

عنوان المشروع
تأثير إدارة المخاطر السيبرانية على الأداء المالي للمؤسسات المالية
في المملكة العربية السعودية

أسم الطالب
أحمد نور محمد عبد الشكور
٢٠٢١٢٠٢٤٣٥

مشروع تخرج- ١
كلية الإدارة- جامعة ميدأوشن

إشراف
د. منى مصطفى العشري
عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

جدول المحتويات

٢	١. الفصل الأول: الإطار العام للدراسة.....
٣	١,١. المقدمة:
٧	١,٢. مشكلة الدراسة.....
٨	١,٢,١. فجوات على المستوى النظري.....
٩	١,٢,٢. فجوات على المستوى التطبيقي.....
١١	١,٣. أهمية الدراسة.....
١٣	١,٣,١. على المستوى النظري:
١٤	١,٣,٢. على المستوى التطبيقي:
١٥	١,٤. أسئلة الدراسة.....
١٥	١,٥. أهداف الدراسة.....
١٧	١,٦. فرضيات الدراسة.....
١٩	١,٧. نموذج الدراسة.....
٢٠	١,٨. منهجية الدراسة.....
٢١	١,٩. مخطط المشروع المقترح.....
٣٣	قائمة المراجع.....

١. الفصل الأول: الإطار العام للدراسة

١,١. المقدمة:

إدارة المخاطر السيبرانية في المؤسسات المالية لم تعد مجرد جزء عادي من الإدارة اليومية، بل أصبحت عنصرًا محوريًا يحدد مستقبل هذه المؤسسات في مواجهة التحديات المتزايدة التي يفرضها العالم الحديث. ففي ظل التغيرات الاقتصادية السريعة والتطورات التقنية التي لا تهدأ، تجد المؤسسات المالية نفسها أمام معركة مستمرة للحفاظ على استقرارها وقدرتها على المنافسة. في هذا السياق، تُعد إدارة المخاطر المالية أحد الأعمدة الأساسية التي تقوم عليها استدامة المؤسسات، وهذا ما يُجمع عليه الباحثون في مختلف المجالات ذات الصلة. لا يمكن إغفال الارتفاع الملحوظ في الخسائر المالية الناتجة عن الهجمات السيبرانية، كما تشير الدراسات الحديثة. فوفقًا لـ Biener وزملائه (٢٠١٥)، فإن هذه الخسائر تجاوزت مجرد التكاليف المباشرة المرتبطة بإصلاح الأنظمة أو استعادة البيانات المخترقة، لتصل إلى مستويات أعمق وأكثر تعقيدًا. هذه الخسائر تشمل تأثيرات طويلة الأمد مثل تآكل الثقة لدى العملاء والشركاء، وتضرر السمعة التي بنتها المؤسسة على مر السنين. إن الهجوم السيبراني الذي يستهدف مؤسسة مالية لا يقتصر ضرره على النواحي المالية فحسب، بل يمتد ليشمل الأبعاد النفسية والاجتماعية التي قد تؤثر على العلاقات التجارية والاستقرار العام للمؤسسة داخل السوق. وما يعزز هذا الواقع أن إدارة المخاطر لم تعد ترقى أو جزءًا جانبيًا من استراتيجية المؤسسة، بل هي اليوم أحد الأركان الأساسية في بناء استراتيجية شاملة ومستدامة. الاستثمار في الأمن السيبراني، وفقًا للعديد من الخبراء، لم يعد خيارًا يمكن للمؤسسات تجاهله، بل أصبح ضرورة ملحة تفرضها الظروف الراهنة لضمان استمرار المؤسسات وحمايتها من الخسائر المالية المحتملة. يوضح Eling & Wirfs (٢٠١٥) في دراستهما أن المؤسسات التي تركز موارد كافية لتطوير أنظمة الأمن السيبراني تكون في وضع أفضل للتصدي للهجمات السيبرانية والتعافي منها بشكل أسرع. هذا النوع من الاستثمار لا يقتصر على حماية الأصول المالية والبنية التحتية الرقمية فحسب، بل يمتد ليصبح عنصرًا جاذبًا للمستثمرين والعملاء على حد سواء. فالاستثمار في الأمن السيبراني يعزز الثقة في قدرة المؤسسة على حماية بيانات العملاء وتأمين العمليات، وهو ما يترجم إلى مكانة تنافسية أقوى في السوق العالمية. لكن الحديث عن الأمن السيبراني لا يتوقف عند الحاضر فقط، بل يتعداه إلى المستقبل الذي يلوح في الأفق بتحدياته التقنية. يلقي Mosca (٢٠١٨) الضوء على أن الحوسبة الكمية، على سبيل المثال، تشكل تهديدًا كبيرًا لأنظمة التشفير التقليدية التي نعتمد عليها اليوم. فهذه التقنية الجديدة قد تغير الطريقة التي نحمي بها البيانات، مما يعني أن المؤسسات التي لا تستعد لهذه التغيرات التقنية قد تجد نفسها عرضة لاختراقات قد تكلفها أكثر مما تستطيع تحمله. لذلك، أصبح من الضروري الاستثمار في تقنيات تشفير جديدة

قادرة على مقاومة تهديدات الحوسبة الكمية، مثل التشفير القائم على الشبكات (lattice-based cryptography)، لضمان استمرار الحماية على المدى الطويل.

