



أثر ادارة مخاطر الامن السيبراني على دعم الاستقرار والشمول المالي في البنوك

إعداد الطالب/ يحيى ابراهيم حمدي

إشراف

د.منى مصطفى العشيري

العام الدراسي:

2024

· الشكر والتقدير

نود أن نعبر عن شكرنا العميق وتقديرنا الخالص لكل من ساهم في إتمام هذا البحث بنجاح. نشكر كل من قدم الدعم والإرشاد في مسيرة هذا العمل، سواء من خلال تقديم المشورة الأكاديمية أو الدعم التقني والفني. كما نود أن نعبر عن شكرنا لكل الأفراد الذين شاركوا بإجاباتهم على الاستبيانات والمقابلات، حيث ساهمت مشاركاتهم في إثراء نتائج البحث وتحليلاته.

كما نتقدم بالشكر الخاص للمؤسسات والهيئات التي ساهمت بتوفير البيانات والمعلومات الضرورية لإتمام أخيراً، نتمنى أن يكون هذا البحث مساهمة قيمة في مجال إدارة مخاطر الأمن السيبراني، وأن تكون التوصيات المقدمة ذات فائدة عملية للقطاع المالي والبنوك في مسيرتها نحو تحقيق الاستقرار والشمول المالي.

الإهداء

إلى أهلي الأعزاء، الذين كانوا دعماً لا يضاهاى طوال رحلتي الأكاديمية والبحثية، أفضل التقدير والاحترام لكم على حبكم ودعمكم الدائم.

إلى دكاترتي الأفاضل، الذين شاركوني من حكمتهم ومعرفتهم القيمة، أعبر عن امتناني العميق لكم على التوجيه والإرشاد الذين ساعدوني على تحقيق هذا الإنجاز الأكاديمي.

ملخص: هدفت الدراسة إلى التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وتقديم تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي لهذه البنوك، وللإجابة على التساؤلات البحثية واختبار فرضيات الدراسة أعتمد الباحثان على المنهج الوصفي التحليلي، واستخدمت الاستبانة كاداة لجمع المعلومات ووزعت بعد تقييمها وتحكيمها من عدد من المتخصصين على عينة الدراسة والتي بلغت (90) مفردة والمكونة من المدراء العامين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين. وأثبتت نتائج الدراسة أنه يوجد أثر لإدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، كما تقوم البنوك المدرجة في بورصة فلسطين بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي. كما أوصت الدراسة بضرورة قيام البنوك المدرجة في بورصة فلسطين باتخاذ إجراءات للأمن السيبراني لضمان سلامة ومتانة نظم المعلومات المالية والإدارية والحفاظ على الاستقرار والشمول المالي وبما يحقق أهدافها، كما ضرورة وضع نماذج فعالة لإدارة المخاطر السيبرانية المصاحبة لتكنولوجيا المعلومات وهو ما يتطلب الرقابة المستمرة لتحديد هذه المخاطر التي قد تهدد الاستقرار المالي في القطاع المصرفي.

مقدمة:

تعتبر البنوك هدفاً رئيسياً لمجرمي الإنترنت، سواء من الأفراد أو الجهات الحكومية، ولا يوجد كيان حكومي له مصلحة أكبر في حماية أداء المؤسسات المالية من البنك المركزي في أي الدولة. علاوة على ذلك، عند ممارسة سلطاتها الإشرافية والإنفاذ، تتمتع البنوك المركزية برؤية فريدة حول ما إذا كانت المؤسسات المالية الخاضعة للتنظيم، وحتى المؤسسات غير المنظمة في بعض الأحيان، قد اتخذت الخطوات المناسبة لتكون أكثر مرونة ضد الهجمات الإلكترونية. نظرًا لأن البنوك المركزية هي مستودعات للمعلومات الحساسة للغاية المتعلقة بالنظام المالي، فإن لديهم أيضاً مصلحة قوية في الدفاع ضد اختلاس بياناتهم الخاصة

وتشكل الحوادث السيبرانية تهديداً كبيراً للنظام المالي حيث تشير التقديرات إلى أن الهجمات الإلكترونية على المؤسسات المالية التقليدية وعمليات تبادل العملات المشفرة على حد سواء أدت إلى سرقة مليارات الدولارات. وأدت عمليات اختراق الشركات المالية الكبرى ووكالات الإبلاغ عن ائتمان المستهلكين وتجار التجزئة والوكالات الحكومية إلى اختراق المعلومات الشخصية لمئات الملايين من الأفراد، تعرض خرق البيانات لمقدمي الخدمات من الأطراف الثالثة الملكية الفكرية والمعلومات السرية لشركاتهم المالية المخدومة لمخاطر كبيرة. أصابت هجمات برامج الفدية مئات الآلاف من أنظمة الكمبيوتر على مستوى العالم.

يساهم عدد من العوامل في المخاطر السيبرانية في البنوك، بما في ذلك الاتجاه المتزايد في العولمة، والاستخدام والاعتماد المبكر للتكنولوجيا سريعة التطور، والاعتمادات الكبيرة والترابط داخل كل من النظام المالي والبنية التحتية لتكنولوجيا المعلومات، والتطور المتزايد لمجرمي الإنترنت، والطبيعة الجوهرية لأعمال وخدمات المؤسسات المالية. وإدراكاً منهم للمخاطر المرتبطة بالأمن السيبراني، بدأ المشرفون والمنظمون في جميع أنحاء العالم في اتخاذ خطوات تهدف إلى التخفيف من المخاطر الإلكترونية في المؤسسات المالية، بما في ذلك تعزيز قدرات المرونة وتنفيذ خطط للاستجابة الفعالة للهجمات الإلكترونية والتعافي منها.

لقد أتاح التطور المتسارع الذي شهده قطاع التكنولوجيا المالية الكثير من الفرص أمام البنوك والمؤسسات المالية تحولاً كبيراً لتحسين مستوى الخدمات المقدمة للعملاء من خلال قنوات جديدة ومبتكرة، والتي أحدثت مؤخراً تغيير ملموس في الخدمات المقدمة من قطاع البنوك، حيث ساهم هذا التطور التقني في قيام البنوك بتقديم الخدمات المالية الرقمية بشكل أكبر وخاصةً تعزز من إمكانية الوصول إلى الخدمات المالية الرقمية ببسر وكفاءة وأمان، الأمر الذي أدى إلى توفير الوقت والجهد والمال، لكن بنفس الوقت فإن هذه التطورات التكنولوجية المتسارعة قد تؤدي إلى زيادة تعرض البنوك إلى مخاطر جديدة (مخاطر الأمن السيبراني)، وقد تؤدي إلى تعطل الخدمات المالية الضرورية للأنظمة المالية، وتقويض

الأمن والثقة بالنظام المصرفي، وعدم قيام البنوك بوضع الشمول المالي ضمن أولوياته، وتعرض الاستقرار المالي للخطر، حيث أن الشمول المالي له أثر إيجابي على الاستقرار المالي ووجود علاقة سببية بين مؤشرات الشمول المالي والاستقرار المالي، ويعد الشمول المالي عاملاً هاماً للاستقرار المالي. حيث أسفرت مخاطر الأمن السيبراني بالفعل عن اختراقات للبيانات التي تم من خلالها الوصول إلى معلومات سرية، الأمر الذي أدى إلى زعزعة أمن المعلومات ناهيك عن الخسائر المالية التي تكبدتها البنوك، كما أن قدرة النظام المصرفي على التصدي للمخاطر السيبرانية يكون من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي لتعزيز الاستقرار المالي. ولغرض ضبط المخاطر السيبرانية وتخفيف الأثر المالي والتحوط منها فإن كثير من البنوك في العالم قامت بتحسين ضوابطها الأمنية ووضع الإجراءات والتدابير والأمن السيبراني التي قد تتعرض لها، حيث شكلت فريق للاستجابة لحوادث الأمن السيبراني لقطاع البنوك بما يساهم في تكثيف الجهود والاستغلال الأمثل للطاقت لتطوير منظومة الأمن السيبراني على مستوى قطاع البنوك، وإصدار تعليمات لكيفية إدارة المخاطر السيبرانية، ووضع السياسات لإدارة أمن المعلومات والأمن السيبراني.

حيث من الضروري على البنوك تكوين مخصصات مالية لمواجهة الخسائر الناتجة عن المخاطر السيبرانية، بالإضافة إلى معالجة نقاط الضعف في أنظمة الرقابة الداخلية، وإعداد خطة لإدارة المخاطر السيبرانية تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات والتعافي منها في زمن قياسي لاسترجاع البيانات ومعالجة الأحداث التشغيلية، حيث أن عملية إعداد وتصميم معالجات للمخاطر السيبرانية تتم من خلال تحديد مصادر بداية هذه المخاطر واحتمالية حدوثها.

مشكلة الدراسة:

تعتبر البنوك من أكثر المؤسسات المالية التي تولي عناية خاصة وكبيرة لإدارة مخاطر الأمن السيبراني؛ لأن الآثار المحتملة للاختراق السيبراني تنطوي على تعرض البنوك لخسائر مالية مباشرة وغير مباشرة ناجمة عن الهجمات السيبرانية، وتعطيل الأعمال، والضرر على السمعة، وغيرها، ولا يمكن بأي حال من الأحوال إغفال المخاطر المتزايدة للهجمات السيبرانية التي تعتبر البنوك هدفاً جذاباً لها نظراً لدورها الحيوي في الوساطة المالية، ما قد يهدد الاستقرار والشمول المالي، ومن هذا المنطلق تمكن مشكلة الدراسة من خلال طرح التساؤلات التالية:

السؤال الرئيس:

ما أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين؟

ومن السؤال الرئيس تتفرع التساؤلات الفرعية التالية:

1. ما أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي في البنوك المدرجة في بورصة فلسطين؟

2. ما أثر إدارة مخاطر الأمن السيبراني على تعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين؟

أهداف الدراسة:

تهدف الدراسة أساساً للتأصيل العلمي من خلال التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وفي سبيل تحقيق هذا الهدف الرئيس لابد من تحقيق الأهداف الفرعية التالية:

1. بيان أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي في البنوك المدرجة في بورصة فلسطين.

2. التعرف على أثر إدارة مخاطر الأمن السيبراني على تعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في كونها محاولة علمية حديثة في توضيح أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، وتتأكد أهمية هذه الدراسة من خلال ما يمكن أن تقدمه من تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي للبنوك المدرجة في بورصة فلسطين، وتنقسم أهمية الدراسة إلى قسمين:

الأهمية العلمية: تتبع الأهمية العلمية للدراسة في كونها من الدراسات المثيرة والتي تبحث في أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وبالتالي قد تساهم هذه الدراسة في زيادة المعرفة للباحثين بحيث يستطيع الباحثين الاعتماد عليها واستقصاء المعلومات اللازمة في إعداد دراساتهم المستقبلية ذات العلاقة.

الأهمية العملية: تبرز الأهمية العملية للدراسة من خلال مساهمة نتائج الدراسة في معرفة كيفية إدارة مخاطر الأمن السيبراني، بالإضافة إلى ما تحققه تقدمه من توصيات لدعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين.

فرضيات الدراسة: بناءً على مشكلة وأهداف الدراسة يمكن صياغة الفرضيات كما يلي:-

الفرضية الرئيسية:

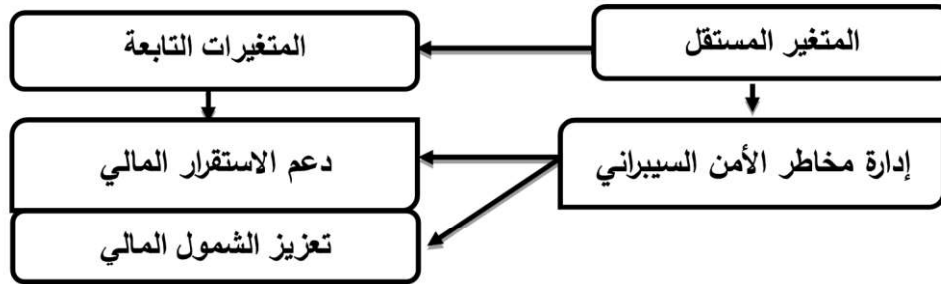
يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين؟

ويتفرع من الفرضية الرئيسية الفرضيات الفرعية التالية:

الفرضية الأولى: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي في البنوك المدرجة في بورصة فلسطين.

الفرضية الثانية: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين.

نموذج الدراسة:



شكل رقم (1) أنموذج الدراسة

حدود الدراسة:

تمثلت حدود الدراسة فيما يلي:

1. الحدود الزمانية: تم إعداد هذا الدراسة خلال عام 2022.
2. الحدود المكانية: يطبق هذا الدراسة على البنوك المدرجة في بورصة فلسطين.
3. الحدود البشرية: تتكون من مدير عام، مدير فرع، مدير الدائرة المالية، مدير إدارة المخاطر.
4. الحدود العلمية: دراسة أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك.

الدراسات السابقة والإطار الفكري

أولاً: الدراسات السابقة

1. دراسة (Saon, Miglanic, 2019):

هدفت هذه الدراسة إلى دراسة كيفية تمكين تقنيات الذكاء الاصطناعي والبلوك تشين للمساهمة في تدعيم الشمول المالي. في حين أن إمكانات تقنية block chain، بشكل عام والعقود الذكية، على وجه الخصوص، لجعل الخدمات المالية أكثر كفاءة وفعالية من حيث التكلفة وشاملة لا جدال فيها، فهناك قلق فيما يتعلق بقابلية التوسع وقابلية التشغيل البيئي وتأثير التكلفة والتنظيم. يؤدي أيضاً إلى الافتقار إلى للفهم والخبرة وخلق حواجز ثقافية تجعل الابتعاد عن النظام القديم أكثر صعوبة. ويمكن لتقنية Block chain أن تغير قواعد اللعبة إذا تم تبنيها على نطاق واسع وكان هناك اتفاق على بنية التكنولوجيا التي يجب وضعها لتبنيها. بقدر ما يتعلق الأمر بالذكاء الاصطناعي، فهي تقنية ناشئة وهناك تحديات مثل

ها
سرعة المعاملات وعملية التحقق وحدود البيانات. وضعها التنظيمي غير مؤكد وهناك مخاوف تتعلق بالتكامل (داخل المنظمة، بسبب النظام البيئي الحالي)، وندرّة المواهب، والتكاليف المتضمنة. إن إمكانيات هاتين التقنيتين في تحقيق قدر أكبر من الشمول المالي واضحة بلا شك. ويعتمد ما إذا كان ذلك سيحدث على العديد من العوامل بالإضافة إلى مدى سرعة اعتماد هذه التقنيات من قبل معظم لاعبي التكنولوجيا المالية.

2. دراسة (Vucinic, 2020):

هدفت الدراسة إلى دراسة الآثار المحتملة لتطورات التكنولوجيا المالية على الاستقرار المالي، وتأثير التكنولوجيا المالية على هيكل السوق بالإضافة إلى فوائد ومخاطر الابتكارات المالية المدفوعة تقنيًا على الاستقرار المالي. وتؤكد نتائج الدراسة على أهمية التعاون الدولي للمنظمين من أجل الحفاظ على الاستقرار المالي في العالم الحديث من التغيرات والابتكارات التكنولوجية، حيث قامت FinTech بتغيير توقعات المستهلكين وتفضيلاتهم مع زيادة عدد المستخدمين الذين يتوقعون خدمات سريعة وسهلة الوصول متاحة على الهواتف المحمولة والأجهزة الإلكترونية الأخرى. كما أظهرت نتائج الدراسة أن التكنولوجيا الجديدة توفر مساحة لتوسيع الخدمات المالية ولكنها تشكل أيضاً مخاطر إضافية على النظام المالي من حيث مخاطر التمويل الأصغر والمخاطر المالية الكلية.

