

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ماجستير إدارة المخاطر



إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية
دراسة تطبيقية على البنك الأهلي السعودي

إعداد الطالب/

أحمد سعد آل تركي

إشراف/

د. الفیصل عبد الحمید

د. فايز جراد

العام الدراسي:

2025

الفصل الأول

المقدمة:

يشهد القطاع المصرفي تطوراً متسارعاً نتيجة الاعتماد المتزايد على التقنيات الرقمية والأنظمة الإلكترونية، الأمر الذي أدى إلى تحول جوهري في طبيعة الخدمات المالية وطرق تقديمها. في هذا السياق، أصبحت المخاطر الرقمية من أبرز التحديات التي تواجه المؤسسات المالية، خاصة في ظل تصاعد التهديدات السيبرانية وتزايد الاعتماد على البنية التحتية الرقمية.

تعد إدارة المخاطر الرقمية ضرورة استراتيجية لحماية المعلومات المصرفية الحساسة وضمان استمرارية الأعمال في بيئة شديدة التغيير. ومن هذا المنطلق، جاءت هذه الدراسة لتسلط الضوء على واقع إدارة المخاطر الرقمية في البنك الأهلي السعودي، أحد أبرز المؤسسات المالية في المملكة العربية السعودية، ولتبحث في مدى تأثير تلك الإدارة على تعزيز أمن المعلومات في بيئة مصرفية رقمية متقدمة.

حيث 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 وفعال 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 لمواجهة التحديات المتزايدة.

وفي ظل التوسع المتزايد في استخدام الأنظمة الرقمية في المؤسسات المصرفية، ظهرت العديد من التحديات المرتبطة بأمن المعلومات نتيجة للثغرات المحتملة في النظم أو الهجمات السيبرانية المتعمدة. وتعد إدارة المخاطر الرقمية أداة رئيسية للتعامل مع هذه التحديات. إلا أن مدى فعالية هذه الإدارة في تحقيق مستوى عالي من أمن المعلومات لا يزال غير واضح بشكل كافٍ، مما يستدعي إجراء دراسة ميدانية معمقة.

وبناء على ما سبق، يمكن صياغة مشكلة الدراسة في السؤال الرئيسي الآتي:

" ما مدى تأثير إدارة المخاطر الرقمية على أمن المعلومات في البنك الأهلي السعودي "

-أهمية الدراسة-

تبرز أهمية هذه الدراسة من خلال عدة اعتبارات، أهمها أنها تتناول موضوعا حيويا في بيئة العمل المصرفي المعاصرة، حيث ان أي خلل في أمن المعلومات قد يؤدي إلى خسائر مالية جسيمة، إضافة الى التأثير على سمعة المؤسسة المصرفية.

ومن جانب آخر، فإن الدراسة تقدم قيمة علمية من خلال ربط المفاهيم النظرية المتعلقة بالمخاطر الرقمية بتطبيقات واقعية في بيئة العمل الفعلية.

وتكمن الأهمية العملية للدراسة في إمكانية استخدامها من قبل الإدارات المختصة في البنوك السعودية، لتطوير السياسات والإجراءات المرتبطة بالأمن السيبراني، بما يسهم في حماية البنية التحتية وتقليل فرص الاختراق أو التسريب.

حيث تكتسب دراسة إدارة المخاطر الرقمية في البنوك في المملكة العربية السعودية متمثلة في البنك الأهلي السعودي 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.

-أهداف الدراسة-

تهدف هذه الدراسة الى ما يلي:

- التعرف على طبيعة وأشكال المخاطر الرقمية التي تواجه البنك الأهلي السعودي.
- تقييم السياسات والإجراءات المتبعة لإدارة تلك المخاطر.
- تحليل العلاقة بين تطبيق إدارة المخاطر الرقمية ومستوى أمن المعلومات.
- تقديم توصيات عملية قابلة للتطبيق تساهم في تحسين إدارة المخاطر الرقمية.