إن أهمية إدارة المخاطر السيبرانية تتجلى أيضًا في فهم العلاقة المعقدة بين المتغيرات المختلفة التي تؤثر على الأداء المالي للمؤسسات. فالعلاقة بين الاستثمار في الأمن السيبراني والأداء المالي ليست علاقة بسيطة أو مباشرة، بل هي علاقة معقدة تتداخل فيها عدة عوامل تشمل التكنولوجيا، الحوكمة، والبيئة التنظيمية التي تعمل فيها المؤسسة. يدعو Saidov (٢٠٢٣) إلى فهم المخاطر السيبرانية النظامية، وهي المخاطر التي تنشأ عن الاعتماد الكبير على الأنظمة التكنولوجية المتطورة. فهم هذه المخاطر يتطلب من المؤسسات تطوير استراتيجيات متكاملة لإدارة المخاطر تجمع بين الجوانب التقنية والمالية والإدارية، وذلك لضمان استقرار المؤسسة وقدرتها على التكيف مع التغيرات السريعة.

من منظور استراتيجي، يمثل الاستثمار في إدارة المخاطر السيبرانية أحد الركائز الأساسية للاستدامة والابتكار في المؤسسات المالية. يؤكد Shackelford (٢٠١٢) أن المؤسسات التي تتبنى سياسات قوية في مجال الأمن السيبراني ليست فقط قادرة على تجنب الخسائر المالية الناتجة عن الهجمات، بل تزيد أيضًا من جاذبيتها لدى المستثمرين الذين يبحثون عن استثمار آمن في شركات تتمتع بأنظمة أمان متطورة. في هذا السياق، يصبح الأمن السيبراني عنصرًا أساسيًا في استراتيجيات الحوكمة المؤسسية، حيث يساهم في بناء سمعة إيجابية للمؤسسة ويعزز من قدرتها على جذب واستبقاء العملاء والمستثمرين.

وفي ظل هذه التحديات المتزايدة، تجد المؤسسات المالية نفسها مضطرة إلى تطوير استراتيجيات متقدمة لإدارة المخاطر السيبرانية، تشمل الاستعداد لمواجهة التهديدات المستقبلية مثل تلك المرتبطة بالحوسبة الكمية والذكاء الاصطناعي، وكذلك تعزيز القدرات التشغيلية لتقليل الفجوات التي قد تؤدي إلى تعرض المؤسسات لهجمات سيبرانية.

في المملكة العربية السعودية، تتزايد أهمية إدارة المخاطر السيبرانية مع تبني رؤية ٢٠٣٠، التي تسعى إلى تحويل الاقتصاد السعودي إلى اقتصاد متنوع ومستدام. تعتبر رؤية ٢٠٣٠ خطوة استراتيجية تهدف إلى تعزيز دور القطاع المالي كركيزة أساسية لتحقيق النمو الاقتصادي المستدام. ولكن لتحقيق هذه الرؤية الطموحة، تواجه المملكة تحديات كبيرة، منها التحديات الرقمية والمالية والمعلوماتية التي تتطلب نهجًا شاملاً لإدارة المخاطر. ومع تحول الاقتصاد السعودي نحو مزيد من الانفتاح والاعتماد على التكنولوجيا، يبرز دور إدارة المخاطر في ضمان استقرار المؤسسات المالية وقدرتها على التكيف مع التغيرات السريعة في

السوق. إلى جانب ذلك، يشير Power (٢٠٠٧) إلى أن الطبيعة غير المتوقعة لبعض الأحداث الاقتصادية والتقنية تتطلب من المؤسسات المالية تبني استراتيجيات مرنة وقابلة للتكيف. في ضوء رؤية ٢٠٣٠، التي تسعى إلى تنويع الاقتصاد السعودي وتعزيز دوره في الاقتصاد العالمي، يجب أن تكون المؤسسات المالية السعودية قادرة على مواجهة المخاطر الجديدة والمتغيرة. هذه المرونة تتطلب استخدام أدوات تحليلية متقدمة، بما في ذلك استخدام البيانات الكبيرة (Big Data)، كما أشار Mayer-Schönberger وCukier (٢٠١٣). استخدام البيانات الكبيرة يمكن المؤسسات المالية من تحليل كميات هائلة من المعلومات بشكل سريع وفعال، مما يساعدها في التنبؤ بالمخاطر المالية وإدارتها بشكل أفضل.

