح عن قيام البنك بالإجراءات اللازمة للحد من مخاطر الهجمات السيبرانية بما يحسن الأداء المالي. كما يساعد التوسع في الإفصاح عن المعلومات الخاصة بإجراءات الامن السيبراني على تخفيض تكاليف الوكالة، من خلال تخفيض عدم تماثل معلومات إجراءات الامن السيبراني بين الإدارة والأطراف ذات العلاقة من مساهمين وغيرهم، بما يخفض المخاطر السيبرانية ويحسن الأداء المالي. كما تبني استراتيجيات البنوك على خفض المخاطر السيبرانية الناتجة عن تعقيد عمليات البنك، من خلال التدريب المستمر للموظفين على الحماية من الهجمات السيبرانية، وتحقيق التوازن بين عوائد وتكاليف الاستثمار في تكنولوجيا الامن السيبراني مع مراعاة الكفاءة التشغيلية للبنك **(عبد الباقي وآخرون،٢٠٢١)**. كما يراعى آثار تعقيد عمليات البنوك على الإجراءات الوقائية والعلاجية المناسبة لتخفيف أثر الهجمات السيبرانية **(Peterson ,2020, Tesfaye ,2020)**. ويؤدي ذلك الى زيادة معدل

تداول الأسهم ويخفض تكلفة رأس المال ويحسن إعادة التقييم **(Haji & Mohd Ghazali, 2012)**، بما يؤثر على الأداء المالي. كما تبين اختلاف أثر التعقيد على الأداء المالي بين البنوك الكبيرة والصغيرة، نتيجة ميل البنوك الكبيرة الى زيادة درجة التعقيد، وميل البنوك الصغيرة الى تخفيض التعقيد عن طريق الحد من عدد الفروع **(Buch & Goldberg,2022)** ، حيث يساعد الهيكل البسيط على تعزيز ثقة المستثمرين ويحسن أداء المنشأة. الا ان اختلاف بيئات التطبيق قد يؤدي الى نتائج مختلفة. ولقد تعددت الدراسات التي تناولت علاقة تعقيد عمليات البنك بالأداء المالي، وخلصت بعض هذه الدراسات إلى أن تعقيد عمليات البنك يزيد من مخاطرها ويؤثر سلباً على الأداء المالي للبنوك، بسبب زيادة التكاليف وصعوبة الإدارة واتخاذ القرارات بشكل غير فعال، وتقليل المرونة في التعامل مع التغيرات الاقتصادية والسياسية **(Zaki, & Hassan, 2018; Al-Issa,2016; Almutairi,2016)**. وقد ركزت بعض هذه الدراسات على دراسات الحالة مثل دراسة**(Zaki, & Hassan, 2018)** التي ركزت على بنك القاهرة المصري، ودراسة **(Al-Issa,2016)** التي ركزت على بنك الرياض السعودي. ويعاب على دراسات الحالة الاعتماد على مصادر بيانات محددة ومحدودة، بما يؤدي إلى تحيز النتائج، ويصعب من قابليتها للتعميم **(Yin, 2014)**. لذلك تعتمد الدراسة الحالية على حصر شامل لجميع البنوك السعودية التي تنطبق عليها الشروط. وتقاس درجة تعقيد عمليات البنك بعدة مقاييس أهمها:

-**عدد الفروع وعدد الصرافات**، بما يعكس درجة الانتشار الجغرافي للبنك، والذي يؤثر على استقرار وربحية البنك، حيث تبين ان الانتشار الجغرافي يؤشر على زيادة استقرار البنك ويقلل مخاطر عدم التحصيل ومعدل تقلبات الأرباح، غيرانه يقلل الربحية، خاصة عند وجود فروع اجنبية **(Nyola et.al,2021)**. إذ أن البنوك التي تعمل في أكثر من دولة تحتاج إلى مراعاة الاختلافات في القوانين واللوائح المحلية **(عبد الباقي وآخرون،٢٠٢١)**. ويري آخرون وجود اثر سلبي لتعدد الفروع على الأداء المالي بسبب صعوبة إدارة المنشآت وتعقيد العلاقات الداخلية والخارجية وتعدد الأعمال **(Bloom, et.al,2016)** .

- **تنوع وتطور الخدمات المصرفية**، فكلما تنوعت الخدمات المصرفية او المنتجات التي يقدمها البنك، كلما زادت درجة تعقيد عملياته، وذلك لأن كل منتج أو خدمة لها خصائصها وإجراءاتها الخاصة (**عبد الباقي وآخرون،٢٠٢١**). ويري اخرون وجود أثر إيجابي لتعقيد عمليات البنك من خلال زيادة القدرة على الابتكار والتغيير(**Rindfleisch, 2017**) . ويستخدم الباحث متغير عدد العملاء كمتغير بديل يشير الى تنوع الخدمات المصرفية وتطويرها. فكلما تنوعت الخدمات فإنها تلبي احتياجات متعددة للعملاء بما يزيد من عدد العملاء، كما تعكس التعقيد التنظيمي والإداري.

-**اجمالي الودائع:** تعد زيادة قيمة ودائع البنك أحد اهم عناصر الجذب للهجمات السيبرانية، فقد زادت الهجمات الإلكترونية على البنوك الكبيرة (**Kejwang, 2022**). فكلما كان حجم البنك أكبر، كلما زادت تعقيد عملياته. لأن البنوك الكبيرة تتعامل مع عدد أكبر من العملاء والحسابات، وتقدم مجموعة أوسع من المنتجات والخدمات. وقد تم استهداف أكثر من نصف البنوك التجارية في العالم بنوع واحد على الأقل من هذه الهجمات (**Security Intelligence Solutions, 2020**). **كما** تبين ان ٧٠٪ من الخروقات الأمنية السيبرانية التي تمت دراستها كانت تستهدف المنشآت المالية (**Data Breach Investigations Report, 2021**)، بما زاد من المخاطر المالية وأثرها على الأداء المالي للبنوك بشكل معنوي سلبي (**Gweyi ,2018; Gatzert & Schubert, 2022**). وقد خلص آخرون الى ان هذا الأثر إيجابي (**السلطان والجليد،٢٠٢٠**)، في حين خلص فريق ثالث الى ان هذا الأثر متناقض، كون تأثيره إيجابي على الأداء الابتكاري والنمو، وتأثيره سلبي على الأداء المالي. وقد تم تفسير هذا التناقض بواسطة نظرية الموانع والفرص (**barriers & opportunities theory**)، فقد يؤدي تعقيد المنشأة الى إعاقة العمليات الداخلية والتنفيذية، لكنه في نفس الوقت يوفر فرصاً للابتكار والتطوير.

-**حجم الأصول:** وتعبر عن القدرات والامكانيات المادية والبشرية والتكنولوجية للبنك والتي تؤثر على قيمته السوقية، حيث تملك البنوك الكبيرة موارد مالية كبيرة، وتستخدم نظم معلومات متطورة، كما تتعرض لمخاطر متعددة تشغيلية وسوقية وغيرها. لذلك يزيد تعقيد عمليات البنك في البنوك الكبيرة (**عبد الباقي وآخرون،٢٠٢١**)، وبالتالي يتم استخدام حجم الأصول للتعبير عن تعقيد عمليات البنك (**Al-Ahmari & Al-Rashidi,2018; Al Eidan &**

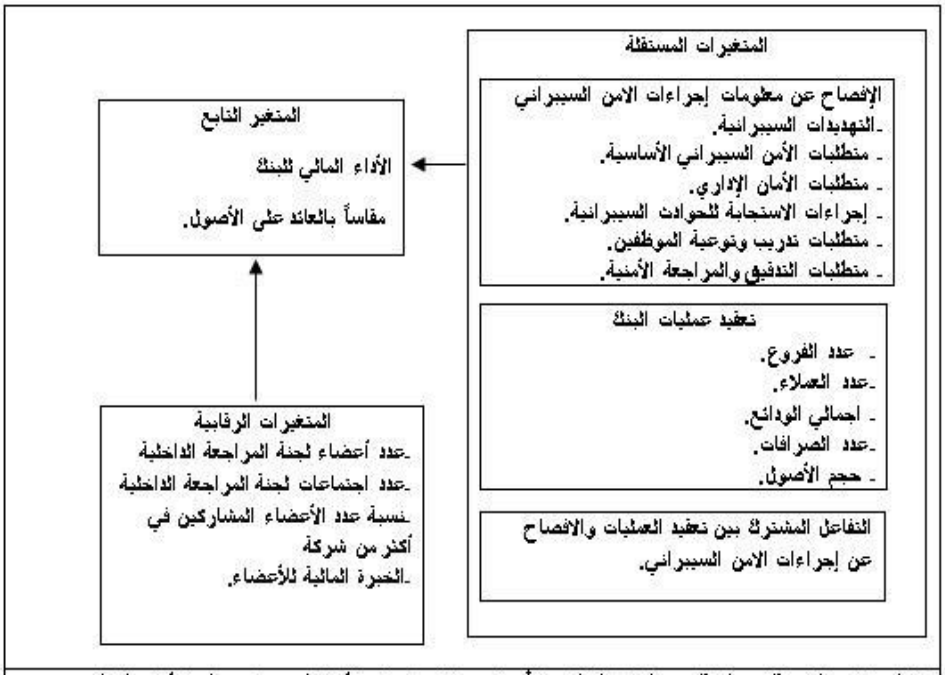
Alsubaie,2019، **عبد الباقي وآخرون،٢٠٢١**) ، كما تؤثر على تحديد إجراءات الأمن السيبراني **(Kamiya et al., 2021)** . ولقد تبين وجود علاقة إيجابية بين حجم الأصول والأداء المالي للبنوك، نتيجة تحسن الجوانب المالية والإدارية والكفاءة وتطوير الخدمات المصرفية. في حين ذهب البعض الى ان هذه العلاقة غير معنوية **(موسى وآخرون،٢٠٢٣)**. ويقاس حجم المنشأة باللوغاريتم الطبيعي لإجمالي الأصول في نهاية العام **(McShane & Nguyen, 2020; Kamiya et al., 2021; Gatzert & Schubert, 2022)**. ولقد اختلفت الدراسات في توصيف علاقة حجم الشركة بمستوي الإفصاح الاختياري. إذ ذهب البعض الى أنها علاقة طردية معنوية، فالمنشآت الكبرى اعلى في مستوي الإفصاح عن المعلومات، لتلبية التوقعات المتزايدة للمستخدمين، ولقدرتها على تحمل تكاليف هذا الإفصاح، ورغبتها في تخفيض تكاليف الوكالة بالتوسع في الإفصاح **(Buertey & Pae 2021; Aris,2020; Abdillah et al.,2019)**. في حين ذهب آخرون الى ان هذه العلاقة سلبية، حيث تتمتع المنشآت الصغيرة بمرونة أكبر وسرعة في اتخاذ القرارات بما يسمح لها بجذب واقتناص فرص استثمارية جديدة **(Dey et al ,2020)**، وذهب فريق ثالث الى عدم وجود علاقة معنوية **(Mahboub,2019)**.

يخلص الباحث بما سبق الى ان تعقيد عمليات البنك تؤثر في الأداء المالي له، كما تتعدد مؤشرات قياس درجة تعقيد عمليات البنك مثل عدد الفروع وعدد الصرافات واجمالي الودائع وحجم الأصول. كما تبين اختلاف نتائج الدراسات في تحديد اثار هذه المتغيرات. لذلك يستخدم الباحث هذه المؤشرات لتقديم دليل تطبيقي على اثارها على الأداء المالي للبنوك السعودية.

ووفقا لكل ما سبق يلخص الباحث الفجوة البحثية في اختبار العلاقة بين الإفصاح عن إجراءات الامن السيبراني والأداء المالي للبنوك. إضافة الى اختبار علاقة تعقيد عمليات البنك بالأداء المالي. ثم اختبار العلاقة المشتركة بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك، وتقديم دليل تطبيقي على البنوك السعودية. إذ انها الدراسة الاولي– في حدود علم الباحث– التي تدرس أثر العلاقة المشتركة لتعقيد عمليات البنك والإفصاح عن إجراءات الأمن السيبراني على الأداء المالي للبنوك باستخدام بيانات فعلية.

٧-اشتقاق وصياغة الفروض:

بناءً على ما سبق يعتقد الباحث بوجود علاقة معنوية بين كلٍ من الإفصاح عن إجراءات الامن السيبراني وتعقيد عمليات البنك كمتغيرين مستقلين والأداء المالي للبنك كمتغير تابع، كما يعتقد بان التفاعل المشترك بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني يؤثر على الأداء المالي للبنوك. الا ان هذا الاعتقاد يحتاج الى دليل تطبيقي يؤيده او ينفيه، في ظل عدم وجود دراسات سابقة لهذه العلاقة بالتطبيق على البنوك السعودية. ومن ثم تمثل هذه الدراسة –على حد علم الباحث– الاولي في السوق السعودي التي تختبر أثر التفاعل المشترك بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك. ويوضح الشكل التالي رقم (١) نموذج يصف هذه العلاقة:



شكل (١): إطار مقترح لتعقيد عمليات البنك والإفصاح عن إجراءات الأمن السيبراني على الأداء المالي

وقد اعتمد بعض الدراسات السابقة على دراسة الحالة لبنك معين عند دراسة العلاقة بين الإفصاح عن إجراءات الأمن السيبراني والأداء المالي للبنوك **(Zaki, & Hassan, 2018;**

(Al-Issa,2016 ، بما يؤدي إلى تحيز النتائج، ويصّعب قابليتها للتعميم (Yin, 2014). لذلك تعتمد هذه الدراسة على حصر شامل لجميع البنوك السعودية التي تنطبق عليها الشروط.

