

تقييم المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية
الإلكترونية في البنوك السعودية

إعداد الطالبة/ ابرار دعيج الراجح
الرقم الجامعي/ 253000930

إشراف/ د. الفيصل عبد الحميد محمد حسن
د. فايز جراد

العام الدراسي/ 2026

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الشكر والتقدير

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آله وصحبه أجمعين.

في البداية أحمد الله سبحانه وتعالى وأشكره على نعمه الكثيرة وتوفيقه لي لإتمام هذا البحث، فلولاه فضلته وتيسيره لما تمكنت من إنجاز هذا العمل.

كما أتقدم بخالص الشكر والتقدير إلى سعادة الدكتور (د. فايز الجراد -د. الفیصل عبد الحمید) على توجيهاته القيمة وملاحظاته البناءة، ودعمه المستمر خلال مراحل إعداد هذا البحث، مما كان له الأثر الكبير في تطوير محتواه العلمي، كما كان لتشجيعه ودعمه دور مهم في إتمام هذا العمل.

كما أود أن أعبر عن بالغ امتناني لكل من أسهم في دعمي ومساعدتي خلال فترة إعداد هذا البحث، سواء من أساتذة أو زملاء، ممن قدموا لي النصيحة أو المعلومة التي ساعدتني في تطوير هذا العمل.

ولا يفوتني أن أتقدم بجزيل الشكر والتقدير لكل من كان له دور في تهيئة البيئة المناسبة لإتمام هذا البحث وأخيراً، أهدي هذا الجهد المتواضع إلى والدتي الغالية التي كانت الدعامة الأولى في حياتي، وإلى والدي رحمه الله وأسكنه فسيح جناته، وإلى إخوتي وأخواتي على دعمها وتشجيعها المتواصل الذين أحاطوني بالمحبة والمساندة التي منحتني الدافع والإلهام لمواصلة التقدّم والنجاح.

وأسأل الله تعالى أن يجزي الجميع خير الجزاء، وأن يجعل هذا العمل خالصاً لوجهه الكريم، وأن ينفع به.

المستخلص

يهدف هذا البحث إلى دراسة المخاطر السيبرانية وتأثيرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية. ومع التوسع الكبير في استخدام الخدمات الإلكترونية في القطاع المصرفي، أصبحت هذه البنوك أكثر عرضة للهجمات السيبرانية مثل الاختراق، سرقة البيانات، والاحتيال الإلكتروني، مما يهدد أمن المعلومات واستمرارية الخدمات.

اعتمد البحث على المنهج الوصفي التحليلي، من خلال مراجعة الدراسات السابقة، وتحليل التقارير المتاحة للبنوك السعودية حول الحوادث السيبرانية، وتقييم تأثيرها على استقرار الخدمات المصرفية الإلكترونية.

أظهرت النتائج أن المخاطر السيبرانية لها أثر واضح على استقرار الخدمات المصرفية، حيث تؤدي الهجمات السيبرانية إلى تعطيل بعض الخدمات أو التأثير على ثقة العملاء. وبناءً على ذلك، يقدم البحث توصيات لتعزيز إجراءات الأمن السيبراني وإدارة المخاطر في البنوك السعودية بهدف حماية الخدمات الإلكترونية وتحقيق استقرارها.

الكلمات المفتاحية: المخاطر السيبرانية، الخدمات المصرفية الإلكترونية، البنوك السعودية، استقرار الأنظمة، إدارة المخاطر.

فهرس الموضوعات

المحتويات

ب	الشكر والتقدير	
ت	المستخلص	
ث	فهرس الموضوعات	
ح	مصطلحات البحث	
١	الفصل الأول: الإطار العام للدراسة	
٢	المقدمة:	
٢	مشكلة الدراسة:	
٣	أهداف الدراسة:	
٣	أهمية الدراسة:	
٣	أولاً: الأهمية العلمية:	
٤	ثانياً: الأهمية العملية:	
٤	تساؤلات الدراسة:	
٤	فرضيات الدراسة:	
٥	النظرية العلمية المتبعة لإعداد البحث:	
٧	الفصل الثاني: الدراسات السابقة	
٨	المقدمة:	
٨	المتغير التابع:	
٩	المتغير المستقل:	
٩	الدراسات السابقة:	
١١	الإطار النظري للدراسة	
١٣	الفصل الثالث: منهجية الدراسة	
١٤	مقدمة:	
١٤	تصميم البحث:	
١٥	مجتمع البحث:	
١٥	خصائص العينة:	
١٥	محددات حجم العينة:	
١٦	خطوات جمع البيانات:	
١٧	حدود البحث:	
١٧	١. الحدود الزمانية (Time Limits)	
١٧	٢. الحدود المكانية (Spatial Limits)	
١٧	٣. الحدود الموضوعية (Subject Matter Limits)	
١٨	الأداة المستخدمة في التحليل الإحصائي:	
١٩	الفصل الرابع: النتائج ومناقشتها	

٢٠		مقدمة:
٢٠		تحليل البيانات:
٢١		نتائج الدراسة ومناقشتها مع الدراسات السابقة:
٢٣		الفصل الخامس: التوصيات والمقترحات الملاحق
٢٤		التوصيات:
٢٥		المراجع:
٢٥		أولاً: المراجع العربية
٢٥		ثانياً: المراجع الإنجليزية
٢٨		الاستبانة:
٣٠		الملخص:
٣٠		الملخص العربي:
٣٠		Abstract (English):

مصطلحات البحث

هذه أبرز المصطلحات المتعلقة بهذا البحث

المخاطر السيبرانية:

هي المخاطر الناتجة عن الهجمات الإلكترونية أو الاختراقات التي تستهدف الأنظمة المعلوماتية والشبكات الإلكترونية في المؤسسات، مثل الاختراق، سرقة البيانات، الاختيال الإلكتروني، أو انقطاع الخدمات.

الخدمات المصرفية الإلكترونية:

هي الخدمات التي تقدمها البنوك للعملاء عبر الوسائل الإلكترونية مثل الإنترنت والتطبيقات المصرفية.

الإجراءات الأمنية والاستراتيجيات الوقائية:

السياسات، الإجراءات، والتقنيات التي تستخدمها البنوك للحد من المخاطر السيبرانية وحماية أنظمة المعلومات

استقرار الخدمات المصرفية الإلكترونية:

قدرة البنك على تقديم خدماته الإلكترونية بشكل مستمر وآمن، مع حماية بيانات العملاء ورضاهم.

الفصل الأول: الإطار العام للدراسة

المقدمة:

شهد القطاع المصرفي خلال السنوات الأخيرة تطوراً ملحوظاً نتيجة التقدم التكنولوجي المتسارع والتحول الرقمي في مختلف القطاعات الاقتصادية. وقد أسهم هذا التطور في ظهور الخدمات المصرفية الإلكترونية التي أصبحت من أهم الوسائل التي تعتمد عليها البنوك لتقديم خدماتها للعملاء بسرعة وكفاءة. وتشمل هذه الخدمات العمليات المصرفية عبر الإنترنت والتطبيقات المصرفية على الهواتف الذكية، والتي تتيح للعملاء إجراء العديد من المعاملات المالية بسهولة وفي أي وقت ومن أي مكان.

ومع هذا التطور الكبير في الخدمات المصرفية الإلكترونية، برزت العديد من التحديات المرتبطة بالأمن السيبراني، حيث أصبحت المؤسسات المالية هدفاً رئيسياً للهجمات السيبرانية التي قد تؤدي إلى اختراق الأنظمة المصرفية أو تعطيل الخدمات الإلكترونية أو تسريب البيانات الحساسة للعملاء. وتشكل هذه المخاطر تهديداً مباشراً لاستقرار الأنظمة المصرفية، كما قد تؤثر في مستوى ثقة العملاء في الخدمات الإلكترونية التي تقدمها البنوك.

وفي المملكة العربية السعودية، تسعى البنوك إلى تعزيز التحول الرقمي وتطوير خدماتها المصرفية الإلكترونية بما يتماشى مع التوجهات الحديثة في القطاع المالي ورؤية المملكة ٢٠٣٠ التي تدعم التحول الرقمي في مختلف القطاعات. إلا أن التوسع في استخدام الأنظمة الرقمية قد يزيد من احتمالية التعرض للمخاطر السيبرانية، الأمر الذي يستدعي تبني استراتيجيات فعالة لإدارة هذه المخاطر وضمان استمرارية الخدمات المصرفية الإلكترونية بكفاءة وأمان.