وفي هذا السياق، يُعتبر التحول الرقمي الذي تشهده المملكة جزءاً أساسياً من رؤية ٢٠٣٠، ولكنه يجلب معه تحديات جديدة، لاسيما فيما يتعلق بالأمن السيبراني. المخاطر السيبرانية أصبحت تشكل تهديداً متزايداً للمؤسسات المالية، حيث تعتمد الكثير من العمليات المالية اليوم على التكنولوجيا الرقمية. وفقاً لما ذكره McCarthy وCampbell (٢٠١٢)، فإن تقييم المخاطر السيبرانية يجب أن يكون جزءاً لا يتجزأ من استراتيجية إدارة المخاطر العامة في المؤسسات المالية. ويتطلب ذلك وضع خطط دقيقة لحماية البيانات الحساسة وضمان استمرارية العمليات في حالة حدوث هجمات سيبرانية.

علاوة على ذلك، تواجه المؤسسات المالية السعودية تحديات متزايدة في مجال الحوكمة المؤسسية والبنية التحتية الحديثة وتحديث البيئة التنظيمية، حيث أصبح الالتزام بالشفافية والمساءلة جزءاً أساسياً من استراتيجيات إدارة المخاطر. يشير Lam (٢٠٠٣) إلى أن الحوكمة المؤسسية الجيدة تعزز من فعالية استراتيجيات إدارة المخاطر من خلال ضمان الامتثال للإجراءات والسياسات المطلوبة. في إطار رؤية ٢٠٣٠، تسعى المملكة إلى تعزيز الشفافية والحوكمة الجيدة في القطاع المالي، مما يعزز الثقة ويجذب المزيد من الاستثمارات.

تظهر إدارة المخاطر كأحد الأعمدة الأساسية لضمان نجاح المؤسسات المالية في المملكة العربية السعودية في ظل رؤية ٢٠٣٠. إن تحقيق الأهداف الطموحة لهذه الرؤية يتطلب من المؤسسات المالية تبني ممارسات إدارة مخاطر متقدمة وشاملة تتماشى مع التحديات الرقمية والمالية والمعلوماتية التي تواجهها. يجب أن تكون هذه الممارسات مرنة وقابلة للتكيف مع التغيرات السريعة في السوق، وتعتمد على فهم عميق للبيئة التنظيمية والسياسات المؤسسية، مع الاستفادة من الأدوات التحليلية المتقدمة مثل البيانات الكبيرة والتقنيات الأمنية السيبرانية.

في ضوء التحديات المتزايدة التي تواجه المؤسسات المالية في المملكة العربية السعودية، فإن القدرة على التكيف مع التطورات السريعة والتحولات الكبيرة تعتبر أمراً بالغ الأهمية. المؤسسات التي تستطيع استباق هذه التحديات والتعامل معها بمرونة واستجابة سريعة ستكون في وضع أفضل للحفاظ على استقرارها ونموها في المستقبل. لذلك، تُعد إدارة المخاطر السيبرانية استراتيجية حاسمة ليس فقط لحماية الأصول والمؤسسات، بل أيضاً لتعزيز قدرة المؤسسات المالية على الابتكار وتحقيق الاستدامة في بيئة أعمال عالمية متزايدة التعقيد.

كيف تؤثر ممارسات إدارة المخاطر السيبرانية على الأداء المالي لهذه المؤسسات، وما دور المتغيرات المعدلة والوسيط في هذه العلاقة؟

لتحقيق فهم دقيق للعلاقة بين إدارة المخاطر السيبرانية وأداء المؤسسات المالية في المملكة العربية السعودية، سيعتمد هذا البحث على منهجية وصفية تحليلية، حيث سيتم جمع البيانات من مصادر متنوعة تشمل التقارير المالية للمؤسسات، والدراسات السابقة، والمقابلات مع خبراء في مجال إدارة المخاطر. سيتم استخدام أدوات تحليل إحصائية متقدمة لتحليل البيانات واستخلاص النتائج المتعلقة بتأثير ممارسات إدارة المخاطر السيبرانية على الأداء المالي. ستتم دراسة المتغيرات المستقلة مثل ممارسات إدارة المخاطر المختلفة، والمتغيرات التابعة مثل الأداء المالي، بالإضافة إلى المتغيرات المعدلة والوسيط مثل حجم المؤسسة، والبيئة التنظيمية، وجودة الإدارة.

هذا البحث سيساهم في تقديم رؤى عملية للمؤسسات المالية في السعودية حول كيفية تحسين استراتيجيات إدارة المخاطر السيبرانية وتعزيز أدائها المالي، مع الأخذ بعين الاعتبار التحديات الفريدة التي تواجهها في السياق المحلي.

١,٢. مشكلة الدراسة

تتمثل مشكلة هذه الدراسة في الفجوة الكبيرة التي لا تزال قائمة بين الفهم النظري والتطبيق العملي لإدارة المخاطر السيبرانية وتأثيرها الحاسم على الأداء المالي للمؤسسات المالية في المملكة العربية السعودية. على الرغم من الجهود المستمرة لتعزيز الأمن السيبراني، تجد العديد من هذه المؤسسات نفسها تواجه تحديات جمة في تطوير استراتيجيات فعالة لإدارة المخاطر السيبرانية، لاسيما في مواجهة التهديدات المتزايدة التي تفرضها التكنولوجيا الحديثة مثل الذكاء الاصطناعي والحوسبة الكمية.