3. دراسة (Khan, Malaika, 2021):

بحثت هذه الدراسة في التكنولوجيا المالية ومجال الأمن السيبراني ذي الصلة من منظور إدارة مخاطر البنك المركزي، واعتمدت هذه الدراسة على النتائج المستخلصة من قاعدة بيانات المادة الرابعة لصندوق النقد الدولي، وخيارات تقييم البنوك المختارة، حيث سلطت الدراسة الضوء على ضرورة معالجة المخاطر المتعلقة بالتكنولوجيا المالية والأمن السيبراني للبنوك المركزية من خلال تفعيل الإدارة السليمة للمخاطر الداخلية من خلال إنشاء وتعزيز نهج متكامل لإدارة المخاطر في جميع أنحاء المنظمة، بما في ذلك وحدة مخصصة لإدارة المخاطر، والتوعية والتدريب المستمر لأعضاء مجلس الإدارة والموظفين، وخطوط إبلاغ واضحة، وتقييم المرونة السيبرانية والوضع الأمني، وربط إدارة المخاطر بالتخطيط الاستراتيجي. وبالنظر إلى الطبيعة سريعة التطور لمثل هذه المخاطر، ويمكن للبنوك المركزية الاستفادة من المدخلات المنتظمة وفي الوقت المناسب من الخبراء الخارجيين.

4. دراسة (Varga, et al., 2021):

هدفت الدراسة إلى التحقيق في الوعي بالوضع السيبراني في البنوك في السويد، من خلال فحص عناصر المعلومات اللازمة لصورة تشغيلية مشتركة، واستكشاف كيفية إدراك الجهات الفاعلة الرئيسية للتهديدات السيبرانية، تم جمع البيانات من خلال المقابلات مع الجهات الفاعلة الرئيسية في القطاع بالتزامن مع ممارسة إدارة الأزمات على المستوى الوطني. وتم تحليل البيانات ومقارنتها بالنظرية. وظهرت النتائج أن الجهات الفاعلة في البنوك السويدي لديها مفهوم عمل متطور لإدارة الأزمات. ومع ذلك، فإن المعلومات

حول الخصوم العقلانيين الذين يتسببون في اضطرابات طويلة الأمد ربما لا يتم جمعها وتحليلها واستخدامها بشكل منهجي. وإن القطاع البنوك يدرك التهديدات السيبرانية ضد البنية التحتية المالية الأساسية، وكذلك ضد توافر خدمة تكنولوجيا المعلومات وسرية البيانات، إلى جانب المالية والمخاوف الخاصة بشأن احتمال فقدان السمعة بسبب الهجمات الإلكترونية. وهناك أيضاً مخاوف خاصة بشأن التهديد من الداخل.

5. دراسة (Inoussa, 2021):

هدفت الدراسة إلى دراسة تأثير التكنولوجيا المالية على الشمول المالي من خلال بناء مقياسين منفصلين لتقييم الشمول المالي التقليدي والرقمي ولتقديم ثلاثة مؤشرات جديدة للشمول المالي. والتحقيق في آثار الشمول المالي المدفوع بالتكنولوجيا المالية على النمو الاقتصادي وعدم المساواة في الدخل باستخدام مجموعة من 16 دولة من دول أفريقيا الواقعة جنوب الصحراء الكبرى مع بيانات من FAS وقاعدة بيانات Findex العالمية عبر عامي 2014 و2017، وعلى وجه التحديد استخدمت المؤشرات لتقييم تأثير الشمول المالي المدفوع بالتكنولوجيا المالية على النمو الاقتصادي وعدم المساواة في الدخل، وظهرت النتائج ثلاثة استنتاجات رئيسية من نتائج الدراسة. أولاً، يعد الشمول المالي القائم على التكنولوجيا المالية استراتيجية أفضل من الشمول المالي التقليدي لإدخال الفقراء وسكان الريف في النظام المالي. ثانياً، يمكن أن يساهم الشمول المالي المدفوع بالتكنولوجيا المالية في النمو الاقتصادي في أفريقيا جنوب الصحراء الكبرى. ثالثاً، يقلل الشمول المالي القائم على التكنولوجيا المالية من عدم المساواة في الدخل. مع تزايد اعتبار الشمول المالي أداة أساسية في تنفيذ أهداف التنمية المستدامة، كما تساهم نتائج هذه الدراسة في أدبيات الشمول المالي، وإلقاء الضوء على دور الشمول المالي القائم على التكنولوجيا المالية في تعزيز التنمية الشاملة والمستدامة. كما أن الأفكار المكتسبة من هذه الدراسة تضع الأساس للبحث المستقبلي في محددات الشمول المالي والطرق المختلفة التي قد تدعم بها التكنولوجيا المالية التنمية المستدامة المتوازنة.

6. دراسة (Eisenbach, Lee, 2022):

هدفت الدراسة إلى توضيح كيف يمكن أن تنتقل الهجمات الإلكترونية على بنك كبير واحد أو مجموعة من البنوك الصغيرة أو مزود خدمة مشترك من خلال نظام المدفوعات، حيث من المرجح أن يتم تضخيم أي هجوم إلكتروني على أكثر البنوك الأمريكية نشاطاً والذي يضعف من قدرات تلك البنوك على إرسال المدفوعات للتأثير على السيولة في العديد من البنوك الأخرى في النظام. سيكون مدى التضخيم أكبر إذا استجابت البنوك بشكل استراتيجي، وهو ما من المرجح أن يفعله إذا كان هناك عدم يقين بشأن الهجوم. قد يكون التأثير على المناطق الجغرافية ذات البنوك المركزية أكبر، وحددت أيضاً طرقاً أخرى يمكن أن يصبح بها النظام معطلاً والتي تسلط الضوء على أهمية جميع البنوك في الشبكة، وليس فقط البنوك الكبرى، وإذا تم توصيل عدد من البنوك الصغيرة أو متوسطة الحجم من خلال نقطة ضعف مشتركة، مثل مزود خدمة مهم، فقد يؤدي ذلك إلى انتقال

ها

صدمة عبر الشبكة. وبالمثل، فإن البنوك التي لديها أصول قليلة نسبياً ولكن تدفقات مدفوعات كبيرة لديها أيضاً القدرة على إضعاف النظام.

التعقيب على الدراسات السابقة:

- **أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة:**

1. من حيث الموضوع:

تناولت الدراسات السابقة مناقشة موضوع " أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك"، ولكنها ركزت على دراسة واقع الأمن السيبراني ومخاطره في البنوك المدرجة في بورصة فلسطين العاملة في قطاع غزة بدولة فلسطين وأثرها في دعم الاستقرار والشمول المالي.

2. من حيث المكان: تنوعت أماكن تطبيق الدراسات السابقة (السويد، أمريكا، جنوب أفريقيا، كندا).

3. من حيث المنهج: اعتمدت الدراسات السابقة المنهج الوصفي التحليلي.

4. من حيث الأدوات: استخدمت معظم الدراسات المنهج الوصفي كأداة للدراسة.

5. من حيث العينات: تنوعت عينات الدراسات السابقة فبعض الدراسات كانت على الشركات ومنها على البنوك، أما الدراسة الحالية فكانت العينة من البنوك المدرجة في بورصة فلسطين.

- **ما يميز الدراسة الحالية عن الدراسات السابقة:** تتميز الدراسة الحالية في عدة نقاط؛ أهمها:

- تعتبر الدراسة الحالية بناءً معرفياً وتراكيمياً للدراسات السابقة حول الموضوع، وتأتي استكمالاً لما بدأه الباحثون؛ فهي تُبنى على ما توصلوا إليه من نتائج، وما قدموه من توصيات.

- تركز الدراسة الحالية على دراسة أثر مخاطر الأمن السيبراني على دعم وتعزيز الاستقرار والشمول المالي، وهي بذلك تعتبر أكثر تخصصاً من الدراسات السابقة، كونها تناولت دراسة الأثر بين متغيرين في موضوعها وهي مخاطر الأمن السيبراني والاستقرار والشمول المالي.

- تضع الدراسة الحالية حلولاً عملية لمخاطر الأمن السيبراني في البنوك المدرجة في بورصة فلسطين لدعم وتعزيز الاستقرار والشمول المالي.

ثانياً: الاطار الفكري

1. الامن السيبراني وإدارة مخاطره

1-1. مخاطر الأمن السيبراني

الأسواق المالية أهدافاً جذابة بشكل متزايد لمجرمي الإنترنت مع تعزيز الدول المتقدمة لدفاعات الإللكترونية. ويؤدي انتشار الخدمات المالية الرقمية وزيادة الترابط بين الأنظمة والأسواق المالية إلى تفاقم التهديد الذي تشكله الهجمات الإلكترونية على القطاعات المالية في البلدان النامية وكذلك على الصعيد العالمي، ويعد بناء مرونة قوية على الإنترنت أمراً بالغ الأهمية لاستقرار الأسواق المالية وكذلك لتحقيق الشمول المالي، ويمكن للهجمات السيبرانية أن تثبط جهود الشمول المالي لأنها، إذا نجحت، قد تردع العملاء عن تبني منتجات وخدمات مالية جديدة.

وتعتبر المخاطر الإلكترونية شكلاً من أشكال المخاطر التشغيلية وتعرف على أنها مخاطر الخسارة الناتجة عن الحوادث الرقمية الناجمة عن الحوادث الداخلية والخارجية. أو أطراف ثالثة، بما في ذلك السرقة أو النزاهة المعرضة للخطر أو تلف المعلومات أو أصول التكنولوجيا، والاحتيايل الداخلي والخارجي، وتعطيل الأعمال. وهذا التعريف يتوافق إلى حد كبير مع جهود القطاع الخاص المتزامنة المعروفة لتحديد المخاطر السيبرانية، على سبيل المثال، مبادرة مخاطر الأمن السيبراني والمعلوماتية الخاصة بشركة ORX. وقد تؤدي حوادث المخاطر السيبرانية إلى إضعاف سرية وسلامة وتوافر البيانات والمعلومات، والتشغيل السليم للبنية التحتية لتكنولوجيا المعلومات.

حيث أن أنظمة الأمن السيبراني هي أنظمة مدعومة بالذكاء الاصطناعي للحماية من الانتهاكات الأمنية المحتملة ومنعها، ويستخدم الذكاء الاصطناعي لتطبيق الخدمات المصرفية عبر الهاتف المحمول وتطوير حلول الذكاء الاصطناعي لدعم العملاء وأتمتة العمليات والموارد البشرية والأمن واكتشاف الاحتيايل. (Saon, Miglanic, 2019)

وقد عرف مخاطر الأمن السيبراني على أنه المخاطر التشغيلية لأصول المعلومات والتقنية التي تؤثر على سرية أو توافر أو سلامة المعلومات أو أنظمة المعلومات. (Kumar, Thomas, 2022)، وإن سرقة بيانات وهوية المستهلك، وكذلك والتلاعب بها، باعتبارها تهديدات إلكترونية رئيسية تؤثر على أعمال البنوك. والتهديدات التي تتعرض لها البنية التحتية المالية، والمخاطر التي تشكلها البرامج الضارة المدمرة (Piotrowski, 2022)، وإن تصنيف المخاطر السيبرانية والمحفزات الكامنة وراءها يمكن أن يؤدي إلى وجود تعريف وفهم مشترك عبر البنوك، بما في ذلك بين السلطات والمشاركين من القطاع الخاص، وإلى زيادة تسهيل تبادل المعلومات والتعاون المناسب في إدارة المخاطر الإلكترونية. حيث تم تنظيم تصنيف المخاطر الإلكترونية للأمن السيبراني إلى :

1. **مسببات المخاطر السيبرانية:** الطريقة التي يتم من خلالها تنفيذ هجوم إلكتروني ضار من خلال:

- **رفض الخدمة:** هو هجوم يغمر الأنظمة أو الخوادم أو الشبكات بحركة مرور لاستنفاد الموارد وعرض النطاق الترددي. نتيجة لذلك، النظام غير قادر على تلبية الطلبات المشروعة. ورفض الخدمة الموزع (DDoS) هو عندما يستخدم المهاجمون عدة أجهزة مختربة لتنفيذ الهجوم.

ها

- **هجوم التنصت:** يدخل المهاجمون أنفسهم في معاملة ثنائية الأطراف وذلك بمجرد مقاطعة المهاجمين لحركة المرور، يمكنهم تصفية البيانات وسرقتها.
 - **التصيد الاحتيالي:** هو ممارسة إرسال اتصالات احتيالية التي تبدو أنها واردة من مصدر حسن السمعة، عادةً عبر البريد الإلكتروني. والهدف منه سرقة البيانات الحساسة مثل بطاقة الائتمان ومعلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية.
 - **هجوم كلمة المرور:** يحدث عندما تحصل أطراف غير مصرح لها على حق الوصول إلى كلمة مرور الشخص من خلال النظر حول مكتب الشخص، و"استنشاق" الاتصال بالشبكة للحصول على كلمات مرور غير مشفرة، واستخدام الهندسة الاجتماعية، والحصول على إمكانية الوصول إلى قاعدة بيانات كلمة المرور أو التخمين المباشر (القوة الغاشمة أو هجوم القاموس).
 - **حقن SQL:** يحدث حقن لغة الاستعلام الهيكلية (SQL) عندما يقوم المهاجم بإدراج تعليمات برمجية ضارة في خادم يستخدم SQL ويجبر الخادم على الكشف عن المعلومات الخاصة به عادة لا.
 - **البرمجة النصية عبر المواقع:** تستخدم هجمات البرمجة النصية عبر المواقع موارد ويب تابعة لجهات خارجية لتشغيل البرامج النصية في متصفح الويب الخاص بالضحية أو التطبيق القابل للبرمجة.
 - **البرامج الضارة:** برنامج مصمم بقصد ضار يحتوي على ميزات أو قدرات يمكن أن تسبب ضررًا مباشرًا أو غير مباشر للكيانات أو أنظمة المعلومات الخاصة بها.
 - **استغلال Zero-day:** ثغرة أمنية في الأجهزة أو البرامج الثابتة أو البرامج غير المعروفة سابقاً.
 - **أخرى:** أي نوع آخر من الهجمات الإلكترونية التي لم يتم تعريفها. ستعمل هذه الفئة كفئة "النقاط الكل" للهجمات الإلكترونية ذات النوع المعروف ولكن لم يتم التقاطها بواسطة فئة أخرى موجودة.
 - **غير معروف:** عندما يكون نوع الهجوم الإلكتروني غير معروف للمؤسسة.
2. **نتيجة الحادث السيبراني: نتيجة حادث إلكتروني يؤدي إلى:**
- **اضطراب الأعمال وفشل النظام والتنفيذ:** هي الحوادث الداخلية أو الخارجية التي تعطل العمل أو تتسبب في فشل البرامج / الأجهزة / تكنولوجيا المعلومات.
 - **خرق البيانات:** تعني فقدان البيانات أو التعرض الذي يتضمن معلومات التعريف الشخصية.
 - **سرقة أو فقدان معلومات غير معلومات:** تعني سرقة أو فقدان التكنولوجيا أو الملكية الفكرية أو المعلومات التجارية أو أي معلومات أخرى ليست معلومات تحديد الهوية الشخصية.
 - **سرقة الأموال:** هي الحوادث التي أدت إلى خسارة فورية ومباشرة للأموال وتم تنفيذها عبر قناة رقمية.
3. **النية: مؤشر لمعرفة ما إذا كان الحادث الإلكتروني متعمدًا أم عرضيًا:**

• **متعمد:** عندما يكون الحادث الإلكتروني كيداً / متعمداً.