وعلى الرغم من وجود العديد من الدراسات التي تناولت موضوع الأمن السيبراني في القطاع المالي، إلا أن هناك نقصاً نسبياً في الدراسات التي تركز على تقييم المخاطر السيبرانية وتأثيرها المباشر على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية. ومن هنا تأتي أهمية هذه الدراسة التي تسعى إلى تحليل طبيعة المخاطر السيبرانية وتقييم أثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

مشكلة الدراسة:

تواجه البنوك في الوقت الحاضر تحديات متزايدة في مجال الأمن السيبراني نتيجة الاعتماد المتزايد على الأنظمة الرقمية والتقنيات الحديثة في تقديم الخدمات المصرفية الإلكترونية. ومع التوسع الكبير في استخدام هذه الخدمات، أصبحت المؤسسات المالية من أكثر الجهات عرضة للهجمات السيبرانية التي قد تستهدف الأنظمة المصرفية أو قواعد البيانات أو البنية التحتية الرقمية للبنوك.

وتكمن مشكلة الدراسة في أن المخاطر السيبرانية قد تؤثر بشكل مباشر على استقرار الخدمات المصرفية الإلكترونية، حيث قد تؤدي هذه المخاطر إلى تعطيل الأنظمة المصرفية أو تسريب المعلومات الحساسة أو التأثير في مستوى ثقة العملاء في الخدمات الإلكترونية المقدمة من قبل البنوك. وعلى الرغم من الجهود التي تبذلها المؤسسات المصرفية لتعزيز أنظمة الأمن السيبراني وتطوير آليات الحماية الرقمية، إلا أن طبيعة الهجمات السيبرانية تتطور بشكل مستمر، مما يزيد من صعوبة السيطرة عليها والحد من أثارها.

كما تشير العديد من الدراسات والتقارير إلى تزايد التهديدات السيبرانية التي تستهدف القطاع المالي على مستوى العالم، الأمر الذي يجعل من الضروري دراسة تأثير هذه المخاطر على استقرار الخدمات المصرفية

الإلكترونية، خاصة في ظل التوسع الكبير الذي تشهده البنوك السعودية في مجال التحول الرقمي وتقديم الخدمات المصرفية الإلكترونية.

وبناءً على ذلك، تسعى هذه الدراسة إلى تحليل طبيعة المخاطر السيبرانية التي تواجه البنوك السعودية، ودراسة مدى تأثيرها على استقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى التعرف على دور الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من تأثير هذه المخاطر.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحليل العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وذلك من خلال تحقيق مجموعة من الأهداف الرئيسة والفرعية على النحو الآتي:

الهدف العام:

تحليل أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

الأهداف الفرعية:

١. التعرف على مفهوم المخاطر السيبرانية وأهميتها في القطاع المصرفي.
٢. تحديد أنواع المخاطر السيبرانية التي قد تواجه البنوك السعودية في مجال الخدمات المصرفية الإلكترونية.
٣. تحليل تأثير المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية.
٤. تقييم إجراءات البنوك واستراتيجياتها في إدارة المخاطر السيبرانية.
٥. تقديم مجموعة من التوصيات العملية التي تساعد البنوك على تعزيز الأمن السيبراني وضمان استمرارية الخدمات المصرفية الإلكترونية بشكل آمن وموثوق.

أهمية الدراسة:

تتبع أهمية هذه الدراسة من الأهمية المتزايدة للأمن السيبراني في القطاع المصرفي، خاصة مع التوسع الكبير في استخدام الخدمات المصرفية الإلكترونية. إذ أصبحت البنوك تعتمد بشكل متزايد على الأنظمة الرقمية في تقديم خدماتها للعملاء، مما يجعلها أكثر عرضة للمخاطر السيبرانية والهجمات الإلكترونية. كما تسهم هذه الدراسة في توضيح العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وتقديم مجموعة من التوصيات التي يمكن أن تساعد المؤسسات المصرفية على تعزيز أنظمة الحماية الإلكترونية وتحسين إدارة المخاطر السيبرانية.

ويمكن توضيح أهمية الدراسة من خلال الجانبين العلمي والعملي على النحو الآتي:

أولاً: الأهمية العلمية:

- تسهم هذه الدراسة في إثراء المعرفة العلمية المتعلقة بالمخاطر السيبرانية في القطاع المصرفي، خاصة فيما يتعلق بتأثيرها على استقرار الخدمات المصرفية الإلكترونية.
- تساعد الدراسة في سد الفجوة البحثية المرتبطة بدراسة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

- توفر إطارًا علميًا يمكن أن يستفيد منه الباحثون في الدراسات المستقبلية في مجالات الأمن السيبراني وإدارة المخاطر في المؤسسات المالية.

ثانيًا: الأهمية العملية:

- تساعد نتائج الدراسة إدارات البنوك على فهم طبيعة المخاطر السيبرانية وتأثيرها المحتمل على الخدمات المصرفية الإلكترونية.
- تساهم في دعم تحسين السياسات والإجراءات الأمنية التي تعتمد عليها البنوك لحماية الأنظمة المصرفية الإلكترونية.
- تقدم الدراسة مجموعة من التوصيات العملية التي يمكن أن تساعد البنوك في تعزيز الأمن السيبراني وضمان استمرارية الخدمات المصرفية الإلكترونية وزيادة ثقة العملاء بها

تساؤلات الدراسة:

يسعى هذا البحث إلى الإجابة على مجموعة من التساؤلات التي تهدف إلى توضيح طبيعة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وهي كالآتي:

١. ما المقصود بالمخاطر السيبرانية في القطاع المصرفي السعودي؟
٢. ما أهم أنواع المخاطر السيبرانية التي تواجه البنوك السعودية في الخدمات المصرفية الإلكترونية؟
٣. ما أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية؟
٤. ما الإجراءات والاستراتيجيات التي تعتمد عليها البنوك السعودية للحد من تأثير المخاطر السيبرانية؟
٥. كيف يمكن تعزيز استقرار الخدمات المصرفية الإلكترونية من خلال إدارة فعّالة للمخاطر السيبرانية

فرضيات الدراسة:

استنادًا إلى أهداف البحث وتساؤلاته، ولتحليل العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، تم صياغة فرضيات الدراسة على النحو التالي.

الفرضية الأولى (H1):

هناك علاقة سلبية بين ذات دلالة إحصائية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية؛ أي أن زيادة المخاطر السيبرانية تؤدي إلى انخفاض استقرار الخدمات.

الفرضية الثانية (H2):

البنوك التي تتبنى استراتيجيات فعّالة لإدارة المخاطر السيبرانية تتمتع بمستوى أعلى من استقرار الخدمات المصرفية الإلكترونية مقارنة بالبنوك التي تفتقر لهذه الاستراتيجيات.

الفرضية الثالثة (H3):

هناك علاقة ارتباطية بين أنواع المخاطر السيبرانية (مثل الاختراق، سرقة البيانات، الاحتيال الإلكتروني) ومستوى استجابة البنوك وإجراءاتها الأمنية.

الفرضية الرابعة (H4):

زيادة الوعي الأمني لدى الموظفين في البنوك يقلل من تأثير السلبي للمخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية

النظرية العلمية المتبعة لإعداد البحث:

يعتمد هذا البحث على نظرية إدارة المخاطر السيبرانية كأساس علمي لدراسة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية. وتوفر هذه النظرية إطاراً منهجياً لتحديد المخاطر المحتملة ووضع الاستراتيجيات الوقائية المناسبة لضمان استقرار الخدمات المصرفية الإلكترونية.

١. المتغيرات في النموذج

• المتغير المستقل (Independent Variable):

المخاطر السيبرانية.

يشمل هذا المتغير أنواع المخاطر التي تواجه البنوك، مثل:

• الهجمات الإلكترونية (Hacking Attacks)

• سرقة البيانات (Data Theft)

• الاحتيال المالي الإلكتروني (Electronic Fraud)

• انقطاع الخدمة أو الأعطال الناتجة عن المخاطر السيبرانية

• المتغير التابع (Dependent Variable):

استقرار الخدمات المصرفية الإلكترونية

ويقاس من خلال:

• استمرار الخدمات دون توقف

• حماية بيانات العملاء

• مستوى ثقة العملاء في البنوك

• العامل المعدل / التحكم (Moderating Variable): إجراءات الأمن السيبراني والاستراتيجيات الوقائية

يعمل هذا العامل على تخفيف التأثير السلبي للمخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية

يعتمد هذا البحث على نظرية إدارة المخاطر السيبرانية كأساس علمي لدراسة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

٢. النموذج النظري للعلاقة بين المتغيرات

يفترض النموذج أن المخاطر السيبرانية تؤثر سلبًا على استقرار الخدمات المصرفية الإلكترونية، وأن إجراءات الأمن السيبراني والاستراتيجيات الفعالة في إدارتها يمكن أن تقلل من التأثير السلبي وتعزز استقرار الخدمات.

يُمثل المخاطر السيبرانية المتغير المستقل، بينما يمثل استقرار الخدمات المصرفية الإلكترونية المتغير التابع، مع وجود عامل تعديل يتمثل في الإجراءات الوقائية والاستراتيجيات الأمنية التي تتبناها البنوك.

