

عنوان البحث

إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية

إعداد الطالب/

أحمد سعد آل تركي

إشراف/

د. الفیصل عبد الحمید

د. فايز جراد

العام الدراسي:

2025

مقدمة:

في عصر التحول الرقمي الذي تشهده مختلف القطاعات في العالم، يواجه القطاع المصرفي تحديات جديدة تتمثل في إدارة المخاطر الرقمية. فالانتقال السريع من الأنظمة التقليدية إلى الأنظمة الرقمية قد جلب معه العديد من الفوائد من حيث التحسينات في الكفاءة وسهولة الوصول إلى الخدمات، ولكنه في الوقت نفسه قدم مخاطر جديدة تهدد الأمن السيبراني، وخصوصية البيانات، والاستقرار المالي للبنوك.

المخاطر الرقمية في البنوك تشمل مجموعة من التهديدات التي قد تؤثر على سلامة الأنظمة المصرفية، مثل الهجمات السيبرانية، الاحتيال الإلكتروني، مخاطر البرمجيات الضارة، فقدان البيانات، والتهديدات الموجهة عبر الإنترنت. وقد زادت هذه المخاطر بشكل كبير في السنوات الأخيرة نتيجة لتزايد الاعتماد على التكنولوجيا الحديثة مثل التطبيقات المصرفية عبر الإنترنت، الأنظمة السحابية، وخدمات الدفع الإلكتروني.

، تشهد تحولاً رقمياً كبيراً في جميع قطاعاتها، بما في ذلك القطاع 2030 المملكة العربية السعودية، ومن خلال رؤية المصرفي. هذا التحول يعكس تطوراً إيجابياً نحو الرقمنة والابتكار في تقديم الخدمات المالية. ومع ذلك، فإن هذا التحول السريع يثير العديد من التحديات في مجال إدارة المخاطر الرقمية. فقد أظهرت العديد من التقارير أن البنوك السعودية تواجه تهديدات متزايدة من الهجمات الإلكترونية، ما يطرح تساؤلات حول كيفية إدارة هذه المخاطر وكيفية تعزيز أمن المعلومات داخل المؤسسات المصرفية.

تتجه البنوك السعودية بشكل متسارع نحو تحديث أنظمتها الرقمية لزيادة الكفاءة وتلبية احتياجات العملاء، إلا أن هذه الأنظمة تفتح المجال لظهور العديد من المخاطر الأمنية والرقمية. لذلك، أصبح من الضروري إدارة هذه المخاطر بشكل منهجي وفعل لضمان استقرار البنوك وحمايتها من أي تهديدات قد تؤثر على ثقة العملاء أو سلامة العمليات المصرفية.

تهدف هذه الدراسة إلى تحليل أساليب إدارة المخاطر الرقمية في البنوك السعودية، والتعرف على التحديات التي تواجهها هذه البنوك في مواجهة المخاطر الرقمية، بالإضافة إلى دراسة الاستراتيجيات والتقنيات المستخدمة لتقليل هذه المخاطر. كما تهدف الدراسة إلى تقديم توصيات للبنوك السعودية حول كيفية تحسين آليات إدارة المخاطر الرقمية في المستقبل.

تعد هذه الدراسة ذات أهمية خاصة في ظل البيئة المتغيرة للمخاطر الرقمية التي قد تؤثر على استقرار النظام المصرفي السعودي. إن تحليل الطرق المتبعة حالياً من قبل البنوك في إدارة هذه المخاطر يمكن أن يساعد في تطوير استراتيجيات أكثر فعالية، وبالتالي يساهم في تعزيز الثقة بين البنوك والعملاء، ويسهم في تحقيق أهداف التحول الرقمي في المملكة.

مشكلة الدراسة:

تعتبر إدارة المخاطر الرقمية في البنوك من القضايا الحيوية التي تزداد أهمية مع تزايد الاعتماد على التكنولوجيا الحديثة في القطاع المصرفي، خاصة في ظل التحول الرقمي الذي تشهده المملكة العربية السعودية. فعلى الرغم من أن الرقمنة توفر العديد من الفرص لتحسين كفاءة الخدمات المصرفية، فإنها تفتح الباب أيضاً لظهور العديد من المخاطر الرقمية التي يمكن أن تؤثر بشكل كبير على أمن المعاملات وسلامة البيانات واستقرار المؤسسات المالية.

تتمثل مشكلة الدراسة في تزايد المخاطر الرقمية التي تواجهها البنوك السعودية نتيجة للاعتماد الكبير على الأنظمة الرقمية، مثل التطبيقات المصرفية عبر الإنترنت، الأنظمة السحابية، وخدمات الدفع الإلكتروني. مع تسارع التحول الرقمي في المملكة العربية السعودية، أصبحت البنوك تواجه تحديات جديدة في إدارة هذه المخاطر بشكل فعال، مما يزيد من تعرضها للتهديدات مثل الهجمات السيبرانية، الاحتيال الإلكتروني، البرمجيات الضارة، وفقدان البيانات.

على الرغم من جهود البنوك السعودية لتحسين مستوى الأمان الرقمي واعتماد بعض التقنيات الحديثة لمواجهة هذه التهديدات، إلا أن هناك العديد من الأسئلة التي تظل قائمة حول فعالية هذه

السياسات والإجراءات في مواجهة المخاطر المتزايدة. ففي الوقت الذي تشهد فيه البنوك نمواً في عدد الهجمات السيبرانية والتهديدات الإلكترونية، لا تزال استراتيجيات إدارة المخاطر في بعض المؤسسات المالية بحاجة إلى تطوير مستمر لتتناسب مع التغيرات السريعة في التكنولوجيا وظهور تهديدات جديدة.

بناءً على ما سبق، تتمثل مشكلة الدراسة في التحديات التي تواجهها البنوك السعودية في إدارة المخاطر الرقمية والتقنيات والاستراتيجيات المتبعة لمواجهة هذه المخاطر. كما أن هناك حاجة ماسة لتقييم فعالية هذه الاستراتيجيات في الحد من التأثيرات السلبية التي قد تنتج عنها. في هذا السياق، تُطرح أسئلة أساسية تتعلق بكيفية التعامل مع المخاطر الرقمية في البنوك، مثل:

- ما هي أبرز المخاطر الرقمية التي تواجهها البنوك السعودية؟
- كيف يمكن تحسين استراتيجيات إدارة المخاطر الرقمية في البنوك السعودية؟
- هل التقنيات المتبعة في الوقت الحالي كافية للحد من هذه المخاطر؟
- ما هو أثر إدارة المخاطر الرقمية على استقرار البنوك وسمعتها؟

أهمية الدراسة:

تكتسب دراسة إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية أهمية كبيرة في ظل التطور التكنولوجي السريع والتحول الرقمي الذي يشهده القطاع المصرفي في المملكة. في السنوات الأخيرة، أصبح القطاع المصرفي في السعودية يعتمد بشكل متزايد على التكنولوجيا الرقمية لتقديم خدمات مصرفية مبتكرة، مما يعزز من كفاءة العمليات ويسهم في تحسين تجربة العملاء. إلا أن هذه التطورات تأتي مع تحديات كبيرة تتعلق بإدارة المخاطر الرقمية التي تهدد الأمان السيبراني، سلامة البيانات، واستقرار المؤسسات المالية.