• **غير مقصود:** عندما يكون الحادث السيبراني غير مقصود.

4. **المنشأ:** مؤشر لمعرفة ما إذا كانت الحادثة الإلكترونية قد نشأت في المؤسسة أو في جهة خارجية:

• **طرف خارجي:** عند وقوع الحادث السيبراني لدى طرف ثالث / بائع أو أي كيان خارجي آخر.

• **طرف غير خارجي:** عندما بدأ الحادث الإلكتروني في المؤسسة أو الشركة التابعة لها.

5. **فئة حدث بازل (II):** فئة حدث بازل المخصصة للحادث السيبراني:

• **الاحتتيال الداخلي:** خسائر ناجمة عن أفعال من نوع الاحتيال أو اختلاس الممتلكات أو التحايل على اللوائح أو القانون أو سياسة الشركة، باستثناء أحداث التنوع / التمييز، والتي تشمل طرفاً داخلياً واحداً على الأقل.

• **الاحتتيال الخارجي:** خسائر ناجمة عن أفعال من النوع المقصود بها الاحتيال أو اختلاس الممتلكات أو التحايل على القانون من قبل طرف ثالث.

ويستخلص الباحثان أنه يمكن تعريف مخاطر الأمن السيبراني على أنه حدث يمكن ملاحظته في نظام المعلومات، حيث أن الخطر السيبراني يهدد المعلومات التي يعالجها النظام أو يخزنها أو ينقلها. أو ينتهك السياسات أو الإجراءات الأمنية أو سياسات الاستخدام المقبولة، سواء كان ذلك نتيجة لنشاط ضار أم لا. ويمكن أن يؤدي الحادث الإلكتروني إلى خسارة مالية. ويمكن ملاحظته في نظام معلومات لا ينتج عنه بالضرورة خسارة مالية. وهناك تهديدان لتقنيات ناشئة جديدة غير مثبتة وربما مليئة بنقاط الضعف، وانتشار المعلومات المضللة واستخدامها بشكل عام، كما أن التعامل مع المخاطر السيبرانية، والقضايا السيبرانية بشكل عام، يتم النظر إليه بطريقة مختلفة عن إدارة الأنواع الأخرى من المخاطر.

1-2. مخاطر الامن السيبراني في الخدمات المالية عبر الحدود

تشير الابتكارات الرقمية لخدمات الدفع عبر الحدود باستخدام FinTechs مخاطر جديدة، لا سيما فيما يتعلق بالأمن السيبراني. إن الطبيعة المتغيرة للهجمات الإلكترونية ونمو المخاطر السيبرانية مدفوعة بعوامل تشمل التقنيات المتقدمة، وزيادة الترابط بين المؤسسات المالية والأطراف الخارجية، والحوافز الأكثر أهمية لمجرمي الإنترنت لاستهداف الهيئات المالية (Huang, Madnick, 2020) على سبيل المثال، أدى الهجوم الإلكتروني على بنك (Banco de Chile) في عام 2018 إلى تدمير 9000 محطة عمل و500 خادم، بالإضافة إلى تعرض نقاط النهاية للتعامل مع المعاملات على شبكة SWIFT للخطر، كما يتم استخدام الخوارزميات التي تعمل خلف الشاشة لأتمتة الموافقات أو الاستشارات الائتمانية، وتسهيل الامتثال التنظيمي واكتشاف الاحتيال وأتمتة تداول الأصول المالية، وتلعب أدواراً أساسية لخدمات الدفع عبر الحدود. ومع ذلك، فإن سلامة الخوارزميات، والضعف المتأصل في

الخوارزميات المعتمدة، والمسائل الأخلاقية للحكم الذاتي، وما إلى ذلك، تزيد من المخاطر النظامية داخل نظام الدفع عبر الحدود. نظرًا للاعتماد الواسع النطاق للتداول الخوارزمي هذه الأيام، يمكن أن تؤدي هذه التقلبات إلى مزيد من "الانهيارات السريعة"

ويعتبر النظام المالي بنية تحتية مهمة ويتم تعريف أمنه السيبراني على أنه جزء من الأمن السيبراني الوطني. "الاستثناء الأمني" هو مبدأ مهم في بيئة التجارة الدولية، والذي يسمح للحكومات باتخاذ الإجراءات عند الضرورة في حالات "المصلحة الأمنية الأساسية". ومع ذلك، يعتبر هذا الاستثناء الأمني محددًا ذاتيًا، أو ما يسمى "الحكم الذاتي" أو "التفسير الذاتي" ومن المتوقع أن يظل غير واضح في المستقبل القريب. حيث يثير العديد من النزاعات في مجال الأمن السيبراني بين الدول (Tzoneva, Stoyanov, 2022)، وللتغلب على خسائر الأمن السيبراني لابد من وجود مبادئ أساسية مهمة لإنشاء مخطط لتصنيف تأثير الخسائر السيبرانية في إنشاء فئات تجمع تأثيرات الخسارة المتشابهة نسبيًا في طبيعتها وتحتوي على دوافع مماثلة من أجل تسهيل الخطوات القابلة للتنفيذ من منظور إدارة المخاطر، خاصة

1-3. إدارة مخاطر الأمن السيبراني في البنوك

إدارة المخاطر هي عمل أساسي للبنوك، فمن المهم التمييز بين الأنواع المختلفة من المخاطر، حيث أن التمييز الأساسي هو التمييز بين المخاطر المالية وغير المالية. على سبيل المثال، المخاطر التي يتعين على البنوك الاحتفاظ برأس مالها: مخاطر الائتمان (تقصير الأطراف المقابلة)، ومخاطر السوق (انخفاض قيمة الأصول المتداولة)، ومخاطر التشغيل (تلك العمليات الداخلية أو فشل الأنظمة أو أن الأحداث الخارجية المعاكسة تتحقق)، حيث أن المخاطر الأولى والثانية في هذا التصنيف مالية في الأصل، في حين أن الأخطار الأخيرة، التي تشمل المخاطر السيبرانية، غير مالية في الأصل (Varga, Brynielsson, Franke, 2021)، وتعتمد البنوك على التكنولوجيا السيبرانية (CyberTech)، ولكنها تصبح عرضة للأمن السيبراني. وبالتالي، تصبح زيادة الاستثمار في CyberTech وضرورة استراتيجية للبنوك لمكافحة مخاطر الأمن السيبراني.

وتعد إدارة المخاطر السيبرانية مجالاً تقنياً بطبيعته، ويعتمد الكثير من البيانات المتاحة على مؤشرات تقنية خاصة بالهجمات والأنظمة خاصة بتكنولوجيا المعلومات. في حين أن هذا يتيح استخبارات التهديد السيبراني والوظائف الفنية الأخرى، فإنه لا يمكن الوصول إليه بسهولة لعالم الاجتماع أو الاقتصادي الذي يتطلع إلى تحديد علاقات معينة في البيانات. هناك تعقيد آخر وهو أن البيانات التقنية لتكنولوجيا المعلومات نادراً ما يتم جمعها جنباً إلى جنب مع مقاييس التأثير. كما أن معظم مصادر البيانات الموضحة أعلاه هي من مصادر مختلفة ويتم توفيرها من قبل بائعين مختلفين، Herrera, Munera, Williams, 2021).

التوجيهات التنظيمية المتعلقة بإدارة المخاطر الإلكترونية. يمكن أن يعزز التصنيف المشترك لعمل الوكالات التنظيمية والإشرافية في توفير التوجيه المتعلق بالأمن السيبراني والمرونة الإلكترونية، بما في ذلك تحديد الممارسات الفعالة أو التهديدات الناشئة. على سبيل المثال، والمساعدة في استخدام لغة مشتركة لتعزيز الأساليب التنظيمية الفعالة مع تقليل مخاطر المتطلبات التنظيمية والإشرافية المتكررة والمتضاربة. (Curti, Gerlach, et al., 2019)، وقد تم تطوير معايير جديدة للإبلاغ عن معلومات المخاطر السيبرانية في السنوات الأخيرة عن طريق ORX للمخاطر الإلكترونية وأمن المعلومات (CISR) بما في ذلك حجم الخسائر ومصدرها، ومعلومات عن الجهات الفاعلة في التهديد وهدفها، ونوع أصول تكنولوجيا المعلومات التي تم اختراقها، والثغرة الأمنية المحددة (ضعف البرامج) التي تم استغلالها (Herrera, Munera, Williams, 2021).

ويرى الباحثان أن الافتقار إلى قدرات الحماية الكافية يمكن أن يعرض البيانات لخطر انتهاكات البيانات. في ضوء ذلك، هناك متطلبات من اتفاقية بازل وحوكمة البنوك تتعلق بالأمن السيبراني وتدابير حماية البيانات لمقدمي خدمات الدفع عبر الحدود. والغرض من هذه المتطلبات هو تسهيل الحد الأدنى المعياري لمستوى الأمن السيبراني بالنظر إلى الطبيعة المتطورة للهجمات السيبرانية. حيث تتضمن هذه المتطلبات تدقيق المخاطر الإلكترونية من مزودي الخدمة الخارجيين، بما في ذلك المصدر الأجنبي، ويعتبر هذا أمراً بالغ الأهمية عند التخفيف من المخاطر الإلكترونية من سلاسل التوريد ويقترح أيضاً اختبار رموز المصدر كأحد أفضل الإجراءات لإدارة مخاطر الإنترنت في سلسلة التوريد. ومع ذلك، فإن الكشف عن أكواد المصدر يمكن أن يثير مخاوف بشأن حماية الملكية الذكية، وهي ميزة نسبية للعديد من الشركات الدولية.

1-4. أثر استخدام التكنولوجيا المالية على الاستقرار والشمول المالي في قطاع البنوك:

تلعب التكنولوجيا المالية دوراً متزايداً لتعزيز نظام الدفع عبر الحدود بينما تظهر مخاطر التهديد السيبراني. ومع ذلك، ينبغي أن يقترن الاستخدام المتزايد لهذه التقنيات بتعزيز الرقابة التنظيمية على الأنشطة المالية لحماية الاستقرار المالي، حيث قد تظهر مخاطر جديدة تزيد اتجاهات الرقمنة المالية من

الحاجة إلى الأمن السيبراني لحماية المستهلكين والمنتجين الماليين. ومن ثم، إلى جانب تنفيذ اللوائح ذات الصلة لحماية الأنظمة المالية والتخفيف من مخاطر الأمن السيبراني المحتملة، حيث فرضت العديد من الدول قيوداً على حواجز التجارة الإلكترونية، بهدف تصنيفها في الفئات التالية، التوطين، ويتكون أول تقييد للتجارة من متطلبات التوطين، بما في ذلك البيانات أو توطيّن النظام ذي الصلة. على سبيل المثال، تتطلب الهند أن يتم وضع جميع بيانات الدفع التي تحتفظ بها شركات الدفع في منشآت محلية داخل الدولة ولا يسمح بتصديرها خارج البلاد، ولا حتى للمعالجة. إلى جانب متطلبات البيانات، Huang, (Madnick, 2020).

وعلى الرغم من أن FinTech تخلق فوائد للاستقرار المالي، إلا أنه من المحتمل أن يكون لها تأثير نظامي سلبي على الأخير ويمكن أن تنتج آثاراً سلبية خطيرة يمكن أن تعرض الاقتصاد الحقيقي للخطر، وتعتبر التكنولوجيا المالية إحدى التقنيات الهامة التي يمكن أن تقوض الاستقرار المالي من خلال قنوات التمويل الأصغر والقنوات المالية الكلية. لذلك يمكن أن تخلق التكنولوجيا المالية مخاطر مالية صغيرة وكبيرة على الاستقرار المالي. بينما يعمل رأس المال والسيولة من جانب على تعزيز المرونة المالية، من ناحية أخرى، وتدعم الحوكمة والضوابط القوية المرونة التشغيلية. وتتبع مصادر المخاطر التشغيلية من الحوكمة ومراقبة العمليات، والمخاطر الإلكترونية، والاعتماد على الأطراف الثالثة، والمخاطر القانونية ومخاطر الأعمال المتعلقة بالبنية التحتية الحيوية للأسواق المالية (Vucinic, 2020).

ويشير الشمول المالي إلى عدد المستفيدين الذين يمكنهم الوصول إلى الخدمات المصرفية أو المالية، حيث أن الخطوة الأولى نحو الشمول المالي هي امتلاك حساب على نحو متزايد، يتم استخدام المدفوعات الرقمية في المعاملات المالية. كما يعد إجراء المدفوعات الرقمية أو تلقيها أحد الاستخدامات المهمة لحساب الادخار. مع ذلك، أفاد عدد قليل من الأشخاص باستخدام حساباتهم للادخار ولكن ليس أيضاً لإجراء مدفوعات رقمية أو تلقيها في العام الماضي، كما ساعدت التكنولوجيا في تحقيق التكافؤ بين الجنسين وقلصت الفجوة بين البالغين الأكثر ثراءً والفقراء (Saon, Miglanic, 2019).

وان أحد المنتجات التي تم إنشاؤها من نموذج Fintech هو منصة الإقراض من شخص إلى شخص (P2P)، على الرغم من أن إقراض P2P يقدم خدمات أفضل بتكاليف منخفضة، إلا أنه زاد أيضاً من مخاطر الائتمان. وبالتالي ظهور المخاطر النظامية، ومما لا شك فيه أن الوسائط الرقمية قد زادت من مستوى الشمول المالي عالمياً من 51 بالمائة عام 2011 إلى 69 بالمائة في 2017 والتحدي الذي يواجه البنوك هو تحديد أنسب نموذج للاتصال للتفاعل مع شرائح مختلفة من العملاء من أجل إقناعهم بتبني قنوات مصرفية رقمية. ونظراً للاضطرابات غير النقدية، لا تستطيع المؤسسات المالية التحكم في تجربة العملاء في المعاملات بسبب التكامل وتفقد المؤسسات المالية الرؤية وسيتعين عليها أن تهدف إلى تأمين مكان البطاقة الافتراضية في السوق. (Yadav, Shanmugam, 2022).

أن التطورات السريعة في التكنولوجيا المالية على الأسواق المالية ونماذج

الأعمال للمؤسسات المالية التقليدية من أجل متابعة الاتجاهات الحالية والمنافسة في منافستها سريعة النمو، للوصول إلى الشمول المالي. حيث تتبنى المؤسسات المالية التقليدية التغييرات من أجل تلبية احتياجات السوق. ويمكن أن تكون عوامل جانب العرض والطلب بمثابة محركات للابتكارات المالية، وتبحث للأجيال الجديدة بشكل خاص عن خدمة مالية سريعة وسهلة الوصول يمكن الوصول إليها في أي وقت وفي أي مكان. وفيما يتعلق بذلك، من المرجح أن يستخدموا المدفوعات الإلكترونية أو الخدمات المصرفية عبر الهاتف المحمول أو ائتمانات FinTech أو غيرها من المنتجات بدلاً من استخدام أساليب الخدمات المالية التقليدية. والشاغل الرئيسي هو التأثير الرقمي على استقرار وسلامة أسواق والأنظمة المالية الأوسع.