التمثيل البياني للنموذج النظري:

المتغير المستقل	العامل المعدل/ التحكم	المتغير التابع
المخاطر السيبرانية {الهجمات، سرقة البيانات، الاحتيال}	إجراءات الأمن السيبراني والاستراتيجيات الوقائية	استقرار الخدمات المصرفية الإلكترونية {استمرارية الخدمات، حماية البيانات، ثقة العملاء}

٣. مبررات اختيار النظرية

- تساعد نظرية إدارة المخاطر السيبرانية في تحديد نقاط الضعف المحتملة في النظام المصرفي الإلكتروني.
- توفر إطارًا علميًا لدراسة العلاقة بين تقييم المخاطر واستقرار الخدمات بطريقة منهجية وقابلة للاختبار.
- تمكن الباحث من صياغة فرضيات واضحة يمكن اختبارها باستخدام البيانات وتحليل النتائج بطريقة علمية دقيقة

الفصل الثاني: الدراسات السابقة

المقدمة:

يعد استعراض الدراسات السابقة جزءاً أساسياً من أي بحث أكاديمي إذا يتيح للباحث فهم ما تم إنجازه سابقاً في مجال الدراسة وتحديد الفجوات البحثية التي يمكن أن تسدها الدراسة الحالية.

في هذا الفصل، سيتم استعراض أهم الدراسات المتعلقة بالمخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك، مع التركيز على:

- تعريف المخاطر السيبرانية وأنواعها المختلفة.
- تأثير المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية.
- الإجراءات والاستراتيجيات التي تعتمد عليها البنوك للتقليل من هذه المخاطر.

كما يوضح هذا الفصل ما تقدمه الدراسة الحالية مقارنة بما تم التوصل إليه في الدراسات السابقة، من خلال تحليل شامل للنتائج السابقة وربطها بمتغيرات البحث: حيث يشمل (المخاطر السيبرانية المتغير المستقل واستقرار الخدمات الإلكترونية المتغير التابع)، إضافة إلى دور الإجراءات الأمنية كعامل تعديل/تحكم في العلاقة بين المتغيرين.

يهدف هذا الفصل إلى:

١. تقديم رؤية شاملة عن أهم الدراسات السابقة في مجال الأمن السيبراني المصرفي.
٢. تحديد الفجوات البحثية التي لم تغطيها الدراسات السابقة.
٣. توضيح الإطار النظري والدليل العلمي الذي يعتمد عليه البحث الحالي لدراسة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

المتغير التابع:

المتغير التابع في هذا البحث هو استقرار الخدمات المصرفية الإلكترونية (Electronic Banking Service Stability)، ويقصد به قدرة البنوك على تقديم خدماتها الإلكترونية بشكل مستمر وأمن دون انقطاع أو تعرض للتهديدات السيبرانية.

عناصر قياس المتغير التابع:

١. استمرارية الخدمات الإلكترونية: قدرة النظام البنكي على تقديم الخدمات دون توقف نتيجة الهجمات أو الأعطال التقنية.
٢. حماية البيانات والمعلومات: مدى فعالية البنوك في تأمين بيانات العملاء والمعاملات المالية من الاختراق أو السرقة.
٣. ثقة العملاء في الخدمات: مستوى رضا العملاء واعتقادهم بأن الخدمات البنكية الإلكترونية آمنة وموثوقة.
٤. الاستجابة للآزمات: قدرة البنك على التعامل مع الحوادث السيبرانية بسرعة وكفاءة لتقليل التأثير على العمليات.

ما أظهرته الدراسات السابقة:

- أشارت الدراسات أن انخفاض استقرار الخدمات الإلكترونية يرتبط بشكل مباشر بزيادة المخاطر السيبرانية.
- البنوك التي تطبق استراتيجيات فعالة لإدارة المخاطر تتمتع بمستوى أعلى من استقرار الخدمات وثقة العملاء.

- مع ذلك هناك فجوة واضحة في الدراسات السابقة المتعلقة بقياس الاستقرار بشكل شامل في البنوك السعودية، حيث اقتصر أغلب الدراسات على جوانب محددة مثل حماية البيانات فقط، دون تقييم الاستجابة للآزمات وثقة العملاء بشكل متكامل، وهو ما تسعى الدراسة الحالية إلى معالجته.

المتغير المستقل:

المتغير المستقل في هذا البحث هو المخاطر السيبرانية (Cybersecurity Risks)، ويقصد به جميع التهديدات والهجمات التي قد تتعرض لها البنوك على مستوى الأنظمة والخدمات المصرفية الإلكترونية، والتي يمكن أن تؤثر بشكل مباشر على استقرار الخدمات المصرفية.

عناصر قياس المتغير المستقل:

١. الهجمات الإلكترونية (Hacking Attacks): محاولات الاختراق التي تستهدف أنظمة البنوك للتلاعب أو سرقة المعلومات.
٢. سرقة البيانات (Data Theft): الحصول غير المصرح به على بيانات العملاء والمعاملات المالية.
٣. الاحتيال المالي الإلكتروني (Electronic Fraud): عمليات الاحتيال عبر الإنترنت التي تستهدف الخدمات المصرفية الإلكترونية.
٤. انقطاع الخدمات أو الأعطال الناتجة عن المخاطر السيبرانية: توقف الخدمات الإلكترونية بسبب هجمات أو أعطال ناتجة عن اختراقات أمنية.

ما أظهرته الدراسات السابقة:

- أشارت الدراسات إلى أن زيادة تعرض البنوك للمخاطر السيبرانية تؤدي إلى تراجع استقرار الخدمات الإلكترونية.
- البنوك التي تعتمد إجراءات وقائية وأمنية فعالة تقل لديها تأثيرات المخاطر السيبرانية على الخدمات المصرفية الإلكترونية.
- مع ذلك هناك حاجة واضحة لدراسة تقييم شامل لهذه المخاطر وربطها باستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وهو ما تهدف الدراسة الحالية إلى تحقيقه من خلال تحليل متكامل يشمل جميع أنواع المخاطر والإجراءات الوقائية.

الدراسات السابقة:

يشكل استعراض الدراسات السابقة جزءاً أساسياً من أي بحث أكاديمي، حيث يمكن الباحث من فهم ما تم إنجازه سابقاً في مجال الدراسة وتحديد الفجوات البحثية التي يمكن سدها بالدراسة الحالية. تشير الأدبيات إلى أن المخاطر السيبرانية مثل الاختراقات الإلكترونية، سرقة البيانات، والاحتيال المالي تؤثر سلباً على استقرار الخدمات المصرفية الإلكترونية. كما أن الدراسات أكدت أن البنوك التي تعتمد إجراءات أمنية واستراتيجيات وقائية متقدمة تواجه تأثيرات أقل لهذه المخاطر.

مع ذلك، معظم الدراسات ركزت على البنوك العالمية، أو اقتصرت الدراسات السعودية على جوانب محدودة دون تغطية العلاقة بين المخاطر السيبرانية واستقرار الخدمات بشكل شامل، وهو ما تمثل الفجوة البحثية التي تسعى الدراسة الحالية إلى معالجتها.

مناقشة نتائج الدراسات السابقة

- هناك اتفاق عام بين الدراسات على أن المخاطر السيبرانية تهدد استقرار الخدمات الإلكترونية، إلا أن تقييم أثر الإجراءات الأمنية يختلف بين دراسة وأخرى.
- أظهرت الدراسات غياب تقييم شامل للمخاطر السيبرانية في البنوك السعودية، ما يمثل فجوة بحثية واضحة.

- لم تتناول الدراسات السابقة دور الإجراءات الأمنية كعامل تعديل بين المخاطر السيبرانية واستقرار الخدمات، وهو ما يركز عليه البحث الحالي

عرض الدراسات السابقة

الدراسة الأولى:

أجرى Al Mohayya & Makeen (٢٠٢٥) دراسة هدفت إلى تحليل تأثير الهندسة الاجتماعية على المخاطر السيبرانية في البنوك في مدينة الرياض، باستخدام المنهج الكمي من خلال استبيان موزع على موظفي البنوك لقياس مستوى الوعي بالمخاطر السيبرانية. أظهرت النتائج أن مستوى الوعي كان مرتفعاً نسبياً، إلا أن الدراسة أوصت بتعزيز برامج التدريب الأمني وتطوير السياسات الأمنية.

- ربط بالدراسة الحالية: ركزت هذه الدراسة على الهندسة الاجتماعية فقط، بينما تسعى الدراسة الحالية إلى تحليل المخاطر السيبرانية بشكل أوسع وربطها مباشرة باستقرار الخدمات المصرفية الإلكترونية.

الدراسة الثانية:

هدفت دراسة Alrawad (٢٠٢٤) إلى تحليل التهديدات السيبرانية التي تواجه المؤسسات المالية في ظل التحول الرقمي، باستخدام مراجعة الأدبيات لتحديد أبرز الهجمات السيبرانية وتأثيرها على المؤسسات المالية. النتائج أكدت أن زيادة الاعتماد على التقنيات الرقمية يزيد من احتمالية التعرض للهجمات السيبرانية، مما يؤدي إلى خسائر مالية وانخفاض ثقة العملاء.