-تساؤلات الدراسة

ليتسنى لنا تحقيق أهداف الدراسة، سيتم الإجابة عن التساؤلات الآتية:

- 1- ما أنواع المخاطر الرقمية الشائعة في البنك الأهلي السعودي؟
- 2- كيف تؤثر تلك المخاطر على سرية وتكامل وتوافر المعلومات المصرفية؟
- 3- ما مدى فاعلية السياسات والإجراءات المتبعة في البنك لإدارة المخاطر الرقمية؟
- 4- هل توجد علاقة ذات دلالة إحصائية بين إدارة المخاطر الرقمية وكفاءة أمن المعلومات؟

- فروض الدراسة:

- الفرضية الرئيسية:

توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق إدارة المخاطر الرقمية ومستوى أمن المعلومات في البنك الأهلي السعودي.

- الفرضية الفرعية:

- 1- توجد فروق ذات دلالة إحصائية في مستوى أمن المعلومات تعزى الى اختلاف مستوى تبني إجراءات الحماية الرقمية.
- 2- توجد علاقة ارتباط بين درجة تهديد المخاطر الرقمية وتطور نظم الحماية المستخدمة.

-النظرية العلمية المتبعة لإعداد البحث

تعتمد هذه الدراسة على نظرية إدارة المخاطر المؤسسية

(Enterprise Risk Management- ERM) والتي تركز على التنبؤ بالمخاطر وتحليلها ومن ثم تصميم استجابات منهجية تسهم في تقليل تأثيرها على أداة المنظمة. وتعد هذه النظرية إطاراً شاملاً يمكن الإدارة من فهم شامل للمخاطر على جميع المستويات، بما في ذلك المخاطر الرقمية.

ومن خلال هذه النظرية، يتم دمج إدارة المخاطر الرقمية في صميم العمليات المؤسسية واتخاذ القرار، بحيث لا يقتصر الأمر فقط على الجانب التقني، بل يشمل الأبعاد الإدارية والتنظيمية والإستراتيجية.

ويستند هذا البحث بشكل خاص إلى نموذج COSO-ERM، الذي يعد أحد الأطر العالمية المعتمدة لتحديد وتقييم وإدارة المخاطر داخل المؤسسات، كما يأخذ البحث في اعتباره نموذج Risk IT Framework الصادر عن معهد ISACA، والذي يوضح العلاقة بين تكنولوجيا المعلومات وإدارة المخاطر المؤسسية، ويوفر أدوات منهجية لربط المخاطر الرقمية بأهداف العمل.

ومن خلال هذا الإطار النظري، يسعى الباحث إلى توظيف هذه المفاهيم والنماذج لتفسير وتقييم آليات إدارة المخاطر الرقمية في البنك الأهلي السعودي، وتحليل مدى توافقها مع أفضل الممارسات العالمية.

الفصل الثاني

الدراسات السابقة

-مقدمة:

تعد الدراسات السابقة من الركائز الأساسية التي يستند إليها أي بحث علمي، حيث إنها تسهم في بناء خلفية معرفية حول موضوع الدراسة، وتساعد في تحديد الفجوات البحثية، وفهم السياقات النظرية والتطبيقية ذات الصلة.

ومن خلال مراجعة الأدبيات السابقة، يمكن للباحث الاستفادة من المناهج المستخدمة والنتائج المتوصل إليها، مما يدعم صياغة إطار نظري متين يعزز من جودة التحليل والنتائج.

وفي هذا الفصل، سيتم عرض ومناقشة عدد من الدراسات التي تناولت موضوع إدارة المخاطر الرقمية وأثرها على أمن المعلومات، سواء في البيئة المصرفية أو في القطاعات ذات علاقة، وتقديم تحليل نقدي يبرز أوجه الاتفاق والاختلاف ويحدد ما ستضيفه هذه الدراسة.

تهدف هذه المراجعة إلى تسليط الضوء على أبرز ما توصلت إليه البحوث المحلية والعالمية ذات الصلة، مع التركيز على مدى جاهزية البنوك للتعامل مع المخاطر الناشئة عن التحول الرقمي، وأهم السياسات والتقنيات المعتمدة في التخفيف من هذه المخاطر.

كما تسعى هذه المراجعة إلى تحليل أوجه الاتفاق والاختلاف بين نتائج الدراسات، واستخلاص أبرز الممارسات والتوصيات التي يمكن الاستفادة منها في السياق السعودي، وبشكل خاص البنك الأهلي السعودي

-الدراسات السابقة:

• دراسة (العزب،2023):

هدفت هذه الدراسة إلى التعرف أثر التهديدات السيبرانية على أداء البنوك التجارية في جمهورية مصر العربية، حيث اعتمد الباحث على المنهج الوصفي التحليلي، واستخدم الاستبانة كأداة لجمع البيانات من عينة مكونة من 423 موظفا في القطاع المصرفي، توصلت الدراسة إلى أن ارتفاع معدلات الهجمات السيبرانية يؤدي إلى انخفاض مستوى ثقة العملاء وزيادة النفقات التشغيلية للبنوك وأوصت بضرورة تعزيز استراتيجيات إدارة المخاطر الرقمية وربطها بأنظمة الحوكمة.