إن المخاطر التي تلوح في الأفق مع تطور هذه التقنيات الجديدة ليست مجرد تحديات نظرية؛ فهي قد تزداد تعقيداً بمرور الوقت، مما يُصعّب من قدرة المؤسسات المالية على حماية نفسها. على سبيل المثال، بينما يحمل الذكاء الاصطناعي وعوداً كبيرة بتحسين الكفاءة التشغيلية وتقديم خدمات مالية مبتكرة، فإنه أيضاً يأتي مصحوباً بمخاطر غير مسبوقة. في هذا السياق، حذر Bostrom & Yudkowsky (2014) من أن الذكاء الاصطناعي يمكن أن يمكّن من ظهور هجمات سيبرانية جديدة وأكثر تعقيداً، مثل تلك التي تستخدم تقنيات تعلم الآلة لاكتشاف واستغلال الثغرات الأمنية بطرق تتجاوز الفهم التقليدي لهذه التهديدات.

وعلاوة على ذلك، فإن إدارة المخاطر السيبرانية ليست مجرد مسألة تقنية، بل تمثل عبئاً مالياً كبيراً على المؤسسات المالية. حيث يتطلب الأمر تخصيص ميزانيات كبيرة لتطوير وتحديث أنظمة الأمن السيبراني، فضلاً عن الحاجة إلى توظيف خبراء متخصصين في هذا المجال وتدريب الموظفين على كيفية التعامل مع التهديدات السيبرانية المتطورة (Schneier 2015). أشار إلى أن نهجاً شاملاً في إدارة المخاطر السيبرانية يجب أن يأخذ في الاعتبار التكاليف المرتبطة بحماية الأنظمة، والاستثمار في التكنولوجيا الحديثة، وتطوير استراتيجيات استجابة فعالة للطوارئ. هذه التكاليف يمكن أن تشكل ضغطاً إضافياً على المؤسسات المالية، مما يؤثر بشكل مباشر على مصاريفها العامة وقدرتها على تحقيق أرباح مستدامة.

عند تحليل متغيرات الدراسة، يظهر بوضوح أن القصور في إدارة المخاطر السيبرانية، بالإضافة إلى عدم الفهم الكامل لتأثير هذه المخاطر على الأداء المالي، يمكن أن يؤدي إلى تدهور استقرار المؤسسات المالية. كما أن البيئة التنظيمية المتغيرة وحجم المؤسسات يلعبان دوراً كبيراً في كيفية إدارة هذه المخاطر. فمن ناحية، قد تتمكن المؤسسات الكبيرة ذات الموارد الوفيرة من تخصيص ميزانيات أكبر

لحماية نفسها ضد المخاطر السيبرانية، مما قد يؤدي إلى تحسين أدائها المالي. بينما قد تواجه المؤسسات الأصغر صعوبات أكبر في التكيف مع التهديدات السيبرانية المتزايدة نظرًا لمحدودية مواردها.

في هذا السياق، تظهر الحاجة الملحة لفهم أعمق لتأثير إدارة المخاطر السيبرانية على الأداء المالي للمؤسسات المالية في المملكة العربية السعودية، خاصة في ظل التطورات التكنولوجية السريعة واستخدام تقنيات الذكاء الاصطناعي والحوسبة الكمية. تهدف هذه الدراسة إلى استكشاف كيفية تأثير هذه المخاطر على الاستقرار المالي للمؤسسات، وتقديم توصيات لتعزيز قدرتها على مواجهة التحديات المستقبلية، بما يتماشى مع طموحات رؤية ٢٠٣٠ التي تسعى إلى تحويل المملكة إلى مركز مالي عالمي يتمتع بمستويات عالية من الأمن والاستدامة.

"كيف يمكن تطوير استراتيجيات إدارة المخاطر السيبرانية في المؤسسات المالية؟"

١,٢,١. فجوات على المستوى النظري

• فجوة في الأدبيات المتعلقة:

برز فجوة كبيرة في الأدبيات المتعلقة بتأثير المتغيرات المعدلة والوسيط على العلاقة بين إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية في المملكة العربية السعودية. معظم الدراسات الموجودة تركز بشكل كبير على العلاقة المباشرة بين إدارة المخاطر السيبرانية والأداء المالي، متجاهلة بذلك تأثير المتغيرات الأخرى التي قد تعزز أو تحد من هذه العلاقة. على سبيل المثال، الحوكمة المؤسسية تعتبر متغيرًا وسيطًا حاسمًا قد يؤثر بشكل كبير على كيفية تحويل استراتيجيات إدارة المخاطر السيبرانية إلى نتائج مالية ملموسة كما لا يزال هناك نقص في الأبحاث التي تستكشف بعق كيفية تأثير الحوكمة على العلاقة بين إدارة المخاطر السيبرانية والأداء المالي.