1-5. أثر مخاطر الامن السيبراني على الاستقرار والشمول المالي للبنوك:

تبتت البنوك بشكل متزايد دورها في تعزيز الشمول المالي إلى جانب أهدافها التقليدية المتمثلة في الحفاظ على استقرار الأسعار والاستقرار المالي. ولتحقيق هذه الغاية، لا تستخدم بعض البنوك المركزية القواعد واللوائح فحسب، بل تستخدم أيضاً الابتكار من خلال التدخل المباشر في نظام المدفوعات الفورية المدعوم من البنك المركزي. والذي يمكن أن يحدثه البنك المركزي على تحقيق الاندماج والمنافسة في صناعة المدفوعات. وأن دور البنك في المدفوعات يمكن أن يكون أداة فعالة لتعزيز الإدماج وتعزيز المنافسة، لا سيما عندما يبدو الفاعلون الخاصون غير راغبين أو غير قادرين على القيام بذلك بأنفسهم. ومع ذلك، فإن شرعية التدخلات المبتكرة للبنك المركزي في المدفوعات والذي يمكن للبنوك أن تمضي فيه في إجراءاتها المبتكرة دون المبالغة في تقدير أيديها أو إزاحة المبادرة والبراعة الخاصة، Bolzani (2022)، وتغطي البنوك خمس وظائف واسعة. وهي من أجل (Saon, Miglanic, 2019):

- إجراء المدفوعات واستلامها، بما في ذلك عبر الحدود.
- الادخار لتمكين من الاستهلاك أو الاستثمار لاحقاً.
- الاقتراض للتمكين من الاستهلاك أو الاستثمار الآن.
- إدارة المخاطر على الدخل والمدخرات والمعاملات.

قد تحفز Fintech مكاسب الكفاءة في البنوك، وتقدم منتجات وخدمات أفضل وأكثر استهدافاً، وتعمق الشمول المالي. ومع ذلك، قد يشكل أيضاً مخاطر إذا كان تطبيقه يقوض المنافسة والثقة ونقل السياسة النقدية والاستقرار المالي. على الرغم من الاعتراف بأن المخاطر السيبرانية تشكل تهديداً كبيراً للاستقرار المالي، إلا أن قياس وتحليل المخاطر الإلكترونية في البنوك لم ينضج إلى الحد الذي يمكن فيه قياسها وإدارتها باستمرار مقابل تقبل المخاطر المؤسسية والنظر إليها من منظور النظام من خلال المنظّمون والمشرفون. وهذا يعيق الجهود المبذولة لقياس وإدارة هذه المخاطر بشكل فعال، مما يقلل من

استعداد المؤسسات الفردية والجماعية للتعامل مع التهديدات الإلكترونية على مستوى النظام ومعالجة تكنولوجيا المعلومات أو أبعاد هندسة النظام للمخاطر السيبرانية، بل التركيز على جوانب إدارة المخاطر المالية للمخاطر السيبرانية (Tzoneva, Stoyanov, 2022).

أن المخاطر السيبرانية تمتد إلى جميع المجالات الرئيسية لعمليات البنوك، والاستقرار المالي، والنزاهة المالية، والشمول المالي، وأنظمة الدفع، وإدارة العملات النقدية. على الرغم من أن هذه المخاطر المتعلقة بالأمن السيبراني تؤثر في المقام الأول على المؤسسات الخاضعة للإشراف والمشاركين في الأسواق المالية، إلا أنها تؤثر أيضاً على التعرض للمخاطر التي يواجهها البنك نفسه. بالإضافة إلى ذلك، يمكن أن تتفاقم المخاطر التشغيلية المتعلقة بالنظام الداخلي، بما في ذلك تكنولوجيا المعلومات (والأمن السيبراني) والموارد البشرية وإدارة استمرارية الأعمال، من خلال زيادة استخدام أدوات التكنولوجيا المالية أيضاً. لذلك، تحتاج إدارة المخاطر السيبرانية للبنك إلى تشكيل خط دفاع مناسب للمخاطر المتعلقة بالتكنولوجيا المالية.

وعلى الرغم من أن مخاطر الأمن السيبراني ليست جديدة على الإطلاق، فإن السرعة والميل الذي تحدث به تطورات في البنوك إلا أن إدارات تكنولوجيا المعلومات والمشرفين الماليين هم أول "وحدات عمل" داخل العديد من البنوك لتحديد مخاطر الأمن السيبراني. لذلك تحتاج البنوك إلى تعزيز إدارتها الداخلية للمخاطر لتشمل مساعدة شاملة على مستوى البنك في تحديد المخاطر المتعلقة بالتكنولوجيا ومخاطر الأمن السيبراني وتخفيفها والإبلاغ عنها ومراقبتها بالنسبة للبنك، حيث أن حوكمة المخاطر وثقافة المخاطر القوية أمران حاسمان. هذه تتطلب توعية قوية من البنك. وأن يكون المحافظين وأعضاء مجلس الإدارة على دراية بالمخاطر المتعلقة بالأمن السيبراني التي تديرها البنك، وكيف أن هناك حاجة واضحة لإطار عمل لإدارة المخاطر السيبرانية. ويشمل ذلك الوصول إلى موظفي البنك المركزي وتدريبهم (لا يقتصر على المشرفين ومتخصصي تكنولوجيا المعلومات - على الرغم من أن برنامج التدريب على التكنولوجيا المالية وإدارة المخاطر وتدريب موحد ومتسق ومركّز على التكنولوجيا والالكترونية)، بالإضافة إلى تعزيز فهم أعضاء مجلس الإدارة أنفسهم لتطورات التكنولوجيا المالية على مستوى أكثر دقة، حيث أن إدارة المخاطر يجب أن تأخذ في الحسبان دمج العاملين السيبرانيين في فرق إدارة الأزمات.

الدراسة الميدانية:

أولاً: منهج الدراسة:

تم استخدام المنهج الوصفي التحليلي في إجراء الدراسة لكونه من أكثر المناهج استخداماً في الدراسات الاجتماعية والإنسانية، وكذلك تم استخدام المصادر الثانوية والتي تشمل الأبحاث التي كتبت في موضوع الدراسة، وكذلك ما تم نشره من أبحاث علمية ومقالات في الدوريات المتخصصة وكذلك

القوانين والتشريعات المرتبطة بموضوع الدراسة. وفيما يتعلق بالمصادر الأولية اعتمد الباحثان على استبانة تم تصميمها وتوزيعها خصيصاً لغرض الدراسة، وكذلك تم تفريغ الاستبانة من خلال استخدام برنامج SPSS الإحصائي، كما تم حساب الاختبارات الإحصائية المناسبة والضرورية لموضوع الدراسة.

ثانياً: مجتمع وعينة الدراسة:

1. مجتمع الدراسة: بلغ مجتمع الدراسة (120) مدراء عامين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين.
2. عينة الدراسة: تم توزيع الاستبانة على عينة عشوائية بلغت (90) مدراء عامين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين، وكانت النتائج على النحو التالي:

المتغير	البيان	العدد	النسبة المئوية
المؤهل العلمي	بكالوريوس	70	77.8%
	ماجستير	17	18.9%
	دكتوراه	3	3.3%
	المجموع	90	100.0%
المسمى الوظيفي	مدير عام	20	22.3%
	مدير فرع	31	34.5%
	مدير مالي	22	24.5%
	مدير دائرة المخاطر	17	18.9%
	المجموع	90	100.0%
سنوات الخبرة	أقل من 5 سنوات	13	14.4%
	5-10 سنوات	17	18.9%
	10-15 سنة	33	36.7%
	أكثر من 15 سنوات	27	30.0%
	المجموع	90	100%

ثالثاً: أداة الدراسة:

لقد تم تقسيم الاستبانة إلى جزأين كما يلي:

- الجزء الأول: ويتكون من البيانات الديمغرافية لعينة الدراسة ويتكون من 3 فقرات.
 - الجزء الثاني: ويتناول أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، وقد تم تقسيم هذه الاستبانة إلى ثلاثة محاور.
- وقد اعتمد الطالبان على المقياس الخماسي للإجابة عن الفقرات ، حسب ما هو موضح في الجدول رقم (2).

جدول رقم (2) مقياس ليكرت الخماسي

7

التصنيف	موافق بدرجة كبيرة جداً	موافق بدرجة كبيرة	محايد	غير موافق	غير موافق بدرجة كبيرة
الدرجة	5	4	3	2	1

رابعاً:

صدق الاتساق الداخلي:

يقصد بصدق الاتساق الداخلي مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إليه هذه الفقرة، وقد قام الطالبان بحساب الاتساق الداخلي للاستبانة وذلك من خلال حساب معاملات الارتباط بين كل فقرة من فقرات مجالات الاستبانة والدرجة الكلية للمجال نفسه.

جدول (3) معامل الارتباط بين كل فقرة من فقرات المجال الأول (إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي) والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سبيرمان	القيمة الاحتمالية (Sig)
1	تؤدي مخاطر الأمن السيبراني إلى اختراقات للبيانات التي تتم من خلالها الوصول إلى معلومات سرية عن أعمال البنك.	0.60	دالة عند مستوى دلالة 0.05

2	تدرك إدارة البنك أن مخاطر أمن المعلومات يمكن أن تزعزع الاستقرار المالي وتحقق خسائر مالية يمكن أن يتكبدها البنك.	0.74	دالة عند مستوى دلالة 0.05
3	يقوم البنك بضبط المخاطر السيبرانية وتخفيف الأثر المالي والتحوط منها من خلال وضع الإجراءات والتدابير للأمن السيبراني بهدف دعم الاستقرار المالي له.	0.81	دالة عند مستوى دلالة 0.05
4	يوجد فريق للاستجابة لحوادث الأمن السيبراني على مستوى البنك بما يساهم في تكثيف الجهود للاستغلال الأمثل للطاقت لتطوير منظومة الأمن السيبراني لتعزيز الاستقرار المالي للبنك.	0.55	دالة عند مستوى دلالة 0.05
5	يصدر البنك تعليمات لكيفية إدارة المخاطر السيبرانية، ووضع السياسات لإدارة أمن المعلومات والأمن السيبراني.	0.69	دالة عند مستوى دلالة 0.05
6	يعتبر إدماج المخاطر السيبرانية بصورة أفضل في تحليل الاستقرار المالي من شأنه تحسين القدرة على فهم المخاطر على	0.66	دالة عند مستوى دلالة 0.05

	مستوى النظام وتخفيف حدتها.		
7	يؤدي تقليل المخاطر النظامية المرتبطة بالبنك إلى دور إيجابي على الاستقرار المالي.	0.68	دالة عند مستوى دلالة 0.05

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يوضح جدول (3) معامل الارتباط بين كل فقرة من فقرات المجال الأول والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha = 0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (4) معامل الارتباط بين كل فقرة من فقرات المجال الثاني (إدارة مخاطر الأمن السيبراني ودعم الشمول المالي) والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سييرمان	القيمة الاحتمالية (Sig)
1	يقوم البنك بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي.	0.74	دالة عند مستوى دلالة 0.05
2	يقوم البنك بإعداد وتصميم معالجات للمخاطر السيبرانية تتم من خلال تحديد مصادر بداية هذه المخاطر واحتمالية حدوثها.	0.80	دالة عند مستوى دلالة 0.05

3	يقوم البنك بإعداد خطة لإدارة المخاطر السيبرانية والتي تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات السيبرانية والتعافي منها في زمن قياسي، مما يعزز الشمول المالي.	0.86	دالة عند مستوى دلالة 0.05
4	يقوم البنك بالتغلب على المخاطر السيبرانية الناجمة عن التحول المتزايد الى رقمنة العمليات المالية.	0.67	دالة عند مستوى دلالة 0.05
5	يقوم البنك بزيادة التركيز على تعزيز الوعي بالأمن السيبراني بين موظفيه.	0.69	دالة عند مستوى دلالة 0.05
6	يقوم البنك بتطوير أطر الرقابة والاستجابة الفعالة للمخاطر السيبرانية، بما في ذلك ضمان تنفيذ ممارسات إدارة المخاطر العامة السليمة المتعلقة بالمخاطر السيبرانية.	0.71	دالة عند مستوى دلالة 0.05
7	يقوم البنك بعقد دورات تدريبية لموظفيه تتعلق بالأمن السيبراني والشمول المالي.	0.60	دالة عند مستوى دلالة 0.05

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يوضح جدول (4) معامل الارتباط بين كل فقرة من فقرات المجال الثاني والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha = 0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (5) معامل الارتباط بين كل فقرة من فقرات المتغير المستقل (مخاطر الأمن السيبراني) والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سبيرمان	القيمة الاحتمالية (Sig)
1	تعد الخدمات المالية الإلكترونية في البنك من أكثر الخدمات التي تتعرض للمخاطر المتعلقة بالأمن السيبراني.	0.64	دالة عند مستوى دلالة 0.05
2	تعتبر البرامج الضارة واحدة من أكثر التقنيات المستخدم في تحقيق الهجمات السيبرانية.	0.79	دالة عند مستوى دلالة 0.05
3	يقوم البنك بوضع خطط للتعامل مع أي خطر سيبراني يهدد معاملاته الإلكترونية في المستقبل وكيفية التعامل معه.	0.72	دالة عند مستوى دلالة 0.05
4	يقوم البنك بالاعتماد على المعايير والأطر الدولية المعروفة في إدارة المخاطر للتحوط للمخاطر السيبرانية.	0.67	دالة عند مستوى دلالة 0.05
5	يعمل البنك بشكل مستمر على تطوير وتحديث خطط استمرارية العمل بحيث تأخذ بالاعتبار الهجمات السيبرانية.	0.81	دالة عند مستوى دلالة 0.05
6	يقوم البنك بتقييم مخاطر الأمن السيبراني باستمرار لحماية بياناته من الوصول غير المصرح به أو التدمير.	0.80	دالة عند مستوى دلالة 0.05
7	تقدم إدارة المخاطر لإدارة البنك تقرير يشتمل على معلومات هامة حول المخاطر السيبرانية.	0.76	دالة عند مستوى دلالة 0.05
8	يقوم البنك بوضع إجراءات فعالة للحد من المخاطر السيبرانية لحماية عملائه.	0.75	دالة عند مستوى دلالة 0.05

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يوضح جدول (5) معامل الارتباط بين كل فقرة من فقرات المتغير التابع والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha = 0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

الصدق البنائي:

يعتبر الصدق البنائي أحد مقاييس صدق الأداة الذي يقيس مدى تحقق الأهداف التي تريد الأداة الوصول إليها، ويبين مدى ارتباط كل مجال من مجالات الدراسة بالدرجة الكلية لفقرات الاستبانة. وللتحقق من الصدق البنائي قام الطالبان بحساب معاملات الارتباط بين درجة كل مجال من مجالات الاستبانة والمجالات الأخرى، وكذلك درجة كل مجال بالدرجة الكلية للاستبانة كما في جدول (6).
جدول (6) معامل الارتباط بين درجة كل مجال من مجالات الاستبانة والدرجة الكلية للاستبانة

الرقم	المجال	معامل الارتباط سبيرمان	القيمة الاحتمالية (sig)
1	الاستقرار المالي	0.71	دالة عند مستوى دلالة 0.05
2	الشمول المالي	0.76	دالة عند مستوى دلالة 0.05
3	مخاطر الأمن السيبراني	0.74	دالة عند مستوى دلالة 0.05
	الدرجة الكلية	0.73	دالة عند مستوى دلالة 0.05

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يتضح من جدول (6) أن جميع معاملات الارتباط في جميع مجالات الاستبانة دالة إحصائياً وبدرجة قوية عند مستوى معنوية ($\alpha = 0.05$) وبذلك تعتبر جميع مجالات الاستبانة صادقةً لما وضعت لقياسه.

أ- طريقة التجزئة النصفية (Spilt-half):

حيث تم تجزئة فقرات الاستبانة إلى جزأين (الفقرات ذات الأرقام الفردية ، والفقرات ذات الأرقام الزوجية) ثم تم حساب معامل الارتباط بين درجات الفقرات الفردية ودرجات الفقرات الزوجية وبعد ذلك تم تصحيح معامل الارتباط بمعادلة سبيرمان براون Spearman Brown:

معامل الارتباط المعدل = $\frac{2r}{1+r}$ حيث r معامل الارتباط بين درجات الفقرات الفردية ودرجات الفقرات

الزوجية . وتم الحصول على النتائج الموضحة في جدول (7).