• دراسة (الحمادي،2023):

تناولت هذه الدراسة مدى التزام البنوك الخليجية بمعايير الحوكمة الرقمية في إدارة المخاطر السيبرانية، وخلصت الى ان هناك تفاوتاً في تبني هذه المعايير بين البنوك الكبرى والصغرى، وأوصت بضرورة بناء إطار موحد للامتثال الرقمي في القطاع المصرفي الخليجي، وتطوير المهارات التقنية للعاملين في أقسام الأمن السيبراني.

• Gunawan and Melinda (2021):

Examined the effect of cybersecurity governance on data protection in Indonesian financial institutions. The study used a distributed to 352 employees. The analysis using SPSS showed that institutions with structured cybersecurity policies had significantly better data protection and incident response mechanisms, highlighting the importance of policy clarity and employee awareness.

• AL Harthy and Khan (2020):

Investigated the role of digital risk management framework in enhancing cyber resistance among Saudi Banks. The researcher utilized a mixed method approach, combining interviews with IT executives and quantitative data from compliance reports. Finding indicated a strong positive correlation between structured risk management practices and lower data breach incidents.

ومن خلال مراجعة الدراسات السابقة، يلاحظ اتفاق واضح على أهمية إدارة المخاطر الرقمية في تقليل التهديدات الإلكترونية وتحقيق مستوى أعلى من أمن المعلومات. كما أجمعت معظم الدراسات على أن وجود سياسات واضحة وإجراءات مدروسة، يعزز من قدرة المؤسسات المصرفية على مواجهة التحديات الرقمية.

ومع ذلك تباينت الدراسات من حيث المجال الجغرافي والمستوى المؤسسي. فبينما ركزت بعض الدراسات على مؤسسات مالية في بيئات آسيوية أو عربية، لم تركز الكثير منها على الحالة السعودية تحديداً، وهو ما تسعى هذه الدراسة لتغطيته. كما أن غالبية الدراسات اعتمدت على النهج الوصفي فيما تسعى هذه الدراسة الى الدمج بين التحليل النظري والتطبيق الميداني من خلال دراسة حالة البنك الأهلي السعودي.

وتجدر الإشارة الى ان بعض الدراسات ركزت فقط على الجانب الفني لإدارة المخاطر دون التطرق الى البعد الإداري والحوكمي، مما يبرز حاجة البحث الحالي الى تقديم معالجة أكثر شمولاً تأخذ في الاعتبار تكامل الأبعاد التقنية والإدارية والتنظيمية.

ويهدف هذا البحث إلى سد هذه الفجوة من خلال دراسة تطبيقية تستند إلى أسس علمية ومنهجية، وتسهم في تطوير نموذج وطني لإدارة المخاطر الرقمية في القطاع المصرفي السعودي.

-الإطار النظري:

يرتكز الإطار النظري للدراسة على عدد من المفاهيم الجوهرية التي ترتبط بمضمون الدراسة، وتساعد في بناء أرضية وأمن المعلومات وتشمل:

1. مفهوم المخاطر الرقمية:

تعرف بأنها تهديدات أو الأحداث التي تؤثر سلباً على أنظمة المعلومات أو البيانات أو العمليات الإلكترونية نتيجة خلل تقني، أو هجمات خارجية أو ثغرات داخلية.

2. أنواع المخاطر الرقمية:

تشمل هجمات التصيد الإلكتروني والبرامج الخبيثة والفدية الإلكترونية والتهديدات الداخلية من الموظفين، وانكشاف الثغرات الأمنية غير المكتشفة.

3. مفهوم أمن المعلومات:

هو حماية العمليات من التلاعب، أو السرقة، أو الضياع، أو التعديل غير المصرح به، ويستند إلى ثلاثة محاور رئيسية:

- السرية (confidentiality).
- التكامل (Integrity).
- التوافر (Availability).