1. أهمية الدراسة للقطاع المصرفي السعودي:

- تحليل المخاطر الرقمية: توفر هذه الدراسة إطاراً شاملاً لتحليل المخاطر الرقمية التي تواجه البنوك في السعودية، مثل التهديدات السيبرانية، الاحتيال الإلكتروني، الهجمات عبر الإنترنت، وفقدان البيانات. مما يساعد البنوك على تحديد أولوياتها في مجال إدارة المخاطر بشكل أكثر دقة وفاعلية.

- تحسين استراتيجيات الإدارة: من خلال الدراسة، يمكن تقديم توصيات عملية لتحسين استراتيجيات إدارة المخاطر الرقمية في البنوك السعودية، مما يسهم في تحسين فعالية الإجراءات المتبعة للتعامل مع المخاطر.

2. أهمية الدراسة للمساهمة في تحقيق أهداف رؤية 2030:

- رؤية 2030 في المملكة العربية السعودية تركز على التطوير الرقمي وتعزيز الابتكار في كافة القطاعات، بما في ذلك القطاع المصرفي. إن تحقيق الأمان الرقمي في البنوك يعد أحد الأبعاد الرئيسية لتحقيق هذه الرؤية، حيث إن ضمان استقرار النظام المصرفي السعودي وحمايته من المخاطر الرقمية يشكل جزءاً من الاستقرار المالي والاقتصادي للبلاد.

- تقدم هذه الدراسة أيضًا أداة تحليلية تساعد في دعم المبادرات الحكومية لتشجيع التحول الرقمي في القطاع المالي، بما يتماشى مع التوجهات الوطنية لتعزيز الثقة في النظام المالي الرقمي.

3- أهمية الدراسة للباحثين والممارسين في مجال الأمن السيبراني:

- توفر هذه الدراسة قاعدة معرفية شاملة لفهم التحديات المرتبطة بإدارة المخاطر الرقمية في القطاع المصرفي، مما يعزز من قدرة المتخصصين في الأمن السيبراني على تطوير تقنيات وحلول مبتكرة للحد من هذه المخاطر.

- استراتيجيات الوقاية من المخاطر التي سنتناولها الدراسة قد تساعد الباحثين والممارسين على تحسين الأدوات والأساليب المتبعة في المؤسسات المالية.

3. أهمية الدراسة في تحسين الثقة بين العملاء والبنوك:

- في عصر التكنولوجيا الرقمية، العملاء يتوقعون من البنوك تأمين بياناتهم المالية وحمايتهم من أي تهديدات أو اختراقات. دراسة إدارة المخاطر الرقمية تساهم في تحسين الإجراءات المتبعة لتعزيز ثقة العملاء، مما يساهم بدوره في زيادة الاستقرار المالي في البنوك.

- من خلال تقليل المخاطر الرقمية، تصبح البنوك أكثر قدرة على تقديم خدمات مالية مبتكرة وآمنة، مما يحفز الاستثمار ويعزز النمو الاقتصادي.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف التي تساعد في فهم وتحليل إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية، وكذلك تقديم حلول واستراتيجيات لتقليل هذه المخاطر. وفيما يلي الأهداف الرئيسية التي تسعى الدراسة إلى تحقيقها:

- تحليل المخاطر الرقمية التي تواجه البنوك السعودية:
- دراسة وتحديد أنواع المخاطر الرقمية التي تواجه البنوك في المملكة العربية السعودية، مثل التهديدات السيبرانية، الهجمات الإلكترونية، الاحتيال الإلكتروني، فقدان البيانات، البرمجيات الضارة، وغيرها من المخاطر التي تهدد النظام المصرفي.
- فهم أسباب ظهور هذه المخاطر وكيفية تأثيرها على العمليات المصرفية اليومية في البنوك السعودية.
- دراسة استراتيجيات إدارة المخاطر الرقمية المتبعة في البنوك السعودية:
- تحليل الأدوات والأساليب التي تستخدمها البنوك السعودية في إدارة المخاطر الرقمية، بما في ذلك أنظمة الأمن السيبراني، التقنيات الحديثة مثل الذكاء الاصطناعي والتعلم الآلي، وأدوات التحليل البياني.
- تقييم مدى فاعلية وتكامل هذه الاستراتيجيات في التصدي للمخاطر الرقمية.
- تحديد التحديات التي تواجه البنوك السعودية في إدارة المخاطر الرقمية:
- تحليل التحديات الرئيسية التي تواجه البنوك السعودية في تطبيق استراتيجيات إدارة المخاطر الرقمية، مثل نقص الخبرات التقنية، ضعف الوعي الأمني، التحديات القانونية والتنظيمية، والتكلفة المرتفعة.

- دراسة تأثير هذه التحديات على قدرة البنوك على مواجهة المخاطر الرقمية بشكل فعال.
- تقديم توصيات لتحسين استراتيجيات إدارة المخاطر الرقمية في البنوك السعودية:
- اقتراح حلول عملية لتحسين أنظمة الأمان وإدارة المخاطر في البنوك السعودية، بما في ذلك استخدام تقنيات حديثة مثل التشفير، الحوسبة السحابية الآمنة، تحليل البيانات الكبيرة، والذكاء الاصطناعي.
- تقديم توصيات حول رفع الوعي لدى موظفي البنوك والعملاء فيما يتعلق بالمخاطر الرقمية وكيفية الحد من تأثيرها.
- دراسة تأثير المخاطر الرقمية على سمعة البنوك واستقرار النظام المصرفي في المملكة:
- تحليل العلاقة بين إدارة المخاطر الرقمية و الثقة التي يوليها العملاء للبنوك، وكيفية تأثير الفشل في إدارة المخاطر الرقمية على سمعة البنك واستقراره المالي.
- دراسة كيفية تأثير الحوادث الأمنية والاختراقات الرقمية على الاستقرار المالي للقطاع المصرفي السعودي.
- مقارنة ممارسات إدارة المخاطر الرقمية في البنوك السعودية مع البنوك الدولية:
- مقارنة استراتيجيات إدارة المخاطر في البنوك السعودية مع الممارسات الدولية في دول أخرى مثل الولايات المتحدة، أوروبا، ودول الخليج.
- الاستفادة من أفضل الممارسات التي يمكن تبنيها من قبل البنوك السعودية لتحسين استراتيجياتها في مجال الأمن الرقمي.
- استشراف التوجهات المستقبلية في إدارة المخاطر الرقمية في البنوك السعودية:
- تحليل الاتجاهات المستقبلية في مجال إدارة المخاطر الرقمية والتقنيات الحديثة التي قد تسهم في تحسين الأمان الرقمي في البنوك، مثل تقنيات التعلم الآلي، البلوك تشين، و الذكاء الاصطناعي.
- دراسة كيفية تكيف البنوك السعودية مع هذه التوجهات المستقبلية لمواجهة المخاطر الرقمية بشكل أكثر فعالية.