ويسعي الباحث الى تقديم دليل تطبيقي حول أثر اختلاف مستوي الإفصاح عن إجراءات الأمن السيبراني بين البنوك التجارية السعودية. لذلك يمكن صياغة الفرض الأول في صورته العدمية كما يلي: ***لا يختلف مستوي الإفصاح عن إجراءات الأمن السيبراني بين البنوك التجارية السعودية.***

كما خلص الباحث من استعراض الدراسات السابقة الى وجود علاقة معنوية بين الإفصاح عن إجراءات الأمن السيبراني والأداء المالي للبنوك، حيث تحسن الإجراءات الفعالة للأمن السيبراني من جودة الخدمات المصرفية وتقلل التكاليف، بما يبرر الاستثمار في تقنيات الأمن السيبراني، ويساهم في توفير بيئة آمنة للعملاء ويحمي البيانات المالية الحساسة للبنوك، بما يحسن الأداء المالي للبنوك (Qasim,2021; Kumar,2021; Zhang,2022; Yang & Alghamdi,2021; Wang,2020 ;Alramahi, 2021 ;Adetiloye, 2019). لذلك يختبر الباحث العلاقة بين الإفصاح عن إجراءات الامن السيبراني والأداء المالي للبنك. بالتالي يمكن صياغة الفرض الثاني في صورته العدمية كما يلي: ***لا توجد علاقة معنوية بين الإفصاح عن إجراءات الأمن السيبراني والأداء المالي للبنوك التجارية السعودية.***

كما خلص الباحث من استعراض الدراسات السابقة الى استخدام عدة مؤشرات لقياس درجة تعقيد عمليات البنك (**عدد الفروع وعدد الصرافات واجمالي الودائع وحجم الأصول**)، حيث تبين اختلاف نتائج الدراسات في تحديد الاثار المختلفة لهذه المتغيرات. إذ ذهب البعض الى ان الأثر سلبي لأن تعقيد عمليات البنك يزيد من مخاطرها ويؤثر سلباً على أداء البنوك، بسبب زيادة التكاليف وصعوبة تعامل الإدارة مع التغيرات الاقتصادية والسياسية، وصعوبة اتخاذ القرارات بشكل فعال (Al- Zaki, & Hassan, 2018; Almutairi,2016; Issa,2016; Buch & Goldberg,2022). وذهب اخرون الى انه ايجابي

(Al-Ahmari & Al-Rashidi,2018; Al Eidan & Alsubaie,2019 (السلطان والجليد، ٢٠٢٠. في حين ذهب فريق ثالث الى انه متعارض Larsen et al, 2019). لذلك يري الباحث ضرورة التوصل الى دليل تطبيقي عن علاقة تعقيد عمليات البنك بالأداء المالي للبنوك السعودية، حيث تمت اغلب الدراسات السابقة اعتمادا على قوائم استقصاء ولم تعتمد على بيانات فعلية. كما يري الباحث ان اختلاف بيئات التطبيق قد يؤدي الى نتائج مختلفة. ولم تختبر هذه الدراسات هذه العلاقات في قطاع البنوك السعودية. كما تؤثر جودة لجنة المراجعة بشكل طردي معنوي على الإفصاح الاختياري (Buertey & Pae 2021; Dey et al, 2020; Firmansyah & Irwanto, 2020) ، حيث خلص آخرون انها علاقة سلبية معنوية (صالح، على ، ٢٠٢١). لذلك يمكن صياغة الفرض الثالث في صورته العدمية كما يلي: ***لا توجد علاقة معنوية بين تعقيد عمليات البنك والأداء المالي للبنك***. ورغبة في اثراء البحث يتم اشتقاق **الفروض الفرعية مع كل مقياس لتعقيد عمليات البنك كما يلي:**

الفرض الفرعي الاول- لا توجد علاقة معنوية بين عدد الفروع والأداء المالي للبنوك.

الفرض الفرعي الثاني - لا توجد علاقة معنوية بين عدد العملاء والأداء المالي للبنوك.

الفرض الفرعي الثالث- لا توجد علاقة معنوية بين اجمالي الودائع والأداء المالي للبنوك.

الفرض الفرعي الرابع - لا توجد علاقة معنوية بين عدد الصرافات والأداء المالي للبنوك.

الفرض الفرعي الخامس - لا توجد علاقة معنوية بين حجم الأصول والأداء المالي للبنوك.

كما يعتقد الباحث بأن تعقيد عمليات البنك في حد ذاته يؤدي الى زيادة مخاطر الامن السيبراني، بما يلزم معه ضرورة اتخاذ إجراءات لتقليل هذه المخاطر. ويستلزم ذلك الإفصاح عن إجراءات مخاطر إدارة الامن السيبراني التي تؤثر في الأداء المالي للبنوك. ومن هنا برزت أهمية اختبار أثر العلاقة المشتركة لتعقيد عمليات البنك ومستوي الإفصاح عن إجراءات الامن السيبراني على الأداء المالي للبنك. ولإثراء البحث يسعي الباحث من خلال هذا الفرض الى

اختبار العلاقة المشتركة بين تعقيد العمليات والإفصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك السعودية. غير ان اختبار هذه العلاقة المشتركة في السوق السعودي يحتاج الى تقديم دليل عملي، في ظل عدم وجود دراسات تناولت هذا الموضوع (وفقا لعلم الباحث). لذلك تختبر الدراسة التطبيقية هذه العلاقة، ومن ثم يمكن صياغة الفرض الرابع في صورته العدمية كما يلي: ***لا يوجد تأثير ذو دلالة إحصائية للعلاقة(التفاعلية) المشتركة بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك.***

ورغبة في اثراء البحث يتم اشتقاق الفروض الفرعية مع كل مقياس لتعقيد عمليات البنك كما يلي:

الفرض الفرعي الاول- لا يوجد تأثير ذو دلالة إحصائية للعلاقة المشتركة بين عدد الفروع والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك.

الفرض الفرعي الثاني - لا يوجد تأثير ذو دلالة إحصائية للعلاقة المشتركة بين عدد العملاء والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك.

الفرض الفرعي الثالث-لا يوجد تأثير ذو دلالة إحصائية للعلاقة المشتركة بين اجمالي الودائع والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك.

الفرض الفرعي الرابع - لا يوجد تأثير ذو دلالة إحصائية للعلاقة المشتركة بين عدد الصرافات والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك.

الفرض الفرعي الخامس -لا يوجد تأثير ذو دلالة إحصائية للعلاقة المشتركة بين حجم الأصول والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك.

٨- الدراسة التطبيقية واختبار الفروض:

١/٨-مجتمع الدراسة وعينتها والفترة الزمنية وأسلوب جمع البيانات: يتمثل مجتمع الدراسة في جميع البنوك السعودية المرخصة من قبل البنك المركزي السعودي والمقيدة في هيئة سوق المال السعودية وعددها ١٣ بنكا. وتتمثل عينة الدراسة في البنوك التي تتوفر بها جميع بيانات متغيرات الدراسة، وعدم تغير السنة المالية خلال فترة الدارسة، ووجود تداول نشط على أسهمها، حيث بلغ عددها ١٠ بنوك. إذ تم استبعاد بنكين نظرا لأنهما حصلا على الترخيص ولم يزاولا النشاط وهما بنك إس تي سي والبنك السعودي الرقمي. كما تم استبعاد بنك الخليج الدولي – السعودية لعدم وجود تداول نشط عليه خلال فترة الدراسة. وفيما يلي اسماء هذه البنوك:

جدول رقم (١) أسماء البنوك السعودية المستخدمة كعينة للدراسة التطبيقية	
البنك الأهلي السعودي	مصرف الانماء
مصرف الراجحي	البنك السعودي الفرنسي
بنك الرياض	البنك السعودي للاستثمار
البنك السعودي البريطاني	بنك الجزيرة
البنك العربي الوطني	بنك البلاد

ولقد تم تجميع البيانات من واقع التقارير المالية المنشورة للبنوك لجميع المتغيرات فيما عدا متغير الإفصاح عن إجراءات الأمن السيبراني، حيث استخدم الباحث أسلوب تحليل المحتوي الوصفي لقياس هذا المتغير، من خلال تفريغ دليل الأمن السيبراني للبنوك السعودية وتحليل محتوى التقارير المالية السنوية والمعلومات المتوفرة على الموقع الإلكتروني للبنك لمدة ٥

أعوام في الفترة من عام ٢٠١٨ الى عام ٢٠٢٢ بإجمالي عدد مشاهدات ٥٠ مشاهدة ، وعلى موقع هيئة سوق المال السعودي **https://2u.pw/eo2OrW** //،**وموقع https://www.argaam.com/** ، لاستيفاء البيانات الكمية لمتغيرات البحث.

٢/٨- **متغيرات الدراسة:** يوضح الجدول التالي رقم (٢) توصيفاً للمتغيرات المستقلة والتابعة والرقابية والتي سوف يتضمنها التحليل الإحصائي ونموذج الدراسة المقترح.

جدول رقم (٢) متغيرات الدراسة التطبيقية

الرمز	المتغير	طريقة قياسه	الدراسات السابقة
Y	الأداء المالي مقاس بالعائد على الأصول	صافي الدخل ÷ اجمالي الأصول	(Kamiya et al., 2021; Bokhari & Manzoor,2022; Pedron et al.,2021; Amara, 2022; McShane & Nguyen, 2020.
X1	إجراءات الأمن السيبراني	عدد مؤشرات الإفصاح الفعلي من ٧٧	موسى وآخرون،٢٠٢٣

X2	التهديدات السيبرانية	عدد مؤشرات الإفصاح الفعلي من ١١	الدليل الاسترشادي للبنوك الصادر عن هيئة السوق المالية في المملكة العربية السعودية، ويقاس بالعدد الفعلي المفصح عنه في كل مكون الى اجمالي عدد المؤشرات في كل مكون.
X3	المتطلبات الأساسية	عدد مؤشرات الإفصاح الفعلي من ١٧	
X4	متطلبات الأمان الإداري	عدد مؤشرات الإفصاح الفعلي من ٧	
X5	إجراءات الاستجابة للحوادث	عدد مؤشرات الإفصاح الفعلي من ٩	
X6	متطلبات تدريب وتوعية الموظفين	عدد مؤشرات الإفصاح الفعلي من ١٨	
X7	متطلبات التدقيق والمراجعة الأمنية	عدد مؤشرات الإفصاح الفعلي من ١٥	
X8	عدد الفروع	العدد الفعلي المذكور	(Buch & Goldberg,2022)
X9	عدد العملاء	العدد الفعلي المذكور	Rindfleisch, 2017
X10	اجمالي الودائع	العدد الفعلي المذكور	
X11	عدد الصرافات	العدد الفعلي المذكور	
X12	حجم الأصول	اللوغاريتم الطبيعي لإجمالي الأصول	Wang & Xing, 2020 ; lmarzouky et al.,) (2021; Wara et al.,2020)
X13	فعالية لجنة المراجعة الداخلية	عدد أعضاء لجنة المراجعة الداخلية	Gatzert & Schubert, 2022
X14		عدد اجتماعات لجنة المراجعة الداخلية	،(Habbash & Alagla,2015)
X15		نسبة عدد الأعضاء المشاركين في أكثر من شركة	(Makhlouf et al. ,2017)
x16		الخبرة المالية=عدد أعضاء اللجنة الذين لديهم خبرة محاسبية ÷عدد أعضاء لجنة المراجعة	(Daryaei et al.,2022) Al Lawati et al., 2021, Buallay & Al-Ajmi, 2019)

X17	التفاعل المشترك بين X8،X1	X1*X8	التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني ومقاييس تعقيد عمليات البنك المختلفة من اقتراح الباحث.
X18	التفاعل المشترك بين X9،X1	X1*X9	
X19	التفاعل المشترك بين X10،X1	X1*X10	
X20	التفاعل المشترك بين X11،X1	X1*X11	
X21	التفاعل المشترك بين X12،X1	X1*X12	

٨ /٣-**نموذج الدراسة:** لا يحتاج الفرض الأول إلى بناء نموذج كمي؛ حيث يتم اختباره من خلال دراسة التباين بين بنوك العينة حول الإفصاح عن إجراءات الأمن السيبراني باستخدام تحليل**One way ANOVA**. اما بقية الفروض فيتم تصميم نماذج الدراسة لها بما يتفق مع فروض الدراسة التطبيقية، حيث يركز الفرضان الثاني والثالث على اختبار معنوية العلاقة بين الإفصاح عن معلومات إجراءات الأمن السيبراني وتعقيد عمليات البنك كمتغيرين مستقلين على الأداء المالي للبنك كمتغير تابع، اما المتغير الرقابي فهو فعالية لجنة المراجعة الداخلية **(مقاسه بعدد أعضاء اللجنة وعدد اجتماعاتها ونسبة عدد المشاركين في اكثر من شركة والخبرة المالية للجنة المراجعة)**. ويقترح الباحث نموذج الانحدار المتعدد الأول التالي:

$$Yij = \beta0 + \beta1\ X1\ ij + \beta8\ X8\ ij + \beta9\ X9\ ij + \beta10\ X10\ ij + \beta11\ X11\ ij + \beta12\ X12\ ij + \beta13\ X13\ ij + \beta14\ X14\ ij + \beta15\ X15\ ij + \beta16\ X16\ ij + \varepsilon.$$

وتتمثل متغيرات هذا النموذج فيما يلي:

Y ij الاداء المالي للبنك (j) عن العام i مقاساً بالعائد على الأصول.

β 0 المقدار الثابت لنموذج الانحدار

X1j عدد مؤشرات الإفصاح الفعلي للبنك (j) في العام i

X8 j عدد الفروع للبنك (j) في العام i.

X9 j	عدد العملاء (j) في العام i.
X10 j	اجمالي الودائع للبنك (j) في العام i.
X11 j	عدد الصرافات للبنك (j) في العام i.
X12 j	اللوغاريتم الطبيعي لإجمالي الأصول للبنك (j) في العام i.
X13 j	عدد أعضاء لجنة المراجعة الداخلية للبنك (j) في العام i.
X14 j	عدد اجتماعات لجنة المراجعة الداخلية للبنك (j) في العام i.
X15j	نسبة عدد المشاركين في أكثر من بنك للبنك (j) في العام i.
X16j	الخبرة المالية للجنة المراجعة للبنك (j) في العام i
β1: B16	معاملات نموذج الانحدار المتدرج
ε	بواقي نموذج الانحدار المتدرج.

ويركز الفرض الرابع على اختبار معنوية العلاقة المشتركة بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني كمتغير مستقل على الأداء المالي للبنوك كمتغير تابع.في ظل نفس المتغيرات الرقابية من X13 الى X16.ويقترح الباحث نموذج الانحدار المتعدد الثاني التالي:

$$Yij = \beta0 + \beta13\ X13\ ij + \beta14\ X14\ ij + \beta15\ X15\ ij + \beta16\ X16\ ij + \beta17\ X17\ ij + \beta18\ X18\ ij + \beta19\ X19\ ij + \beta20\ X20\ ij + \beta21\ X21\ ij + \varepsilon.$$

وتتمثل متغيرات هذا النموذج فيما يلي:

Y ij	الاداء المالي للبنك (j) عن العام i مقاساً بالعائد على الأصول.
β 0	المقدار الثابت لنموذج الانحدار.
X13 j	عدد أعضاء لجنة المراجعة الداخلية للبنك (j) في العام i.
X14 j	عدد اجتماعات لجنة المراجعة الداخلية للبنك (j) في العام i.
X15j	نسبة عدد المشاركين في أكثر من بنك للبنك (j) في العام i.
X16j	الخبرة المالية للجنة المراجعة للبنك (j) في العام i
X17j	التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الفروع
X18j	التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد العملاء
X19j	التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني واجمالي الودائع
X20j	التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الصرافات
X21j	التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وحجم الأصول
β13:B21	معاملات نموذج الانحدار المتدرج
ε	بواقي نموذج الانحدار المتدرج.