• فجوة في النماذج النظرية الحالية:

النماذج النظرية الحالية لإدارة المخاطر السيبرانية قد لا تكون كافية للتعامل مع التهديدات السيبرانية المتطورة باستمرار. هناك حاجة إلى تطوير نماذج نظرية جديدة تأخذ في الاعتبار الطبيعة الديناميكية للتهديدات السيبرانية خصوصًا مع صعود الذكاء الاصطناعي وتطور الأبحاث في الكمبيوترات الكمية الذين يأتیان في قمة هذه التهديدات، على الرغم من أن التكنولوجيا المالية (Fintech) أصبحت جزءًا لا يتجزأ من العمليات المالية في المملكة، إلا أن هناك نقصًا في الدراسات التي تستكشف كيفية إدارة

المخاطر السيبرانية الناتجة عن هذا التحول الرقمي. ومع ذلك، لا تزال هناك فجوة تطبيقية في كيفية تصميم وتنفيذ هذه الاستراتيجيات بشكل يتماشى مع التهديدات السيبرانية المتزايدة.

- **الفجوة في فهم العلاقة بين المخاطر السيبرانية والمخاطر التشغيلية الأخرى:**

هناك فجوة نظرية تتعلق بكيفية تفاعل المخاطر السيبرانية مع أنواع أخرى من المخاطر التشغيلية (مثل المخاطر المالية، المخاطر القانونية، إلخ). بينما يتم التعامل مع المخاطر السيبرانية غالبًا على أنها فئة منفصلة، فإن القليل من الأبحاث يتناول كيفية تكاملها مع إدارة المخاطر الشاملة.

١,٢,٢. فجوات على المستوى التطبيقي

- **جودة البنية التحتية:**

تتفاوت المؤسسات المالية في جودة وتحديث البنية التحتية التقنية المستخدمة لحماية أنظمتها وبياناتها. في بعض الأحيان، قد تكون البنية التحتية قديمة أو غير مهيأة بشكل كافٍ لمواجهة التهديدات السيبرانية المتطورة. وعدم تحديث البنية التحتية بشكل مستمر يعرض المؤسسة لثغرات أمنية يمكن استغلالها من قبل القراصنة. هذا التفاوت في تحديثات البنية التحتية يمثل فجوة تطبيقية كبيرة في قدرة المؤسسة على تنفيذ استراتيجيات الأمن السيبراني بشكل فعال.

- **عدم كفاية الاستثمار في الأمن السيبراني:**

قد تواجه المؤسسات المالية تحديات في تخصيص الموارد المالية الكافية للاستثمار في تكنولوجيا الأمن السيبراني، بما في ذلك الحلول التقنية، التدريب، وتحديث البنية التحتية. هذا النقص في الاستثمار يمكن أن يكون نتيجة لعدم وجود فهم كافٍ لأهمية الأمن السيبراني أو بسبب قيود الميزانية. ويؤدي نقص الاستثمار إلى ضعف في الأنظمة الأمنية، مما يزيد من تعرض المؤسسة للتهديدات السيبرانية ويقلل من فعالية استراتيجيات إدارة المخاطر السيبرانية.

- **التحديات في الامتثال التنظيمي والتشريعي:**

تواجه المؤسسات المالية صعوبة في التكيف مع التشريعات والقوانين المتغيرة باستمرار المتعلقة بالأمن السيبراني. رغم وجود نظريات توضح أهمية الامتثال، إلا أن التطبيق العملي قد يتعثر بسبب تعقيدات التنظيمات وعدم وضوحها في بعض الأحيان. ويؤدي عدم الامتثال الكامل للتنظيمات القانونية إلى زيادة احتمالية حدوث اختراقات سيبرانية.

- **التدريب والوعي الأمني:**

قد يفقر موظفو البنوك المركزية إلى الوعي الكافي بالتهديدات السيبرانية وأفضل الممارسات الأمنية. هذا يمكن أن يجعلهم عرضة للهجمات التي تعتمد على الهندسة الاجتماعية، مثل التصيد الاحتيالي؛ لذلك التدريب يمثل فجوة تطبيقية حقيقية في إدارة المخاطر السيبرانية. إذا لم يتم تطوير وتنفيذ برامج تدريبية فعالة ومستمرة على جميع المستويات داخل المؤسسة، فإن ذلك يمكن أن يؤدي إلى ثغرات أمنية خطيرة. لسد هذه الفجوة، تحتاج المؤسسات إلى تبني نهج شامل في التدريب يشمل التحديث المستمر، الممارسة العملية، وإشراك جميع الموظفين في تعزيز الأمن السيبراني.

- **عدم كفاية إجراءات إدارة المخاطر السيبرانية:**

قد لا تكون إجراءات إدارة المخاطر السيبرانية في بعض البنوك المركزية شاملة أو فعالة بما يكفي للتعامل مع مجموعة واسعة من المخاطر، بما في ذلك المخاطر السيبرانية. هناك حاجة إلى تطوير وتطبيق السياسات وإجراءات إدارة مخاطر أكثر قوة.