جدول (7) طريقة التجزئة النصفية لقياس ثبات الاستبانة

م	المجال	معامل الارتباط سبيرمان	معامل الارتباط المعدل سبيرمان
---	--------	------------------------	-------------------------------

0.83	0.71	الاستقرار المالي	1
0.86	0.75	الشمول المالي	2
0.87	0.76	مخاطر الأمن السيبراني	3
0.85	0.74	جميع المجالات	

8. تقوم البنوك المدرجة في بورصة فلسطين بالاعتماد على المعايير والأطر الدولية المعروفة في إدارة المخاطر للتحوط للمخاطر السيبرانية.
9. تقدم إدارة المخاطر لإدارات البنوك المدرجة في بورصة فلسطين تقرير يشتمل على معلومات هامة حول المخاطر السيبرانية، والإجراءات الفعالة للحد منها لحماية عملائها.

ثانياً: التوصيات

الفصل الثالث

منهجية البحث

المقدمة

منهجية البحث في هذا الفصل تهدف إلى استكشاف تأثير إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك. سيتم تناول الطرق المستخدمة لتقييم وتحليل المخاطر السيبرانية، واستراتيجيات الحد من تلك المخاطر، وكيفية تطبيقها في السياق البنكي لتحقيق أقصى قدر من الفعالية. سيتم الاعتماد على تحليل بيانات من مؤسسات مالية مختلفة، بالإضافة إلى مراجعة الأدبيات والدراسات السابقة في هذا المجال. هذه المنهجية تهدف إلى تقديم رؤية شاملة ومتكاملة حول دور إدارة مخاطر الأمن السيبراني في تعزيز الاستقرار والشمول المالي في النظام المصرفي.

التعريفات الإجرائية لمتغيرات البحث

مقدمة

تعد التعريفات الإجرائية لمتغيرات البحث من الخطوات الأساسية في إعداد الدراسات الأكاديمية والبحوث التطبيقية، حيث تساعد في تحديد وتوضيح المفاهيم والمتغيرات المستخدمة في الدراسة. من خلال التعريفات الإجرائية، يمكن للباحثين تحويل المفاهيم النظرية إلى متغيرات قابلة للقياس والملاحظة، مما يساهم في تحسين دقة وموثوقية النتائج.

في هذا الفصل، سنقوم بتحديد التعريفات الإجرائية لمتغيرات البحث المرتبطة بدراسة أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك. يتضمن ذلك تحديد المتغيرات المستقلة، التابعة، والوسيطة، وكيفية قياس كل منها بطرق كمية ونوعية. هذه التعريفات ستساعد في فهم العلاقات بين المتغيرات وتحليل البيانات بشكل أكثر فعالية ودقة، مما يساهم في تقديم توصيات مبنية على أسس علمية قوية لتحسين سياسات وإجراءات الأمن السيبراني في القطاع المصرفي.

التعريفات الإجرائية لمتغيرات البحث

1. إدارة مخاطر الأمن السيبراني:

- التعريف الإجرائي: مجموعة من السياسات والإجراءات والتقنيات التي تعتمد عليها البنوك لتحديد وتقييم وتقليل المخاطر السيبرانية التي يمكن أن تهدد أمن المعلومات والأنظمة الإلكترونية .

- القياس: يمكن قياس إدارة مخاطر الأمن السيبراني من خلال الاستبيانات التي تتناول الإجراءات الأمنية المطبقة، نسبة الحوادث السيبرانية المبلغ عنها، ومدى فعالية استجابة البنك لتلك الحوادث.

2. الاستقرار المالي:

- التعريف الإجرائي: الحالة التي تتمكن فيها البنوك من تقديم خدماتها المالية بشكل مستمر وآمن دون التعرض لخسائر مالية كبيرة نتيجة للهجمات السيبرانية.

- القياس: يمكن قياس الاستقرار المالي من خلال مؤشرات الأداء المالي للبنك، مثل نسبة الربحية، نسبة القروض المتعثرة، ومستويات الاحتياطيات النقدية.

3. الشمول المالي:

- التعريف الإجرائي: القدرة على الوصول إلى واستخدام الخدمات المالية من قبل جميع شرائح المجتمع، بما في ذلك الأفراد ذوي الدخل المنخفض والمناطق النائية، دون مواجهة حواجز تكنولوجية أو أمنية.

- القياس: يمكن قياس الشمول المالي من خلال نسبة الأفراد الذين لديهم حسابات مصرفية، استخدام الخدمات المصرفية عبر الإنترنت، ومدى انتشار الفروع وأجهزة الصراف الآلي في المناطق الريفية.

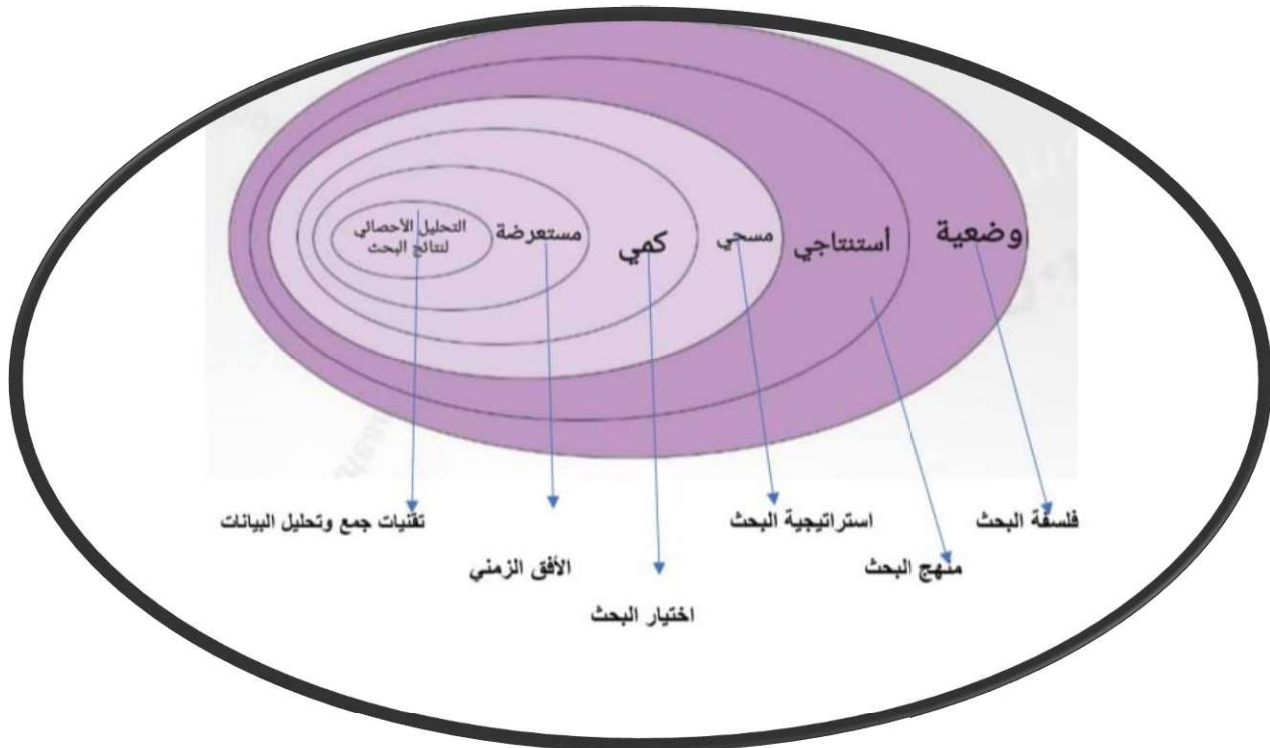
4. الهجمات السيبرانية:

- التعريف الإجرائي: أي محاولة غير مشروعة للوصول إلى نظم المعلومات أو البيانات الخاصة بالبنوك بهدف التلاعب بها أو سرقتها أو تعطيلها.
- القياس: يمكن قياس الهجمات السيبرانية من خلال عدد الحوادث السيبرانية المسجلة، أنواع الهجمات، والأضرار الناجمة عن تلك الهجمات.

5. الإجراءات الأمنية:

- التعريف الإجرائي: التدابير والتقنيات التي تعتمد عليها البنوك لحماية نظمها وبياناتها من التهديدات السيبرانية.
- القياس: يمكن قياس الإجراءات الأمنية من خلال مدى اعتماد البنوك على تقنيات التشفير، جدران الحماية، برامج مكافحة الفيروسات، وتدريب الموظفين على الوعي الأمني.

تصميم البحث



مجتمع البحث وطرق تقنيات اخذ العينة

مجتمع البحث

يتألف مجتمع البحث من جميع الموظفين العاملين في البنوك التجارية في المملكة العربية السعودية. تشمل هذه البنوك مجموعة متنوعة من المؤسسات المالية التي تقدم خدمات مصرفية مختلفة، مثل الحسابات الجارية والتوفير، القروض، والخدمات الاستثمارية. يتم توزيع موظفي البنوك على عدة أقسام مثل العمليات المصرفية، التكنولوجيا المالية، الموارد البشرية، المالية، التسويق، والإدارة. يبلغ عدد الموظفين في البنوك التجارية في المملكة العربية السعودية ما يقارب 50,000 موظف، مما يوفر بيئة غنية لدراسة أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي.

عدد الموظفين	مجتمع البحث
50,000	البنوك التجارية في السعودية

عينة البحث

تمثل عينة البحث مجموعة من الموظفين الذين سيتم اختيارهم من بين موظفي البنوك التجارية في المملكة العربية السعودية. سيتم اختيار 50 موظف للمشاركة في الاستبيان، مع مراعاة التنوع في الأقسام والوظائف لضمان تمثيل شامل لمجتمع البحث. ستشمل العينة موظفين من مختلف المستويات الإدارية، بدءًا من العاملين في خدمات العملاء وحتى الإداريين والقيادات التنفيذية.

حجم العينة	عينة البحث المستهدفة
50	موظفو البنوك التجارية

طرق وتقنيات أخذ العينة

لضمان تمثيل دقيق لمجتمع البحث، سيتم استخدام طريقة العينة الطبقية العشوائية (Stratified Random Sampling). تتضمن هذه الطريقة تقسيم مجتمع البحث إلى طبقات (أقسام) بناءً على الأقسام والوظائف المختلفة. من ثم، سيتم اختيار عينة عشوائية من كل طبقة لضمان تمثيل متوازن لجميع الفئات المختلفة داخل المجتمع.

1. تحديد الطبقات :سيتم تقسيم الموظفين إلى مجموعات بناءً على أقسامهم

ووظائفهم (مثل العمليات المصرفية، التكنولوجيا المالية، الموارد البشرية، المالية، التسويق، والإدارة).

2. اختيار العينة العشوائية :سيتم اختيار عينة عشوائية من كل طبقة بناءً على

حجمها النسبي داخل مجتمع البحث. يضمن هذا النهج تمثيل جميع الأقسام بشكل مناسب.

3. جمع البيانات :سيتم استخدام استبيانات مهيكلية لجمع البيانات من الموظفين

المختارين. ستغطي الاستبيانات مواضيع متعلقة بالأمن السيبراني، والاستقرار المالي، والشمول المالي، بالإضافة إلى خصائص ديموغرافية للمشاركين.

طريقة أخذ العينات	التقنية المستخدمة
احتمالية	العينة العشوائية البسيطة

استبيان البحث كأداة لاستكمال الدراسة

يعتبر الاستبيان من الأدوات البحثية الأساسية التي تُستخدم لجمع البيانات من مجتمع البحث. يتيح الاستبيان للباحثين الحصول على معلومات مباشرة من المشاركين حول موضوع الدراسة بشكل منهجي ومنظم. في هذه الدراسة، سيتم استخدام استبيان مهيكل

لجمع البيانات حول تأثير إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك التجارية بالمملكة العربية السعودية.

أهداف الاستبيان

1. تقييم مستوى إدارة مخاطر الأمن السيبراني :تحديد مدى اعتماد البنوك على

سياسات وإجراءات وتكنولوجيا الأمن السيبراني.

2. قياس مستوى الاستقرار المالي :تقييم مدى تأثير الهجمات السيبرانية على

الاستقرار المالي للبنوك.

3. تحديد مستوى الشمول المالي :معرفة مدى تأثير الأمن السيبراني على استخدام

الخدمات المالية من قبل مختلف شرائح المجتمع.

تصميم الاستبيان

يتألف الاستبيان من أربعة أقسام رئيسية:

1. المعلومات الديموغرافية:

- العمر
- الجنس
- القسم/الوحدة
- المسمى الوظيفي
- سنوات الخبرة

المحور الأول: أهمية إدارة مخاطر الأمن السيبراني في البنوك التجارية

المحور الثاني: تأثير إدارة مخاطر الأمن السيبراني على استقرار النظام المالي

المحور 3: تحديات وفرص إدارة مخاطر الأمن السيبراني في البنوك

المحور الرابع: استراتيجيات تحسين إدارة مخاطر الأمن السيبراني في البنوك التجارية

طريقة جمع البيانات

سيتم جمع البيانات باستخدام الاستبيان كأداة رئيسية. سيتم توزيع الاستبيان على عينة البحث المستهدفة (100 موظف من البنوك التجارية في المملكة العربية السعودية) عبر البريد الإلكتروني أو من خلال توزيع نسخ ورقية داخل البنوك. سيُطلب من المشاركين ملء الاستبيان وإعادته في مدة زمنية محددة. لضمان جمع بيانات موثوقة، سيتم توفير تعليمات واضحة حول كيفية ملء الاستبيان وضمان سرية المعلومات المقدمة.

جدول المتغيرات المستقلة

البيانات	عدد	المتغير
4		مستوى إدارة مخاطر الأمن السيبراني
4		رضا الموظفين عن السياسات الأمنية
4		فعالية التدابير الأمنية المتبعة

جدول المتغير التابع (الاستقرار المالي والشمول المالي)

البيانات	عدد	المتغير
10		الاستقرار المالي
10		الشمول المالي

أنواع البيانات

في هذه الدراسة، سيتم استخدام الاستبيان كأداة رئيسية لجمع البيانات، وسيتم تحليل هذه البيانات باستخدام برنامج التحليل الإحصائي SPSS. تتدرج أنواع البيانات المستخدمة في الاستبيان إلى بيانات نوعية وبيانات كمية، مما يسهم في تقديم فهم شامل لتأثير إدارة مخاطر الأمن السيبراني على الاستقرار والشمول المالي في البنوك التجارية.

البيانات النوعية (Qualitative Data)

البيانات النوعية هي البيانات التي تعبر عن الأوصاف والخصائص ولا يمكن قياسها بعددٍ مباشر. في هذه الدراسة، تشمل البيانات النوعية:

1. الآراء والمواقف: تتعلق بآراء الموظفين حول سياسات الأمن السيبراني ومدى فعاليتها.

2. التجارب الشخصية: تجارب الموظفين مع الحوادث السيبرانية وكيفية تأثير هذه الحوادث على الثقة في النظام المصرفي.