٤/٨- **اختبار الفروض:** ويوضح الجدول التالي رقم (3) تفريغاً لإحصائيات الإفصاح عن إجراءات الأمن السيبراني من التقارير المالية للبنوك السعودية وفق دليل البنوك السعودية اجمالا ووفق المكونات الفرعية للدليل.

جدول رقم (٣) احصائيات الإفصاح عن إجراءات الأمن السيبراني وفق دليل البنوك السعودية اجمالا ووفق المكونات التفصيلية												المتوسط العام
بيان		الاهلي	الراجحي	الرياض	الأول	العربي	الانماء	الفرنسي	الاستثمار	الجزيرة	البلاد	
مؤشرات الدليل	المتوسط	٤٠	٣٩.٨	٤٠.٤	٤١.٢	٤٢.٦	٤٤.٦	٤٠.٦	٤٥.٤	٤٢.٤	٤٢.٢	٤١.٩٢
	كل المؤشرات (٧٧ مؤشر)											
	النسبة	٥٢٪	٥٢٪	٥٢٪	٥٤٪	٥٥٪	٥٨٪	٥٣٪	٥٩٪	٥٥٪	٥٥٪	٠.٥٤٤٤١٦
التهديدات السيبرانية	المتوسط	٤.٦	٤.٨	٤.٢	٤.٦	٤.٤	٥.٤	٤.٨	٦.٢	٦.٢	٤.٤	٤.٩٦
	كل المؤشرات (١١ مؤشر)											
	النسبة	٤٢٪	٤٤٪	٣٨٪	٤٢٪	٤٠٪	٤٩٪	٤٤٪	٥٦٪	٥٦٪	٤٠٪	٠.٤٥٠٩٠٩
متطلبات الأمن السيبراني الأساسية	المتوسط	١٠	٨.٨	١٠.٢	٩.٨	٨.٢	٩.٢	٩.٦	١٠	٨.٦	٨.٨	٩.٣٢
	كل المؤشرات(١٧ مؤشر)											
	النسبة	٥٩٪	٥٢٪	٦٠٪	٥٨٪	٤٨٪	٥٤٪	٥٦٪	٥٩٪	٥١٪	٥٢٪	٠.٥٤٨٢٣٥
الأمان الإداري للبنوك	المتوسط	٢.٤	٣.٤	٣.٦	٣.٢	٣.٦	٥	٣.٢	٣.٨	٤	٤.٤	٣.٦٦
	كل المؤشرات (٧ مؤشرات)											
	النسبة	٣٤٪	٤٩٪	٥١٪	٤٦٪	٥١٪	٧١٪	٤٦٪	٥٤٪	٥٧٪	٦٣٪	٠.٥٢٢٨٥٧
الاستجابة لحوادث الأمن السيبراني	المتوسط	٤.٦	٤	٤.٦	٤	٤.٨	٥.٨	٤.٦	٦	٥.٢	٤.٢	٤.٧٨
	كل المؤشرات (٩ مؤشر)											
	النسبة	٥١٪	٤٤٪	٥١٪	٤٤٪	٥٣٪	٦٤٪	٥١٪	٦٧٪	٥٨٪	٤٧٪	٠.٥٣١١١١
التدريب والتوعية للموظفين	المتوسط	١٠.٤	١٠	١٠.٤	١٠.٢	١٢.٢	١٠.٤	١١	١١.٦	٩.٦	١١	١٠.٦٨
	كل المؤشرات (١٨ مؤشر)											
	النسبة	٥٨٪	٥٦٪	٥٨٪	٥٧٪	٦٨٪	٥٨٪	٦١٪	٦٤٪	٥٣٪	٦١٪	٠.٥٩٣٣٣٣
التدقيق والمراجعة الأمنية	المتوسط	٨.٢	٨.٦	٧.٤	٩.٦	٩.٢	٩	٨.٢	٧	٧.٨	٩	٨.٤
	كل المؤشرات (١٥ مؤشر)											
	النسبة	٥٥٪	٥٧٪	٤٩٪	٦٤٪	٦١٪	٦٠٪	٥٥٪	٤٧٪	٥٢٪	٦٠٪	٠.٥٦

المصدر: من اعداد الباحث

يتبين من الجدول السابق رقم (٣) ان متوسط الإفصاح عن إجراءات الأمن السيبراني للبنوك السعودية هي ٤٢ مؤشراً تقريبا من بين ٧٧ مؤشراً بنسبة ٥٤٪. وتتفق هذه النتيجة مع دراسة **(Eijkelenboom & Nieuwesteeg, 2021)** والتي ذهبت الى توسع المنشآت في الإفصاح عن معلومات الأمن السيبراني، في حين تختلف مع دراسة **(Héroux & Fortin, 2020)**، والتي ذهبت الى انخفاض مستوي هذا الإفصاح. وقد يرجع ذلك الى اختلاف بيئة التطبيق. كما تبين ان اعلى متوسط للإفصاح كان لمتطلبات التدريب والتوعية الأمنية لموظفي البنك حيث

بلغ متوسط الإفصاح عن ١١ مؤشراً تقريبا من أصل ١٨ مؤشراً بنسبة تصل الى ٦٠٪ تقريبا. وتتفق هذه النتيجة مع ما توصلت اليه دراسات (**قوجيل وطيبة،٢٠٢٢؛ Beshir & Wu et al.,2020;Abdulrahim ,2019; Bashir,2018; Yang & Wang,2020**).

إذ يعد الاهتمام بالتدريب والتوعية للموظفين اهم خطوة للحماية للسيبرانية، ومن ثم تزيد البنوك الإنفاق عليه لرفع مستوى الوعي وتوفير بيئة آمنة للعملاء، بما يحسن الأداء المالي للبنك. كما تبين ان اقل متوسط للإفصاح لإجراءات التعامل مع التهديدات السيبرانية، قد بلغ متوسط الإفصاح عن ٥ مؤشرات من بين ١١ مؤشراً بنسبة ٤٥٪ تقريبا. وتعد هذه النتيجة منطقية، حيث لا ترغب البنوك في الإفصاح الاختياري عن التهديدات السيبرانية التي تتعرض لها.

كما يعرض الجدول رقم (٤) التالي نتائج تحليل الارتباط **Pearson Correlation** في ظل مستوي معنوية ٥٪ أولا لجميع المتغيرات:

جدول رقم (٤) مصفوفة ارتباط Pearson Correlation بين جميع المتغيرات لمفردات العينة

		Y1	X1	X8	X9	X10	X11	X12	X13	X14	X15	X16
Y1	Pearson Correlation	1	.011	-.147	-.025	.352*	-.176	.983**	.373**	-.106	.176	.254
	Sig. (2-tailed)		.941	.307	.865	.012	.221	.000	.008	.463	.220	.076
X1	Pearson Correlation		1	-.162	-.268	-.017	-.219	-.031	.360*	-.067	-.259	-.049
	Sig. (2-tailed)			.261	.060	.907	.127	.830	.010	.644	.069	.738
X8	Pearson Correlation			1	.293*	.211	.935**	.172	.015	.169	.281*	.267
	Sig. (2-tailed)				.039	.142	.000	.231	.915	.242	.048	.061
X9	Pearson Correlation				1	.347*	.302*	.082	-.391**	.064	.229	.262
	Sig. (2-tailed)					.014	.033	.570	.005	.656	.110	.067
X10	Pearson Correlation					1	.227	.310*	-.198	.116	.096	.159
	Sig. (2-tailed)						.112	.028	.167	.423	.506	.271
X11	Pearson Correlation						1	.198	-.014	.090	.326*	.290*
	Sig. (2-tailed)							.169	.925	.533	.021	.041
X12	Pearson Correlation							1	-.380**	-.117	.165	.273
	Sig. (2-tailed)								.007	.418	.252	.055
X13	Pearson Correlation								1	-.004	-.134	-.023
	Sig. (2-tailed)									.979	.354	.873
X14	Pearson Correlation									1	.094	-.057
	Sig. (2-tailed)										.518	.693
X15	Pearson Correlation										1	.459**
	Sig. (2-tailed)											.001
X16	Pearson Correlation											1
	Sig. (2-tailed)											

*. Correlation is significant at the 0.05 level (2-tailed).

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

يخلص الباحث من نتائج الجدول السابق رقم (٤) الى وجود علاقة ارتباط طردية ذات دلالة معنوية عند ٥٪ لمتغيرات اجمالي الودائع وحجم الأصول وعدد أعضاء لجنة المراجعة الداخلية، اما بقية المتغيرات فعلاقتها غير معنوية بالأداء المالي للبنوك. ولتفسير هذه العلاقات يستخدم الباحث نماذج الانحدار المقترحة لاختبار فروض الدراسة من خلال التركيز على مستوي المعنوية ومعامل التحديد R^2، ومعامل التحديد المعدل للتعبير عن القوة التفسيرية للمتغيرات المستقلة كما يلي:

١/٤/٨-اختبار الفرض الأول: يقضى هذا الفرض بعدم اختلاف مستوي الإفصاح عن إجراءات الأمن السيبراني بين البنوك التجارية السعودية وبعضها البعض. ويتم اختباره من خلال مقارنة التباين في الإفصاح عن إجراءات الأمن السيبراني بين بنوك العينة باستخدام تحليل**One way ANOVA**. ويلخص الجدول التالي رقم (٥) نتائج التحليل:

جدول رقم (٥) يوضح نتائج اختبار (ANOVA)

		Sum of Squares	df	Mean Square	F	Sig.
X1	Between Groups	164.080	9	18.231	.802	.617
	Within Groups	909.600	40	22.740		
	Total	1073.680	49			
X2	Between Groups	23.920	9	2.658	1.772	.104
	Within Groups	60.000	40	1.500		
	Total	83.920	49			
X3	Between Groups	21.680	9	2.409	.808	.611
	Within Groups	119.200	40	2.980		
	Total	140.880	49			
X4	Between Groups	22.820	9	2.536	4.528	.000
	Within Groups	22.400	40	.560		
	Total	45.220	49			
X5	Between Groups	21.780	9	2.420	.942	.501
	Within Groups	102.800	40	2.570		
	Total	124.580	49			
X6	Between Groups	27.280	9	3.031	.660	.739
	Within Groups	183.600	40	4.590		
	Total	210.880	49			
X7	Between Groups	31.200	9	3.467	.677	.725
	Within Groups	204.800	40	5.120		
	Total	236.000	49			

يتبين من الجدول السابق رقم (٥) ان قيمة مستوي المعنوية الخاصة بجميع المتغيرات < ٥٪ سواء للدليل ككل او لمكوناته الفرعية فيما عدا **X4** الخاص بمتطلبات الأمان الإداري للبنوك، حيث يبلغ مستوي المعنوية **000.** < ٥٪. ويعد هذا الاختلاف منطقي، كونه يرتبط باستراتيجية وسياسة كل بنك في التعامل مع إجراءات الأمن السيبراني. ويؤكد ذلك معرفة المؤشرات التفصيلية له والتي تتمثل في تحديد مسؤوليات الأمن السيبراني، من خلال توفير تفاصيل الأذونات لموظفي البنك، وتحديد صلاحيات الوصول إلى الأنظمة والبيانات داخل البنك وفرض إجراءات صارمة حول كيفية هذا الوصول، وضبطها على أساس الحاجة والحد الأدنى للصلاحيات. ويتم وضع إجراءات إدارية واضحة للحد من المخاطر السيبرانية، من خلال التحقق من الهوية والوصول وتحديد الصلاحيات وإدارة التغيير وتطوير خطط التعامل مع الحوادث والتدقيق الداخلي والتدقيق الخارجي، وتحديد معايير أمان الأنظمة والبيانات. كما يتم أيضا تطوير وتحديث سياسات الأمن السيبراني بشكل دوري وتوفير الحماية اللازمة للأنظمة والبيانات والعملاء، والالتزام بالمعايير القانونية والتنظيمية، وتوفير الدعم والتقنيات اللازمة للتعامل مع التهديدات السيبرانية. كما يتم تدريب موظفي البنك لزيادة الوعي الأمني عن التهديدات السيبرانية، مع التدقيق والتقييم الدوري لإجراءات الأمن السيبراني، على ان تقييم هذه الإجراءات دوريا لتحسينها. ووفقا لنتائج الجدول السابق يتم قبول فرض العدم الأول، حيث لا يختلف مستوي الإفصاح عن إجراءات الأمن السيبراني بين البنوك التجارية السعودية وبعضها البعض. وتختلف هذه النتيجة مع دراسات **(موسي وآخرون ،٢٠٢٣، Héroux & Fortin, 2020)**. وقد يرجع سبب الاختلاف في اعتماد هذه الدراسات على قطاعات مختلفة وتركيز الدراسة الحالية على البنوك التجارية فقط، التي تلتزم أكثر بالإفصاح عن إجراءات الأمن السيبراني في السعودية بسبب صرامة التشريعات والإجراءات، إضافة الى اعتماد هذه الدراسة على بيانات فعلية.