4. إدارة المخاطر الرقمية:

هي عملية متكاملة تشمل تحديد المخاطر، وتقييم درجة خطورتها، وتحديد أولويات المعالجة، ثم اختيار وتطبيق استجابات مناسبة تقلل من تأثيرها إلى الحد الأدنى.

5. الحوكمة الرقمية:

تشير إلى الأطر التنظيمية والإدارية التي تضمن الاستخدام السليم والأمن لتكنولوجيا المعلومات في المؤسسات، وتعزز من الاتساق والامتثال للتشريعات.

ويبنى الإطار النظري في هذه الدراسة على الربط بين هذه المفاهيم، وتحليلها في سياق مصرفي سعودي، يهدف إلى الوصول إلى نموذج تطبيقي يوضح تأثير جودة إدارة المخاطر الرقمية على حماية المعلومات المصرفية.

الفصل الثالث

منهجية الدراسة

-مقدمة:

يعد اختيار المنهجية العلمية المناسبة عنصرا أساسيا في بناء أي دراسة علمية جادة، إذ تمكن الباحث من تحقيق أهداف البحث والإجابة على تساؤلاته من خلال جمع وتحليل بيانات واقعية باستخدام أدوات ومنهجيات دقيقة. وانطلاقا من طبيعة مشكلة الدراسة، التي تبحث في العلاقة بين إدارة المخاطر الرقمية وأمن المعلومات، فقد تم اعتماد منهجية وصفية تحليلية تجمع بين التحليل النظري والتطبيق الميداني، بهدف الوصول إلى نتائج علمية موثوقة تسهم في تطوير الممارسات الفعلية داخل المؤسسات المصرفية، وتحديدًا في البنك الأهلي السعودي.

وبالإضافة إلى ما سبق، فقد تم اختيار المنهج الوصفي التحليلي كإطار عام للدراسة، لما له من قدرة على وصف الظواهر المتعلقة بإدارة المخاطر الرقمية وتحليلها ضمن السياق المصرفي، كما تم استخدام المنهج المسحي لجمع البيانات من عينة الدراسة المتمثلة في موظفي البنك الأهلي السعودي، من خلال تصميم استبانة علمية محكمة تقيس أبعاد المخاطر الرقمية ومدى إدراك العاملين لها. واعتمدت الدراسة على أدوات تحليل كمية وإحصائية باستخدام برنامج SPSS لتحليل النتائج واختبار الفروض، بما يسهم في الوصول إلى نتائج علمية دقيقة يمكن تعميمها واستثمارها في تطوير سياسات إدارة المخاطر الرقمية داخل البنوك السعودية.

-المنهجية وطرق البحث:

تندرج هذه الدراسة ضمن البحوث التطبيقية التي تهدف الى معالجة مشكلة عملية في بيئة واقعية. وتم اعتماد المنهج الوصفي التحليلي، الذي يعد من أنسب المناهج لدراسة الظواهر المعاصرة من خلال وصفها كما هي وتحليل العلاقة بين متغيراتها.

تستخدم هذا المنهج في هذه الدراسة بغرض وصف مستوى تطبيق إدارة المخاطر الرقمية وتحليل علاقتها بأمن المعلومات في البنك الأهلي السعودي، وذلك من خلال جمع بيانات ميدانية من الموظفين وتحليلها باستخدام أدوات إحصائية تساعد على اختبار الفروض والإجابة عن تساؤلات الدراسة.

وبهدف تعزيز موثوقية النتائج ودقتها، تم تصميم أداة الدراسة (الاستبانة) بناء على مجموعة من الأدبيات العلمية والدراسات السابقة ذات العلاقة، مع مراعاة الجوانب المتعلقة بالصدق والثبات حيث تم عرض الاستبانة على عدد من المحكمين المتخصصين في مجال إدارة المخاطر والحوكمة الرقمية.

كما تم اختيار عينة عشوائية طبقية من موظفي البنك الأهلي السعودي، لضمان تمثيل مختلف الإدارات والمستويات الوظيفية، مما يتيح إمكانية التعميم النسبي للنتائج على مجتمع الدراسة.

وتم إدخال البيانات وتحليلها باستخدام برنامج SPSS، لتطبيق مجموعة من الأساليب الإحصائية مثل التكرارات والنسب والمئوية، والانحدار البسيط، وتحليل التباين (ANOVA)، وذلك لاختبار الفروض ومعرفة طبيعة العلاقة بين المتغيرات المدروسة.