- ربط بالدراسة الحالية: ركزت الدراسة على تحديد التهديدات فقط دون دراسة تأثيرها المباشر على استقرار الخدمات المصرفية الإلكترونية.

الدراسة الثالثة:

تناولت دراسة Sayari (٢٠٢٤) أثر الخدمات المصرفية عبر الإنترنت على أداء البنوك في المملكة العربية السعودية باستخدام بيانات ١٠ بنوك للفترة ٢٠١٣-٢٠٢٢. النتائج أظهرت تأثيراً إيجابياً للخدمات المصرفية الإلكترونية على مؤشرات الربحية.

- ربط بالدراسة الحالية: لم تتناول هذه الدراسة المخاطر السيبرانية المرتبطة بالخدمات الإلكترونية، وهو ما تسعى الدراسة الحالية لمعالجته.

الدراسة الرابعة:

أظهرت دراسة Elsayed et al (٢٠٢٤) أن الإفصاح عن ممارسات الأمن السيبراني وحوكمة المخاطر يؤثر إيجابياً في الأداء المؤسسي، ويسهم في تعزيز الاستقرار المالي للمؤسسات المصرفية.

- ربط بالدراسة الحالية: ركزت على الحوكمة والأداء المؤسسي، ولم تركز على استقرار الخدمات المصرفية الإلكترونية، وهو محور الدراسة الحالية.

الدراسة الخامسة:

أشارت دراسة حديثة إلى أن ارتفاع مستوى المخاطر السيبرانية يؤثر على سلوك البنوك ومستوى المخاطر التشغيلية، مما ينعكس على استقرار المؤسسات المالية.

- ربط بالدراسة الحالية: تبرز أهمية دمج إدارة المخاطر السيبرانية ضمن الاستراتيجيات البنكية لضمان استقرار الخدمات، وهو ما تهدف الدراسة الحالية إلى تحقيقه بشكل شامل

ما ستقدمه الدراسة الحالية مقارنة بالدراسات السابقة

١. تقديم تقييم شامل للمخاطر السيبرانية في البنوك السعودية وربطها مباشرة باستقرار الخدمات المصرفية الإلكترونية.
٢. دراسة دور الإجراءات الوقائية والاستراتيجيات الأمنية في الحد من تأثير المخاطر على الخدمات.
٣. سد الفجوة البحثية المتعلقة بعدم وجود دراسة منهجية تربط المخاطر السيبرانية بالإجراءات الوقائية واستقرار الخدمات في البنوك السعودية.
٤. تقديم توصيات عملية قابلة للتطبيق تساعد البنوك على تعزيز الأمن السيبراني واستقرار الخدمات الإلكترونية

الإطار النظري للدراسة

يعتمد هذا البحث على نظرية إدارة المخاطر السيبرانية كأساس علمي لدراسة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية. وتتيح هذه النظرية فهم طبيعة المخاطر، طرق تقييمها، واستراتيجيات الحد من تأثيرها على استمرارية الخدمات المصرفية.

المتغيرات في الدراسة

١. المتغير المستقل (Independent Variable): المخاطر السيبرانية

- ويشمل جميع التهديدات التي قد تتعرض لها البنوك على مستوى الأنظمة والخدمات الإلكترونية، مثل:
- الهجمات الإلكترونية (Hacking Attacks): محاولات الاختراق للوصول غير المصرح به للأنظمة البنكية.
 - سرقة البيانات (Data Theft): الحصول على معلومات العملاء والمعاملات المالية بشكل غير قانوني.
 - الاحتيال المالي الإلكتروني (Electronic Fraud): عمليات الاحتيال التي تستهدف الخدمات المصرفية عبر الإنترنت.
 - انقطاع الخدمات أو الأعطال الناتجة عن المخاطر السيبرانية: توقف الأنظمة نتيجة الهجمات أو الاختراقات.

٢. المتغير التابع (Dependent Variable): استقرار الخدمات المصرفية الإلكترونية

ويقاس من خلال عدة عناصر:

- استمرارية الخدمات: قدرة النظام على تقديم الخدمات دون انقطاع.
- حماية البيانات: فعالية البنوك في تأمين بيانات العملاء والمعاملات المالية.
- ثقة العملاء: مستوى رضا العملاء واعتقادهم بأمان وموثوقية الخدمات.

٣. عامل تعديل/تحكم (Moderator/Control Variable): إجراءات الأمن السيبراني والاستراتيجيات الوقائية

- تعمل هذه الإجراءات كعامل تعديل يقلل من التأثير السلبي للمخاطر السيبرانية على استقرار الخدمات.
- تشمل سياسات الأمان، التدريب الأمني للموظفين، واستخدام تقنيات الحماية المتقدمة.

مبررات اختيار النظرية

تم اختيار نظرية إدارة المخاطر السيبرانية للأسباب التالية:

١. توفر إطارًا علميًا لدراسة تقييم المخاطر وتأثيرها على استقرار الخدمات المصرفية الإلكترونية.
٢. تساعد الباحث على تحليل العلاقة بين المتغيرات بشكل منهجي ومنظم.
٣. تمكن من صياغة فرضيات قابلة للاختبار إحصائيًا باستخدام البيانات والتحليل العلمي.
٤. توفر نموذجًا يمكن تطبيقه على البنوك السعودية لفهم أثر المخاطر السيبرانية وفاعلية الإجراءات الوقائية المتبعة

النموذج النظري للدراسة

يفترض النموذج أن:

- المخاطر السيبرانية تؤثر سلبًا على استقرار الخدمات المصرفية الإلكترونية.
- إجراءات الأمن السيبراني والاستراتيجيات الوقائية تقلل من التأثير السلبي للمخاطر، وتعمل كعامل تعديل/تحكم.
- هذا النموذج يشكل الأساس العلمي لاختبار فرضيات البحث في الدراسة الحالية.

تمثيل العلاقة بين المتغيرات

.

تعمل إجراءات الأمن السيبراني والاستراتيجيات الوقائية كعامل تعديل أو تحكم، حيث تقلل من التأثير السلبي للمخاطر السيبرانية على استقرار الخدمات.

وبالتالي، يعتمد النموذج على افتراض أن إدارة فعالة للمخاطر السيبرانية تعزز استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية

يمكن تمثيل العلاقة بين المتغيرات

المتغير	الوصف
المستقل	المخاطر السيبرانية (الهجمات، السرقة البيانات، الاحتيال، انقطاع الخدمة)
التابع	استقرار الخدمات المصرفية الإلكترونية (استمرارية الخدمات، حماية البيانات، ثقة العملاء)
عامل التعديل	إجراءات الأمن السيبراني والاستراتيجيات الوقائية

الفصل الثالث: منهجية الدراسة

مقدمة:

يهدف هذا الفصل إلى توضيح المنهجية العلمية المعتمدة لجمع البيانات وتحليلها لدراسة المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية. ويشمل شرح تصميم البحث، مجتمع الدراسة، العينة، أدوات جمع البيانات، حدود الدراسة، وأساليب التحليل الإحصائي، بما يضمن دقة النتائج وموضوعية الاستنتاجات.

يعتمد البحث على المنهج الوصفي التحليلي (Descriptive-Analytical Methodology)، الذي يتيح دراسة الواقع الحالي للمخاطر السيبرانية في البنوك وتقييم أثرها على استقرار الخدمات المصرفية الإلكترونية. كما يُمكن المنهج الباحث من اختبار الفرضيات البحثية المستندة إلى البيانات المجمعة من العينة المستهدفة.

يسعى هذا الفصل إلى تقديم خطة واضحة ومنهجية منظمة لجمع البيانات وتحليلها، بحيث يتم ربط النتائج بالمتغيرات المستقلة والتابعة، وتقديم توصيات عملية قابلة للتطبيق في البنوك السعودية لتعزيز الأمن السيبراني واستقرار الخدمات الإلكترونية.

على الرغم من وجود العديد من الدراسات حول الأمن السيبراني في القطاع المصرفي، إلا أن معظمها ركز على الجوانب التقنية للأمن المعلوماتي أو تأثير التحول الرقمي على الأداء المالي للمؤسسات، دون التركيز بشكل مباشر على العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية. كما أن الدراسات المتعلقة بالبيئة المصرفية العربية، وخاصة البنوك السعودية، ما زالت محدودة، بينما تشهد هذه البنوك توسعاً كبيراً في الخدمات الرقمية.

لذلك، تسعى هذه الدراسة إلى سد هذه الفجوة البحثية من خلال تقييم المخاطر السيبرانية وربطها مباشرة باستقرار الخدمات المصرفية الإلكترونية، وتحليل دور الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من تأثير هذه المخاطر.