٨/٤/٢-اختبار الفرض الثاني: تم اختبار هذا الفرض من خلال تطبيق نموذج الدراسة المقترح الأول لاختبار معنوية العلاقة بين الإفصاح عن إجراءات الامن السيبراني والأداء المالي للبنوك التجارية السعودية، مع إضافة المتغيرات الرقابية لجودة لجنة المراجعة

الداخلية **(حجم اللجنة وعدد اجتماعاتها ونسبة الأعضاء المشاركين في أكثر من شركة والخبرة المالية للجنة)**. ويتم التركيز على الإشارة ومستوي المعنوية ونتيجة اختبار F ومعامل التحديد المعدل **Adj R^2** من واقع جدول تحليل التباين،**ANOVA** للنموذج ككل، لبيان المعنوية واتجاه العلاقة، وتحديد الجزء المفسر. ويلخص الجدول رقم (٦) نتائج النموذج وقيم معاملات الانحدار:

جدول رقم (٦) يوضح نتائج علاقة الإفصاح عن إجراءات الأمن السيبراني بالأداء المالي للبنك (العائد على الأصول)

بيان	الرمز	Sig.	F	Adj R^2
النموذج ككل		.300a	2.925	.302
المتغيرات المستقلة والرقابية		Sig.	t-test	Coefficients (Beta)
الدليل ككل	X1	.222	-1.240	-.193
عدد أعضاء لجنة المراجعة الداخلية	X13	.066	1.886	.286
عدد اجتماعات اللجنة	X14	.882	-.150	-.021
المشاركين في أكثر من شركة	X15	.053	1.985	.325
الخبرة المالية للجنة المراجعة	X16	.984	.020	.003

يتبين من نتائج الجدول السابق رقم (٦) ان النموذج ككل غير معنوي عند مستوي معنوية **.300** **>٥٪**، كما بلغت نسبة معامل التحديد المعدل **30.2%**. وتفسر هذه النسبة التغير في الأداء المالي للبنوك نتيجة التغير في الإفصاح عن إجراءات الامن السيبراني، وتؤكد هذه النتيجة انخفاض إحصائية F. وتدعم هذه النتيجة ضرورة الاستجابة لتوصية تقرير أمن المعلومات في الشرق الأوسط" **لشركة Cisco لعام ٢٠٢١** بضرورة تعزيز القدرة على الاستجابة للهجمات السيبرانية في المنطقة، من خلال إنشاء فرق الاستجابة للطوارئ السيبرانية، وتعزيز القوانين واللوائح السيبرانية في المنطقة، لتعزيز الحماية القانونية للمعلومات، وتطوير إجراءات الأمن السيبراني، ومن ثم زيادة الإفصاح عنها. كما تختلف هذه النتيجة مع دراسات **(Al-Ahmari& Al-Rashidi,2018;Al-Suwailem,2020;López,2022;Batista,2022;cheong,2021; Zhang,2022)، موسي وآخرون، ٢٠٢٣**. ويرجع ذلك الى التركيز على قطاع البنوك فقط، واعتماد هذه الدراسة على بيانات فعلية بخلاف الدراسات السابقة التي اعتمدت في معظمها على

قوائم استقصاء. ووفقا لهذه النتيجة يقبل الباحث فرض العدم الثاني، حيث لا توجد علاقة معنوية بين الإفصاح عن إجراءات الامن السيبراني والأداء المالي للبنوك التجارية السعودية.

٨/٤/٣-اختبار الفرض الرئيسي الثالث وفروضه الفرعية: تم اختبار هذا الفرض من خلال تطبيق نموذج الدراسة المقترح الأول لاختبار العلاقة بين مقاييس تعقيد عمليات البنك كمتغيرات مستقلة، والاداء المالي للبنك كمتغير تابع، مع نفس المتغيرات الرقابية. وبنفس آلية اختبار الفرض السابق. ويلخص الجدول رقم (٧) نتائج النموذج وقيم معاملات الانحدار:

جدول رقم (٧) يوضح نتائج علاقة تعقيد عمليات البنك والاداء المالي للبنك				
بيان	الرمز	Sig.	F	Adj R^2
النموذج ككل		.000a	18.575	.594
المتغيرات المستقلة والرقابية		Sig.	t-test	Coefficients (Beta)
عدد الفروع	X8	.629	.488	-.194
عدد العملاء	X9	.521	-.650	-.095
اجمالي الودائع	X10	.005	3.067	.357
عدد الصرافات	X11	.894	.134	-.071
حجم الأصول	X12	.050	-2.002	.246
عدد أعضاء لجنة المراجعة	X13	.437	.787	.341
عدد الاجتماعات لجنة المراجعة	X14	.918	.103	.015
المشاركين في أكثر من شركة	X15	.180	-1.374	-.234
الخبرة المالية للجنة المراجعة	X16	.001	3.856	2.584

يتبين من نتائج الجدول السابق رقم (٧) ان النموذج ككل معنوي عند مستوي معنوية **000>** ٥٪، وبلغت نسبة معامل التحديد المعدل **59.4%**، وهي أعلى من نفس النسبة المقابلة في الفرض الثاني السابق. بما يعني تحسن القوة التفسيرية للنموذج. وتؤكد هذه النتيجة ارتفاع قيمة إحصائية F ، حيث زادت من **2.925** الى **18.575**.وتتفق هذه النتيجة مع الإطار النظري للبحث في ان تعقيد العمليات يؤثر على الأداء المالي للبنك، كما تتفق مع نتائج

دراسات **(Al-Sheikh & Al-Olyan,2020;Al-Qahtani & Al-Maneea,2019; Al-Shammary & Al-Samayi,2021)**. وتفسير ذلك هو ان تعقيد عمليات البنك يزيد من المخاطر السيبرانية، ومن ثم يزيد من إجراءات الأمن السيبراني للبنك. وتعد هذه المعلومات هامة للأطراف ذات العلاقة، لذلك يتم التوسع في الإفصاح عن هذه المعلومات. ووفقاً لنظرية الإشارة فإن هذا يعطي إشارات إيجابية للمستثمرين على قيام البنك بالإجراءات اللازمة، بما يحسن الأداء المالي للبنك. كما تقدم هذه النتيجة دليلاً تطبيقياً لعله الأول في السوق السعودي– على حد علم الباحث– حول علاقة تعقيد عمليات البنك بالأداء المالي للبنك. ويخلص الباحث بما سبق الى رفض فرض العدم الرئيسي الثالث، حيث توجد علاقة معنوية بين تعقيد عمليات البنك والاداء المالي للبنك. ورغبة من الباحث في تحقيق مزيد من التحليل حول أثر كل مقياس من مقاييس تعقيد عمليات البنك يقوم الباحث باختبار الفروض الفرعية لكل مقياس على حده كما يلي:

٨/٣/٤/١– اختبار الفرض الفرعي الأول: يختبر هذا الفرض معنوية العلاقة بين عدد الفروع والاداء المالي للبنك. ويتبين من الجدول السابق وجود علاقة عكسية غير معنوية بين المتغيرين، حيث بلغ مستوي المعنوية **.629> ٥٪**. وتدعم هذه النتيجة دراسات **(Zaki, & Hassan, 2018; Nyola et al,2021)**، حيث يؤثر زيادة عدد الفروع والتعقيد الجغرافي سلباً على الأداء المالي للبنوك، ويفسر ذلك بواسطة نظرية التكاليف الإدارية **(transaction cost theory)** نتيجة زيادة تكاليف التنسيق وتقليل الكفاءة، ونظرية الموارد المعتمدة على الرؤية **(resource-based view)**، حيث يُصعب التعقيد من عملية اتخاذ القرارات، ويؤثر على تخصيص الموارد بشكل فعال بما يزيد المخاطر التي يتعرض لها البنك. ووفقا لهذه النتيجة يقبل الباحث فرض العدم الفرعي الأول.

٨/٣/٤/٢– اختبار الفرض الفرعي الثاني: يختبر هذا الفرض معنوية العلاقة بين عدد العملاء والاداء المالي للبنك. ويتبين من الجدول السابق وجود علاقة عكسية غير معنوية بين عدد العملاء والاداء المالي للبنك، حيث يبلغ مستوي معنوية **.521>٥٪**. وتدعم هذه النتيجة دراسة **(الخطيب وعبد الحليم، ٢٠١٨)**. وتفسير ذلك ان زيادة عدد العملاء يشير

الى تنوع الخدمات المصرفية بما يحمل البنك تكاليف إضافية، ويؤثر ذلك سلبا على الأداء المالي للبنك. ويخلص الباحث بذلك الي قبول فرض العدم الفرعي الثاني.

٨/٣/٤/٣- اختبار الفرض الفرعي الثالث: يختبر هذا الفرض معنوية العلاقة بين إجمالي الودائع والاداء المالي للبنك. ويبين الجدول السابق وجود علاقة طردية معنوية بين المتغيرين حيث بلغ مستوي المعنوية ٥٪ تماما، وتدعم هذه النتيجة دراسة **(Larsen et al, 2019)** والتي خلصت الى أن التعقيد يؤثر بشكل متناقض على أداء المنشأة، لوجود تأثير إيجابي على الأداء الابتكاري والنمو، وتأثير سلبي على الأداء المالي. ويفسر هذا التناقض بواسطة نظرية الموانع والفرص **(barriers & opportunities theory)**، فقد يعيق التعقيد العمليات الداخلية والتنفيذية، لكنه يوفر فرصاً للابتكار والتطوير. كما تقدم دليلاً إضافياً حول الاثر الإيجابي الناتج عن جذب مزيد من الودائع، بما يعني زيادة فرص الاستثمار، وجذب ثقة المودعين والمستثمرين بما يحسن من الاداء المالي للبنك. وتتفق هذه النتيجة مع **دراسة (السلطان والجليد، ٢٠٢٠)**. كما تتفق مع مقتضي نظرية الشرعية بزيادة مستوي الإفصاح عن المعلومات الجيدة. ويخلص الباحث الي رفض فرض العدم الفرعي الثالث.

٨/٣/٤/٤-اختبار الفرض الفرعي الرابع: يختبر هذا الفرض معنوية العلاقة بين عدد الصرافات والاداء المالي للبنك. ويتبين من الجدول السابق وجود علاقة عكسية غير معنوية بين عدد الصرافات والاداء المالي للبنك، حيث بلغ مستوي المعنوية**894.** <٥٪. وتدعم هذه النتيجة دراسة **(Houghton,et al, 2009)**. كما تختلف عما توصلت اليه دراسة **(Al-Shammary & Al-Samayi,2021)**، حيث تواجه المنشآت التي تمتلك شبكات متعددة تحديات أكثر تعقيداً. ويفسر ذلك بواسطة نظرية الرأسمالية الاجتماعية **(social capital theory)**، حيث تزداد إجراءات الحماية السيبرانية لمواقع متعددة نتيجة تعدد الصرافات. وتدعم هذه النتيجة الفرض الفرعي الأول والثاني. وبالتالي يتم قبول فرض العدم الفرعي الرابع.

٨/٣/٤/٥-اختبار الفرض الفرعي الخامس: يختبر هذا الفرض معنوية العلاقة بين حجم الأصول والاداء المالي للبنك. ويتبين من الجدول السابق وجود علاقة طردية معنوية بينهما عند مستوي معنوية ٥٪. وتدعم هذه النتيجة دراسات **(Al Eidan& Alsubaie,2019;**

Al-Shammary & Al-Samayi,2021). ويرجع ذلك الى أن زيادة اجمالي الأصول يعني زيادة فرص الاستثمار امام البنك. وتقدم دليلاً إضافياً حول الاثر الإيجابي لزيادة حجم الأصول على الاداء المالي للبنك في السوق السعودي. ووفقا للنتيجة السابقة يتم رفض الفرض الفرعي الخامس.

اما عن علاقات المتغيرات الرقابية لجودة لجنة المراجعة بالأداء المالي، فتبين نتائج الجدول السابق وجود علاقة طردية معنوية بين الخبرة المالية للجنة المراجعة والأداء المالي للبنك بمستوي معنوية ٥٪، وتدعم هذه النتيجة **دراسة (عبد الفتاح، ٢٠٢١، أبو الخير وطه،٢٠٢٣)**. ويرجع ذلك الي ان توفر التأهيل المالي المناسب يساعد أعضاء اللجنة على مناقشة الموضوعات والفقرات التي يمكن الإفصاح عنها بشكل مفصل، بما يؤثر ايجابيا على الأداء المالي للبنك.

٨/٤/٤-اختبار الفرض الرئيسي الرابع وفروضه الفرعية: خلص الباحث من اختبار الفرض الثاني الى عدم وجود علاقة معنوية بين الإفصاح عن إجراءات الامن السيبراني والأداء المالي للبنوك السعودية، كما خلص الباحث في الفرض الثالث الى وجود علاقة طردية معنوية بين تعقيد عمليات البنك والأداء المالي للبنوك. وتعميقا لهذا التحليل يتم اختبار هذا الفرض من خلال تطبيق نموذج الدراسة المقترح الثاني لتحديد معنوية العلاقة المشتركة بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك، مع نفس المتغيرات الرقابية. وبنفس الية اختبار الفرض السابق. ويلخص الجدول رقم (٨) نتائج النموذج وقيم معاملات الانحدار:

جدول رقم (٨) يوضح نتائج علاقة تعقيد عمليات البنك والاداء المالي للبنك مقاس بالعائد على الأصول				
بيان	الرمز	Sig.	F	Adj R^2
النموذج ككل		.000a	98.738	.947
المتغيرات المستقلة والرقابية		Sig.	t-test	Coefficients (Beta)
عدد أعضاء لجنة المراجعة	X13	.152	-1.460	-.058
عدد الاجتماعات لجنة المراجعة	X14	.723	.356	.013
المشاركين في اكثر من شركة	X15	.202	1.297	.050
الخبرة المالية للجنة المراجعة	X16	.906	-.119	-.005
التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الفروع	X17	.431	-.796	-.075
التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد العملاء	X18	.097	-1.702	-.068
التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وحجم الودائع	X19	.022	2.392	.090
التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الصرافات	X20	.800	.255	-.024
التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وحجم الأصول	X21	.000	22.906	.932

يتبين من نتائج الجدول السابق رقم (٨) ان النموذج ككل معنوي عند مستوي معنوية **000>** ٥٪، مع تحسن معامل التحديد المعدل **94.7%**، بما يعني وجود تحسن كبير في القوة التفسيرية للنموذج، وتؤكد هذه النتيجة ارتفاع قيمة إحصائية F ، حيث وصلت الى **98.738.** وكلما تحسن معامل التحديد وارتفعت قيمة F الإحصائية تحسنت القوة التفسيرية للنموذج.