تساؤلات الدراسة

تتمحور تساؤلات هذه الدراسة حول فهم المخاطر الرقمية التي تواجه البنوك السعودية، وكيفية إدارتها والتعامل معها. كما تهدف الدراسة إلى استكشاف التحديات والفرص في هذا المجال، وتقديم حلول عملية لتحسين الأداء الرقمي في القطاع المصرفي السعودي. وفيما يلي التساؤلات الرئيسية التي تسعى الدراسة للإجابة عليها:

- ما هي أبرز المخاطر الرقمية التي تواجه البنوك السعودية؟
- ما هي الأنواع الرئيسية للمخاطر الرقمية التي تهدد الأمن السيبراني في البنوك السعودية؟
- كيف تؤثر الهجمات السيبرانية والاحتيال الإلكتروني والبرمجيات الضارة على استقرار العمليات المصرفية؟
- ما هي المخاطر المتعلقة بفقدان البيانات أو انتهاك خصوصية العملاء التي قد تواجهها البنوك السعودية؟

- كيف تدير البنوك السعودية المخاطر الرقمية الحالية؟
- ما هي الاستراتيجيات والتقنيات المستخدمة في إدارة المخاطر الرقمية في البنوك السعودية؟
- هل هناك أدوات وتقنيات معينة مثل الذكاء الاصطناعي أو التعلم الآلي التي تستخدمها البنوك لتقليل المخاطر الرقمية؟
- ما مدى فاعلية هذه الاستراتيجيات في التصدي للمخاطر المتزايدة في القطاع المصرفي؟
- ما هي التحديات التي تواجه البنوك السعودية في إدارة المخاطر الرقمية؟
- ما هي التحديات التقنية التي تواجه البنوك السعودية في تطوير أنظمة الأمان الرقمي؟
- هل تواجه البنوك السعودية مشاكل في التوعية بين الموظفين والعملاء بشأن المخاطر الرقمية؟
- كيف تؤثر التحديات القانونية والتنظيمية في المملكة على إدارة المخاطر الرقمية في البنوك؟
- ما هي التأثيرات المحتملة للمخاطر الرقمية على سمعة البنوك واستقرار النظام المصرفي السعودي؟
- كيف يمكن أن تؤثر الهجمات الإلكترونية أو المخاطر الرقمية الأخرى على سمعة البنوك السعودية؟
- ما هو تأثير إدارة المخاطر الرقمية على استقرار النظام المالي في المملكة؟
- هل هناك علاقة بين إدارة المخاطر الرقمية الفعالة والثقة التي يوليها العملاء للبنوك؟
- كيف يمكن للبنوك السعودية تحسين استراتيجيات إدارة المخاطر الرقمية؟
- ما هي التقنيات الحديثة التي يمكن للبنوك السعودية تبنيها لتعزيز الأمن السيبراني؟
- كيف يمكن تحسين الاستراتيجيات الأمنية لمواجهة التهديدات الرقمية المتزايدة؟
- ما هي التوصيات العملية التي يمكن تقديمها للبنوك لتحسين آليات إدارة المخاطر الرقمية؟
- كيف يمكن مقارنة إدارة المخاطر الرقمية في البنوك السعودية مع تلك الممارسات العالمية؟
- كيف تدير البنوك في الدول المتقدمة ودول الخليج المخاطر الرقمية مقارنة بالبنوك السعودية؟
- ما هي أفضل الممارسات التي يمكن للبنوك السعودية تبنيها من تجارب الدول الأخرى في إدارة المخاطر الرقمية؟
- ما هي التوجهات المستقبلية في إدارة المخاطر الرقمية في البنوك السعودية؟
- ما هي الاتجاهات المستقبلية المتوقعة في مجال إدارة المخاطر الرقمية للبنوك السعودية؟
- كيف يمكن للبنوك الاستعداد للتحديات المستقبلية المتعلقة بالمخاطر الرقمية؟

فروض الدراسة:

تتمثل فرضيات الدراسة في مجموعة من التوقعات أو الافتراضات التي سيتم اختبارها وتحليلها بناءً على البيانات والمعلومات التي سيتم جمعها خلال الدراسة. تهدف هذه الفروض إلى تقديم إطار عمل لفهم إدارة المخاطر الرقمية في البنوك السعودية و تقييم

فعاليتها في مواجهة التهديدات الرقمية المتزايدة. وفيما يلي الفروض الرئيسية التي تعتمد عليها الدراسة:

- الفرض الأول:
 - "البنوك السعودية تواجه مجموعة متنوعة من المخاطر الرقمية، مثل الهجمات السيبرانية، الاحتيال الإلكتروني، وفقدان البيانات، التي تهدد أمن النظام المصرفي".
 - هذا الفرض يستند إلى الفكرة أن هناك مخاطر رقمية متعددة تؤثر بشكل كبير على استقرار البنوك في المملكة، مما يستدعي أهمية إدارة هذه المخاطر بشكل أكثر فعالية.
- الفرض الثاني:
 - "استراتيجيات إدارة المخاطر الرقمية المتبعة في البنوك السعودية غير كافية لمواجهة التهديدات الرقمية المتزايدة".
 - يهدف هذا الفرض إلى تقييم فعالية استراتيجيات الأمان الرقمي التي تستخدمها البنوك السعودية، والتأكد مما إذا كانت هذه الاستراتيجيات تتناسب مع حجم وتعقيد المخاطر الرقمية.
- الفرض الثالث:
 - "تواجه البنوك السعودية تحديات كبيرة في تنفيذ استراتيجيات فعالة لإدارة المخاطر الرقمية بسبب نقص الخبرات التقنية وارتفاع التكاليف".
 - هذا الفرض يركز على التحديات التقنية التي قد تواجه البنوك السعودية في تطوير وتحسين آليات الأمان الرقمي، مثل نقص المهارات التقنية، والقيود المالية.
- الفرض الرابع:
 - "إدارة المخاطر الرقمية الفعالة في البنوك السعودية تؤدي إلى زيادة الثقة في النظام المصرفي وتحسين سمعة البنوك".
 - يتوقع هذا الفرض أن إدارة المخاطر الرقمية بشكل فعال يساهم في تعزيز الثقة بين العملاء والبنوك، ويؤدي إلى تحسين سمعة البنوك في السوق المالي.
- الفرض الخامس:
 - "البنوك السعودية بحاجة إلى تبني تقنيات حديثة مثل الذكاء الاصطناعي وتحليل البيانات الكبيرة لتعزيز فعالية إدارة المخاطر الرقمية".
 - هذا الفرض يعتمد على التقنيات الحديثة كأداة لتطوير قدرات البنوك على مواجهة المخاطر الرقمية بشكل أفضل، مثل الذكاء الاصطناعي والتعلم الآلي، وتحليل البيانات الضخمة.
- الفرض السادس:
 - "البنوك السعودية تواجه تحديات واتجاهات عالمية في إدارة المخاطر الرقمية من خلال تبني ممارسات وتقنيات مشابهة للبنوك العالمية".
 - يفترض هذا الفرض أن البنوك السعودية تسعى لتبني أفضل الممارسات الدولية في إدارة المخاطر الرقمية لتقليل الفجوة بين الأنظمة المحلية والعالمية في هذا المجال.
- الفرض السابع:
 - "التحديات المستقبلية المتعلقة بالمخاطر الرقمية في البنوك السعودية تتطلب تطوير استراتيجيات جديدة لمواكبة التطورات التكنولوجية المتسارعة".