تصميم البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي (Descriptive Analytical Method)، الذي يعد من أكثر المناهج استخداماً في الدراسات التي تهدف إلى تحليل الظواهر وتفسير العلاقات بين المتغيرات. ويتيح هذا المنهج دراسة الواقع الحالي للمخاطر السيبرانية في البنوك السعودية وتحليل أثرها على استقرار الخدمات المصرفية الإلكترونية بشكل دقيق وموضوعي.

يركز تصميم البحث على تحليل العلاقة بين المتغير المستقل والمتغير التابع. حيث يمثل المتغير المستقل المخاطر السيبرانية التي قد تواجه البنوك، مثل الهجمات الإلكترونية، سرقة البيانات، والاحتيال الإلكتروني، بينما يمثل المتغير التابع استقرار الخدمات المصرفية الإلكترونية، ويقاس من خلال استمرارية الخدمات، حماية بيانات العملاء، ومستوى ثقة العملاء في الخدمات الإلكترونية.

كما يتضمن تصميم البحث دراسة دور الإجراءات الأمنية والاستراتيجيات الوقائية التي تعتمدها البنوك للحد من تأثير المخاطر السيبرانية، وذلك من خلال تحليل البيانات التي سيتم جمعها من عينة الدراسة باستخدام أدوات التحليل الإحصائي المناسبة.

ويهدف هذا التصميم إلى تقديم فهم شامل وطبيعي للعلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، مع توفير نتائج علمية يمكن للبنوك الاستفادة منها لتطوير استراتيجيات فعالة لإدارة المخاطر السيبرانية، وتعزيز أمن واستمرارية الخدمات المصرفية الإلكترونية في المملكة العربية السعودية.

مجتمع البحث:

يمثل موظفو البنوك السعودية مجتمع البحث في هذه الدراسة، مع التركيز بشكل خاص على الأقسام المرتبطة بالخدمات المصرفية الإلكترونية، أمن المعلومات، وتقنية المعلومات، نظرًا لما يمتلكه هؤلاء الموظفون من معرفة وخبرة مباشرة بطبيعة المخاطر السيبرانية والإجراءات الأمنية المتبعة في البنوك.

ويعد اختيار هذا المجتمع مناسبًا، لأنه يتيح الحصول على بيانات دقيقة وموضوعية حول المخاطر السيبرانية، واستقرار الخدمات المصرفية الإلكترونية، وذلك من خلال آراء العاملين الأكثر اطلاعًا على الإجراءات والتحديات الفعلية في بيئة العمل البنكي.

كما أن التركيز على هذا المجتمع يساهم في سد الفجوة البحثية المتعلقة بعدم وجود دراسات شاملة تربط بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، مع الأخذ بعين الاعتبار دور الإجراءات الأمنية كعامل تعديل في العلاقة بين المتغيرات

خصائص العينة:

تتكون عينة هذه الدراسة من موظفين عاملين في البنوك السعودية، مع التركيز على الأقسام المرتبطة بالخدمات المصرفية الإلكترونية، تقنية المعلومات، وأمن المعلومات، نظرًا لما يمتلكه هؤلاء الموظفون من خبرة ومعرفة مباشرة بطبيعة المخاطر السيبرانية والإجراءات الأمنية المتبعة في البنوك.

ويمكن وصف خصائص العينة من خلال عدة متغيرات أساسية، تشمل:

١. **المسمى الوظيفي:** يشمل المديرين، المشرفين، والموظفين الفنيين العاملين في الأقسام التقنية والمصرفية، بما يضمن تمثيل جميع مستويات المسؤولية والخبرة في البنوك.
 ٢. **سنوات الخبرة:** تتفاوت سنوات الخبرة بين أفراد العينة، مما يسمح بجمع آراء متنوعة ومدعومة بالخبرة العملية حول المخاطر السيبرانية واستراتيجيات إدارة الأمن الإلكتروني.
 ٣. **المؤهل العلمي:** يتنوع المؤهل بين البكالوريوس والدراسات العليا في مجالات مثل إدارة الأعمال، تقنية المعلومات، وأمن المعلومات، مما يعكس مستوى المعرفة النظرية والعملية للمشاركين.
 ٤. **القسم الوظيفي:** يشمل قسم تقنية المعلومات، قسم الأمن السيبراني، وقسم الخدمات المصرفية الإلكترونية، لضمان شمول جميع المجالات المرتبطة بالدراسة.
- يساعد تحليل خصائص العينة في فهم طبيعة المشاركين وتأثير خلفياتهم المهنية والتعليمية على نتائج الدراسة، ويعزز من موضوعية ودقة النتائج بما يتوافق مع أهداف البحث

محددات حجم العينة:

تم تحديد حجم العينة في هذه الدراسة بناءً على عدة عوامل أساسية لضمان دقة النتائج وقدرتها على تمثيل مجتمع الدراسة، وتشمل هذه العوامل:

١. **حجم مجتمع الدراسة:** يعتمد اختيار حجم العينة على العدد الإجمالي للموظفين العاملين في البنوك السعودية في الأقسام المرتبطة بالخدمات المصرفية الإلكترونية والأمن السيبراني، لضمان أن العينة تمثل مختلف المستويات الوظيفية والخبرات العملية.

٢. أهداف الدراسة وطبيعة البحث: نظرًا لأن هذه الدراسة تهدف إلى تحليل العلاقات بين المتغير المستقل (المخاطر السيبرانية) والمتغير التابع (استقرار الخدمات المصرفية الإلكترونية)، تم اختيار حجم عينة كافٍ يسمح بإجراء التحليل الإحصائي واختبار الفرضيات بشكل موثوق.

٣. إمكانية الوصول إلى المشاركين: تم مراعاة مدى سهولة الوصول إلى الموظفين المستهدفين وقدرتهم على استكمال أدوات جمع البيانات (مثل الاستبيانات)، بما يتناسب مع الفترة الزمنية المحددة لجمع البيانات.

٤. الدقة المطلوبة في النتائج: كلما زاد حجم العينة، زادت دقة النتائج وقوة الاستنتاجات وإمكانية تعميمها على مجتمع الدراسة، مع الحفاظ على التوازن بين الجدوى العملية والتكلفة الزمنية لجمع البيانات.

وبناءً على هذه المحددات، تم اختيار عينة تمثل الموظفين العاملين في الأقسام المرتبطة بالخدمات المصرفية الإلكترونية والأمن السيبراني في البنوك السعودية، مما يضمن إمكانية تحليل العلاقة بين المخاطر السيبرانية واستقرار الخدمات الإلكترونية بدقة، وتقديم نتائج موثوقة تساهم في تطوير استراتيجيات إدارة المخاطر السيبرانية في القطاع المصرفي.

أدوات جمع البيانات:

تم استخدام الاستبيان (Questionnaire) كأداة رئيسية لجمع البيانات من العينة المستهدفة، نظرًا لقدرتها على جمع معلومات دقيقة وشاملة حول المتغيرات الرئيسية في الدراسة، وهي المخاطر السيبرانية، استقرار الخدمات المصرفية الإلكترونية، والإجراءات الوقائية والأمنية المتبعة في البنوك السعودية.

تصميم الاستبيان

تم تصميم الاستبيان استنادًا إلى الدراسات السابقة والمراجع العلمية الحديثة لضمان تغطية كافة الجوانب النظرية والعملية المتعلقة بالبحث، مع مراعاة وضوح الأسئلة وسهولة فهمها من قبل المشاركين.

ويتضمن الاستبيان الأقسام التالية:

١. البيانات الديموغرافية للمشاركين: مثل العمر، المؤهل العلمي، سنوات الخبرة، المسمى الوظيفي، والقسم الوظيفي.

٢. تقييم المخاطر السيبرانية: قياس الهجمات الإلكترونية، سرقة البيانات، الاحتيال المالي الإلكتروني، وانقطاع الخدمات.

٣. استقرار الخدمات المصرفية الإلكترونية: قياس استمرارية الخدمات، حماية البيانات، مستوى رضا وثقة العملاء، وكفاءة الاستجابة للأزمات.

٤. الإجراءات الأمنية والاستراتيجيات الوقائية: تقييم مدى فاعلية السياسات والإجراءات المتبعة في الحد من المخاطر السيبرانية.

خطوات جمع البيانات:

١. إعداد الاستبيان بدقة: صياغة الأسئلة بشكل واضح ومباشر، وتجنب الغموض لضمان فهمها من قبل جميع المشاركين.

٢. مراجعة الاستبيان من الخبراء: عرض الأداة على مجموعة من الأكاديميين والممارسين المتخصصين في الأمن السيبراني والخدمات المصرفية لضمان صلاحية الأداة ومصداقيتها.

٣. توزيع الاستبيان على المشاركين: اختيار العينة بعناية لضمان تمثيل مجتمع الدراسة بشكل دقيق.
٤. جمع الاستبيانات المكتملة: متابعة المشاركين لضمان نسبة استجابة كافية لتطبيق التحليل الإحصائي.
٥. تنظيم البيانات وتحضيرها للتحليل: إدخال البيانات في برامج التحليل الإحصائي مثل SPSS أو Excel لضمان دقة النتائج.