وقد يرجع هذا التحسن الى استخدام العلاقة المشتركة بين التعقيد والافصاح عن مخاطر الامن السيبراني. كما تقدم هذه النتيجة دليل تطبيقي لعله الأول–وفقا لعلم الباحث– على أثر التفاعل المشترك بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك السعودية. ويرجع تفسير هذه النتيجة الى ان تعقيد عمليات البنك يدفع البنك الى اتخاذ إجراءات أكثر تعقيدا مثل زيادة التوسع في استخدام والاعتماد على التكنولوجيا الحديثة لإدارة عملياته بشكل أكثر كفاءة، او تطوير أنظمة وإجراءات مناسبة لإدارة العمليات بشكل آمن وفعال، او زيادة المبالغ المخصصة لتدريب الموظفين على كيفية التعامل مع العمليات المعقدة، ومع مخاطر الامن السيبراني. ومن ثم فإن التفاعل المشترك بين المتغيرين قد ادي الى زيادة الافصاح، حيث أن هذه المعلومات هامة للأطراف ذات العلاقة، كما يعطي للإفصاح عن هذه المعلومات إشارات إيجابية للمستثمرين على قيام البنك بالإجراءات اللازمة، بما زاد من تأثيره على الأداء المالي للبنك. كما تدعم هذه النتيجة نتيجة الفرض الرئيسي الثالث السابق. ويخلص الباحث بما سبق الى رفض فرض العدم الرئيسي الرابع. ورغبة من الباحث في تحقيق مزيد من التحليل حول الأثر المشترك لكل مقياس من مقاييس التعقيد يختبر الفروض الفرعية التالية:

٨/٤/٤/١– اختبار الفرض الفرعي الأول: يختبر هذا الفرض معنوية علاقة التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الفروع على الاداء المالي للبنك. ويتبين من الجدول السابق وجود علاقة عكسية غير معنوية بين المتغيرين، حيث بلغ مستوي المعنوية **.431>٥٪**. وتدعم هذه النتيجة نتيجة الفرض الفرعي الأول من الفرض الرئيسي الثالث السابق، وتفسير ذلك يعود الى ان زيادة عدد الفروع يؤدي الى زيادة تعقيد عمليات البنك نتيجة زيادة الحاجة الى أنظمة وإجراءات أكثر تعقيداً، بما يؤدي إلى زيادة التكاليف. ويؤثر على الأداء المالي للبنك. ويخلص الباحث بما سبق الي قبول فرض العدم الفرعي الأول.

٨/٤/٤/٢– اختبار الفرض الفرعي الثاني: يختبر هذا الفرض معنوية العلاقة بين التفاعل المشترك للإفصاح عن إجراءات الامن السيبراني وعدد العملاء على الاداء المالي للبنك. ويتبين من الجدول السابق وجود علاقة عكسية غير معنوية بين المتغيرين، حيث بلغ مستوي المعنوية **.097>٥٪**. وتدعم هذه النتيجة دراسة **(Larsen et al, 2019)** التي خلصت الى

أن التعقيد يؤثر بشكل متناقض على أداء المنشأة، فالمنطق يقضي بأن زيادة عدد العملاء معلومة جيدة، تدفع إدارة البنك الى تحسين الأداء الابتكاري والنمو، بما يحسن الأداء المالي، لكن هذه الزيادة قد تزيد من مخاطر الأخطاء البشرية، بما قد يؤدي إلى خسائر مالية للبنك. وتدعم هذه النتيجة نتيجة الفرض الفرعي الثاني من الفرض الثالث الرئيسي السابق، بما يقدم دليل تطبيقي إضافي حول أثر التفاعل المشترك بين عدد العملاء والافصاح عن إجراءات الامن السيبراني على الاداء المالي للبنوك السعودية. ويخلص الباحث بذلك الي قبول فرض العدم الفرعي الثاني.

٨/٤/٤/٣- **اختبار الفرض الفرعي الثالث:** يختبر هذا الفرض معنوية العلاقة بين التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وحجم الودائع على الاداء المالي للبنك. ويبين الجدول السابق وجود علاقة طردية معنوية بين المتغيرين حيث بلغ مستوي المعنوية**.022> ٥**٪. وتدعم هذه النتيجة نتيجة الفرض الفرعي الثالث من الفرض الرئيسي الثالث السابق، وتفسير ذلك يعود الى ان زيادة حجم الودائع معلومة جيدة يتم الإفصاح عنها وفق ما تقضي به نظرية الإشارة، ويجعل ذلك البنك أكثر جاذبية لهجمات المهاجمين بسبب زيادة الأموال به، بما يجعل البنك يتخذ مزيداً من إجراءات الحماية السيبرانية، ومن ثم تزيد المعلومات المفصح عنها الخاصة بهذه الإجراءات. وتقدم هذه النتيجة دليلاً تطبيقياً إضافياً حول الاثر الإيجابي الناتج عن جذب مزيد من الودائع على الاداء المالي للبنك. ويخلص الباحث الي رفض فرض العدم الفرعي الثالث.

٨/٤/٤/٤-**اختبار الفرض الفرعي الرابع:** يختبر هذا الفرض معنوية العلاقة بين التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الصرافات على الاداء المالي للبنك. ويبين الجدول السابق وجود علاقة عكسية غير معنوية، حيث بلغ مستوي المعنوية **.800>٥**٪. وتدعم هذه النتيجة نتيجة الفرض الفرعي الرابع من الفرض الرئيسي الثالث السابق، حيث تتطلب زيادة عدد الصرافات زيادة إجراءات الحماية السيبرانية لمواقع متعددة، بما يؤدي إلى انخفاض الكفاءة، وانخفاض الأرباح. وتدعم هذه النتيجة الفرضين الفرعيين الأول والثاني. وبالتالي يتم قبول فرض العدم الفرعي الرابع.

٨/٤/٤/٥-**اختبار الفرض الفرعي الخامس:** يختبر هذا الفرض معنوية العلاقة بين التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وحجم الأصول والاداء المالي للبنك. ويتبين من الجدول السابق وجود علاقة طردية معنوية بينهما، حيث مستوي المعنوية**.000>** ٥٪. وتدعم هذه النتيجة نتيجة الفرض الفرعي الخامس من الفرض الثالث الرئيسي السابق، بما يقدم دليلاً تطبيقياً إضافياً حول الاثر الإيجابي لزيادة حجم الأصول على الاداء المالي للبنك في سوق البنوك السعودي، نتيجة جذب ثقة المودعين والمستثمرين وزيادة فرص الاستثمار امام البنك. كما تعد معلومة حجم الأصول من المعلومات الهامة والتي يجب الإفصاح عنها بمقتضي نظرية الشرعية، كما تعتبر معلومة جيدة يتم الإفصاح عنها بمقتضي نظرية الإشارة. ويخلص الباحث الي رفض فرض العدم الفرعي الخامس. اما العلاقة مع المتغيرات الرقابية لجودة لجنة المراجعة الداخلية فجميعها غير معنوية عند مستوي معنوية ٥٪.

٩-النتائج والتوصيات والبحوث المستقبلية: -

٩/١ - النتائج: أدت زيادة الهجمات السيبرانية الى زيادة الاهتمام بإجراءات الأمن السيبراني في البنوك كونها أكثر عرضة من غيرها لهذه الهجمات. ويمثل الإفصاح عن هذه المعلومات تحدياً امام الإدارة، لتحديد مستوي الإفصاح المناسب من هذه المعلومات، والتي حتما ستصل الى السوق سواء عن طريق التقارير المالية او غيرها، ومن الأفضل ان تصل عن طريق التقارير المالية. وقد تناولت الدراسة أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي. لذلك أثارت هذه الدراسة أربعة تساؤلات رئيسية، الأول هل تختلف مستويات الإفصاح عن إجراءات الأمن السيبراني وفقا لدليل البنوك السعودية فيما بينها؟ والثاني ما هي العلاقة بين الإفصاح عن إجراءات الأمن السيبراني وفقا لهذا الدليل وأداء البنك؟ اما الثالث فيتمثل في ما هي العلاقة بين تعقيد عمليات البنوك السعودية وادائها؟ بينما يتضمن التساؤل الرابع ما هو أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات الأمن السيبراني على الأداء المالي؟ وتمثل الإجابة عن هذه التساؤلات اهداف البحث. كما تمثلت عينة الدراسة في جميع البنوك السعودية المرخصة والمسجلة في تداول وعليها تداول نشط خلال الفترة من ٢٠١٨ الى

٢٠٢٢، حيث بلغ عدد المشاهدات ٥٠ مشاهدة. وتم تجميع البيانات من واقع التقارير المالية المنشورة للبنوك والمواقع الالكترونية لها. ولقد خلص الباحث الى النتائج التالية:

– تؤثر إجراءات الأمن السيبراني على الأداء المالي للبنوك، كونها تساعد في حمايتها من الخسائر الناتجة عن الهجمات السيبرانية، ويخفض تكاليف التعافي منها، ويزيد من دقة وموثوقية البيانات المالية، ويحسن من سمعة البنك.

– تعتمد البنوك كسائر المنشآت عند تطبيق إجراءات إدارة مخاطر الأمن السيبراني على معايير وإرشادات عالمية مثل **ISO 27001،ISO 27002** او محلية مثل الدليل الاسترشادي للبنوك الصادر عن هيئة السوق المالية السعودية لتحقيق أقصى قدر من الحماية. ولقد ركزت الدراسة على الدليل الأخير عند اجراء الدراسة التطبيقية.

– تقع مسئولية إنشاء وتحسين نظام لإدارة مخاطر الأمن السيبراني على الإدارة، وفق الاتجاهات الاستراتيجية والعمليات التشغيلية لها، لتحقيق التحسين المستمر، والموازنة بين السلطة والمسئولية.

– تراعي البنوك عند تقييم إجراءات وتقنيات إدارة مخاطر الامن السيبراني المزايا طويلة الاجل مثل إمكانيات التحديث والقابلية للتعديل، وتوفير خدمات الدعم الفني، بما يحسن سمعتها، ويجذب مزيداً من المودعين، وينعكس إيجابا على الأداء المالي لها.

– يؤدي رفع وعي وقدرات ومهارات العنصر البشري–خاصة المحاسبين والمراجعين – عند التعامل مع مخاطر الامن السيبراني، الى تراكم الخبرة الفنية التقنية لديهم، بما يساعد في الحماية من الهجمات السيبرانية.

–لا يختلف مستوي الإفصاح عن إجراءات الأمن السيبراني وفق الدليل الاسترشادي للبنوك الصادر عن هيئة سوق المال السعودية بين البنوك التجارية السعودية، فيما عدا متطلبات الأمان الإداري، كونها ترتبط باستراتيجية كل بنك في التعامل مع هذه الإجراءات.

– لا توجد علاقة معنوية بين الإفصاح عن إجراءات الامن السيبراني وفقا للدليل كامل والأداء المالي للبنوك التجارية السعودية في ظل مستوي معنوية ٥٪.

– اختلفت معنوية العلاقة بين المقاييس المختلفة لتعقيد عمليات البنك والأداء المالي، حيث تبين وجود علاقة طردية معنوية بين متغيرات إجمالي الودائع واجمالي الأصول والأداء المالي للبنك كمتغير تابع. في حين لا توجد علاقة معنوية بين عدد الفروع وعدد العملاء وعدد الصرافات وأداء البنك المالي كمتغير تابع، في ظل مستوي معنوية ٥٪.

– يوجد تأثير معنوي للتفاعل المشترك بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك السعودية، بمستوي معنوية ٥٪.

– توجد علاقة معنوية لأثر متغيري التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وحجم الودائع، والتفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وحجم الأصول على الأداء المالي للبنك بمستوي معنوية ٥٪. في حين لا توجد علاقة معنوية لأثر متغيرات التفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الفروع، والتفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد العملاء، والتفاعل المشترك بين الإفصاح عن إجراءات الامن السيبراني وعدد الصرافات على الأداء المالي للبنك بمستوي معنوية ٥٪.

–تمثلت مساهمة الباحث في اختبار العلاقة بين الإفصاح عن إجراءات الامن السيبراني وفق الدليل الاسترشادي للبنوك الصادر عن هيئة سوق المال السعودية وتعقيد عمليات البنك على الأداء المالي للبنك اعتمادا على بيانات فعلية. كما انها الدراسة الأولى –على حد علم الباحث –التي تختبر العلاقة المشتركة بين تعقيد عمليات البنك والافصاح عن إجراءات الامن السيبراني على الأداء المالي للبنوك السعودية.

٢/٩–التوصيات: يوصي الباحث بالتوصيات التالية:

– اصدار لجنة معايير اعداد التقارير المالية الدولية معيار خاص بإدارة مخاطر إجراءات الامن السيبراني لتعزيز الإفصاح عنه بما يفيد مستخدمي المعلومات المحاسبية.

– ادراج دليل لإدارة مخاطر الامن السيبراني في القطاع المصرفي ضمن توصيات اللجان المصرفية الدولية مثل بازل، وانشاء مراكز بحثية خاصة بإدارة مخاطر الامن السيبراني

بالبنوك تهتم بالتدريب وتحديد الإجراءات الواجب تطبيقها في البنوك التقليدية والبنوك الإسلامية.

-اصدار الجهات المهنية معيار لمراجعة إجراءات إدارة مخاطر الامن السيبراني في البنوك.

-توافر الإمكانيات التكنولوجية للجنة المراجعة الداخلية بالبنوك لتمكينها من وضع الضوابط الأمنية الكافية للحماية من الهجمات السيبرانية، بما يحسن الإفصاح عن المخاطر السيبرانية.

-إصدار البنك المركزي السعودي قانون ملزم للبنوك للإفصاح عن إجراءات الأمن السيبراني، أسوةً بالبورصة الأمريكية أو الكندية، لمواكبة زيادة التعرض للهجمات السيبرانية، رؤية ٢٠٣٠.

-اجراء دراسات مقارنة بين الأسواق المالية المختلفة للعلاقة بين الإفصاح عن إجراءات الأمن السيبراني والاداء المالي، مع مراعاة أثر جودة المراجعة على هذه العلاقة.

-إجراء مزيد من الأبحاث لقياس آثار إدارة مخاطر الامن السيبراني في ظل تعقيد هيكل الملكية على الأداء المالي لقطاعات مختلفة.

- تشجيع المنشآت على اعداد تقرير عن مدي التزامها بمتطلبات إدارة مخاطر الامن السيبراني ومزايا تطبيقه، وامتثالها لإرشادات **ISO 27001**، **ISO 27002** لحين اصدار إرشادات محلية.

- تشجيع شركات التأمين على إصدار وثائق تأمين ضد المخاطر السيبرانية في البنوك.

٣/٩-البحوث المستقبلية: يقترح الباحث تناول الموضوعات البحثية التالية:

-الإفصاح عن تقرير إدارة مخاطر الامن السيبراني كمتغير معدل للعلاقة بين دقة توقعات المحللين الماليين والاداء المالي.

-أثر التفاعل المشترك بين آليات حوكمة الشركات والإفصاح عن مخاطر إدارة الامن السيبراني على الخسائر الائتمانية المتوقعة في البنوك – دراسة مقارنة بين البنوك التقليدية والاسلامية.

-أثر الإفصاح عن تقرير إدارة مخاطر الامن السيبراني على قرارات منح الائتمان والقرارات الاستثمارية في البنوك التجارية والاستقرار المالي.