-مجتمع البحث:

يتكون مجتمع الدراسة من جميع موظفين البنك الأهلي السعودي، وبجهد خاص العاملين في الإدارات ذات العلاقة بإدارة المخاطر وتقنية المعلومات وأمن المعلومات، لما لهم من إطلاع مباشر على الإجراءات والسياسات المطبقة في هذا المجال.

أما عينة الدراسة، فستكون عشوائية بسيطة، وتقدر بحوالي (70 إلى 100) موظف، يتم اختيارهم بما يضمن تمثيلاً جيداً لمجتمع الدراسة. وقد تم اختيار هذه العينة بناء على توفر إمكانية الوصول إلى الموظفين، والتنوع الوظيفي داخل الأقسام المستهدفة، ما يسمح بجمع بيانات أكثر دقة وتنوعاً تعكس واقع الممارسات الإدارية والفنية المتعلقة بالمخاطر الرقمية وأمن المعلومات.

أدوات الدراسة:

ستعتمد هذه الدراسة على أداة الاستبانة كأداة رئيسية لجمع البيانات من الميدان. وتم اخيار الاستبانة نظرا لفعاليتها في جمع آراء عدد كبير من المشاركين بطريقة منظمة وقابلة للتحليل الإحصائي. وسيتم تصميم الاستبانة بما يتوافق مع أهداف الدراسة، وتنقسم إلى ثلاثة محاور رئيسية:

1- البيانات الديموغرافية: وتشمل معلومات حول المشارك

(الوظيفة، القسم، سنوات الخبرة، المؤهل العلمي...)

2- فقرات تقيس مستوى إدارة المخاطر الرقمية: مثل

وجود السياسات، تقييم المخاطر، أدوات الرقابة الرقمية.

3- فقرات تقيس كفاءة أمن المعلومات:

من حيث السرية، التوافر، والتكامل، آليات الحماية المعتمدة.

وسيتم التأكد من صدق الأداة من خلال عرضها على عدد من المحكمين ذوي الخبرة، كما سيتم اختبار ثباتها باستخدام معامل كرونباخ ألفا على عينة تجريبية، لضمان موثوقية النتائج.

-حدود البحث:

تخضع هذه الدراسة لعدد من الحدود التي ينبغي توضيحها لتحديد نطاق التطبيق وتشمل:

• الحدود الموضوعية:

تركز الدراسة على العلاقة بين متغيرين أساسيين هما: إدارة المخاطر الرقمية، وأمن المعلومات، دون التطرق إلى المتغيرات الأخرى ذات العلاقة مثل التحول الرقمي أو رضا العملاء.

• الحدود المكانية:

تطبق الدراسة على موظفي البنك الأهلي السعودي، وهو أكبر المؤسسات المصرفية في المملكة، ويعد نموذجا ملائما لدراسة السياسات المتقدمة في مجال الأمن السيبراني.

• الحدود الزمانية:

يتم تنفيذ الدراسة خلال الفصل الدراسي الثاني من العام الأكاديمي 2024 وهو الإطار الزمني الذي سيتم من خلاله جمع وتحليل البيانات.

• الحدود البشرية:

تقتصر المشاركة على العاملين في الإدارات الفنية والإدارية المرتبطة مباشرة بموضوع الدراسة لضمان موثوقية البيانات ودقتها.

الفصل الرابع

النتائج والتوصيات

-مقدمة:

يعرض هذا الفصل نتائج الدراسة الميدانية التي تم جمعها باستخدام أداة الاستبانة الموجهة إلى موظفي البنك الأهلي السعودي، حيث تم تحليل البيانات باستخدام الأساليب الإحصائية المناسبة للوصول إلى نتائج دقيقة وموثوقة.

ويتضمن الفصل تقديمًا لنتائج تحليل البيانات الديموغرافية، ونتائج تحليل فقرات الدراسة المتعلقة بإدارة المخاطر الرقمية وأمن المعلومات، إضافة إلى اختيار الفرضيات الأساسية والفرعية، وأخيرًا تقديم التوصيات المقترحة في ضوء النتائج المتوصل إليها.