البيانات الكمية (Quantitative Data)

البيانات الكمية هي البيانات التي يمكن قياسها بعددياً وتحليلها إحصائياً. سيتم جمع هذه البيانات عبر استبيان مهيكّل وتحليلها باستخدام برنامج SPSS. تشمل البيانات الكمية:

طرق وإجراءات تحليل البيانات

لتحقيق فهم شامل لتأثير إدارة مخاطر الأمن السيبراني على الاستقرار والشمول المالي في البنوك التجارية، سيتم استخدام عدة طرق وإجراءات لتحليل البيانات التي تم جمعها عبر الاستبيان. سوف يتم تنفيذ التحليل باستخدام برنامج التحليل الإحصائي SPSS لضمان الدقة والموثوقية في النتائج.

إعداد البيانات

جمع البيانات:

- جمع الاستبيانات المعبأة من المشاركين وتخزينها بشكل آمن.
- إدخال البيانات في برنامج SPSS ، والتأكد من دقة الإدخال وتصحيح أي أخطاء.

تحضير البيانات:

- ترميز الأسئلة النوعية والكمية في الاستبيان.
- تنظيف البيانات من القيم الشاذة أو المفقودة لضمان صحة التحليل.

التحليل الوصفي (Descriptive Analysis)

الإحصاءات الوصفية:

- استخدام الأوامر الوصفية في SPSS لحساب المتوسطات، الانحرافات المعيارية، والنسب المئوية.
- عرض التوزيعات التكرارية لمتغيرات مثل العمر، الجنس، القسم الوظيفي، سنوات الخبرة، وما إلى ذلك.

الخاتمة

في هذه الدراسة، تم استكشاف تأثير إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك التجارية بالمملكة العربية السعودية. تم جمع البيانات باستخدام استبيان مهيكل وتم تحليلها باستخدام برنامج التحليل الإحصائي SPSS للوصول إلى نتائج موثوقة وشاملة. من خلال تحليل البيانات الكمية والنوعية، تم تسليط الضوء على أهمية الأمن السيبراني كعامل حاسم في تعزيز استقرار النظام المالي وزيادة شمولية الخدمات المالية.

النتائج المحتملة

1. تحسين الاستقرار المالي للبنوك:

- قد تُظهر النتائج أن البنوك التي تعتمد سياسات وإجراءات فعالة لإدارة مخاطر الأمن السيبراني تتمتع بمستوى أعلى من الاستقرار المالي. يمكن أن تكون الهجمات السيبرانية أقل تأثيراً على العمليات اليومية والأداء المالي لهذه البنوك، مما يقلل من الخسائر المالية ويعزز الثقة بين العملاء والمستثمرين.

2. زيادة الشمول المالي:

- من المحتمل أن تشير النتائج إلى أن تحسين الأمن السيبراني يزيد من الشمول المالي من خلال تشجيع المزيد من العملاء على استخدام الخدمات المصرفية عبر الإنترنت. يمكن أن تعزز التدابير الأمنية الفعالة ثقة العملاء في استخدام الخدمات الرقمية، مما يزيد من معدل استخدام هذه الخدمات بين مختلف الفئات السكانية.

3. رضا الموظفين عن السياسات الأمنية:

- قد تُظهر النتائج أن رضا الموظفين عن سياسات وإجراءات الأمن السيبراني يلعب دوراً كبيراً في تحقيق الأهداف الأمنية للبنك. يمكن أن يؤدي رضا الموظفين إلى تحسين التزامهم بالإجراءات الأمنية وتعزيز قدرتهم على التصدي للهجمات السيبرانية بفعالية.

4. توصيات لتحسين إدارة مخاطر الأمن السيبراني:

- استنادًا إلى التحليل، قد يتم تقديم توصيات للبنوك لتحسين سياساتها وإجراءاتها في إدارة مخاطر الأمن السيبراني. يمكن أن تشمل هذه التوصيات تعزيز التدريب والتوعية للموظفين، تبني تقنيات أمان متقدمة، وتطوير خطط استجابة شاملة للهجمات السيبرانية.

5. العلاقة بين الأمن السيبراني والأداء المالي:

- قد تكشف النتائج عن وجود علاقة إيجابية بين مستوى إدارة مخاطر الأمن السيبراني والأداء المالي للبنوك. يمكن أن تكون البنوك التي تستثمر في تحسين أمنها السيبراني أكثر قدرة على الحفاظ على استقرارها المالي وزيادة أرباحها على المدى الطويل.

الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

مقدمة

في هذا الفصل، سنقوم بعرض النتائج التي تم الحصول عليها من خلال تحليل البيانات التي تم جمعها باستخدام الاستبيان، يهدف هذا الفصل إلى تقديم تحليل إحصائي شامل للبيانات من أجل اختبار الفرضيات المطروحة في الدراسة وتفسير النتائج المستخلصة. سنبدأ بعرض البيانات الديموغرافية للعينة المدروسة، ثم ننتقل إلى تحليل الفرضيات باستخدام الأساليب الإحصائية المناسبة.

يعد التحليل الإحصائي خطوة حاسمة لفهم العلاقات بين المتغيرات المختلفة في الدراسة، مثل تأثير الحوافز والتدريب على إنتاجية الموظفين في بنك البحرين الوطني. من خلال استخدام تقنيات تحليل البيانات المختلفة، سنتمكن من تقييم مدى قوة وتأثير هذه العوامل على أداء الموظفين واستقرار النظام المالي.

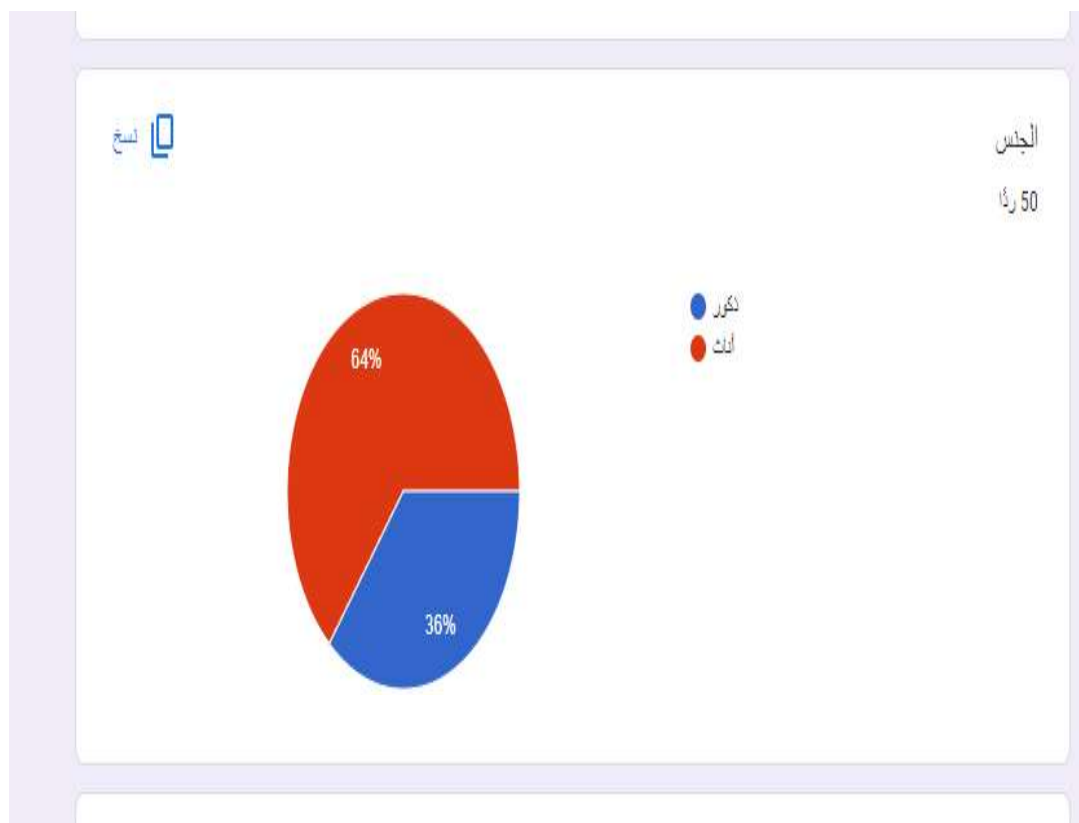
سوف يتناول هذا الفصل أيضاً مناقشة النتائج التي تم الحصول عليها من التحليل الإحصائي، مع مقارنتها بالدراسات السابقة وتقديم تفسير معمق لهذه النتائج. الهدف من ذلك هو تقديم فهم أعمق للظواهر المدروسة واقتراح توصيات عملية لتحسين أداء الموظفين وإدارة المخاطر في البنوك التجارية.

توصيف عينة الدراسة (الإحصاءات الوصفية لعينة الدراسة)

أولاً: البيانات الأولية

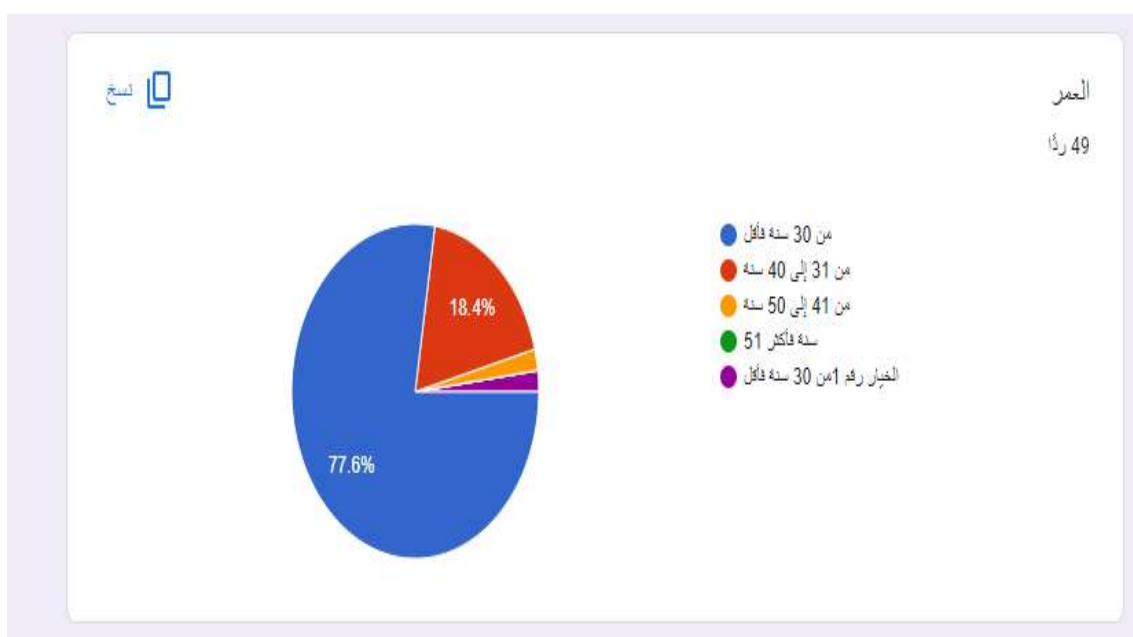
• الجنس

يوضح توزيع عينة الدراسة وفقاً لمتغير الجنس، فبلغت نسبة الذكور 36%، بينما بلغت نسبة الإناث 64%.



• العمر

يوضح توزيع عينة الدراسة وفقاً لمتغير العمر فبلغت نسبة من 30 سنة إلى أقل من 40 سنة 77.6%، بينما بلغت نسبة من هم من 31 سنة إلى 40 سنة 18.4%، كما بلغت نسبة من هم من 41 سنة إلى 50 سنة 2%، 51 سنة فأكثر 2%.

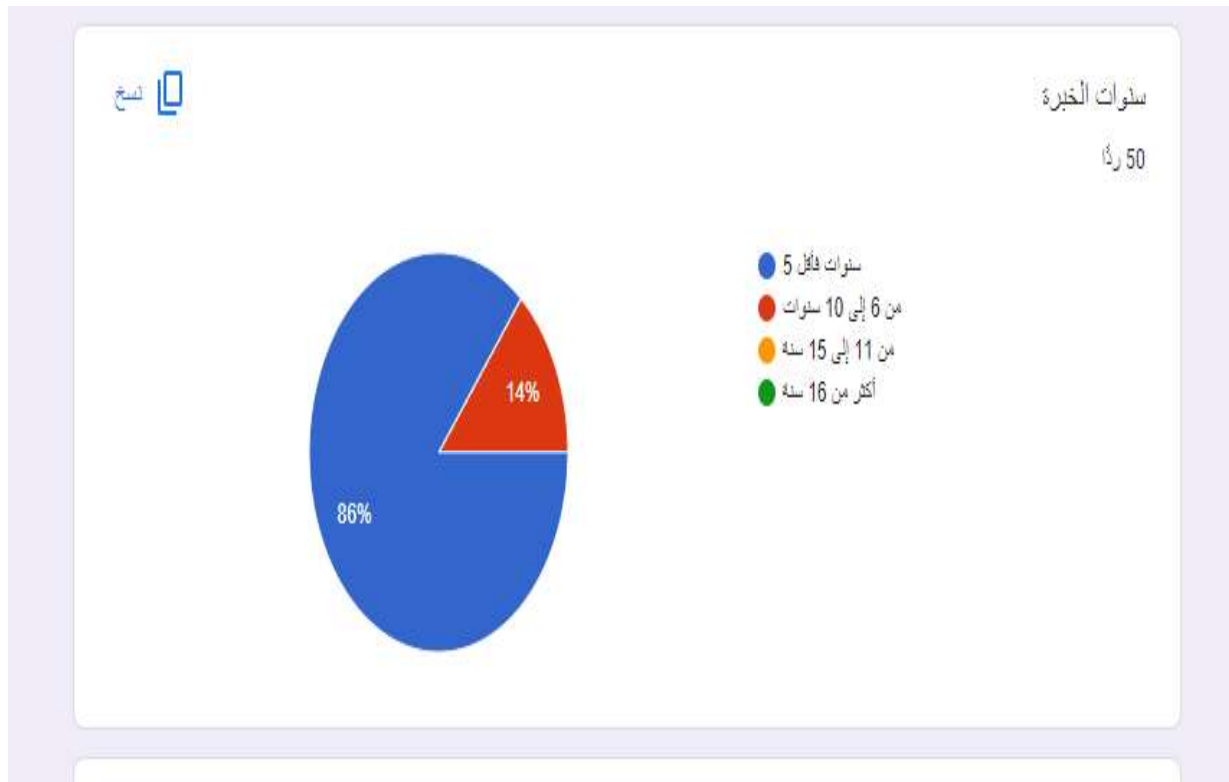


• المؤهل العلمي

يوضح توزيع عينة الدراسة وفقاً لمتغير المؤهل العلمي فبلغت نسبة الحاصلين على الدبلوم الجامعي 22.4%، بينما بلغت نسبة الحاصلين على البكالوريوس 53.1%، بينما بلغت نسبة الماجستير 20.4%، كما بلغت نسبة دكتوراه 5%.

• سنوات الخبرة

يوضح توزيع عينة الدراسة وفقاً لمتغير المؤهل العلمي فبلغت 5 سنوات فأقل 286%، بينما بلغت نسبة من 6 سنوات إلى 10 سنوات 14%.



اختبار الصدق والثبات

جدول رقم (1) أوزان العبارات حسب مقياس ليكرت الخماسي

العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الوزن	5	4	3	2	1

صدق أداة الدراسة

تم استخدام معامل ألفا كرونباخ للاستبانة ومحاورها لقياس ثبات وصدق أداة الدراسة والجدول رقم (2) يوضح

نتائج الثبات والصدق:

جدول نتائج الثبات والصدق

المحور	عدد العبارات	معامل ألفا كرونباخ
أهمية إدارة مخاطر الأمن السيبراني في البنوك التجارية	4 عبارات	0.929
تأثير إدارة مخاطر الأمن السيبراني على استقرار النظام المالي	4 عبارات	0.923

0.958	4 عبارات	تحديات وفرص إدارة مخاطر الأمن السيبراني في البنوك
0.972	4 عبارات	استراتيجيات تحسين إدارة مخاطر الأمن السيبراني في البنوك التجارية
0.985	16 عبارة	معامل ألفا الكلي

تشير نتائج معامل ألفا كرونباخ إلى أن أداة الدراسة تتمتع بمستوى عالي من الصدق والثبات، حيث بلغ معامل ألفا كرونباخ لجميع محاور الاستبيان قيمة عالية أكبر من 70%، كما بلغ معامل ألفا الكلي 98.5%.