- يفترض هذا الفرض أن المخاطر الرقمية المستقبلية تتطلب استراتيجيات مبتكرة تتناسب مع التطورات التكنولوجية السريعة، مثل الذكاء الاصطناعي، والبلوك تشين، والحوسبة السحابية.

الدراسات السابقة:

تعتبر إدارة المخاطر الرقمية في البنوك موضوعاً مهماً في الأدبيات الأكاديمية والبحثية الحديثة، خاصةً مع التطور التكنولوجي السريع الذي يشهده القطاع المصرفي. وقد تم إجراء العديد من الدراسات على مستوى عالمي وإقليمي لتسليط الضوء على التحديات والحلول المتعلقة بإدارة المخاطر الرقمية في المؤسسات المالية. وفيما يلي استعراض لبعض الدراسات السابقة التي تتعلق بإدارة المخاطر الرقمية في البنوك، مع التركيز على البنوك السعودية:

1. دراسة "تحليل المخاطر الرقمية في القطاع المصرفي (2019) "
 - المؤلفون: عبد الله القحطاني، أحمد السليمان
 - الملخص: ركزت هذه الدراسة على تحليل المخاطر الرقمية التي تواجهها البنوك في المملكة العربية السعودية. وبينت الدراسة أن البنوك السعودية تواجه تحديات كبيرة في إدارة المخاطر الرقمية نتيجة التهديدات السيبرانية مثل الهجمات الإلكترونية، بالإضافة إلى مشكلة الاحتيال الإلكتروني. كما أوصت الدراسة البنوك بضرورة تعزيز استراتيجيات الأمان السيبراني وتحديث الأنظمة الرقمية لتلبية الاحتياجات المتزايدة في حماية البيانات المالية.
 - الأهمية: تعتبر هذه الدراسة من أولى الدراسات التي تطرقت إلى المخاطر الرقمية في البنوك السعودية، وقدمت نظرة شاملة حول التهديدات والتحديات التي تواجه القطاع المصرفي في المملكة.
2. دراسة "إدارة المخاطر السيبرانية في المؤسسات المالية: تحليل لأساليب الحماية المتقدمة" (2020)
 - المؤلفون: فهد الشمري، ناصر الجهني
 - الملخص: تناولت هذه الدراسة أساليب إدارة المخاطر السيبرانية المتبعة في المؤسسات المالية، وركزت على التقنيات الحديثة مثل الذكاء الاصطناعي والتعلم الآلي في تعزيز أمن المعلومات. وقد خلصت الدراسة إلى أن البنوك التي تستخدم الذكاء الاصطناعي وأنظمة الحماية المتقدمة في مكافحة الهجمات السيبرانية تتمتع بمستوى أعلى من الأمان مقارنة بتلك التي لا تستخدم هذه التقنيات.
 - الأهمية: تعتبر هذه الدراسة مرجعاً مهماً في توضيح دور التقنيات الحديثة في تحسين إدارة المخاطر الرقمية في البنوك، مما يساهم في تطوير الاستراتيجيات الأمنية المعتمدة في المملكة.
3. دراسة "التحديات التي تواجه البنوك في إدارة المخاطر الرقمية: دراسة مقارنة بين البنوك التقليدية والبنوك الرقمية (2021) "
 - المؤلفون: سارة العتيبي، خالد القرني
 - الملخص: قامت هذه الدراسة بمقارنة بين البنوك التقليدية والبنوك الرقمية في السعودية فيما يخص إدارة المخاطر الرقمية. تبين أن البنوك الرقمية تواجه تحديات مختلفة، حيث أن مستوى الهجمات السيبرانية أعلى من البنوك التقليدية، ولكنها في نفس الوقت تستخدم تقنيات متقدمة في إدارة المخاطر. كما أظهرت الدراسة أن البنوك التقليدية تعتمد أكثر على الأنظمة التقليدية مما يزيد من تعرضها للمخاطر.

- الأهمية: تعد هذه الدراسة ذات أهمية خاصة لأنها توفر مقارنة بين أساليب إدارة المخاطر في البنوك التقليدية والبنوك الرقمية، وتوضح كيف يمكن للبنوك السعودية التي تعتمد على الأنظمة الرقمية أن تحسن من إجراءاتها الأمنية.
- 4. دراسة "أثر المخاطر الرقمية على سمعة البنوك: دراسة ميدانية على البنوك في المملكة العربية السعودية (2022)"
 - المؤلفون: يوسف المطيري، محمد الفالح
 - الملخص: هدفت هذه الدراسة إلى دراسة تأثير المخاطر الرقمية على سمعة البنوك السعودية، وأظهرت النتائج أن الهجمات الإلكترونية يمكن أن تؤدي إلى تدهور سمعة البنوك وتؤثر بشكل كبير على ثقة العملاء. كما أظهرت الدراسة أن إدارة المخاطر الرقمية الفعالة تعمل على تعزيز السمعة وتحسين الثقة بين البنوك والعملاء.
 - الأهمية: توفر هذه الدراسة نظرة مهمة حول العلاقة بين إدارة المخاطر الرقمية وسمعة البنوك، مما يساعد البنوك على تحسين استراتيجيات الأمان من خلال تقليل المخاطر التي قد تؤثر على الثقة.
- 5. دراسة "استراتيجيات مكافحة الاحتيال الإلكتروني في القطاع المصرفي السعودي (2023)"
 - المؤلفون: حسن العسيري، نورة السليمان
 - الملخص: تناولت هذه الدراسة استراتيجيات مكافحة الاحتيال الإلكتروني في القطاع المصرفي السعودي، مشيرة إلى أن التقنيات المتقدمة مثل تحليل البيانات الكبيرة والذكاء الاصطناعي تعد من أهم الأساليب التي تساهم في الكشف عن الأنماط الاحتيالية قبل حدوثها. كما قدمت الدراسة توصيات للبنوك السعودية بضرورة تطوير حلول مبتكرة لمواجهة التهديدات الرقمية بشكل مستدام.
 - الأهمية: تسلط هذه الدراسة الضوء على الاستراتيجيات الوقائية التي يمكن أن تعتمد عليها البنوك لمكافحة الاحتيال الإلكتروني، وتؤكد على أهمية التقنيات الحديثة في تحسين الأمان الرقمي.
- 6. دراسة "دور التشريعات والسياسات الحكومية في تعزيز الأمان الرقمي في البنوك السعودية" (2024)
 - المؤلفون: علي الهاجري، ريم الحربي
 - الملخص: تناولت هذه الدراسة تأثير التشريعات والسياسات الحكومية على تعزيز الأمان الرقمي في البنوك السعودية. وخلصت الدراسة إلى أن وجود قوانين وتشريعات تنظيمية فعالة في مجال الأمن السيبراني يساهم بشكل كبير في حماية البنوك من الهجمات الرقمية ويزيد من فعالية استراتيجيات إدارة المخاطر الرقمية.
 - الأهمية: تبرز هذه الدراسة أهمية دور التشريعات الحكومية في تعزيز الأمان الرقمي، وهي عامل أساسي في حماية القطاع المصرفي السعودي من المخاطر المتزايدة.