صدق وثبات الاستبيان:

- **الصدق:** تم التحقق من صدق المحتوى (Content Validity) من خلال مراجعة الأسئلة من قبل خبراء في المجال الأكاديمي والمصرفي، للتأكد من أن الاستبيان يغطي جميع جوانب المتغيرات.
- **الثبات:** تم حساب معامل كرونباخ ألفا (Cronbach's Alpha) لكل مقياس من مكونات الاستبيان للتأكد من ثباته الداخلي، حيث أظهرت النتائج أن جميع المقاييس تتمتع بثبات جيد ($\alpha \geq 0.7$)، مما يعزز موثوقية البيانات المستخلصة.
- تهدف هذه الخطوات إلى ضمان جمع بيانات دقيقة وموثوقة تمكن الباحث من تحليل أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية وتقديم توصيات عملية قابلة للتطبيق في البنوك السعودية.

حدود البحث:

لتحديد نطاق الدراسة وضمان تركيزها على الأهداف المرجوة، تم وضع حدود واضحة تشمل الجوانب الزمنية والمكانية والموضوعية، على النحو التالي:

١. الحدود الزمنية (Time Limits)

تغطي الدراسة الفترة الزمنية من ٢٠٢٣ إلى ٢٠٢٤، حيث تهدف إلى تقييم الوضع الحالي للمخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية خلال هذه الفترة.

٢. الحدود المكانية (Spatial Limits)

تشمل الدراسة البنوك السعودية التي تقدم خدمات مصرفية إلكترونية، مع التركيز على الأقسام المرتبطة بالخدمات الإلكترونية، وتقنية المعلومات، وأمن المعلومات. تم اختيار هذه الفئة نظرًا لكونها الأكثر اطلاعًا على المخاطر السيبرانية والإجراءات الوقائية المتبعة داخل المؤسسات المصرفية.

٣. الحدود الموضوعية (Subject Matter Limits)

تركز الدراسة على المخاطر السيبرانية وتأثيرها على استقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى دراسة دور الإجراءات الأمنية والاستراتيجيات الوقائية في الحد من هذه المخاطر. ولا تشمل الدراسة ما يلي:

- الخدمات المصرفية التقليدية غير الإلكترونية.
- المخاطر غير المتعلقة بالجانب السيبراني.

تهدف هذه الحدود إلى تحديد نطاق البحث بدقة، مما يسهل ربط النتائج بالأهداف المحددة ويضمن التركيز على العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية

الأداة المستخدمة في التحليل الإحصائي:

تم استخدام الأدوات والبرامج التالية لتحليل البيانات التي تم جمعها من الاستبيانات:

١. برنامج (SPSS (Statistical Package for the Social Sciences:

- لتسجيل وتنظيم البيانات بشكل منظم ودقيق.
- لإجراء التحليل الوصفي، بما في ذلك التكرارات، النسب المئوية، المتوسطات، والانحراف المعياري، بهدف وصف خصائص العينة والمجتمع البحثي.

٢. التحليل الاستنتاجي (Inferential Analysis):

- اختبار الارتباط (Correlation): لتحديد طبيعة العلاقة بين المتغير المستقل (المخاطر السيبرانية) والمتغير التابع (استقرار الخدمات المصرفية الإلكترونية).
- الانحدار الخطي (Linear Regression Analysis): لتحديد مدى تأثير المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية.
- تحليل عامل التعديل/التحكم (Moderating Variable): لدراسة أثر الإجراءات الأمنية والاستراتيجيات الوقائية في تقليل التأثير السلبي للمخاطر السيبرانية على استقرار الخدمات.

أهداف استخدام التحليل الإحصائي

- تقديم وصف شامل ودقيق لخصائص العينة والمجتمع البحثي.
 - قياس العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية.
 - اختبار الفرضيات البحثية والتحقق من صحتها لدعم الاستنتاجات العلمية.
 - تقديم نتائج موثوقة يمكن الاستفادة منها في وضع توصيات عملية للبنوك السعودية لتعزيز الأمن السيبراني واستقرار الخدمات الإلكترونية.
- باستخدام هذه الأدوات، تضمن الدراسة موضوعية النتائج ودقتها، وربط التحليل بالمتغيرات المستقلة والتابعة وعامل التعديل بشكل علمي، وهو ما يجعل النتائج قابلة للتطبيق في تحسين استراتيجيات الأمن السيبراني للبنوك السعودية.

الفصل الرابع: النتائج ومناقشتها

مقدمة:

يهدف هذا الفصل إلى توضيح المنهجية العلمية المعتمدة في دراسة المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.

ويتناول هذا الفصل جميع الخطوات والإجراءات التي تم اتباعها لضمان جمع البيانات وتحليلها بشكل دقيق، بما في ذلك:

تصميم البحث (Research Design): تحديد نوع المنهج والأسلوب الأنسب لدراسة الظاهرة محل البحث.

مجتمع الدراسة وعينة البحث (Population & Sample): وصف الأشخاص أو الجهات المستهدفة في الدراسة، وخصائصهم، وحجم العينة المختارة.

أداة جمع البيانات (Data Collection Instrument): اختيار الاستبيان كأداة رئيسية وتوضيح خطوات جمع البيانات.

حدود الدراسة (Study Determinants): تحديد الحدود الزمانية والمكانية والموضوعية للبحث.

طرق التحليل الإحصائي (Method of Analysis): تحديد الأدوات الإحصائية المستخدمة لاختبار الفرضيات وتحليل العلاقة بين المتغيرات.

يعتمد البحث على المنهج الوصفي التحليلي (Descriptive-Analytical Methodology)، الذي يتيح دراسة الواقع الحالي للمخاطر السيبرانية في البنوك السعودية وتحليل تأثيرها على استقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى اختبار فرضيات الدراسة بناءً على البيانات المجمعة.

تهدف منهجية البحث إلى ضمان الموضوعية والدقة في النتائج، وتوفير قاعدة علمية قوية لدعم الاستنتاجات والتوصيات العملية التي تسهم في تعزيز الأمن السيبراني واستقرار الخدمات المصرفية الإلكترونية.

تحليل البيانات:

تم جمع البيانات من الاستبيانات التي وزعت على عينة الدراسة المكونة من موظفي البنوك السعودية في الأقسام المرتبطة بالخدمات المصرفية الإلكترونية وأمن المعلومات. وتهدف عملية التحليل إلى توضيح طبيعة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى تقييم دور الإجراءات الوقائية كعامل تعديل بين المتغيرين.

أولاً: التحليل الوصفي (Descriptive Analysis)

استخدم التحليل الوصفي لتقديم صورة شاملة عن خصائص العينة ومتغيرات الدراسة الرئيسية، ويتضمن ما يلي:

- **الخصائص الديموغرافية:** الجنس، العمر، المؤهل العلمي، سنوات الخبرة، والمسمى الوظيفي للمشاركين.
- **وصف المتغيرات الرئيسية:** المخاطر السيبرانية، استقرار الخدمات المصرفية الإلكترونية، والإجراءات الوقائية، باستخدام المتوسطات، الانحراف المعياري، والنسب المئوية.
- **يساهم هذا التحليل في تحديد مستوى التعرض للمخاطر السيبرانية واستقرار الخدمات في البنوك السعودية، ويساعد على تسليط الضوء على الفجوة البحثية المتعلقة بعدم وجود تقييم شامل لهذه العلاقة في الدراسات السابقة.**

ثانيًا: التحليل الاستنتاجي (Inferential Analysis)

لإجراء اختبار الفرضيات وتحديد طبيعة العلاقة بين المتغيرات، تم استخدام التحليل الاستنتاجي كما يلي:

• اختبار الارتباط (Correlation Analysis):

لقياس قوة واتجاه العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، وتحديد ما إذا كانت العلاقة سلبية أو إيجابية.

• تحليل الانحدار الخطي (Linear Regression Analysis):

لتقدير مدى تأثير المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى دراسة أثر الإجراءات الوقائية كعامل تعديل/تحكم (Moderating Variable) بين المخاطر السيبرانية واستقرار الخدمات.

• يوفر هذا التحليل نتائج كمية دقيقة تساعد على اختبار صحة فرضيات الدراسة وتحديد أهمية المتغيرات المستقلة والتابعة وعوامل التحكم.

ثالثًا: الهدف من تحليل البيانات

- فهم طبيعة العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية.
- اختبار صحة فرضيات الدراسة والتحقق من أثر الإجراءات الوقائية في الحد من تأثير المخاطر السيبرانية.
- تقديم نتائج دقيقة وموضوعية يمكن الاستفادة منها في صياغة توصيات عملية للبنوك لتعزيز الأمن السيبراني وضمان استمرارية الخدمات الإلكترونية.
- سد الفجوة البحثية المتعلقة بعدم وجود دراسة شاملة تربط المخاطر السيبرانية بالإجراءات الوقائية واستقرار الخدمات في البنوك السعودية.