- **قصور في التعاون وتبادل المعلومات:**

قد يكون هناك نقص في التعاون وتبادل المعلومات بين المؤسسات المالية ومؤسسات الأمن السيبراني الأخرى. يمكن أن يؤدي هذا إلى عدم كفاية المعلومات الاستخباراتية حول التهديدات، مما يجعلها أكثر عرضة للهجمات.

١,٣. أهمية الدراسة

هذه الدراسة تهدف إلى تقديم إسهام مهم في الأدبيات العلمية من خلال تقديم فهم أعمق وشامل للعلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية في المملكة العربية السعودية. في عالم يتسم بتعقيدات مالية متزايدة، لم تعد إدارة المخاطر مجرد إجراء وقائي، بل أصبحت ضرورة استراتيجية تساهم في بناء استقرار مالي طويل الأمد (John C. Hull (2012)، وهو أحد الأسماء البارزة في مجال إدارة المخاطر المالية، يؤكد أن "إدارة المخاطر أصبحت جزءاً لا يتجزأ من الاستراتيجية الشاملة للمؤسسات المالية، حيث تسهم بشكل كبير في تعزيز استقرارها المالي على المدى الطويل". من خلال هذا البحث، نسعى إلى سد الفجوات القائمة في الأدبيات من خلال تحليل دقيق لتأثير المتغيرات المعدلة والوسيط، مع التركيز على الخصوصيات المحلية للسوق السعودي.

في هذا السياق، يتفق Douglas W. Hubbard (2009) على ضرورة تكييف استراتيجيات إدارة المخاطر مع السياقات المحلية، حيث يشير إلى أن "عدم تخصيص استراتيجيات إدارة المخاطر للسياق المحلي يمكن أن يؤدي إلى نتائج غير متوقعة تؤثر سلباً على الأداء المالي". هذه الرؤية تبرز أهمية التركيز على السياق السعودي لتطوير استراتيجيات إدارة مخاطر فعالة تتماشى مع التحديات الفريدة التي تواجهها المؤسسات المالية في المملكة.

على المستوى الأكاديمي، يُتوقع أن يساهم هذا البحث في تطوير قاعدة معرفية متقدمة تكون مرجعاً للباحثين الذين يدرسون إدارة المخاطر في سياقات مشابهة Robert S. Kaplan و Anette Mikes (2012). قدما نموذجاً للإدارة المتكاملة للمخاطر في المؤسسات، مشددين على أن "الدمج بين إدارة المخاطر واستراتيجيات المؤسسة يتيح تحسين الأداء المالي وتقليل التعرض للمخاطر". هذا البحث يهدف إلى توسيع نطاق الدراسات الأكاديمية لتشمل تأثير عوامل مثل جودة الإدارة، الحوكمة، والمستوى التقني على إدارة المخاطر في السياقات المحلية، مما يعزز من فهم أعمق لكيفية تحسين الأداء المالي.

لتحقيق هذا الفهم العلمي العميق، يمكن سد الفجوات بين المتغيرات النظرية والتطبيقية من خلال تطوير إطار عمل يجمع بين النماذج النظرية المستخدمة في إدارة المخاطر السيبرانية والممارسات الفعلية التي تطبقها المؤسسات المالية مما يبرز أهمية تكامل النظريات مع التطبيقات العملية لتحسين إدارة المخاطر السيبرانية في السياق السعودي.

إلى جانب ذلك، يجب إجراء تحليل متعمق للمتغيرات المعدلة مثل البيئة التنظيمية وحجم المؤسسة، بالإضافة إلى المتغيرات الوسيطة مثل جودة الإدارة ومستوى التقنية مما يدل على ضرورة تحليل العلاقة التفاعلية بين هذه المتغيرات وكيفية تأثيرها على النتائج المالية للمؤسسات.

من خلال دراسة دراسات حالة محلية، يمكن توضيح كيفية تأثير المتغيرات السياقية في المملكة العربية السعودية على إدارة المخاطر السيبرانية. هذه الدراسات تساعد في فهم كيفية تأثير البيئة التنظيمية المحلية على استراتيجيات إدارة المخاطر السيبرانية، وهو ما يتماشى مع ما ذكره Robert S. Kaplan و (1996) حيث أكدوا أن "تكيف الاستراتيجيات مع الظروف المحلية يزيد من فرص نجاحها"، مما يشير إلى أهمية الدراسات التي تتناول البيئة المحلية وكيفية تأثيرها على إدارة المخاطر.

استنادًا إلى نتائج هذا التحليل، يمكن تطوير استراتيجيات مخصصة للمؤسسات المالية السعودية تأخذ في الاعتبار حجم المؤسسة، مستوى تبني التكنولوجيا، والضغوط التنظيمية .