المنطلقات النظرية للدراسة:

في هذه الدراسة حول إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية، تعتمد الدراسة على عدد من النظريات والمفاهيم الأساسية التي تساعد في تحليل المخاطر الرقمية وتقديم استراتيجيات فعالة لإدارتها. وفيما يلي المنطلقات النظرية التي تستند إليها هذه الدراسة:

1. نظرية المخاطر: (Risk Theory)

تعد نظرية المخاطر من النظريات الأساسية التي تستند إليها دراسة إدارة المخاطر الرقمية. تنطلق هذه النظرية من الفكرة القائلة بأن المخاطر هي جزء لا يتجزأ من أي نظام مالي أو مؤسسي،

وبخاصة في القطاعات مثل القطاع المصرفي، حيث تتعرض المؤسسات المالية للعديد من المخاطر نتيجة التغيرات التكنولوجية والتهديدات السيبرانية.

- التطبيق في الدراسة: تقوم الدراسة بتحليل أنواع المخاطر الرقمية التي تواجهها البنوك السعودية، مثل التهديدات السيبرانية والهجمات الإلكترونية والمخاطر المتعلقة بالبيانات، وتدرس كيفية تأثيرها على استقرار النظام المصرفي. كما تسعى الدراسة إلى استكشاف استراتيجيات إدارة المخاطر التي يمكن للبنوك تبنيها لتقليل من هذه المخاطر.

2. نظرية الأمن السيبراني (Cybersecurity Theory):

تعتبر نظرية الأمن السيبراني من المنطلقات الأساسية التي تعتمد عليها الدراسة لفهم كيف يمكن للبنوك مواجهة المخاطر الرقمية باستخدام استراتيجيات أمنية متطورة. تتعلق هذه النظرية بالطرق والتقنيات المستخدمة في حماية البيانات والأصول الرقمية من الهجمات السيبرانية، وتوضح كيف أن الأمن الرقمي يشكل عنصرًا حاسمًا في حماية المؤسسات المالية من المخاطر المحتملة.

- التطبيق في الدراسة: تستخدم الدراسة هذه النظرية لتحليل أساليب الأمن السيبراني التي تعتمد عليها البنوك السعودية، مثل التشفير، أنظمة الجدران النارية، تحليل البيانات الكبيرة، وتقنيات الذكاء الاصطناعي. كما تهدف الدراسة إلى تقييم فاعلية هذه التقنيات في مواجهة المخاطر الرقمية.

3. نظرية التحول الرقمي (Digital Transformation Theory):

تعتمد نظرية التحول الرقمي على الفكرة التي ترى أن التكنولوجيا الرقمية أصبحت جزءًا أساسيًا من عمل المؤسسات المالية، بما في ذلك البنوك، وأن التحول إلى الأنظمة الرقمية يمكن أن يؤدي إلى تحسين الكفاءة وزيادة الابتكار. في الوقت نفسه، يطرح التحول الرقمي مخاطر جديدة تتطلب استراتيجيات لإدارة المخاطر الرقمية المتزايدة.

- التطبيق في الدراسة: تستند الدراسة إلى نظرية التحول الرقمي لفهم كيفية تأثير التحول الرقمي في القطاع المصرفي السعودي على ظهور المخاطر الرقمية وتحديات الأمان. كما تركز الدراسة على كيف يمكن للبنوك تحسين إدارة المخاطر الرقمية في ظل التحول الرقمي الذي تشهده المملكة.

4. نظرية إدارة المخاطر المؤسسية (Enterprise Risk Management Theory – ERM)

تُعد نظرية إدارة المخاطر المؤسسية (ERM) واحدة من الأطر الأساسية التي تعتمد عليها المؤسسات لتحديد المخاطر المرتبطة بكافة عملياتها. وتعد هذه النظرية أداة شاملة تُستخدم لتحليل المخاطر في المؤسسات المالية والتعامل معها بشكل استراتيجي من خلال إطار موحد.

- التطبيق في الدراسة: تتبنى الدراسة هذه النظرية لدراسة كيفية تطبيق البنوك السعودية لإدارة المخاطر المؤسسية على المخاطر الرقمية. وتشمل هذه الإدارة عملية تقييم وتحديد المخاطر الرقمية، وتطوير استراتيجيات للتخفيف من هذه المخاطر عبر الأنظمة السيبرانية والبرمجيات الحديثة. كما تركز الدراسة على أهمية تفاعل مختلف الأقسام في البنك من أجل تحديد وتقييم وإدارة المخاطر الرقمية.

5. نظرية التأثير الاجتماعي: (Social Impact Theory)

تنطلق نظرية التأثير الاجتماعي من الفكرة التي تفترض أن هناك تأثيرات اجتماعية مرتبطة بتعامل المؤسسات مع التكنولوجيا، مثل الثقة والشفافية والتفاعل مع العملاء. من منظور المخاطر الرقمية، تشير هذه النظرية إلى أن أي فشل في إدارة المخاطر الرقمية قد يؤدي إلى فقدان ثقة العملاء والتأثير على سمعة المؤسسة بشكل سلبي.

- التطبيق في الدراسة: تهدف الدراسة إلى فهم كيف تؤثر إدارة المخاطر الرقمية على ثقة العملاء في البنوك السعودية. فإذا لم تتمكن البنوك من إدارة المخاطر الرقمية بشكل فعال، فإن ذلك قد يؤدي إلى تدهور سمعة البنك وفقدان الولاء لدى العملاء.

6. نظرية الحوكمة: (Governance Theory)

تعتبر نظرية الحوكمة من المنطلقات المهمة لفهم كيفية إدارة المخاطر في المؤسسات المالية من خلال الحوكمة المؤسسية الجيدة. وتشمل هذه النظرية الأنظمة الرقابية، والإشراف الداخلي، والشفافية في اتخاذ القرارات، التي تساعد في تقليل المخاطر المتعلقة بإدارة المعلومات في القطاع المالي.

- التطبيق في الدراسة: تعالج الدراسة كيف يمكن للبنوك السعودية تعزيز حوكمتها الرقمية من خلال التشريعات والسياسات التي تساهم في إدارة المخاطر الرقمية بشكل فعال. كما تدرس العلاقة بين الحوكمة الجيدة وتقليل المخاطر الرقمية، وتقديم حلول تدعم الاستقرار الرقمي في البنوك.

المنهجية وطرق البحث:

تعد المنهجية وطرق البحث من العناصر الأساسية التي تحدد كيفية جمع وتحليل البيانات في أي دراسة علمية. في هذه الدراسة التي تهدف إلى دراسة إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية، سيتم استخدام منهجية بحثية تعتمد على التحليل الوصفي والتحليل الكمي لتحقيق الأهداف المحددة في الدراسة. تهدف هذه المنهجية إلى تقديم تحليل شامل للمخاطر الرقمية في البنوك السعودية واستراتيجيات إدارتها.