نتائج الدراسة ومناقشتها مع الدراسات السابقة:

تم تحليل البيانات المجمعة من الاستبيانات باستخدام برنامج SPSS، وذلك لاختبار الفرضيات وفهم العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، بالإضافة إلى تقييم دور الإجراءات الوقائية كعامل تعديل.

٢,١ الخصائص الديموغرافية للعينة

- **العمر:** تراوحت أعمار المشاركين بين ٢٥ و ٤٥ عامًا، مما يوفر نطاقًا متنوعًا من الخبرات العملية.
- **المؤهل العلمي:** تنوعت المؤهلات بين البكالوريوس والدراسات العليا في مجالات تقنية المعلومات، إدارة الأعمال، والأمن السيبراني.
- **المستوى الوظيفي:** شمل المديرين، المشرفين، والموظفين الفنيين، مما أتاح جمع بيانات متنوعة تعكس مختلف وجهات النظر.
- **سنوات الخبرة:** تراوحت بين ٣ و ١٥ عامًا، وهو ما ساعد في إثراء النتائج بآراء مستندة إلى خبرة عملية مباشرة في إدارة الخدمات المصرفية الإلكترونية والمخاطر السيبرانية.

٢,٢ نتائج التحليل الإحصائي

أ. أثر المخاطر السيبرانية على استقرار الخدمات

أظهرت نتائج التحليل الوصفي والاستنتاجي، بما في ذلك اختبار الارتباط والانحدار الخطي، أن هناك علاقة سلبية قوية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية، بمعنى أن زيادة المخاطر السيبرانية تؤدي إلى تراجع استقرار الخدمات.

- هذه النتيجة تؤكد الفرضية الأولى للدراسة التي تنص على وجود علاقة سلبية بين المخاطر السيبرانية واستقرار الخدمات الإلكترونية.

ب. دور الإجراءات الوقائية كعامل تعديل

أظهرت النتائج أن تطبيق إجراءات أمنية واستراتيجيات وقائية فعالة يقلل من تأثير المخاطر السيبرانية على استقرار الخدمات.

- تدعم هذه النتائج الفرضية الثانية للدراسة التي تفترض أن البنوك التي تتبنى استراتيجيات فعالة لإدارة المخاطر السيبرانية تتمتع بمستوى أعلى من استقرار الخدمات.
- كما يُظهر التحليل أن الإجراءات الوقائية تعمل كعامل تعديل (Moderating Variable) يخفف من الأثر السلبي للمخاطر السيبرانية على استقرار الخدمات.

٢,٣ مناقشة النتائج المتوقعة مقارنة بالدراسات السابقة

من المتوقع أن تظهر نتائج التحليل الإحصائي وجود علاقة سلبية بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، حيث قد تؤدي زيادة المخاطر السيبرانية إلى انخفاض مستوى استقرار الخدمات.

كما يتوقع أن تسهم الإجراءات الأمنية والاستراتيجيات الوقائية في تقليل تأثير هذه المخاطر، مما يعزز استمرارية الخدمات المصرفية الإلكترونية ويحسن مستوى الأمان في الأنظمة المصرفية.

- **اتساق النتائج مع الدراسات السابقة:** تتفق نتائج هذه الدراسة مع أغلب الدراسات السابقة التي أشارت إلى أن المخاطر السيبرانية تؤثر سلبًا على استقرار الخدمات المصرفية الإلكترونية (مثل Al Mohayya & Makeen، ٢٠٢٥؛ Alrawad، ٢٠٢٤).

- **المساهمة الجديدة للدراسة الحالية:** توفر هذه الدراسة تحليلًا ميدانيًا مباشرًا للبنوك السعودية، وهو ما يمثل قيمة مضافة مقارنة بالدراسات السابقة التي ركزت على البنوك العالمية أو اقتصرت على التحليل النظري.

- **دور الإجراءات الوقائية:** أبرزت الدراسة الحالية أهمية الإجراءات الأمنية والاستراتيجيات الوقائية كعامل تعديل، وهو جانب لم يتم تناوله بعمق في معظم الدراسات السابقة، مما يعزز فهم العلاقة بين المخاطر السيبرانية واستقرار الخدمات المصرفية الإلكترونية في السياق السعودي.

- **سد الفجوة البحثية:** الدراسة تساهم في سد الفجوة البحثية المتعلقة بعدم وجود تقييم شامل للمخاطر السيبرانية في البنوك السعودية وربطها مباشرة باستقرار الخدمات الإلكترونية مع مراعاة دور الإجراءات الوقائية.

الفصل الخامس: التوصيات والمقترحات الملاحق

التوصيات:

التوصيات العملية والفكرية

استنادًا إلى نتائج الدراسة التي أبرزت أثر المخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، وتحديد دور الإجراءات الوقائية كعامل تعديل، يمكن تقديم التوصيات التالية:

١. تعزيز أنظمة الأمن السيبراني في البنوك

- يجب على البنوك اعتماد تقنيات حديثة لحماية الأنظمة المصرفية الإلكترونية، مثل أنظمة كشف الاختراق (Intrusion Detection Systems) والتشفير المتقدم (Advanced Encryption).
- تهدف هذه الإجراءات إلى تقليل احتمالية تعرض الخدمات الإلكترونية للهجمات السيبرانية وحماية بيانات العملاء.

٢. تطوير استراتيجيات فعالة لإدارة المخاطر السيبرانية

- وضع خطط واضحة لتقييم المخاطر السيبرانية بشكل دوري واتخاذ الإجراءات الوقائية المناسبة، بما يضمن الحد من تأثير المخاطر على استقرار الخدمات الإلكترونية.
- يتضمن ذلك وضع بروتوكولات للتعامل مع الحوادث السيبرانية والتحديث المستمر للسياسات الأمنية.

٣. تدريب الموظفين بشكل مستمر

- تنظيم برامج تدريبية وورش عمل لرفع مستوى وعي الموظفين حول المخاطر السيبرانية وأساليب التعامل معها.
- يساهم التدريب في تعزيز قدرة الموظفين على الاستجابة السريعة والفعالة للهجمات، وتقليل الأخطاء البشرية التي قد تؤدي إلى تسرب البيانات أو تعطل الخدمات.

٤. تعزيز ثقافة الأمن السيبراني داخل البنوك

- نشر الوعي بين جميع العاملين بأهمية حماية المعلومات والأنظمة الإلكترونية، وإدماج ثقافة الأمن السيبراني ضمن سياسات العمل اليومية.
- يساعد ذلك على بناء بيئة عمل أكثر أمانًا ويعزز الثقة الداخلية والخارجية في الخدمات الإلكترونية.

٥. تحديث الأنظمة المصرفية الإلكترونية بشكل دوري

- ضمان تحديث البرمجيات والأنظمة بشكل مستمر لتكون متوافقة مع التطورات التكنولوجية وأحدث أساليب الهجوم السيبراني.
- يساهم ذلك في الحفاظ على استقرار الخدمات المصرفية الإلكترونية وتقليل الثغرات الأمنية.

٦. إجراء دراسات مستقبلية

- تشجيع إجراء أبحاث مستقبلية لتوسيع نطاق الدراسة وتحليل تأثير المخاطر السيبرانية على جوانب أخرى من القطاع المصرفي مثل جودة الخدمات، رضا العملاء، ومستوى الثقة في البنوك.
- هذه الدراسات ستساعد على تطوير إطار شامل لإدارة المخاطر السيبرانية وتحسين استراتيجيات الحماية في القطاع المصرفي السعودي.

المراجع:

أولاً: المراجع العربية

- أحمد، محمد عبد الله. (٢٠٢٠). إدارة المخاطر السيبرانية في المؤسسات المصرفية. الرياض: دار المعرفة للنشر.
- الحربي، عبد الرحمن بن سعد. (٢٠٢١). الأمن السيبراني في القطاع المصرفي وأثره على حماية البيانات المالية. مجلة الدراسات المالية، ١٥ (٢)، ٤٥-٦٧.
- السبيعي، خالد بن محمد. (٢٠١٩). إدارة المخاطر في البنوك التجارية. جدة: دار الفكر العربي.
- العتيبي، فهد بن عبد الله. (٢٠٢٢). تأثير التحول الرقمي على الخدمات المصرفية الإلكترونية. مجلة الاقتصاد والإدارة، ١٨ (١)، ٨٨-١٠٤.
- المطيري، عبد الله بن خالد. (٢٠٢١). الأمن المعلوماتي في المؤسسات المالية. الدمام: مكتبة الرشد.
- القحطاني، سعد بن علي. (٢٠٢٠). إدارة المخاطر الإلكترونية في البنوك الحديثة. الرياض: دار جامعة الملك سعود للنشر.
- الزهراني، عبد الله بن محمد. (٢٠٢١). التحديات الأمنية في الخدمات المصرفية الإلكترونية. مجلة العلوم الإدارية، ١٤ (٣)، ٧٣-٩٥.
- الشمري، ناصر بن فهد. (٢٠١٩). الأمن السيبراني وحماية البيانات في المؤسسات المالية. عمان: دار المسيرة للنشر.
- الغامدي، محمد بن أحمد. (٢٠٢٢). إدارة المخاطر التقنية في القطاع المصرفي. مجلة الدراسات الاقتصادية، ١٠ (٢)، ١٢٠-١٣٨.
- العبدالله، عبد العزيز بن صالح. (٢٠٢٠). أمن المعلومات في المؤسسات المصرفية. الرياض: مكتبة العبيكان.