ولا يقتصر الأمر على الاستراتيجيات فحسب؛ فسد الفجوات يتطلب أيضًا تركيزًا كبيرًا على التعليم والتدريب. يمكن أن تشمل برامج التدريب المتخصصة التي تعزز فهم العاملين في المؤسسات المالية لكيفية تطبيق أفضل الممارسات في إدارة المخاطر (Andrew W. Lo (2012). يشير إلى أن "التدريب المستمر يمكن أن يزيد من قدرة المؤسسات المالية على التكيف مع المخاطر المتغيرة"، مما يعني أن التدريب يمكن أن يلعب دورًا حاسمًا في تعزيز جاهزية المؤسسات لمواجهة التحديات المستقبلية.

من خلال سد الفجوات النظرية والتطبيقية بين المتغيرات الموجودة في هذه الدراسة، يسعى البحث إلى تقديم إسهام علمي وأكاديمي كبير يعزز من فهم العلاقة بين إدارة المخاطر السيبرانية والأداء المالي في المؤسسات المالية السعودية. التركيز على التحليل المتعمق، التكامل بين النظرية والتطبيق، واستخدام دراسات الحالة المحلية، كلها خطوات أساسية نحو تقديم توصيات عملية تساهم في تحسين استراتيجيات إدارة المخاطر السيبرانية وتعزيز الاستقرار المالي للمؤسسات المالية في المملكة. إن هذا البحث لا يهدف فقط إلى تحسين الأداء المالي للمؤسسات الحالية، بل يسعى أيضًا إلى وضع أسس قوية لمستقبل أكثر استقرارًا وازدهارًا للمؤسسات المالية في المملكة العربية السعودية.

١,٣,١. على المستوى النظري:

تطوير المعرفة النظرية في مجال إدارة المخاطر والأمن السيبراني: يساهم هذا البحث في إثراء المعرفة النظرية في مجال إدارة المخاطر والأمن السيبراني.

سد الفجوات المعرفية: يهدف هذا البحث إلى سد الفجوات المعرفية الموجودة في الأدبيات الحالية حول إدارة المخاطر والأمن السيبراني في البنوك المركزية. من خلال التركيز على دراسة حالة واقعية، يمكن للبحث أن يوفر رؤى جديدة حول التحديات والفرص في هذا المجال.

تقديم إطار عمل لتحليل المخاطر السيبرانية: يمكن أن يساعد هذا البحث في تطوير إطار عمل نظري لتحليل المخاطر السيبرانية في المؤسسات المالية، والذي يمكن استخدامه من قبل الباحثين والممارسين لتقييم نقاط الضعف وتطوير استراتيجيات فعالة لإدارة المخاطر.

دعم تطوير السياسات الأمنية: يمكن أن توفر نتائج هذا البحث معلومات قيمة لصانعي السياسات والجهات التنظيمية، مما يساعدهم على تطوير سياسات وإرشادات أكثر فعالية لتعزيز الأمن السيبراني في المؤسسات المالية.

تعزيز التعاون البحثي: يمكن أن يشجع هذا البحث على المزيد من التعاون البحثي بين الأكاديميين والممارسين في مجال الأمن السيبراني وإدارة المخاطر، مما يؤدي إلى تطوير حلول مبتكرة للتحديات الأمنية التي تواجه المؤسسات المالية.

١,٣,٢. على المستوى التطبيقي:

- **توفير دروس عملية للمؤسسات المالية:**
يقدم هذا البحث دروسًا عملية يمكن للمؤسسات المالية الأخرى الاستفادة منها لتجنب الوقوع في الأخطاء التي أدت إلى سرقة بنك بنغلاديش مثلاً. يمكن للمؤسسات المالية استخدام نتائج هذا البحث لتقييم نقاط الضعف في أنظمتها الخاصة وتطوير استراتيجيات فعالة لإدارة المخاطر السيبرانية.
- **تعزيز الأمن السيبراني في المؤسسات المالية:**
من خلال تحديد نقاط الضعف في أنظمة الأمن السيبراني في بنك بنغلاديش، يمكن لهذا البحث أن يساعد البنوك المركزية الأخرى على تعزيز دفاعاتها ضد الهجمات السيبرانية.
- **تحسين إدارة المخاطر السيبرانية في المؤسسات المالية:**
يمكن أن يساعد هذا البحث المؤسسات المالية على تطوير إجراءات إدارة مخاطر أكثر فعالية، من خلال تحديد أفضل الممارسات وتقديم توصيات عملية.
- **رفع مستوى الوعي الأمني:**
يمكن أن يساهم هذا البحث في رفع مستوى الوعي الأمني لدى موظفي المؤسسات المالية مما يجعلهم أكثر قدرة على تحديد التهديدات السيبرانية والإبلاغ عنها.
- **تعزيز الثقة في النظام المالي:**
من خلال تعزيز الأمن السيبراني وإدارة المخاطر في المؤسسات المالية، يمكن لهذا البحث أن يساهم في تعزيز الثقة في النظام المالي العالمي.