المعالجة الإحصائية

ستتم المعالجة الإحصائية لبيانات الدراسة من خلال برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) وذلك من خلال الأساليب الإحصائية التالية:

- التكرارات والنسب المئوية والمتوسطات والانحرافات المعيارية للإجابة على محاور الدراسة ووصف مجتمع الدراسة.
- استخدام معامل ألفا كرونباخ للاستبانة ومحاورها لقياس ثبات وصدق أداة الدراسة.
- تحليل الانحدار البسيط لتحديد أثر المتغير المستقل على المتغير التابع.

الإحصاء الوصفي لمتغيرات البحث

ثانياً: الأسئلة الموضوعية

جدول المتوسطات الحسابية والانحرافات المعيارية لمحور أهمية إدارة مخاطر الأمن السيبراني في البنوك

التجارية

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب
إدارة الأمن السيبراني تعزز ثقة العملاء وتحافظ على سمعة البنك.	3.06	1.22119	1
سياسات الأمن السيبراني تحمي البيانات الحساسة من الوصول غير المصرح به.	2.85	1.22578	2
الاستثمار في الأمن السيبراني يقلل من تكاليف الخسائر الناتجة عن الهجمات السيبرانية.	2.66	1.04659	3
الأمن السيبراني يعزز استمرارية العمليات والخدمات المصرفية عبر الإنترنت.	2.52	1.15889	4
أهمية إدارة مخاطر الأمن السيبراني في البنوك التجارية	2.7725	1.05774	

الجدول السابق يوضح المتوسطات الحسابية والانحرافات المعيارية لمحور أهمية إدارة مخاطر الأمن السيبراني في البنوك التجارية والتي بلغ المتوسط الحسابي له 2.7725 بانحراف معياري 1.05774 وهو ما يشير إلى درجة المحايد على عبارات المحور، جاءت عبارة " إدارة الأمن السيبراني تعزز ثقة العملاء وتحافظ على سمعة البنك." في المركز الأول بمتوسط 3.06، بينما جاءت عبارة " سياسات الأمن السيبراني تحمي البيانات الحساسة من الوصول غير المصرح به. في المركز الثاني بمتوسط 2.85، كما جاءت عبارة " الاستثمار في الأمن السيبراني يقلل من تكاليف الخسائر الناتجة عن الهجمات السيبرانية." في المركز الثالث بمتوسط حسابي 2.66، بينما في المركز الأخير جاءت. " الأمن السيبراني يعزز استمرارية العمليات والخدمات المصرفية عبر الإنترنت. بمتوسط حسابي 2.52.

جدول المتوسطات الحسابية والانحرافات المعيارية لمحور المحور الثاني: تأثير إدارة مخاطر الأمن السيبراني

على استقرار النظام المالي

الترتيب	الانحراف المعياري	المتوسط الحسابي	العبرة
2	0.80723	2.93	تحسين الأمن السيبراني يسهم في تقليل التعطيلات المالية الناتجة عن هجمات البرمجيات الخبيثة.
4	1.0721	2.61	الأمان السيبراني يعزز الثقة في النظام المالي ويحد من التقلبات غير المرغوب فيها.
3	1.19409	2.78	سياسات الأمن السيبراني تسهم في تحسين قدرة البنوك على التصدي للتهديدات السيبرانية الجديدة.
1	1.34431	3.03	استراتيجيات الأمن السيبراني تدعم استقرار البنوك وتعزز دورها في النظام المالي العالمي.
	1.01153	2.8375	تأثير إدارة مخاطر الأمن السيبراني على استقرار النظام المالي

الجدول السابق يوضح المتوسطات الحسابية والانحرافات المعيارية لمحور تأثير إدارة مخاطر الأمن

السيبراني على استقرار النظام المالي

والتي بلغ المتوسط الحسابي له 2.8375 بانحراف معياري 1.01153 وهو ما يشير إلى درجة المحايد على

عبارات المحور، جاءت عبارة "تحسين الأمن السيبراني يسهم في تقليل التعطيلات المالية الناتجة عن

هجمات البرمجيات الخبيثة. في المركز الأول بمتوسط 3.03، بينما جاءت عبارة الأمان السيبراني يعزز

الثقة في النظام المالي ويحد من التقلبات غير المرغوب فيها. في المركز الثاني بمتوسط 2.93، كما

جاءت عبارة في المركز الثالث "سياسات الأمن السيبراني تسهم في تحسين قدرة البنوك على التصدي

للتحديات السيبرانية الجديدة." بمتوسط حسابي 2.78، بينما في المركز الأخير جاءت عبارة "استراتيجيات

الأمن السيبراني تدعم استقرار البنوك وتعزز دورها في النظام المالي العالمي." بمتوسط حسابي 2.61.

- جدول المتوسطات الحسابية والانحرافات المعيارية لمحور المحور الثالث: تحديات وفرص إدارة مخاطر

الأمن السيبراني في البنوك

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب
تعقيد الهجمات السيبرانية يتطلب استجابات سريعة وفعالة من قبل البنوك.	2.46	1.64175	4
التوعية والتدريب المستمر يعززان الوعي الأمني لدى الموظفين ويقللان من خطر الهجمات السيبرانية.	2.62	1.2373	3
استخدام التكنولوجيا المتقدمة يفتح آفاقاً جديدة لتحسين إستراتيجيات الأمن السيبراني في البنوك.	2.82	1.23403	2
التعاون الدولي يمثل فرصة لتعزيز القدرة على مكافحة التهديدات السيبرانية عبر الحدود.	3	1.6268	1
تحديات وفرص إدارة مخاطر الأمن السيبراني في البنوك	2.725	1.36584	

الجدول السابق يوضح المتوسطات الحسابية والانحرافات المعيارية لمحور تحديات وفرص إدارة مخاطر الأمن

السيبراني في البنوك

والتي بلغ المتوسط الحسابي له 2.725 بانحراف معياري 1.36584 وهو ما يشير إلى درجة المحايد على عبارات المحور، جاءت عبارة " تعقيد الهجمات السيبرانية يتطلب استجابات سريعة وفعالة من قبل البنوك" في المركز الأول بمتوسط 3، بينما جاءت عبارة ". التوعية والتدريب المستمر يعززان الوعي الأمني لدى الموظفين ويقللان من خطر الهجمات السيبرانية.." في المركز الثاني بمتوسط 2.82، كما جاءت عبارة استخدام التكنولوجيا المتقدمة يفتح أفقاً جديدة لتحسين إستراتيجيات الأمن السيبراني في البنوك. في المركز الثالث بمتوسط حسابي 2.62، بينما في المركز الأخير جاءت عبارة. " التعاون الدولي يمثل فرصة لتعزيز القدرة على مكافحة التهديدات السيبرانية عبر الحدود. بمتوسط حسابي 2.46.

- جدول المتوسطات الحسابية والانحرافات المعيارية لمحور استراتيجيات تحسين إدارة مخاطر الأمن

السيبراني في البنوك التجارية

الترتيب	الانحراف المعياري	المتوسط الحسابي	العبرة
2	1.1638 9	2.83	يجب على البنوك التجارية الاستثمار في تقنيات متقدمة لتعزيز أنظمة الأمن السيبراني .
4	1.0657 2	2.34	يمكن للبنوك التجارية تحسين إدارة مخاطر الأمن السيبراني من خلال تدريب الموظفين على أفضل الممارسات.
1	1.2827 9	2.97	تساهم السياسات والإجراءات الفعالة في تقليل مخاطر الأمن السيبراني في البنوك التجارية.
3	1.2674 6	2.64	يعد التعاون مع الهيئات الحكومية والمؤسسات المالية الأخرى استراتيجية فعالة لتعزيز إدارة مخاطر الأمن السيبراني.
	1.1511 9	2.695	لمحور استراتيجيات تحسين إدارة مخاطر الأمن السيبراني في البنوك التجارية

الجدول السابق يوضح المتوسطات الحسابية والانحرافات المعيارية لمحور استراتيجيات تحسين إدارة مخاطر الأمن السيبراني في البنوك التجارية والتي بلغ المتوسط الحسابي له 2.695 بانحراف معياري 1.15119 وهو ما يشير إلى درجة المحايد على عبارات المحور، جاءت عبارة يجب على البنوك التجارية الاستثمار في تقنيات متقدمة لتعزيز أنظمة الأمن السيبراني.

في المركز الأول بمتوسط 2.97، بينما جاءت عبارة: "يمكن للبنوك التجارية تحسين إدارة مخاطر الأمن السيبراني من خلال تدريب الموظفين على أفضل الممارسات.

في المركز الثاني بمتوسط 2.83، كما جاءت تساهم السياسات والإجراءات الفعالة في تقليل مخاطر الأمن السيبراني في البنوك التجارية. في المركز الثالث بمتوسط حسابي 2.64، بينما في المركز الأخير جاءت عبارة: "يعد التعاون مع الهيئات الحكومية والمؤسسات المالية الأخرى استراتيجية فعالة لتعزيز إدارة مخاطر الأمن السيبراني. بمتوسط حسابي 2.34.

ثالثاً: اختبار الفرضيات

الفرضية الأولى: يوجد أثر ذو دلالة إحصائية بين إدارة مخاطر الامن السيبراني ودعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين

ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	104.448	1	104.448	1621.217	.000 ^b
Residual	6.314	98	.064		
Total	110.762	99			

يوضح الجدول السابق نتائج تحليل ANOVA لاختبار معنوية الانحدار. نلاحظ أن قيمة Sig هي (0.000) وهي أقل من (0.05)، مما يعني قبول الفرضية. بناءً على هذه النتائج، يمكن القول بوجود تأثير دال إحصائيًا بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين.

الفرضية الثانية: يوجد أثر ذو دلالة إحصائية بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين

ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	100.504	1	100.504	208.960	.000 ^b
Residual	47.136	98	.481		
Total	147.640	99			

يوضح الجدول السابق نتائج تحليل ANOVA لاختبار معنوية الانحدار. نلاحظ أن قيمة Sig هي (0.000) وهي أقل من (0.05)، مما يعني قبول الفرضية. بناءً على هذه النتائج، يمكن القول بوجود تأثير دال إحصائيًا بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين.

خلاصة اختبار الفرضيات

نتائج اختبار الفرضيات أكدت أن إدارة مخاطر الأمن السيبراني لها تأثير إيجابي ودال إحصائيًا على كل من دعم الاستقرار والشمول المالي وتعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين. تشير هذه النتائج إلى أهمية تنفيذ استراتيجيات فعالة لإدارة مخاطر الأمن السيبراني لتعزيز استقرار النظام المالي وزيادة شمولية الخدمات المالية المقدمة. من الضروري أن تواصل البنوك تحسين وتطوير هذه الاستراتيجيات لمواجهة التحديات السيبرانية المستمرة وضمان تقديم خدمات مالية مستقرة وشاملة.

الفصل الخامس

الخاتمة

النتائج

التوصيات

خاتمة

تشير النتائج التي توصلت إليها هذه الدراسة إلى أهمية إدارة مخاطر الأمن السيبراني في دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين. فقد أظهرت الفرضيات المدروسة وجود تأثير ذو دلالة إحصائية بين إدارة مخاطر الأمن السيبراني وكلا من دعم الاستقرار المالي وتعزيز الشمول المالي. إن تحقيق الأمان السيبراني يعدّ أحد العوامل الأساسية التي تساهم في حماية الأنظمة المالية والمصرفية من التهديدات المتزايدة، مما يعزز الثقة لدى العملاء ويساهم في استقرار النظام المالي. كما أن تعزيز الشمول المالي من خلال إدارة فعالة لمخاطر الأمن السيبراني يتيح للبنوك تقديم خدمات مالية لمجموعة أوسع من العملاء بطرق آمنة وفعّالة.

من خلال هذه الدراسة، يتضح أن البنوك المدرجة في بورصة فلسطين يجب أن تواصل تطوير وتحسين استراتيجياتها لإدارة مخاطر الأمن السيبراني لضمان تقديم خدمات مالية مستقرة وأمنة. كما ينبغي على هذه المؤسسات تعزيز ثقافة الوعي الأمني بين موظفيها والعملاء لمواجهة التحديات السيبرانية المتزايدة.

في الختام، تسلط هذه الدراسة الضوء على الدور الحاسم لإدارة مخاطر الأمن السيبراني في تحقيق الاستقرار المالي وتعزيز الشمول المالي، مما يستوجب على البنوك الاستثمار في تطوير بنية تحتية أمنية قوية واستراتيجيات فعالة لمواجهة التحديات المستقبلية.

النتائج

في ختام هذه الدراسة، نجد أن إدارة مخاطر الأمن السيبراني تعد عنصراً حيوياً لضمان استقرار وشمول المؤسسات المالية، خاصة البنوك التي تتعرض لتحديات متزايدة من التهديدات السيبرانية المتطورة. من خلال تحليل تأثير إدارة هذه المخاطر، وجدنا أن البنوك التي تستثمر في تعزيز نظمها الأمنية وتنفيذ سياسات فعالة تحقق مستويات أعلى من الاستقرار المالي وتعزز من مشاركة المجتمع في الخدمات المالية.

تشير النتائج إلى أن التفاعل الإيجابي بين الأمن السيبراني والاستقرار المالي يمكن أن يساهم في تعزيز الثقة بين العملاء والمستثمرين، مما يساهم في نمو الاقتصاد والتنمية المستدامة. بالتالي، يُنصح بأن تكون استراتيجيات إدارة مخاطر الأمن السيبراني متكاملة ومستدامة، مع التركيز على التكنولوجيا الحديثة والتدريب المستمر للموظفين، لضمان حماية البيانات والمعلومات الحساسة بشكل فعال.

يمكن أن تلعب البنوك دوراً حاسماً في تعزيز الاستقرار المالي والشمول من خلال اعتماد استراتيجيات قوية لإدارة مخاطر الأمن السيبراني، مما يساهم في تحقيق أهداف التنمية المستدامة على المدى البعيد.

التوصيات

- **تعزيز الاستثمار في التكنولوجيا السيبرانية المتقدمة:** ينبغي على البنوك تعزيز الاستثمار في أنظمة الأمان والتكنولوجيا السيبرانية المتقدمة، مثل أنظمة الكشف عن التهديدات المتقدمة والحلول الذكية للحماية من الاختراقات.
- **تعزيز التدريب والتوعية للموظفين:** يجب على البنوك تكثيف التدريبات والبرامج التوعوية للموظفين بشأن مخاطر الأمن السيبراني وأهمية دورهم في الحفاظ على الأمن الرقمي للمؤسسة.
- **تعزيز التعاون مع الجهات المعنية:** يُنصح بتعزيز التعاون مع الجهات الحكومية والأكاديمية والقطاع الخاص لمشاركة المعرفة والخبرات في مجال إدارة مخاطر الأمن السيبراني، وتطوير السياسات والإجراءات بما يتناسب مع التطورات الجديدة.
- **تحسين استجابة الأزمات وخطط الطوارئ:** يجب على البنوك تطوير وتنفيذ خطط متقدمة للاستجابة للأزمات السيبرانية، بما في ذلك تقييم الضرر وإعادة التأهيل، للحد من التأثيرات السلبية على استقرار النظام المالي.
- **التحفيز على الابتكار والتطوير التكنولوجي:** يمكن للبنوك تعزيز الابتكار في مجالات الأمن السيبراني من خلال دعم البحث والتطوير، والاستثمار في حلول تكنولوجية جديدة تعزز من قدرتها على التصدي للتهديدات السيبرانية المتزايدة.