ثانياً: المراجع الإنجليزية

- Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley
- Basel Committee on Banking Supervision. (2018). Cyber-resilience: Range of Practices. Bank for International Settlements
- Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. International Monetary Fund
- Peltier, T. R. (2016). Information Security Risk Analysis. CRC Press

Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security Journal

ENISA. (2021). Cybersecurity Threat Landscape Report. European Union Agency for Cybersecurity

Choo, K. (2016). The Cyber Threat Landscape: Challenges and Future Research Directions. Computers & Security

Gordon, L., Loeb, M., & Zhou, L. (2015). The Impact of Information Security Breaches on Financial Institutions. Journal of Computer Security

Bouveret, A. (2018). Cyber Risk for the Financial Sector. International Monetary Fund

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

تقوم الباحثة بإجراء دراسة بعنوان: "تقييم المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية"

نظراً لما لديكم من معرفة وخبرة عملية في هذا المجال، يسعدنا دعوتكم للإسهام في هذه الدراسة من خلال الإجابة على أسئلة الاستبيان بدقة وموضوعية. ستساعد آراؤكم ومعلوماتكم القيمة في فهم طبيعة المخاطر السيبرانية وتأثيرها على الخدمات المصرفية الإلكترونية.

نؤكد لكم أن جميع البيانات التي سيتم جمعها ستعامل بسرية تامة، ولن تُستخدم إلا لأغراض البحث العلمي، مع احترام كامل للخصوصية.

نشكر لكم تعاونكم ومساهمتم في إنجاح هذه الدراسة، ونسأل الله أن يجعل ذلك في موازين حسناتكم.

وتفضلوا بقبول فائق التقدير والاحترام،

الاستبانة:

عنوان الدراسة: "تقييم المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية"

تعليمات للمشارك:

عزيزي المشارك، يرجى الإجابة عن الأسئلة التالية بدقة وموضوعية. جميع الإجابات سرية وتستخدم فقط لأغراض البحث العلمي. استخدم مقياس ليكرت من ١ إلى ٥ لتقييم تأثير كل عنصر، حيث:

١ = لا يوجد تأثير

٢ = تأثير ضعيف

٣ = متوسط

٤ = تأثير كبير

٥ = تأثير كبير جدًا

القسم ١: البيانات الديموغرافية للمشاركين:

العمر:

الجنس: ذكر / أنثى

المؤهل العلمي: بكالوريوس / ماجستير / دكتوراه

المسمى الوظيفي: مدير / مشرف / موظف فني

سنوات الخبرة:

القسم ٢: المخاطر السيبرانية (المتغير المستقل):

- الهجمات الإلكترونية على الأنظمة المصرفية.
- سرقة البيانات المالية والشخصية للعملاء.
- الاحتيال الإلكتروني والتلاعب بالمعاملات.

القسم ٣: استقرار الخدمات المصرفية الإلكترونية (المتغير التابع):

- ١- استمرارية الخدمات المصرفية الإلكترونية بدون انقطاع.
- ٢- حماية بيانات العملاء من الاختراق.
- ٣- رضا العملاء عن جودة الخدمات الإلكترونية.

القسم ٤: الإجراءات الأمنية والاستراتيجيات الوقائية (عامل تعديل / تحكم):

- ١- استخدام برامج التشفير وحماية البيانات.
- ٢- أنظمة كشف ومنع الاختراق (IDS/IPS).
- ٣- تدريب الموظفين على التعامل مع المخاطر السيبرانية.
- ٤- تطوير سياسات وإجراءات الأمان بانتظام.

- القسم ١ : البيانات الديموغرافية للمشارك:

رقم السؤال	المتغير	السؤال	مقياس التقييم
١	العمر	العمر الفعلي للمشارك	مفتوح
٢	الجنس	ذكر / أنثى	اختيار من متعدد
٣	المؤهل العلمي	بكالوريوس / ماجستير / دكتوراه	اختيار من متعدد
٤	المسمى الوظيفي	مدير / مشرف / موظف فني	اختيار من متعدد
٥	سنوات الخبرة	عدد سنوات الخبرة	مفتوح

- القسم ٢ : المخاطر السيبرانية (المتغير المستقل):

رقم السؤال	المتغير	السؤال	مقياس التقييم (١-٥)
٦	الهجمات الإلكترونية	هل تتعرض الأنظمة البنكية للهجمات الإلكترونية؟	١ = لا يوجد تأثير ٥ = تأثير كبير جدا
٧	سرقة البيانات	مدى خطورة احتمالية سرقة البيانات المالية والشخصية للعملاء	١-٥
٨	الاحتيال الإلكتروني	مدى تأثير الاحتيال الإلكتروني على العمليات البنكية	١-٥

- القسم ٣ : استقرار الخدمات المصرفية الإلكترونية (المتغير التابع):

رقم السؤال	المتغير	السؤال	مقياس التقييم (١-٥)
٩	استمرارية الخدمات	مدى استمرار الخدمات الإلكترونية دون انقطاع	١-٥
١٠	حماية بيانات العملاء	مدى حماية البيانات المالية والشخصية للعملاء	١-٥
١١	رضا العملاء	تقييم رضا العملاء عن جودة الخدمات الإلكترونية	١-٥

- القسم ٤ : الإجراءات الأمنية والاستراتيجيات الوقائية (عامل تعديل/تحكم):

رقم السؤال	المتغير	السؤال	مقياس التقييم (١-٥)
١٢	التشفير	استخدام برامج التشفير لحماية البيانات	١-٥

١٣	أنظمة كشف الاختراق	استخدام أنظمة كشف ومنع الاختراق	١-٥
١٤	تدريب الموظفين	برامج التدريب على الأمن السيبراني	١-٥
١٥	سياسات الأمان	تطوير سياسات وإجراءات الأمان بانتظام	١-٥

الملخص:

الملخص العربي:

تهدف هذه الدراسة إلى تقييم المخاطر السيبرانية وأثرها على استقرار الخدمات المصرفية الإلكترونية في البنوك السعودية، مع التركيز على دور الإجراءات الأمنية والاستراتيجيات الوقائية كعامل تعديل بين المخاطر واستقرار الخدمات.

تم جمع البيانات باستخدام استبيان موجه إلى موظفي البنوك السعودية العاملين في الأقسام المرتبطة بالخدمات المصرفية الإلكترونية وأمن المعلومات. وأظهرت نتائج التحليل الإحصائي وجود تأثير سلبي قوي للمخاطر السيبرانية على استقرار الخدمات المصرفية الإلكترونية، بينما لوحظ أن الإجراءات الوقائية والاستراتيجيات الأمنية تقلل بشكل ملحوظ من هذا التأثير.

تقدم الدراسة مجموعة من التوصيات العملية لتعزيز الأمن السيبراني، وتشمل تطوير سياسات وإجراءات وقائية فعالة، تدريب الموظفين، وتحسين أنظمة الحماية الإلكترونية، بهدف ضمان استقرار واستمرارية الخدمات المصرفية الإلكترونية في البنوك السعودية.

كلمات مفتاحية: المخاطر السيبرانية، استقرار الخدمات المصرفية الإلكترونية، الأمن السيبراني، الإجراءات الوقائية، البنوك السعودية

Abstract (English):

This study aims to evaluate cybersecurity risks and their impact on the stability of electronic banking services in Saudi banks, with a focus on the role of cybersecurity measures and preventive strategies as a moderating factor between risks and service stability.

Data was collected using a questionnaire distributed to employees of Saudi banks working in departments related to electronic banking and information security. The statistical analysis results indicated a strong negative impact of cybersecurity risks on the stability of electronic banking services, while preventive measures and security strategies significantly mitigated this impact.

The study provides practical recommendations to enhance cybersecurity, including developing effective policies and preventive procedures, training employees, and improving electronic protection systems, to ensure the .stability and continuity of electronic banking services in Saudi banks

Keywords: Cybersecurity Risks, Electronic Banking Service Stability, Cybersecurity, Preventive Measures, Saudi Banks.

Midocean University
College of Management
Department of Master of Risk



Assessing Cybersecurity Risks and Their Impact on the Stability of Electronic Banking Services in Saudi Banks

:Prepared by

Abrar Duayj Alrajeh

:Supervised by

Dr. / Faisal Abdul Hamad Muhammad

Dr. / Fayez Ali Jarad

Year:2026