١٠- قائمة المراجع

١٠/١-المراجع باللغة العربية:

- أبو الخير، أسامة أحمد محمد، أبو موسي، أحمد عبد السلام أحمد، عمران، رجب محمد ،٢٠٢٣، إطار مقترح لاستخدام م تكنولوجيا البلوك تشين Block chain كمرتكز لتعزيز جودة عملية المراجعة في ظل بيئة التحول الرقم" مع دراسة ميدانية في بيئة الاعمال المصرية، ***المؤتمر العلمي الدولي الأول، القيادة الرقمية للفكر المحاسبي ركيزة التميز المهني في بيئة المعلوماتية الفورية بين براعة الفكر...واحترافية التطبيق***"، قسم المحاسبة والمراجعة – كلية التجارة – جامعة مدينة السادات، ٣٢٦: ٣٧٦.

-أبو موسى، أحمد عبدالسلام،٢٠٠٤، أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية، دراسة تطبيقية على المنشآت السعودية، ***مجلة التجارة والتمويل***، جامعة طنطا، العدد الثاني، ص ١: ٥٤.

-الخطيب، علي، وعبد الحليم، جميلة. (٢٠١٨). تأثير التعقيد التنظيمي على الأداء المالي للبنوك الأردنية: دراسة تحليلية. ***المجلة الأردنية للعلوم الاقتصادية***، ٤٤(٣)، ٣٢٥-٣٠٧.

- الرشيدي، طارق عبد العظيم، داليا عباس،٢٠١٩، أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول، دراسة مقارنة في قطاع تكنولوجيا المعلومات، ***مجلة المحاسبة والمراجعة***، كلية التجارة، جامعة بني سويف، المجلد ٨، العدد الثاني، ص ٤٣٩ ٤٨٧.

- الأمير، شمران عبيد خليف، (٢٠٢٢)، أثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني Al Kut ***Journal of Economics and Administrative Sciences,*** 14(45).

- السلطان، عبد العزيز، والجليد، عبد الله. (٢٠٢٠). تأثير الأمن السيبراني على الأداء المالي للبنوك الإسلامية: دراسة تحليلية في المملكة العربية السعودية. ***مجلة العلوم الاجتماعية والإنسانية***، ٤(١)، ٢١-٣٨.

-العيسوي، عبد الحميد وأيمن أبو النضر. ٢٠٢٠. انعكاسات التطورات التكنولوجية فى مجال سلاسل الكتل على أنشطة ومهنة المراجعة مع دراسة استكشافية فى البيئة المصرية. ***مجلة الإسكندرية للبحوث المحاسبية***، كلية التجارة، جامعة الإسكندرية، ٣(٤): ١- ٩١.

-النقيب، سحر عبد الستار، (٢٠٢٠)، دراسة أثر IFRS 9 وجائحة كورونا على الخصائص النوعية للمعلومات المحاسبية بالتطبيق على البنوك المقيدة بالبورصة المصرية، ***مجلة الإسكندرية للبحوث المحاسبية***، جامعة الإسكندرية، عدد خاص بالمؤتمر العلمي الرابع لقسم المحاسبة والمراجعة، ديسمبر، ص ١-٥٧.

-أنديجاني، دلال صالح، و فلمبان، فدوى ياسين، ٢٠٢١، ممارسات تعزيز الوعي بثقافة الأمن السيبراني وتوصياتها في المملكة العربية السعودية. ***المجلة العربية للمعلوماتية وأمن المعلومات***، ع٥، أكتوبر، ص ٧٥: ١٠٢.

-رشوان، عبد الرحمن محمد سليمان، زينب عبدالحفيظ أحمد قاسم،٢٠٢٢، أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، ***المؤتمر العلمي الدولي الأول بعنوان" أثر الأمن السيبراني على الأمن الوطني"خلال الفترة ٢٠ - ٢١ /ديسمبر/ ٢٠٢٢***، جامعة عمان العربية بالاشتراك مع مديرية الأمن العام، ص ١: ٢٨.

-شحاتة، شحاتة السيد. (٢٠٢٢)، نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في المنشآت المقيدة بالبورصة المصرية. ***المجلة العلمية للدراسات والبحوث المالية والإدارية***، جامعة مدينة السادات، كلية التجارة، مج ١٣ , ع ٢، ص ٢٦ :٣٧

- .....، ٢٠٢٠، إطار مقترح لإسناد وظيفة المراجعة الداخلية بدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر في الوحدات الصغيرة ومتوسطة الحجم. ***المجلة العلمية للتجارة والتمويل***، كلية التجارة، جامعة طنطا، ٤٠، ص١٠٩ – ١٢٨.

- شرف، إبراهيم احمد إبراهيم،٢٠٢٣، اثر افصاح المنشآت عن إدارة مخاطر الامن السيبراني على قرارات المستثمرين المصريين غير المحترفين- دراسة تجريبية، ***مجلة الإسكندرية للبحوث المحاسبية***، قسم المحاسبة والمراجعة، كلية التجارة، جامعة الاسكندرية، العدد الاول، المجلد السابع، ص ٢١١ – ٢٨٢.

- عبد الباقي، محمد أحمد عبد الباقي، ومحمد صلاح الدين عبد الرازق، وأحمد محمد أبو عوض،٢٠٢١، تعقيد العمليات المصرفية وأثره على المخاطر التشغيلية، ***المجلة المصرية للدراسات المالية والاقتصادية***، المجلد ١٩، العدد ٤، ٢٠٢١

-على، محمود أحمد، صالح علي،٢٠٢٢، أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم المنشآت المقيدة بالبورصة المصرية: دراسة تجريبية، ***مجلة الإسكندرية للبحوث المحاسبية***، قسم المحاسبة والمراجعة العدد الثالث سبتمبر، المجلد السادس، ص ١: ٤٨.

-على، هبه جمال هاشم ،٢٠٢٣، منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل: دليل تطبيقي، ***المجلة العلمية للدراسات والبحوث المالية والتجارية***، المجلد الرابع – العدد الثاني – الجزء الثاني – يوليو، ص ١: ٥٨.

- قوجيل، محمد ، عبد العزيز طيبة،٢٠٢٢، مخاطر التكنولوجيا المالية وادارتها في القطاع المصرفي- دراسة تنظيمية واحترازية، ***مجلة الاقتصاد والمالية***، المجلد ٨، العدد ٢ ، ص ١٨٥: ١٩٩

-محروس، رمضان عارف، أبو الحمد مصطفي صالح،٢٠٢٢، استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الامن السيبراني، ***مجلة البحوث المالية والتجارية***، المجلد ٢٣، العدد الثالث، يوليو، ص ٤٣٢: ٤٩١.

-موسى، عمرو عادل عبد الفتاح، عبد الحميد أحمد شاهين، محمد موسي على شحاته، ٢٠٢٣، قياس أثر الإفصاح الإلكتروني عن المخاطر السيبرانية على الاداء المالي "دراسة تطبيقية"، ***المؤتمر العلمي الأول، القيادة الرقمية للفكر المحاسبي ركيزة التميز المهني في بيئة المعلوماتية الفورية "بين براعة الفكر...واحترافية التطبيق"*** ، قسم المحاسبة والمراجعة، كلية التجارة، جامعة السادات، ص ٤٣١: ٥١٣.

-نافع، محمود عبد المقصود،٢٠٢٢، اثر تقنيات الثورة الصناعية الرابعة على مهنة المحاسبة والمراجعة: دراسة ميدانية، ***مجلة الإسكندرية للبحوث المحاسبية***، قسم المحاسبة والمراجعة العدد الثالث سبتمبر ، المجلد السادس، ص ٣٩٧: ٤٢٩.

٢/١٠-المراجع باللغة الإنجليزية:

-Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. ***Procedia Computer Science***, 124, 691-697.
-Al-Qahtani, A., & Al-Maneea, A. (2019). The Impact of Organizational Complexity on the Financial Performance of UAE Banks. ***International Journal of Business and Management***, 14(9), 1-11.
-Abdel-Megeed, A. M. (2021). The Impact of Cybersecurity on Financial Performance of Banks in Egypt. ***International Journal of Business & Management Invention,*** 10(5), 45-54. https://www.ijbmi.org/papers/Vol(10)Issue(5)/Version-2/I100502020.pdf.
-Abdulrahim, N. (2019). Managing Cybersecurity as a Business Risk in Information Technology-based Smes (Doctoral dissertation, University of Nairobi). ***Accounting Association*** 15(2): A9-423.
-Adetiloye, K. (2019). Cybersecurity & Bank Performance in Nigeria. ***International Journal of Scientific & Research Publications***, 9(7), 1-9. http://www.ijsrp.org/research-paper-0719.php?rp=P923750.
-Adiloglu, B., & N. Gungor. 2019. Investigation of Increasing Technology use and Digitalization in Auditing. ***Global Business Research Congress*** (GBRC), 9: 20-23.
-Alghamdi, A. (2021). The Relationship between Cybersecurity & Financial Performance of Banks in Saudi Arabia. ***Journal of Accounting & Finance in Emerging Economies***, 7(2), 28-44. https://doi.org/10.26710/jafee.v7i2.1895.
-Al-Issa, M. (2016). Analyzing the impact of corporate structure on the performance of Saudi banks: A case study of the Riyadh Bank. ***International Journal of Economics, Commerce & Management***, 4(4), 23-36.
-Aljifri, M. (2015). Evaluating the impact of corporate governance structure on the value of companies listed in the Saudi Stock Exchange. ***Journal of Management Research***, 7(2), 54-78.

-Al-Masri, M., & Qasim, A. (2021). Cybersecurity & Financial Performance: Evidence from Commercial Banks in the United Arab Emirates. ***International Journal of Economics, Commerce & Management***,9(6),33-49.
http://ijecm.co.uk/wp-content/uploads/2021/06/1364.pdf.
-Almutairi, N. (2016). The impact of corporate governance structure on bank performance: A case study of Kuwaiti banks operating in the local market. ***Journal of Applied Finance & Banking***, 6(4), 91-107.
-Al-Omari, A. A., & Al-Fraih, M. M. (2015). The impact of corporate governance structure on bank performance in Saudi Arabia. ***Journal of Applied Accounting Research***, 16(2), 275-292.
-Al-Otaibi, N. A. (2018). The impact of structure complexity on the performance of Saudi banks. ***International Journal of Economics, Commerce & Management,*** 6(3), 85-95.
-Al-Sheikh, A., & Al-Olyan, E. (2020). The Impact of Organizational Complexity on the Financial Performance of Saudi Banks. ***Journal of Administrative and Economic Studies***, 2(2), 1-16.
-Alramahi, A. (2021). The Impact of Cybersecurity on Financial Performance of Banks in Jordan. ***International Journal of Scientific & Research Publications,*** 11(7), 255-261. http://www.ijsrp.org/research-paper-0719.php?rp=P923750.
-Alrazoq, Y., Al-Turki, M., Al-Rifai, A., & Al-Qahtani, M. (2020). The Impact of Cybersecurity Breaches on the Value of Firms: A Systematic Review & Proposed Research Agenda. ***Journal of Information Privacy & Security***, 16(1), 1-24.
-Al-Shammary, F. A., & Al-Samayi, A. (2021). Analyzing the Relationship between Organizational Complexity and Financial Performance of Saudi Banks. ***Journal of Administrative and Economic Studies***, 3(2), 77-96.
-Atkinson, J. S., Mitchell, J. E., Rio, M., & Matich, G. (2018). Your WiFi Is Leaking: What Do Your Mobile Apps Gossip about You? Future Generation Computer Systems, 80, 546-557. https://doi.org/10.1016/j.future.2016.05.030.
- Audretsch, D. B., & Belitski, M. (2021). Knowledge complexity and firm performance: evidence from the European SMEs. ***Journal of Knowledge Management,*** 25(4), 693-713.

-Badawy, H. A. 2021. The Impact of Assurance Quality & Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study. ***Alexandria Journal of Accounting Research*** 5(3): 1-56.

-Bokhari, S. A. A., & Manzoor, S. (2022). Impact of information security management system on firm financial performance: perspective of corporate reputation & branding. ***American Journal of Industrial & Business Management***, 12(5), 934-954.

-Boss, S. R., Gray, J., & Janvrin, D. J. (2022). Accountants, Cybersecurity Isn't Just for "Techies": Incorporating Cybersecurity into the Accounting Curriculum. ***Issues in Accounting Education***, 37(3), 73-89.

-Buch, C. M., & Goldberg, L. S. (2022). Complexity & riskiness of banking organizations: Evidence from the International Banking Research Network. ***Journal of Banking & Finance***, 134, 106244.

-Calder, A. (2017). Nine Steps to Success : An ISO 27001 Implementation Overview. IT Governance Ltd. https://doi.org/10.2307/j.ctt1wn0skw.

-Cheng, X., Hsu, C., & Wang, T. D. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. ***Communications of the Association for Information Systems***, 50 (1), 26.

-Cram, W. A., Wang, T., & Yuan, J. (2022). Cybersecurity research in accounting information systems: A review & framework. ***Journal of Emerging Technologies in Accounting.***

-Dao, T. K., Tapanainen, T. J., Nguyen, H. T. T., Nguyen, T. H., & Nguyen, N. D. (2017). Information safety, corporate image, & intention to Use online services: Evidence from travel industry in Vietnam.

-Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. ***Computer Law & Security Review***, 40, 105513.

-Fombrun, C. J., Ponzi, L. J., & Newburry, W. (2015). Stakeholder Tracking & Analysis: The RepTrakR System for Measuring Corporate Reputation. ***Corporate Reputation Review***, 18, 3-24. https://doi.org/10.1057/crr.2014.21

-Francis, B., Hasan, I., & Wu, Q. (2019). Do cybersecurity breaches reduce firm value? ***Journal of Accounting & Economics***, 68(1), 101-120.

-Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking & insurance industry: A textual & empirical analysis of determinants & value. ***Journal of Risk & Insurance***, 89(3), 725-763.
-Governance, I. T. (2021). What is cyber security? Definition & best practices.
-Greiner, A. J., Kohlbeck, M. J., & Smith, T. J. (2022). Auditor pricing of abnormal income from sales of available for sale securities: evidence from the banking industry. ***Accounting and Business Research***, 1-35.
-Gweyi, M. O. (2018). Influence of financial risk on financial performance of deposit taking savings & credit co-operatives in Kenya (***Doctoral dissertation***, JKUAT-COHRED).
-Haji, A. A., & Mohd Ghazali, N. A. (2012). The influence of the financial crisis on corporate
voluntary disclosure: Some Malaysian evidence. ***International Journal of Disclosure and Governance***, 9(2), 101-125.
-Hartmann, C. C., & J. Carmenate. 2021. Academic Research on the Role of Corporate Governance & IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy,& Research. ***American Accounting Association*** 15(2): A9-423.
-Han, J., Kim, Y. J., & Kim, H. (2017). An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective.***Computers & Security***, 66, 52-65. https://doi.org/10.1016/j.cose.2016.12.016.
-Hollnagel, E. (2017). Resilience–the challenge of the unstable. In Resilience engineering (pp. 9-17). CRC Press.
-Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. In 2016 49th Hawaii International Conference on System Sciences (HICSS) https://doi.org/10.1007/s10799-013-0156-y.
-Hung, W. H., Chang, I. C., Chen, Y., & Ho, Y. L. (2019). Aligning 4C strategy with Social Network Applications for CRM Performance. ***Journal of Global Information Management*** (JGIM), 27, 93-110. https://doi.org/10.4018/JGIM.2019010105

-Information Systems Audit and Control Association (ISACA),2021,COBIT (Control Objectives for Information and Related Technologies) .https://www.isaca.org/resources/cobit
InformationSystems,51,36-53.
https://doi.org/10.1145/3400043.3400047.
-Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity & accounting: An event, impact, response framework. ***Accounting Horizons***, 36(4), 67-112.
-Javaid, M. I. (2020). The Impact of Cybersecurity on Firm Performance: Evidence from the Banking Industry. ***International Journal of Financial Studies***, 8(3), 46. https://doi.org/10.3390/ijfs8030046.
-Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I., & Olorunyomi, B. R. (2016). Gendered alternative to cyber fraud participation: an assessment of technological driven crime in Lagos State, Nigeria. ***Gender & behaviour***, 14(3), 7672-7692.
-Kamdjoug, J. R. K., Tewamba, H. J. N., & Wamba, S. F. (2018). IT Capabilities, Firm Performance & the Mediating Role of ISRM: A Case Study from a Developing Country. ***Business Process Management Journal***, 25, 476-494.
-Kasanga, J. N. (2021). Outcome of Techniques Employed for Cyber Resiliency by Commercial Banks in Kenya (***Doctoral dissertation***, University of Nairobi).
-Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. ***International Journal of Research in Business & Social Science*** (2147-4478), 11(6), 334-340.
-Khanom, T. (2020). The accountancy profession in the age of digital transformation: challenges & opportunities. ***International Journal of Creative Research Thoughts*** (IJCRT), 8(2), 1525-1533.
-Ki-Aries, D., & Faily, S. (2017). Persona-Centred Information Security Awareness. Computers & Security, 70, 663-674. https://doi.org/10.1016/j.cose.2017.08.001.
-Kovalčíková, A., & Kotlán, R. (2019). Cybersecurity and financial performance: A case study of banks in Central and Eastern Europe. ***International Journal of Public Administration***, 42(7), 618-631.

-Kumar, R. (2021). The Impact of Cybersecurity on the Financial Performance of Banks in India. ***International Journal of Emerging Markets,***16(5),1136-1153. https://doi.org/10.1108/IJOEM-05-2020-0403.
-Lee, I.(2021). Cybersecurity: Risk management framework & investment cost analysis. ***Business Horizons,*** 64(5), 659-671.
-Larsen, M. M., Manning, S., & Pedersen, T. (2019). The ambivalent effect of complexity on firm performance: A study of the global service provider industry. ***Long Range Planning***, 52(2), 221-235.
-Lois, P., Drogalas, G.,Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. ***EuroMed Journal of Business***, 15(2), 205-217.
-Mahboub, R., 2019, The determinants of forward-looking information disclosure in annual reports of Lebanese commercial banks, ***Academy of Accounting and Financial Studies Journal***, 23 (4): 1-18.
-Malatji, M. (2023, January). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In 2023 ***International Conference On Cyber Management & Engineering*** (CyMaEn) (pp. 117-122). IEEE.
-Menon, N. M., & Siponen, M. T. (2020). Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) & Proposal Characteristics. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 51(2), 36-53.
-Mukundan, N., & Sai, L. P. (2014). Perceived Information Security of Internal Users in Indian & Security, 70, 663-674. https://doi.org/10.1016/j.cose.2017.08.001.
(pp. 4842-4848). IEEE. https://doi.org/10.1109/HICSS.2016.600
-Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities & risks. ***International Review of Financial Analysis***, 81, 102103. https://doi.org/10.1016/j.irfa.2021.102103.
-Mutungi, J. B. (2021). Cybersecurity & the Financial Performance of Banks in Kenya. I***nternational Journal of Economics, Commerce & Management,***9(5),34-47.
http://ijecm.co.uk/wp-content/uploads/2021/05/1140.pdf.

-Mwaura, J. W. (2020). Financial risk management & financial performance of savings & credit cooperative societies in Nairobi city county, Kenya.

-National Institute of Standards and Technology (NIST), Special Publication 800 Series ,2021,https://www.nist.gov/publications/nist-special-publication-800-series

-Nechai, A., Pavlova, E., Batova, T., & Petrov, V. (2020). Implementation of Information Security System in Service & Trade. IOP Conference Series: ***Materials Science & Engineering***, 940, Article ID: 012048. https://doi.org/10.1088/1757-899X/940/1/012048.

-Nyola, A. P., Sauviat, A., Tarazi, A., & Danisman, G. O. (2021). How organizational & geographic complexity influence performance: Evidence from European banks. ***Journal of Financial Stability***, 55, 100894.

-Osiemo, J. M. I. (2016). Effects of Risk Management Practices on Financial Performance of Non-Life Insurance Firms Operating in Kisii County, Kenya ***(Doctoral dissertation***, SRI JKUAT).

-Panda, A., & Bower, A. (2020). Cyber security & the disaster resilience framework. ***International Journal of Disaster Resilience in the Built Environment.***

-Peng, J., Quan, J., & Peng, L. (2019). It Application Maturity, Management Institutional Capability & Process Management Capability. ***Journal of Organizational & End User Computing*** (JOEUC), 31, 61-85. https://doi.org/10.4018/JOEUC.2019010104.

-Selimoğlu, S. K., & Saldı, M. H. (2023). Internal Audit Functions in Cyber Security Governance: Turkey's Bank Sector Case. In Glocal Policy and Strategies for Blockchain: Building Ecosystems and Sustainability (pp. 223-254). IGI Global.

-Tariq Beshir, S. & Salahuddin Bashir, S. (2018). The Impact of Cybersecurity on the Financial Performance of Islamic Banks. ***Journal of Financial&AccountingStudies,***7(2),1-17.
https://journals.iium.edu.my/enmjournal/index.php/enmj/article/view/50/44

-Tariq, N. (2018). Impact of cyberattacks on financial institutions. ***Journal of Internet Banking & Commerce***, 23(2), 1-11.

-Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka, G. B., Wamba, S. F., & Bahanag, N. N. M. (2019). Effects of Information Security Management Systems on Firm Performance. ***American Journal of Operations Management & Information Systems***, 4, 99-108.

-Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current & future trends. Information, 13(3), 146.

-Velasco, J., Ullauri, R., Pilicita, L., Jacome, B., Saa, P., & Moscoso-Zea, O. (2018). Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. In 2018 ***International Conference on Information Systems & Computer Science*** (INCISCOS) (pp. 294-300). IEEE.

-Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, 153826-153848.

-Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification & Concealment on Financial Performance: Impact of ISO 27001 & Concealment on Performance. ***Journal of Global Information Management*** (JGIM), 30, 1-16. https://doi.org/10.4018/JGIM.20220701.oa2.

-Yang, C. & Wang, G. (2020). The Effects of Cybersecurity on Financial Performance of Banks in the United States. ***Journal of Financial Crime***, 27(4), 1099-1115. https://doi.org/10.1108/JFC-12-2019-0184

-Yin, R. K. (2014). Case study research: Design & methods Sage publications.

-Zaki, M. & Hassan, A. (2018). The effect of corporate governance structure on bank value: A case study of the National Bank of Egypt. ***Journal of Economics & Political Economy,*** 5(2), 226-240.

-Zhang, Q. (2022). The Effect of Cybersecurity on Financial Performance of Banks in China. ***International Journal of Finance & Economics***. Advance online publication. https://doi.org/10.1002/ijfe.2873

مواقع الكترونية

"-Cybersecurity in Banking & Financial Institutions", Kaspersky, https://www.kaspersky.com/blog/cybersecurity-in-banking/28152.
" -Cybersecurity in Financial Services", PwC, https://www.pwc.com/us/en/industries/financial-services/library/cybersecurity-financial-services.html.
"-Cybersecurity in the Financial Sector: Threats & Solutions", Investopedia, https://www.investopedia.com/articles/investing/111015/cybersecurity-financial-sector-threats-solutions.asp.
"-Cybersecurity Trends in Financial Services", Deloitte, https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-trends-in-financial-services.html.
"-The Importance of Cybersecurity in Banking", NortonLifeLock, https://us.norton.com/internetsecurity-emerging-threats-the-importance-of-cybersecurity-in-banking.html.
-https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability.
https://www.emerald.com/insight/content/doi/10.1108/BPMJ-11-2017-0297/full/html.-
https://www.mcit.gov.eg/Upcont/Documents/Publications_12122018000_ar_AR_National_Cybersecurity_Strategy_2017_2021.pdf.
-Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. Webology, 18(Special Issue on Information Retrieval and Web Search), 294-310.

الملحق رقم (١)

يتضمن دليل الأمن السيبراني للبنوك الصادر عن هيئة السوق المالية في المملكة العربية السعودية ٦ مجموعات رئيسية و٧٧ مؤشراً فرعياً تفصيلياً توفر إرشادات وإجراءات لحماية بيانات البنوك من التهديدات السيبرانية كما يلي:

أولا: تعريف بالتهديدات السيبرانية والتحديات التي تواجهها البنوك، وكيفية التعامل معها. تطبق البنوك استراتيجية شاملة للأمن السيبراني	١
البرمجيات الخبيثة: هي برامج للتسلل إلى أنظمة البنك أو الشبكات أو الأجهزة للوصول إلى البيانات المهمة أو لإيقاف النظام بأكمله. وتنفذ عن طريق رسائل بريد إلكتروني أو نصية مزيفة أو إعلانات غير مرغوب فيها.	١/١
هجمات الحصول على المعلومات: تتم عن طريق اختراق أنظمة البنوك والشبكات والحصول على البيانات الحساسة. وتنفذ هذه الهجمات بسبب الضعف في مستوى الحماية أو عدم التحديث الدوري للنظام.	٢/١
هجمات الإنكار الخدمة: عن طريق إرسال حركة مزيفة إلى أنظمة البنوك والشبكات لإيقاف الخدمة وتعطيل النظام بأكمله. وتتم بسبب الضعف في مستوى الحماية أو عدم التحديث الدوري للنظام.	٣/١
هجمات التصيد الالكتروني: عن طريق إرسال رسائل بريد إلكتروني مزيفة أو إعلانات غير مرغوب فيها للمستخدمين لجعلهم يدخلون بياناتهم الشخصية والمصرفية على مواقع مزيفة.	٤/١
الإجراءات والتدابير اللازمة للتعامل مع التهديدات السيبرانية، لحماية الأنظمة والبيانات وتخفيض مستوى المخاطر السيبرانية، وتشمل هذه التدابير:	٥/١
١. تحديث نظام الأمن السيبراني: للأنظمة والشبكات والبرامج والتطبيقات بشكل دوري لسد الثغرات الأمنية المعروفة. وتنفيذ عمليات تحليل الضمان الأمني واختبار الاختراق الدوري لتحديد الثغرات الأمنية وإصلاحها.	٦/١
٢-تطوير السياسات الأمنية للبنوك لتكون شاملة ومحدثة بشكل دوري لتغطي جميع جوانب الأمن السيبراني. وتطبيقها بشكل صارم، وتحديد المسؤوليات والإجراءات المطلوبة للتعامل مع الحوادث الأمنية والتقارير الدورية.	٧/١

٣. تحسين التدريب والوعي الأمني اللازم للموظفين حول الأمن السيبراني وكيفية التعامل مع الهجمات السيبرانية والتقارير الدورية. وتنفيذ حملات التوعية الأمنية للموظفين والعملاء لتعزيز الوعي الأمني.	٨/١
٤. تطوير التقنيات الأمنية المتقدمة مثل تقنيات التشفير والحماية من الاختراق وتحديثها بشكل دوري. وتحديث الأجهزة والبرامج والتطبيقات بشكل دوري لسد الثغرات الأمنية المعروفة.	٩/١
٥. إدارة المخاطر السيبرانية: من خلال تحديد وتحليل المخاطر السيبرانية المحتملة وتطوير استراتيجيات للتعامل معها. وتنفيذ عمليات تقييم الضمان الأمني واختبار الاختراق الدوري لتحديد الثغرات الأمنية وإصلاحها.	١٠/١
٦. التعاون والشراكة مع الجهات ذات الصلة مثل السلطات التنظيمية والموردين والعملاء لتحسين الأمن السيبراني وتبادل المعلومات للحصول على المشورة والدعم الفني فيما يتعلق بالتهديدات السيبرانية.	١١/١
ثانيا: متطلبات الأمن السيبراني الأساسية للبنوك:	٢
١.الحماية الفنية:	١/٢
-استخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة وتحديثها بشكل دوري.	١/١/٢
-تحديث نظام التشغيل والبرامج والتطبيقات بشكل دوري لسد الثغرات الأمنية المعروفة.	٢/١/٢
-تنفيذ عمليات تحليل الضمان الأمني واختبار الاختراق الدوري لتحديد الثغرات الأمنية وإصلاحها.	٣/١/٢
٢-الأمان الفيزيائي: من خلال توفير مكان آمن ومؤمن للمرافق البنكية والبيانات.	١/٢/٢
وتأمين الأجهزة والمعدات الحساسة وتوفيرها بشكل دوري.	٢/٢/٢
وتحديث نظام الأمان الفيزيائي للمرافق البنكية لتحسين الحماية من الاقتحام والتدخل غير المصرح به.	٣/٢/٢
٣-إجراءات الوصول والتحكم في البيانات:	٣/٢