المراجع

علي، هيام عيد عطية محمد، دياب، محمد عبد القادر، وعباس، حنان جابر حسن. (2023). أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني: دراسة ميدانية *الفكر المحاسبي*، مج27، ع4، 71 - 120. مسترجع من <http://search.mandumah.com.qulib.idm.oclc.org/Record/1435091>

شحمات، مراد، و جصاص، لبنى. (2023). الأمن السيبراني للدول بعد افتراضي لواقع مادي *مجلة الناقد للدراسات السياسية*، مج7، ع2، 99 - 114. مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1453774>

أبو حسين، حنين جميل، والحنيطي، مأمون أحمد راشد. (2021). *الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة* (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمان. مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1208936>

على، محمود أحمد، وعلي، صالح علي صالح. (2022). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية *مجلة الإسكندرية للبحوث المحاسبية*، مج6، ع3، 1 - 48. مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1336570>

أميرهم، جيهان عادل ناجي. (2022). أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين: دراسة ميدانية *مجلة البحوث المالية والتجارية*، ع3، 325 - 377. مسترجع من <http://search.mandumah.com.qulib.idm.oclc.org/Record/1334460>

عبد القادر، صواق، بومدين، بوداود، وأولاد حيمودة، عبد اللطيف. (2023). أثر جاهزية الأمن السيبراني

على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة: دراسة حالة بنك BDL

بغرداية. *أبحاث اقتصادية معاصرة*، مج6، ع1، 353. 372 - مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1386536>

الرشيدي، طارق عبد العظيم يوسف، وناصر، داليا عادل عباس السيد. (2019). أثر الإفصاح عن مخاطر

الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول: دراسة مقارنة في قطاع تكنولوجيا

المعلومات. *مجلة المحاسبة والمراجعة*، ع2، 439. 487 - مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1122133>

أحمد، خالد محمد عثمان. (2023). أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات

إدارة مخاطر الأمن السيبراني على الأداء المالي: دراسة تطبيقية. *مجلة البحوث المحاسبية*، ع4، 1107 -

183. مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1452769>

التوني، شريهان مصطفى محمد. (2023). أثر وعي العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن

السيبراني: دراسة ميدانية على البنوك الحكومية بمحافظة بورسعيد. *مجلة التجارة والتمويل*، ع4، 609 -

653. مسترجع من <http://search.mandumah.com.qulib.idm.oclc.org/Record/1442825>

متولي، مصطفى زكي حسين، وغريب، حسين عبدالعال سالم. (2022). قياس تأثير الإفصاح عن مخاطر

الأمن السيبراني على أتعاب المراجعة الخارجية: دراسة تطبيقية. *المجلة العلمية للدراسات المحاسبية*، مج4،

ع4، 245. 328 - مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1377198>

الزبيد، محمود سليمان سعود، والمشاقبة، محمد ناصر موسى حمدان. (2021). *أثر التدقيق الداخلي في الحد من مخاطر السيبرانية في البنوك التجارية الأردنية* (رسالة ماجستير غير منشورة). جامعة آل البيت،

المفرق. مسترجع من <http://search.mandumah.com.qulib.idm.oclc.org/Record/1167447>

فرج، هاني خليل. (2022). *أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن*

الإلكتروني على قرار الاستثمار بالأسهم: دراسة تجريبية. *مجلة المحاسبة والمراجعة*، ع2، 129. 209 -

مسترجع من <http://search.mandumah.com.qulib.idm.oclc.org/Record/1308742>

أبو الخير، محمد حارس محمد طه. (2023). *أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية: دراسة ميدانية*. *المجلة العلمية للدراسات والبحوث المالية والإدارية*، مج15، ع1، 1. 65 - مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1337809>

الحوامدة، أحمد موسى عبد الرحيم، وعبد المنعم، أسامة علي. (2021). *أثر الحوكمة السيبرانية على جودة*

التدقيق الداخلي في البنوك الأردنية (رسالة ماجستير غير منشورة). جامعة جرش، جرش. مسترجع من

<http://search.mandumah.com.qulib.idm.oclc.org/Record/1243800>

6. Inoussa, H. (2021). The FinTech-driven Approach to Financial Inclusion: A cross-sectional study of how Financial Inclusion furthers Sustainable Development in Sub-Saharan Africa.
7. Jayakumar, S. (2020). Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. *Handbook of Terrorism Prevention and Preparedness*, 871-930.
8. Khan, M. A., & Malaika, M. (2021). Central Bank Risk Management, Fintech, and Cybersecurity. *International Monetary Fund*.
9. Kumar, R., & Thomas, B. (2022). BRICS in Global Governance: A Gradual but Steady Expansion. *Governance and Politics*, 1(1), 100-113.
10. Piotrowski, D. (2022). Consumer perceived ethicality of banks in the era of digitalisation: The case of Poland. *Economics and Business Review*, 8(1), 90-114.
11. Pupentsova, S., & Livintsova, M. (2022). The Enterprises Risk Management in the Context of Digital Transformation. In *International Scientific Siberian Transport Forum* (pp. 1159-1167). Springer, Cham.
12. Saon Raya, S. P., & Miglanic, S., (2019), Use of Blockchain and Artificial Intelligence to promote financial inclusion in India. *TECH MONITOR • Jan-Mar 2019*.
13. Tzoneva, A., Momcheva, G., & Stoyanov, B. (2022, May). Vendor Cybersecurity Risk Assessment in an Autonomous Mobility Ecosystem. In *2022 10th International Scientific Conference on Computer Science (COMSCI)*.
14. Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability?. *International Review of Financial Analysis*, 72, 101587.
15. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & security*, 105, 102239.
16. Vučinić, M. (2020). Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, 9(2), 43-66.
17. Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. *Risk Analysis*, 42(8), 1606-1622.
18. Yadav, M., & Shanmugam, S., (2022), Fintech Lending in India: the Changing Paradigm of Banking, *Journal of the Oriental Institute*, ISSN: 0030-5324, UGC Care list no. 135, 71(15), 225-232.

استمارة الاستبيان

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

في هذا الاستبيان الذي يستهدف فهم وجهات نظر المشاركين حول إدارة مخاطر الأمن السيبراني في البنوك. يهدف هذا الاستبيان إلى استكمال دراسة أكاديمية حول كيفية تأثير إدارة الأمن السيبراني على استقرار النظام المالي وثقة العملاء في الخدمات المصرفية.

سياسات الخصوصية والسرية:

جميع الردود ستظل سرية تامة وستستخدم فقط لأغراض البحث الأكاديمي. لن يتم نشر أو مشاركة أي معلومات تتعلق بالمشاركين بطريقة تمييزية.

شكراً مقدماً على وقتكم وجهودكم في مساعدتنا على تحقيق أهداف هذا البحث.

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

في هذا الأسطوان الذي يستهدف فهم وجهات نظر المشاركين حول إدارة مخاطر الأمن السيبراني في البنوك، يهدف هذا الأسطوان إلى استكمال دراسة أكاديمية حول كيفية تأثير إدارة الأمن السيبراني على استقرار النظام المالي وثقة العملاء في الخدمات المصرفية.

سياسات الخصوصية والسرية: جميع الردود ستظل سرية تامة وستستخدم فقط لأغراض البحث الأكاديمي. لن يتم نشر أو مشاركة أي معلومات تتعلق بالمشاركين بطريقة تميزية.

شكراً مقدماً على وقتكم وجهودكم في مساعدتنا على تحقيق أهداف هذا البحث.

البيانات الديموغرافية

الوصف (اختياري)

الجنس

م

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

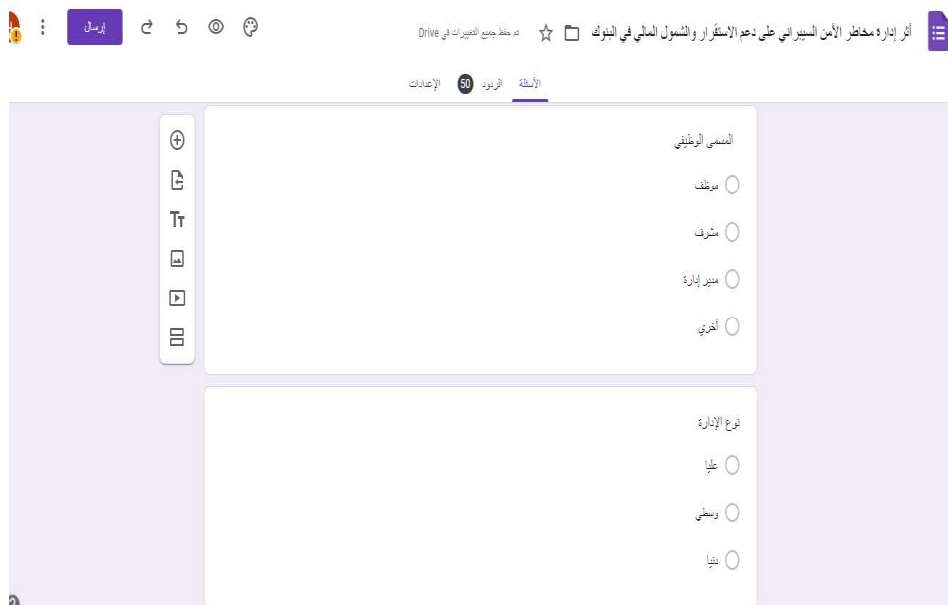
الممر

من 30 سنة فأقل

من 31 إلى 40 سنة

من 41 إلى 50 سنة

51 سنة فأكثر



إرسال

↶ ↷ ⌂ ?

☆

📁

Drive

تم حفظ جميع التغييرات في Drive

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

☰

الإعدادات

50

البريد

الأسئلة

+

📄

🔍

🖼️

▶

☰

نوع الإدارة

عليا ☐

وسطي ☐

دنيا ☐

سنوات الخبرة

5 سنوات فأقل ☐

من 6 إلى 10 سنوات ☐

من 11 إلى 15 سنة ☐

أكثر من 16 سنة ☐

2

إرسال

↶

↷

👁

😊

تم حفظ جميع التغييرات في Drive

☆

📁

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

📄

الإعدادات

الأسئلة

الرموز

50

+

📄

Tt

🖼

▶

☰

المحور الأول: أهمية إدارة مخاطر الأمن السيبراني في البنوك التجارية

(الوصف اختياري)

إدارة الأمن السيبراني تعزز ثقة العملاء وتحافظ على سمعة البنك.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأسئلة 50 الردود الإعدادات

سياسات الأمن السيبراني تحمي البيانات الحساسة من الوصول غير المصرح به.

موافق بشدة ☐

موافق ☐

محايد ☐

غير موافق ☐

غير موافق بشدة ☐

الاستثمار في الأمن السيبراني يقلل من تكاليف الخسائر الناتجة عن الهجمات السيبرانية.

موافق بشدة ☐

موافق ☐

محايد ☐

غير موافق ☐

غير موافق بشدة ☐

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأسئلة الردود الإعدادات

غير موافق بشدة ☐

الاستثمار في الأمن السيبراني يقلل من تكاليف الخسائر الناتجة عن الهجمات السيبرانية.

موافق بشدة ☐

موافق ☐

محايد ☐

غير موافق ☐

غير موافق بشدة ☐

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأشرطة 50 الرموز الإعدادات

الأمن السيبراني يعزز استمرارية العمليات والخدمات المصرفية عبر الإنترنت.

موافق بشدة ☐

موافق ☐

محايد ☐

غير موافق ☐

غير موافق بشدة ☐

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأشرطة 50 الرموز الإعدادات

المحور الثاني: تأثير إدارة مخاطر الأمن السيبراني على استقرار النظام المالي

الوصف (اختياري)

تحسين الأمن السيبراني يساهم في تقليل التعطلات المالية الناتجة عن هجمات البرمجيات الخبيثة.

موافق بشدة ☐

موافق ☐

محايد ☐

غير موافق ☐

غير موافق بشدة ☐

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأسئلة 50 الردود الإعدادات

الأمان السيبراني يعزز الثقة في النظام المالي ويحد من التقلبات غير المرغوب فيها.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

سياسات الأمن السيبراني تسهم في تحسين قدرة البنوك على التصدي للتهديدات السيبرانية الجديدة.

موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأسئلة الردود الإعدادات

سياسات الأمن السيبراني تسهم في تحسين قدرة البنوك على التصدي للتهديدات السيبرانية الجديدة.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

إرسال

تم حفظ جميع التغييرات في Drive

☆

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

الأسئلة

الردود 50 الإعدادات

غير موافق

غير موافق بشدة

استراتيجيات الأمن السيبراني تدعم استقرار البنوك وتميز دورها في النظام المالي العالمي.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

إرسال

تم حفظ جميع التغييرات في Drive

☆

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

الأسئلة

الردود 50 الإعدادات

المحور الثالث: تحديات وفرص إدارة مخاطر الأمن السيبراني في البنوك

الوصف (اختياري)

تعقيد الهجمات السيبرانية يتطلب استجابات سريعة وفعالة من قبل البنوك.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار و الشمول المالي في البنوك

المعبر الثالث: تحديات وفرص إدارة مخاطر الأمن السيبراني في البنوك

الوصف (اختياري)

تعقيد الهجمات السيبرانية يتطلب استجابات سريعة وفعالة من قبل البنوك.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار و الشمول المالي في البنوك

استخدام التكنولوجيا المتقدمة ينتج أفعًا جديدة لتحسين إستراتيجيات الأمن السيبراني في البنوك.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأسئلة الردود 50 الإعدادات

التعاون الدولي يمثل فرصة لتعزيز القدرة على مكافحة التهديدات السيبرانية عبر الحدود.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

الأسئلة الردود 50 الإعدادات

غير موافق بشدة

المحور الرابع: استراتيجيات تحسين إدارة مخاطر الأمن السيبراني في البنوك التجارية
(الوصف اختياري)

يجب على البنوك التجارية الاستثمار في تقنيات متقدمة لتسهيل أنشطة الأمن السيبراني.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك ☆ أم حفظ جميع التغييرات في Drive

الأسئلة 50 الردود الإعدادات

يمكن للبنوك التجارية تحسين إدارة مخاطر الأمن السيبراني من خلال تدريب الموظفين على أفضل الممارسات.

☐ موافق بشدة
☐ موافق
☐ محايد
☐ غير موافق
☐ غير موافق بشدة

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك ☆ أم حفظ جميع التغييرات في Drive

الأسئلة 50 الردود الإعدادات

تساهم السياسات والإجراءات الفعالة في تقليل مخاطر الأمن السيبراني في البنوك التجارية.

☐ موافق بشدة
☐ موافق
☐ محايد
☐ غير موافق
☐ غير موافق بشدة

إرسال

↶ ↷ 🔍 🗨

☆ 📁

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

تم حفظ جميع التغييرات في Drive

☰

الإعدادات

الرموز 50

الأسئلة

⊕

📎

🔍

📄

📺

▶

☰

غير موافق

غير موافق بشدة

يبد التعاون مع الهيئات الحكومية والمؤسسات المالية الأخرى استراتيجية فعالة لتعزيز إدارة مخاطر الأمن السيبراني.

موافق بشدة

موافق

محايد

غير موافق

غير موافق بشدة