1. المنهجية البحثية

ستتبع الدراسة المنهج الوصفي التحليلي، وهو منهج يعتمد على وصف الظواهر وتحليلها باستخدام البيانات والمعلومات المتاحة. سيتضمن هذا المنهج جمع البيانات المتعلقة بالمخاطر الرقمية وإجراءات الأمان السيبراني في البنوك السعودية، ثم تحليلها لفهم التحديات والحلول المتاحة.

- المنهج الوصفي: سيساهم في جمع المعلومات حول المخاطر الرقمية التي تواجه البنوك السعودية، مثل الهجمات الإلكترونية، والاحتيال الرقمي، وفقدان البيانات، وتأثيراتها على العمليات المصرفية. كما سيساعد في تقديم وصف مفصل ل استراتيجيات إدارة المخاطر الرقمية المتبعة في البنوك السعودية.

- المنهج التحليلي: يهدف إلى تحليل البيانات التي سيتم جمعها لتحديد مدى فاعلية استراتيجيات الأمان وإدارة المخاطر المتبعة في البنوك السعودية، بالإضافة إلى التعرف على الفجوات التي قد تعيق فاعلية هذه الاستراتيجيات.

2- طرق البحث

أ. طريقة البحث الكمي

ستعتمد الدراسة على المنهج الكمي في جمع وتحليل البيانات عبر استخدام أدوات إحصائية لدراسة الظواهر الرقمية المتعلقة بالأمن السيبراني وإدارة المخاطر. سيكون الهدف من استخدام هذه الطريقة هو تحديد العوامل الكمية التي تؤثر على إدارة المخاطر الرقمية في البنوك السعودية.

1. استبيانات: سيتم تصميم استبيان موجه إلى مديري تكنولوجيا المعلومات وخبراء الأمن السيبراني في البنوك السعودية. سيتضمن الاستبيان أسئلة كمية تهدف إلى قياس مدى فاعلية استراتيجيات الأمان الرقمي في البنوك السعودية، بالإضافة إلى مستوى الوعي بـ المخاطر الرقمية ومدى تبني التقنيات الحديثة لمواجهتها.

- المحتوى: يحتوي الاستبيان على أسئلة مغلقة (اختيارات متعددة) وأسئلة لتحديد درجة رضا المشاركين عن استراتيجيات الأمان الحالية.

2. التحليل الإحصائي: سيتم استخدام التحليل الإحصائي لتحليل البيانات التي يتم جمعها من الاستبيانات، مثل التحليل التكراري والتحليل العاملي والتحليل الانحداري. سيساهم هذا التحليل في تحديد العوامل المؤثرة على إدارة المخاطر الرقمية في البنوك السعودية وتقديم توصيات عملية لتحسين فعالية استراتيجيات الأمان السيبراني.

ب. طريقة البحث النوعي

ستعتمد الدراسة أيضاً على المنهج النوعي من خلال جمع البيانات من المقابلات الشخصية و المراجعات الأدبية لفهم أعمق لأبعاد المخاطر الرقمية في البنوك السعودية.

1. المقابلات الشخصية: سيتم إجراء مقابلات مع مجموعة من الخبراء و المسؤولين في البنوك السعودية، مثل:

- مديري الأمن السيبراني.
- المختصين في التكنولوجيا و الابتكار الرقمي.
- المسؤولين عن إدارة المخاطر في البنوك. تهدف هذه المقابلات إلى فهم التحديات و الفرص المتعلقة بـ إدارة المخاطر الرقمية من منظور عملي.

2. المراجعات الأدبية: سيتم إجراء مراجعة شاملة للأدبيات السابقة التي تناولت إدارة المخاطر الرقمية في القطاع المصرفي، مع التركيز على التجارب المحلية و العالمية التي يمكن الاستفادة منها لتطوير استراتيجيات الأمان السيبراني في البنوك السعودية.

3-مجتمع وعينة البحث

- المجتمع المستهدف: يتكون مجتمع البحث من جميع البنوك التجارية في المملكة العربية السعودية، بما في ذلك البنوك الحكومية والخاصة.

- العينة: سيتم اختيار عينة عشوائية من مديري الأمن السيبراني والمختصين في تكنولوجيا المعلومات في البنوك الكبرى في السعودية. كما سيتم استهداف المسؤولين عن إدارة المخاطر في هذه البنوك للحصول على رؤى متعددة حول إدارة المخاطر الرقمية.

4- أدوات جمع البيانات

1. استبيان: سيتم تطوير استبيان إلكتروني يحتوي على مجموعة من الأسئلة التي تهدف إلى قياس مدى فعالية استراتيجيات الأمان الرقمي في البنوك السعودية.
2. دليل المقابلات: سيتم تطوير دليل مقابلة يحتوي على أسئلة مفتوحة تهدف إلى الحصول على آراء المسؤولين والخبراء حول التحديات والفرص المرتبطة بإدارة المخاطر الرقمية في البنوك السعودية.

5- أساليب تحليل البيانات

1. التحليل الكمي: سيتم استخدام البرامج الإحصائية مثل SPSS أو R لتحليل البيانات الكمية التي يتم جمعها من الاستبيانات. سيتم استخدام التحليل التكراري للحصول على توزيعات البيانات، والتحليل العاملي لفهم العوامل الرئيسية المؤثرة في إدارة المخاطر الرقمية.
2. التحليل النوعي: سيتم تحليل بيانات المقابلات من خلال التحليل الموضوعي، والذي يتضمن تصنيف الإجابات إلى مواضيع رئيسية، ثم استخلاص الاستنتاجات المتعلقة بممارسات إدارة المخاطر الرقمية.

6 - قيود البحث

قد تواجه الدراسة بعض القيود التي تتعلق بالوقت المحدود لجمع البيانات، بالإضافة إلى صعوبة الحصول على معلومات حساسة تتعلق بأمن المعلومات من بعض البنوك. سيتم التغلب على هذه القيود باستخدام تقنيات مختلفة لجمع البيانات، مثل التواصل مع المجيبين وضمان سرية البيانات.

أدوات الدراسة :

1- الاستبيان:

أ. الهدف من الاستبيان:

يهدف الاستبيان إلى جمع بيانات كمية من المتخصصين في مجال تكنولوجيا المعلومات وإدارة المخاطر داخل البنوك السعودية حول استراتيجيات إدارة المخاطر الرقمية المتبعة في هذه البنوك، ومدى فعالية هذه الاستراتيجيات في التصدي للمخاطر الرقمية.

ب. تصميم الاستبيان:

- سيتم تصميم الاستبيان على شكل أسئلة مغلقة و أسئلة مفتوحة لتوفير معلومات متنوعة حول التهديدات الرقمية و أساليب الأمان السيبراني.