-تحليل البيانات:

تم توزيع عدد (100) استبانة على عينة عشوائية من موظفي البنك الأهلي السعودي، واستعيد منها (85) استبانة صالحة للتحليل الإحصائي، بنسبة استجابة بلغت 85%. وبعد ترميز البيانات وإدخالها في برنامج التحليل الإحصائي (SPSS). تم إجراء التحليلات الآتية:

1. الخصائص الديموغرافية للمشاركين:

أظهرت النتائج تنوع العينة من حيث مؤهلات وسنوات الخبرة والمجالات الوظيفية، حيث بلغت نسبة المشاركين من ذوي الخبرة التي تزيد عن 5 سنوات حوالي 60%، مما يعكس مستوى نضج معرفي ومهني لدى الأفراج المستجيبين، ويضفي موثوقية على البيانات المستخلصة.

2. تحليل محاور إدارة المخاطر الرقمية:

بينت نتائج الاستجابات أن المتوسط العام لتطبيق إدارة المخاطر الرقمية بلغ (3.89 من 5)، ما يشير إلى أن البنك الأهلي السعودي يولي أهمية ملموسة لهذا المجال. ومن أبرز المؤشرات التي سجلت نسبا مرتفعة: وجود سياسات مكتوبة لإدارة المخاطر الرقمية، والقيام بتقييمات دورية، بالإضافة إلى برامج تدريب مستمرة للعاملين.

3. تحليل محاور أمن المعلومات:

أظهر التحليل أن المتوسط العام لمستوى كفاءة نظام أمن المعلومات بلغ (4.02 من 5)، مما يدل على التزام البنك بتطبيق ضوابط أمنية فعالة، خاصة على مستوى سرية المعلومات وسهولة استرجاع البيانات عند الحاجة. وقد أشاد عدد من المشاركين بسرعة الاستجابة عند حدوث تهديد سيبراني.

4. العلاقة بين إدارة المخاطر الرقمية وأمن المعلومات:

بناءً على معامل ارتباط بيرسون (Person Correlation)، وجدت علاقة ارتباط موجبة قوية ذات دلالة إحصائية بين إدارة المخاطر الرقمية وأمن المعلومات، حيث بلغ معامل الارتباط ($r=0.74$) عند مستوى دلالة ($p < 0.01$)، وهو ما يؤكد أن تعزيز إدارة المخاطر ينعكس بشكل مباشر على كفاءة حماية البيانات والأنظمة.

-النتائج:

في ضوء التحليل السابق، يمكن تلخيص أهم النتائج التي توصل إليها الدراسة على النحو الآتي:

- يطبق البنك الأهلي السعودي مجموعة من السياسات والإجراءات في إدارة المخاطر الرقمية، تشمل التقييم الدوري، وخطط الاستجابة للطوارئ، وبرامج التوعية المستمرة.
- يوجد مستوى عال من الوعي بأهمية المعلومات لدى موظفي البنك، خاصة في الأقسام الفنية، مما يعزز من كفاءة التصدي لأي تهديدات محتملة.
- ترتبط فعالية نظام أمن المعلومات ارتباطاً وثيقاً بجودة تطبيق إدارة المخاطر الرقمية، ما يثبت وجود علاقة طردية قوية بين المتغيرين المدروسين.
- هناك حاجة إلى دمج أكبر للحوكمة الرقمية ضمن السياسات اليومية للبنك لتعزيز الاستدامة والامتثال المستمر للمعايير الدولية.

-التوصيات:

بناء على النتائج التي تم التوصل إليها، توصى الدارسة بما يلي:

1. تعزيز التكامل بين إدارة المخاطر الرقمية وأمن المعلومات من خلال مراجعة وتحديث السياسات بشكل دوري لتتواءم مع تطورات التهديدات التقنية.
2. رفع كفاءة العنصر البشري عبر تنفيذ برامج تدريبية متخصصة في الأمن السيبراني وإدارة الحوادث الرقمية، تستهدف العاملين في مختلف الأقسام.
3. اعتماد مؤشرات أداء كمية لقياس فعالية إدارة المخاطر بشكل دوري، وربط هذه المؤشرات بتقارير الأداء المؤسسي.
4. تشجيع الابتكار الأمني الداخلي عبر دعم وحدات الابتكار والبحث داخل البنك، والتعاون مع الجامعات ومراكز البحث العلمي في مجالات الأمن السيبراني.
5. تبني نظام حوكمة تقنية متكامل يشمل الإشراف والتقييم المستمر لأداء النظم الأمنية، مع توثيق إجراءات الاستجابة وتقييم الجاهزية الإلكترونية.