يكون فقط من قبل الأشخاص المصرح لهم وبالطريقة المصرح بها.	١/٣/٢
وتطبيق سياسات الوصول والتحكم في البيانات والتحقق منها بشكل دوري.	٢/٣/٢
-توفير أدوات التحكم في الوصول والتحكم في البيانات مثل إدارة الهوية والوصول ونظام المصادقة المتعددة العوامل.	٣/٣/٢
- وضع سياسات وإجراءات أمنية شاملة مناسبة لجميع جوانب الأمن السيبراني، لحماية الأنظمة والبيانات.	٤/٣/٢
-تحديد المسؤوليات والإجراءات المطلوبة للتعامل مع الحوادث الأمنية والتقارير الدورية.	٥/٣/٢
٤-التدريب والوعي الأمني:	٤/٢
بتوفير التدريب اللازم للموظفين حول الأمن السيبراني وكيفية التعامل مع الهجمات السيبرانية والتقارير الدورية.	١/٤/٢
وتنفيذ حملات التوعية الأمنية للموظفين والعملاء لتعزيز الوعي الأمني.	٢/٤/٢
٥-إدارة المخاطر السيبرانية:	٥/٢
من خلال تحديد وتحليل المخاطر السيبرانية المحتملة وتطوير استراتيجيات للتعامل معها.	١/٥/٢
وتنفيذ عمليات تقييم الضمان الأمني واختبار الاختراق الدوري لتحديد الثغرات الأمنية وإصلاحها.	٢/٥/٢
٦-تطوير التقنيات الأمنية:	٦/٢
- استخدام التقنيات الأمنية المتقدمة مثل تقنيات التشفير والحماية من الاختراق وتحديثها بشكل دوري.	١/٦/٢
- تنفيذ عمليات تحديث الأجهزة والبرامج والتطبيقات بشكل دوري لسد الثغرات الأمنية المعروفة.	٢/٦/٢
ثالثا: متطلبات الأمان الإداري للبنوك:	٣
١.تحديد المسؤوليات الخاصة بالأمن السيبراني وتعيين أشخاص مسؤولين عن تطبيق سياسات الأمن السيبراني ومراقبة الأنشطة السيبرانية داخل البنك.	١/٣

١/١/٣	-توفير تفاصيل واضحة حول المسؤوليات والأذونات للموظفين في البنك لتحديد من يمكنه الوصول إلى البيانات والأنظمة الحيوية والمهام الأخرى ذات الصلة.
٢/٣	٢. تحديد الصلاحيات الخاصة بالوصول إلى الأنظمة والبيانات داخل البنك وضبطها على أساس الحاجة والمبدأ الأساسي للحد الأدنى للصلاحيات.
١/٢/٣	-فرض تفاصيل صارمة حول كيفية الوصول إلى الأنظمة والبيانات ومن يمكنه الوصول إليها، وتحديد الصلاحيات على أساس الوظائف الخاصة بالموظفين.
٣/٣	٣. وضع إجراءات إدارية واضحة للأمن السيبراني، وتحديد المعايير المطلوبة للحفاظ على أمان الأنظمة والبيانات.
١/٣/٣	-تنفيذ إجراءات إدارية للحد من المخاطر السيبرانية، بما في ذلك التحقق من الهوية والوصول وتحديد الصلاحيات المناسبة وإدارة التغيير وتطوير خطط الحماية والتعامل مع الحوادث والتدقيق الداخلي والتدقيق الخارجي.
٤/٣	٤. تطوير سياسات الأمن السيبراني بشكل دوري لتلبية التهديدات السيبرانية المتغيرة باستمرار وتوفير الحماية اللازمة للأنظمة والبيانات والعملاء.
١/٤/٣	-تحديث سياسات الأمن السيبراني بناءً على التحليل الدوري للتهديدات السيبرانية والتقنيات الأمنية المتطورة مع الالتزام بالمعايير والتوجيهات القانونية والتنظيمية.
٢/٤/٣	-توفير الدعم لفريق الأمن السيبراني وتوفير الأدوات والتقنيات الأمنية اللازمة للتعامل مع التهديدات السيبرانية.
٥/٣	٥. توفير التدريب والتوعية اللازمة للموظفين في البنك لزيادة الوعي الأمني وتحسين قدراتهم على الكشف عن التهديدات السيبرانية ومواجهتها.
١/٥/٣	-توفير التدريب اللازم للموظفين حول سياسات الأمن السيبراني والإجراءات والتقنيات الأمنية المتعلقة بالأنظمة والبيانات والتعامل مع الحوادث الأمنية.
٦/٣	٦. التدقيق والتقييم الدوري لسياسات الأمن السيبراني والإجراءات والتقنيات الأمنية المتعلقة بالأنظمة والبيانات للتحقق من فعاليتها وتحديثها بشكل دوري.

١/٦/٣	-تقييم مدى تطبيق سياسات الأمن السيبراني وإجراءاتها والتقنيات الأمنية المتعلقة بالأنظمة والبيانات وتحديد النقاط الضعيفة واتخاذ الإجراءات اللازمة لتحسينها.
٤	*رابعا: إجراءات الاستجابة لحوادث الأمن السيبراني:*
١/٤	١. تقييم المخاطر المحتملة للحادث الأمني وتحديد أولويات الاستجابة.
١/١/٤	-تحديد نوع الهجوم ومصدره ومدى تأثيره على أنظمة وبيانات البنك والعملاء.
٢/٤	٢. التحقق من الحوادث للتحقق بما إذا كانت الحادثة الأمنية قد حدثت فعلياً وتحديد نطاق التأثير الذي تسبب فيه.
١/٢/٤	وتحديد ما إذا كان هناك تعرض لأنظمة الحوسبة أو تم الوصول إلى المعلومات المتعلقة.
٣/٤	٣. الإبلاغ الفوري عن الحادثة الأمنية للجهات المعنية في البنك، مثل فريق الأمن السيبراني وفريق الإدارة العليا.
١/٣/٤	-توثيق جميع الإجراءات المتخذة والتفاصيل ذات الصلة بالحادثة الأمنية.
٤/٤	٤. احتواء الحادث الأمني عن طريق إيقاف الهجوم وتحديد مصدر الهجوم والتحكم في الأضرار الناجمة.
١/٤/٤	-فصل النظام المصاب عن بقية الأنظمة للحفاظ على سلامة الأنظمة الأخرى.
٥/٤	٥-استعادة الأنظمة والبيانات بأسرع وقت ممكن لتجنب فقدان البيانات أو التأثير على العمليات الحيوية للبنك.
١/٥/٤	إجراء اختبارات شاملة لاستعادة الأنظمة والبيانات بعد الاستجابة للحادث الأمني.
٢/٥/٤	تحديد وتصنيف البيانات والأنظمة الحيوية وإعداد خطة احتياطية واستعادة لها.
٦/٤	٦. التحقيق الشامل للحادث الأمني وتحديد أسبابه والتحقق من مدى فعالية سياسات الأمن السيبراني وإجراءاتها.
١/٦/٤	-تحليل الحادث الأمني وتحديد النقاط الضعيفة في الأمن السيبراني واتخاذ الإجراءات اللازمة لتحسينها.

٧/٤	٧. التعزيز والتحسين وتحديث سياسات الأمن السيبراني وإجراءاتها بناءً على نتائج التحقيق وتحليل الحادث الأمني.
١/٧/٤	-توفير التدريب والتوعية للموظفين لتحسين الوعي الأمني وتطوير قدراتهم للكشف عن التهديدات السيبرانية.
٢/٧/٤	-إجراء اختبارات الاختراق الدورية لتحديد أي نقاط ضعف في الأمن السيبراني واتخاذ الإجراءات اللازمة لتصحيحها.
٥	***خامسا: متطلبات التدريب والتوعية الأمنية للموظفين في البنوك:***
١/٥	١. التدريب الأمني
١/١/٥	- يجب على الموظفين في البنك إتمام دورات تدريبية على الأمن السيبراني بشكل دوري.
٢/١/٥	- يجب أن يشمل التدريب الأمني التعريف بالتهديدات الأمنية السيبرانية الحالية وطرق الدفاع ضدها، بما في ذلك الهجمات الإلكترونية والبرمجيات الخبيثة والتصيد الالكتروني.
٣/١/٥	- يجب أن يتم تدريب الموظفين على سياسات الأمن السيبراني وإجراءاتها، وكيفية التعامل مع التهديدات الأمنية والتحقق من هوية العملاء والشركاء والموردين.
٢/٥	٢. التوعية الأمنية: يجب أن يتم توعية الموظفين حول
١/٢/٥	- أهمية الأمن السيبراني وتأثيره على العملاء والشركاء والمؤسسة بشكل عام.
٢/٢/٥	- أهمية الإبلاغ الفوري عن أي حادث أمني أو انتهاك لسياسات الأمن السيبراني.
٣/٢/٥	- أساليب التصيد الالكتروني والبريد الالكتروني المزيف والاحتيال الإلكتروني وكيفية التعرف عليها والتعامل معها.
٤/٢/٥	- خطورة استخدام كلمات المرور الضعيفة وتأمين البيانات الحساسة والجهاز الخاص بهم.
٣/٥	٣-الالتزام بسياسات الأمن السيبراني

– يجب على الموظفين الالتزام بسياسات الأمن السيبراني المحددة من قبل البنك وإدارته.	١/٣/٥
– يجب على الموظفين تطبيق السياسات الأمنية بشكل دقيق والإبلاغ الفوري عن أي انتهاك لتلك السياسات.	٢/٣/٥
– يجب أن يتم تحديث وتطوير سياسات الأمن السيبراني بشكل دوري لتلبية التحديات الجديدة وتحديثات التكنولوجيا.	٣/٣/٥
٤. اختبار التوعية الأمنية: – يجب تقييم مدى فهم الموظفين بشكل صحيح في الأمن السيبراني من خلال:	٤/٥
١. تطوير برنامج تدريب شامل يغطي مجموعة واسعة من موضوعات الأمن السيبراني، مثل الصيد الاحتيالي والهندسة الاجتماعية والبرامج الخبيثة وإدارة كلمات المرور واستجابة الحوادث. يجب تصميم التدريب لتناسب الأدوار والمسؤوليات الخاصة بكل موظف.	١/٤/٥
٢. إجراء جلسات تدريب منتظمة لضمان أن الموظفين مطلعون على آخر التهديدات السيبرانية وأفضل الممارسات. يمكن تنفيذ ذلك من خلال جلسات وجهًا لوجه أو وحدات تدريب عبر الإنترنت أو مزيج من الاثنين.	٢/٤/٥
٣. اختبار معرفة الموظفين بشكل دوري للتأكد من فهمهم للمخاطر ومعرفتهم بكيفية التعامل مع التهديدات المحتملة. يمكن تنفيذ ذلك من خلال اختبارات قصيرة أو محاكاة للتدريب أو طرق اختبار أخرى.	٣/٤/٥
٤. توفير تعليم مستمر للموظفين للحفاظ على تحديثهم بآخر التهديدات وأفضل الممارسات في الأمن السيبراني. يمكن تنفيذ ذلك من خلال النشرات الإخبارية والبريد الإلكتروني والقنوات الأخرى للاتصال.	٤/٤/٥
٥.جعل الأمن السيبراني أولوية والتأكد من فهم الموظفين لأهمية حماية المعلومات الحساسة. من خلال الاتصالات المنتظمة من إدارة كبار المسؤولين التنفيذيين، بالإضافة إلى توفير حوافز للممارسات الجيدة في الأمن السيبراني.	٥/٤/٥
٦. إشراك جميع الموظفين في جهود الأمن السيبراني، وليس فقط أولئك في الأدوار ذات الصلة بتكنولوجيا المعلومات أو الأمن. يجب تدريب جميع	٦/٤/٥

الموظفين على التعرف على الأنشطة المشبوهة والإبلاغ عنها، ويجب تشجيعهم على المشاركة الفعالة في حماية أصول المعلومات الخاصة بالبنك.	
٧. توفير تدريب عملي للموظفين لمساعدتهم على فهم كيفية تنفيذ سياسات وإجراءات الأمان فيعملهم اليومي. يمكن تضمين تمارين ومحاكاة تسمح للموظفين بممارسة الاستجابة للتهديدات السيبرانية.	٧/٤/٥
٨. تعاون مع مزودي خدمات خارجيين، مثل شركات تدريب الأمن السيبراني، لتوفير تدريب ودعم إضافي. يمكن لهؤلاء المزودين توفير خبرات وموارد تساعد البنوك في مواجهة التهديدات المتطورة.	٨/٤/٥
سادسا: متطلبات التدقيق والمراجعة الأمنية الدورية للبنوك:	٦
١.متطلبات الأمان الفني:	١/٦
– تقييم أمان تقنية المعلومات وتحليل مخاطر الأمن السيبراني.	١/١/٦
– تحليل النظم والتطبيقات والأجهزة الأمنية.	٢/١/٦
– تحديد الثغرات الأمنية وتوفير توصيات لتعزيز الأمان.	٣/١/٦
٢. متطلبات الأمان الإداري:	٢/٦
– توفير سياسات وإجراءات الأمن السيبراني للمؤسسة.	١/٢/٦
– تحديد المسؤوليات والصلاحيات وتوفير التدريب والوعي الأمني للموظفين.	٢/٢/٦
– تقييم الامتثال لمعايير الأمن السيبراني واللوائح والقوانين المتعلقة بالأمن السيبراني.	٣/٢/٦
٣. متطلبات الحماية الفيزيائية:	٣/٦
– تقييم الأمان الفيزيائي للبنك والمنشآت الخاصة به.	١/٣/٦
– تدقيق سياسات وإجراءات الوصول والتحكم في البيانات والممتلكات الفيزيائية.	٢/٣/٦
– تحديد المخاطر المتعلقة بالأمان الفيزيائي وتوفير توصيات لتعزيز الأمان.	٣/٣/٦
٤. متطلبات التخطيط والاستجابة لحوادث الأمن السيبراني:	٤/٦
– تقييم خطط الاستجابة لحوادث الأمن السيبراني.	١/٤/٦
– تحديد المخاطر والتهديدات السيبرانية الحالية والمستقبلية وتحليلها.	٢/٤/٦

– تدريب فريق الاستجابة لحوادث الأمن السيبراني وإجراء تدريبات ومحاكاة لحوادث الأمن السيبراني.	٣/٤/٦
٥. متطلبات التدقيق والمراجعة:	٥/٦
– تقييم الأمن السيبراني ومستوى الامتثال لمتطلبات الأمن السيبراني.	١/٥/٦
– تقييم سياسات وإجراءات الأمن السيبراني وتحليل فعالية تنفيذها.	٢/٥/٦
– تحليل النظم والتطبيقات والأجهزة الأمنية وتوفير توصيات لتعزيز الأمان.	٣/٥/٦