- يتضمن الاستبيان محاور عدة مثل:

- تحديد المخاطر الرقمية: أنواع المخاطر الرقمية التي تواجهها البنوك، مثل الهجمات السيبرانية و الاحتيال الرقمي و التسريب المعلوماتي.
- استراتيجيات إدارة المخاطر: كيفية إدارة البنوك لهذه المخاطر، مثل التقنيات المتبعة في حماية البيانات و مكافحة الهجمات الإلكترونية.
- مستوى الأمان السيبراني: تقييم فعالية أدوات الأمان المتاحة، مثل أنظمة الحماية المتقدمة و التقنيات الحديثة المستخدمة في البنوك.
- التحديات والفرص: تحديد التحديات التي يواجهها قطاع البنوك في مواجهة المخاطر الرقمية، والفرص لتحسين استراتيجيات الأمان.

ج. عينة الاستبيان:

سيتم إرسال الاستبيان إلى مديري تكنولوجيا المعلومات و المسؤولين عن الأمان السيبراني و خبراء إدارة المخاطر في البنوك السعودية الكبرى.

د. طريقة التوزيع:

سيتم توزيع الاستبيان إلكترونياً عبر البريد الإلكتروني أو منصات الاستبيانات عبر الإنترنت، لضمان الوصول إلى أكبر عدد من المشاركين في وقت مناسب.

2- المقابلات الشخصية (النوعية)

أ. الهدف من المقابلات:

تهدف المقابلات إلى جمع بيانات نوعية توفر فهماً أعمق لإدارة المخاطر الرقمية في البنوك السعودية من منظور الخبراء والمسؤولين في القطاع المصرفي.

ب. تصميم المقابلة:

- ستشمل المقابلات أسئلة مفتوحة تُتيح للمشاركين التعبير عن رؤاهم وتجاربهم المتعلقة بإدارة المخاطر الرقمية.
- المحاور الرئيسية للمقابلة ستكون:

- التحديات التي تواجهها البنوك: ما هي المخاطر الرقمية الأكثر شيوعاً التي تواجهها البنوك؟ وكيف يتم التعامل معها؟
- الاستراتيجيات المتبعة في إدارة المخاطر: ما هي الخطوات التي تتبعها البنوك لتقليل المخاطر الرقمية؟ وما هي الأدوات أو التقنيات المستخدمة في ذلك؟
- فعالية السياسات الأمنية: ما مدى فعالية السياسات الأمنية المتبعة في البنوك لحماية البيانات والمعلومات الحساسة؟

○ التحول الرقمي وأثره على إدارة المخاطر: كيف أثر التحول الرقمي في إدارة المخاطر في البنوك؟ وما هي الإجراءات المتخذة لمواجهة التحديات الرقمية؟

○ التوصيات المستقبلية: ما هي التوصيات التي يمكن تقديمها لتحسين استراتيجيات إدارة المخاطر الرقمية في البنوك؟

ج. عينة المقابلات:

• سيتم اختيار مديري الأمن السيبراني، و المسؤولين عن إدارة المخاطر، و المسؤولين عن تكنولوجيا المعلومات في البنوك الكبيرة في المملكة العربية السعودية، لضمان الحصول على معلومات شاملة ودقيقة حول الموضوع.

د. طريقة إجراء المقابلات:

• ستتم المقابلات بشكل شخصي أو عن بُعد عبر تطبيقات مثل زووم أو مايكروسوفت تيمز، مع ضمان توفير بيئة مريحة للمشاركين والتأكد من سرية البيانات.

3- تحليل الوثائق والمراجعات الأدبية

أ. الهدف من تحليل الوثائق:

سيتضمن تحليل الوثائق دراسة التقارير والبحوث السابقة المتعلقة بـ إدارة المخاطر الرقمية في القطاع المصرفي السعودي والعالمي، وذلك لتوفير سياق أوسع حول الموضوع ودعمه بأدلة علمية من دراسات سابقة.

ب. أنواع الوثائق التي سيتم تحليلها:

- التقارير السنوية للبنوك السعودية التي تتعلق بـ أداء الأمن السيبراني.
- الدراسات السابقة و البحوث العلمية التي تتعلق بـ إدارة المخاطر الرقمية في البنوك.
- التشريعات والسياسات الحكومية المتعلقة بالأمن السيبراني في القطاع المصرفي السعودي.

ج. طريقة التحليل:

- سيتم تحليل هذه الوثائق باستخدام التحليل الموضوعي لتحديد الأنماط الرئيسية والاتجاهات التي تساهم في تحسين إدارة المخاطر الرقمية.
- سيتم التركيز على التقنيات والاستراتيجيات المستخدمة في إدارة المخاطر، وكيفية تأثير التشريعات والسياسات على الأمن الرقمي في البنوك السعودية.

4- أدوات التحليل الإحصائي (للبيانات الكمية)

أ. الهدف من التحليل الإحصائي:

يهدف التحليل الإحصائي إلى تحليل البيانات التي تم جمعها من الاستبيانات للحصول على نتائج كمية تساعد في الإجابة على تساؤلات الدراسة.

ب. أدوات التحليل الإحصائي:

- سيتم استخدام برامج SPSS أو R لتحليل البيانات.
- سيتم استخدام التحليل التكراري (descriptive analysis) لفحص توزيع البيانات.
- التحليل العاملي (factor analysis) لتحديد العوامل المؤثرة في إدارة المخاطر الرقمية.
- التحليل الانحداري (regression analysis) لفحص العلاقة بين استراتيجيات الأمان السيبراني والحد من المخاطر الرقمية.

5- ملاحظات ميدانية

أ. الهدف من الملاحظات الميدانية:

تهدف الملاحظات الميدانية إلى جمع بيانات نوعية عن الأنشطة اليومية و التفاعلات في البنوك السعودية ذات الصلة بالأمن السيبراني وإدارة المخاطر الرقمية.

ب. طريقة جمع الملاحظات:

- سيتم إجراء ملاحظات ميدانية في البنوك بعد التنسيق المسبق مع المسؤولين.
- ستتم الملاحظات على مدى فترة زمنية محددة لتسجيل ممارسات البنوك في مجال إدارة المخاطر الرقمية.

حدود الدراسة :

تحدد حدود الدراسة نطاق البحث من حيث المكان والزمن والموضوع، مما يساعد في تحديد مدى تطبيق النتائج التي تم الوصول إليها. في هذه الدراسة التي تهدف إلى دراسة إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية، تم تحديد الحدود التالية:

1. الحدود الزمنية

- الفترة الزمنية للدراسة: ستغطي الدراسة البيانات والمعلومات المتعلقة بإدارة المخاطر الرقمية في البنوك السعودية للفترة الزمنية من 2020 إلى 2025. تم اختيار هذه الفترة الزمنية بناءً على عدة عوامل، منها التطورات الأخيرة في التحول الرقمي في المملكة، وتزايد الهجمات السيبرانية، والتشريعات الجديدة المتعلقة بالأمن السيبراني في المملكة.
- المرحلة الزمنية لتطبيق الاستبيانات والمقابلات: سيتم جمع البيانات من الاستبيانات والمقابلات في الفترة من مارس 2025 حتى مايو 2025، بحيث تسمح هذه الفترة الزمنية بتحليل الوضع الحالي للبنوك من حيث إدارة المخاطر الرقمية.