المراجع

-المراجع العربية

- العزب، محمد. (2023). أثر التحديدات السيبرانية على أداء البنوك التجارية في مصر. مجلة البحوث المالية والمصرفية، 17(2)، 155-178.
- الحمادي، فهد. (2022). الحوكمة الرقمية في البنوك الخليجية: الواقع والمأمول. المجلة العربية للإدارة، 42(1)، 98-112.

-المراجع الأجنبية-

- Gunawan, S., & Melinda, T. (2021). The effect of cybersecurity governance on data protection in Indonesian financial institutions. *Journal of Information Security*, 12(3), 85–104.
- AL Harthy, K., & Khan, R. (2020). Digital risk management frameworks and cyber resilience in Saudi banks. *International Journal of Cybersecurity*, 9(4), 211–228.

الملاحق

-الاستبانة:-

عزيزي المشارك،

تهدف هذه الاستبانة إلى دراسة العلق بين إدارة المخاطر الرقمية وأمن المعلومات في البنك الأهلي السعودي، وتستخدم جميع المعلومات لأغراض بحثية فقط، بسرية تامة.

أولاً: البيانات العامة:

- القسم الوظيفي () .
- سنوات الخبرة () .
- المؤهل العلمي () .

ثانياً: إدارة المخاطر الرقمية:

(اختر من 1 إلى 5 حيث: 1 = لا أوافق بشدة، 5 = أوافق بشدة).

1. توجد سياسات مكتوبة لإدارة المخاطر الرقمية في البنك.
2. يتم إجراء تقييم دوري للمخاطر الرقمية.
3. يتلقى الموظفون تدريباً منتظماً في مجال أمن المعلومات.
4. توجد خطة استجابة موقفة لحوادث الأمن السيبراني.
5. يتم تحديث أنظمة الحماية الرقمية بشكل مستمر.

ثالثاً: أمن المعلومات:

(اختر من 1 إلى 5 حيث: 1 = لا أوافق بشدة، 5 = أوافق بشدة).

1. معلومات العملاء محمية بسرية عالية.
2. تتوفر أنظمة احتياطية لحفظ البيانات.
3. يتم مراقبة الأنظمة الأمنية بشكل يومي.
4. توجد سياسة واضحة للتعامل مع الحوادث الأمنية.
5. يتم اختبار نظم الحماية بشكل دوري.

شكراً لمشاركتك وتعاونك في دعم البحث العلمي.

-الملخص Abstract:

شهدت البيئة الرقمية في المملكة العبرية السعودية تطورات رقمية متسارعة، مما أدى إلى تصاعد المخاطر المرتبطة بالأمن السيبراني، وفي هذا السياق، تهدف هذه الدراسة إلى تحليل أثر إدارة المخاطر الرقمية على أمن المعلومات في البنك الأهلي السعودي. تم اعتماد المنهج الوصفي التحليلي واستخدام الاستبانة كأداة رئيسية لجمع البيانات من عينة مكونة من موظفي البنك في إدارات تقنية المعلومات وإدارة المخاطر.

وقد توصلت الدراسة إلى وجود علاقة ارتباط موجبة ذات دلالة إحصائية بين مستوى تطبيق إدارة المخاطر الرقمية ومستوى أمن المعلومات، مما يؤكد أهمية تبني سياسات أمنية فعالة ومحدثة باستمرار. كما أوصت الدراسة بضرورة تعزيز برامج التوعية والتدريب الأمني، وتطوير مؤشرات قياس أداء إلكترونية لمراقبة فعالية نظم الحماية، وتكامل الحوكمة الرقمية مع إدارة المخاطر.

الكلمات المفتاحية: إدارة المخاطر الرقمية، وأمن المعلومات، البنك الأهلي السعودية، الحوكمة السيبرانية.

Midocean University

College of Management

Department of Risk Management

Digital Risk management in Saudi Banks:
An Applied Study on the National Commercial Bank
(NCB)

Prepared by:

AHMED SAAD ALTURKI

Supervised by:

Dr. Al Faisal Abdulhamid

Dr. Fayez Jarad

Year:2025