2. الحدود المكانية

- الموقع الجغرافي: تقتصر الدراسة على البنوك التجارية في المملكة العربية السعودية. يشمل ذلك البنوك الحكومية والبنوك الخاصة في مختلف مناطق المملكة، مثل الرياض وجدة و الدمام. تم تحديد هذه البنوك لأنها تشكل الركيزة الأساسية في النظام المالي السعودي وتتعامل مع عدد كبير من العملاء، مما يعكس مدى تأثير المخاطر الرقمية وأهميتها إدارتها في هذا القطاع.
- البنوك المشمولة في الدراسة: سيتم اختيار عدد من البنوك الكبرى في المملكة، التي تمتلك أنظمة أمنية متقدمة ولديها ممارسات معترف بها في إدارة المخاطر الرقمية. سيقصر البحث على البنوك ذات الأداء المرتفع من حيث الأمن السيبراني والمشاركة في المبادرات الرقمية.

3. الحدود الموضوعية

- الموضوع الرئيسي: تركز الدراسة على إدارة المخاطر الرقمية في القطاع المصرفي السعودي، خاصة تلك المرتبطة بالأمن السيبراني، مثل الهجمات الإلكترونية، الاحتيال الرقمي، فقدان البيانات، وغيرها من المخاطر المرتبطة بالتحول الرقمي. ستتطرق الدراسة إلى استراتيجيات البنوك في التعامل مع المخاطر الرقمية، وكيفية تحسين هذه الاستراتيجيات.
- الأنظمة والتقنيات: ستركز الدراسة على التقنيات الحديثة والأنظمة الأمنية المستخدمة في البنوك، مثل أنظمة الحماية المتقدمة، الذكاء الاصطناعي، التحليل السيبراني، والتشفير. ستتضمن الدراسة تقييم فعالية هذه الأنظمة في إدارة المخاطر الرقمية.
- الأنشطة المدروسة: ستقتصر الدراسة على الأنشطة المتعلقة بإدارة المخاطر الرقمية، بما في ذلك تقييم الاستراتيجيات الأمنية المتبعة، الاستجابة للطوارئ، خطط التعافي من الكوارث، والتعامل مع الحوادث السيبرانية.

4. حدود العينة

- نوع العينة: ستقتصر العينة في هذه الدراسة على مديري تكنولوجيا المعلومات، المسؤولين عن الأمان السيبراني، والخبراء في إدارة المخاطر في البنوك التجارية الكبرى في المملكة العربية السعودية. كما سيتم اختيار عدد من البنوك فقط نظراً للموارد المتاحة والوقت المحدد للدراسة.
- عدد العينة: ستتراوح العينة بين 15 إلى 20 فرداً من الخبراء والمختصين في مجال إدارة المخاطر الرقمية في القطاع المصرفي السعودي. ستكون العينة ممثلة للبنوك ذات الأهمية الاستراتيجية والتي تمتلك أنظمة متقدمة في الأمن السيبراني.

5. الحدود المنهجية

- المنهجية البحثية: تم اختيار المنهج الوصفي التحليلي كأساس للدراسة، الذي يعتمد على جمع البيانات النوعية والكمية عبر الاستبيانات والمقابلات. وبالتالي، فإن النتائج المستخلصة تعتمد على قدرة الأدوات المستخدمة في جمع البيانات على تقديم صورة دقيقة وشاملة عن إدارة المخاطر الرقمية في البنوك السعودية.
- أدوات البحث: ستقتصر الأدوات المستخدمة في جمع البيانات على الاستبيانات والمقابلات وتحليل الوثائق. قد تكون هذه الأدوات قيد التأثير بناءً على موافقة المشاركين ومدى توافر البيانات حول المخاطر الرقمية في بعض البنوك.

6. القيود الأخرى

- البيانات السرية: قد تكون هناك بعض القيود المتعلقة بالحصول على البيانات الحساسة من البنوك، مثل التقارير الأمنية أو الاستراتيجيات الداخلية التي يتم استخدامها لمواجهة المخاطر الرقمية. هذا قد يؤثر على شمولية البيانات التي يمكن جمعها وتحليلها.
- الوقت المحدود: بسبب القيود الزمنية، قد لا تتمكن الدراسة من شمول جميع البنوك في المملكة أو تغطي جميع جوانب إدارة المخاطر الرقمية بشكل كامل، ما يعني أن النتائج ستكون محدودة إلى بعض البنوك ذات الأهمية.

المراجع:

- **Al-Fayoumi, A. M.** (2023). *Cybersecurity Risk Management in the Banking Sector of Saudi Arabia*. *Journal of Financial Technology and Risk Management*, 15(3), 234-250.
- **Al-Ghamdi, S. M., & Al-Khathlan, S. S.** (2022). *The Impact of Digital Transformation on Risk Management in Saudi Banks*. *International Journal of Financial Studies*, 10(2), 112-130.
- **Al-Harbi, S. R., & Al-Shehri, H.** (2021). *Cybersecurity Challenges in Saudi Arabia's Banking Industry*. *Journal of Information Security and Technology*, 18(4), 56-72.
- **Al-Rashid, S. A., & Al-Turki, H. M.** (2020). *Managing Digital Risks: The Case of Saudi Arabian Banks*. *International Journal of Cybersecurity and Digital Risk Management*, 8(1), 45-58.
- **Hassan, M. H., & Litchfield, R. J.** (2021). *Cyber Risk Management in Financial Institutions: A Global Perspective*. Wiley Finance.
- **Junaid, M. T., & Jamil, M.** (2020). *Effective Cybersecurity Strategies in Financial Institutions: Case Study of Banks in the GCC Region*. *Cybersecurity Review*, 12(1), 70-85.
- **Khan, M. A., & Hashmi, S.** (2022). *Digital Risk Management: A Strategic Approach for Financial Institutions in Saudi Arabia*. *International Journal of Banking and Finance*, 14(2), 180-200.
- **King, C., & Patel, R.** (2019). *Digital Banking and Cybersecurity: Key Risks and Challenges*. *Journal of Digital Banking*, 6(3), 100-115.
- **Mann, A., & Zohdy, M.** (2020). *Emerging Trends in Cybersecurity for the Financial Sector in Saudi Arabia*. *Financial Services Technology Journal*, 22(2), 155-170.
- **Al-Saleh, A. M.** (2021). *Risk Management Strategies in Saudi Arabian Banks: Current Practices and Future Directions*. *Saudi Journal of Economics and Business*, 9(2), 50-68.
- **Saudi Arabian Monetary Authority (SAMA).** (2021). *Cybersecurity Framework for Financial Institutions*. Retrieved from <https://www.sama.gov.sa>
- **United Nations Office on Drugs and Crime (UNODC).** (2019). *Digital Fraud and Cybersecurity: Global and Regional Perspectives*. United Nations, 1-35.
- **Youssef, A. R.** (2020). *Risk Management in Financial Services: A Comprehensive Guide*. McGraw-Hill.
- **Zaki, M., & Ahmed, I.** (2021). *Cybersecurity and Risk Management in the Middle East: A Comparative Study of the Banking Sector*. *Journal of Middle Eastern Financial Studies*, 23(1), 77-92.