١,٤ . أسئلة الدراسة

١. ما هي التحديات الحالية التي تواجه المؤسسات المالية في إدارة المخاطر السيبرانية؟
٢. ما العلاقة بين الاستثمار في تقنيات الأمن السيبراني والعائد على الاستثمار في المؤسسات المالية؟
٣. ما هي العلاقة بين الاستثمار وحجم المؤسسة المالية؟
٤. ما هي أفضل الممارسات التي يمكن للمؤسسات المالية اتباعها لتعزيز فعالية إدارة المخاطر السيبرانية؟
٥. كيف يؤثر تدريب الموظفين على فعالية إدارة المخاطر السيبرانية في المؤسسات المالية؟
٦. ما مدى تأثير التعاون مع الجهات الخارجية؟
٧. ما هي الآثار المالية والتشغيلية والسمعة التي تترتب على فشل إدارة المخاطر السيبرانية؟
٨. ما هي اشتراطات البنية التحتية التكنولوجية للمؤسسات المالية؟

١,٥ . أهداف الدراسة

- تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسية التي تسعى إلى تعزيز الفهم حول دور إدارة المخاطر السيبرانية في تحسين الأداء المالي للمؤسسات المالية في المملكة العربية السعودية، وتشمل:
- استكشاف دور المتغيرات المعدلة والوسيط في العلاقة بين إدارة المخاطر السيبرانية والأداء المالي:
- تهدف إلى فهم كيف تؤثر المتغيرات المعدلة، مثل حجم المؤسسة والبيئة التنظيمية، والمتغيرات الوسيطة مثل الحوكمة المؤسسية وجودة الإدارة، على العلاقة بين إدارة المخاطر السيبرانية والأداء المالي. هذا التحليل يهدف إلى تقديم رؤى حول كيفية تحسين هذه العلاقة لتعزيز الأداء المالي.
- تقييم تأثير البيئة التنظيمية والتحديات المحلية على استراتيجيات إدارة المخاطر السيبرانية:
- تسعى إلى تحليل كيفية تأثير البيئة التنظيمية في المملكة العربية السعودية، بما في ذلك القوانين واللوائح المحلية، على تطبيق وتنفيذ استراتيجيات إدارة المخاطر السيبرانية. الهدف هو تحديد التحديات التي تواجه المؤسسات المالية في التكيف مع هذه البيئة وكيفية التغلب عليها.

- تطوير استراتيجيات مخصصة لإدارة المخاطر السيبرانية تتماشى مع الخصوصية المحلية للسوق السعودي:

تهدف إلى تقديم توصيات عملية للمؤسسات المالية حول كيفية تطوير استراتيجيات إدارة مخاطر مخصصة تتناسب مع التحديات الفريدة التي تواجهها في السوق السعودي. يشمل ذلك التكيف مع التحديات السيبرانية والتحولات الاقتصادية والتكنولوجية المستمرة.

- تعزيز الفهم الأكاديمي لإدارة المخاطر السيبرانية في السياقات الاقتصادية الناشئة:

بالإضافة إلى الأهداف التطبيقية، تسعى الدراسة إلى إثراء الأدبيات الأكاديمية من خلال تقديم إسهامات نظرية تسهم في تطوير نماذج جديدة لإدارة المخاطر السيبرانية، مع التركيز على الاقتصادات الناشئة مثل المملكة العربية السعودية.

- تحليل دور التكنولوجيا المالية في تغيير مشهد المخاطر في المؤسسات المالية:

تهدف الدراسة إلى فهم كيف يؤثر الاعتماد المتزايد على التكنولوجيا المالية (Fintech) على ممارسات إدارة المخاطر السيبرانية في المؤسسات المالية السعودية، وكيف يمكن لهذه المؤسسات أن تتكيف مع المخاطر الجديدة المرتبطة بالتكنولوجيا.

من خلال تحقيق هذه الأهداف، تسعى الدراسة إلى تقديم رؤى متعمقة تساعد المؤسسات المالية في المملكة العربية السعودية على تعزيز استراتيجيات إدارة المخاطر السيبرانية وتحقيق أداء مالي أفضل، مع مراعاة التحديات الفريدة والفرص التي تقدمها البيئة المحلية.

١,٦. فرضيات الدراسة

تعتمد هذه الدراسة على مجموعة من الفرضيات التي تسعى إلى اختبار العلاقة بين ممارسات إدارة المخاطر السيبرانية وأداء المؤسسات المالية في المملكة العربية السعودية، مع التركيز على تأثير المتغيرات المعدلة والوسيط. فرضيات الدراسة الرئيسية تشمل ما يلي:

الفرضية الأولى:

H1: هناك علاقة مباشرة ذات دلالة إحصائية بين ممارسات إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية في المملكة العربية السعودية.

هذه الفرضية تفترض أن تطبيق استراتيجيات فعالة لإدارة المخاطر السيبرانية، يساهم في تحسين النشاط التشغيلي من حيث الربحية والاستقرار المالي.

الفرضية الثانية:

H2: يؤثر حجم المؤسسة المالية كمتغير معدل على العلاقة بين إدارة المخاطر السيبرانية والأداء المالي. هذه الفرضية تفترض أن تأثير ممارسات إدارة المخاطر السيبرانية على الأداء المالي يختلف باختلاف حجم المؤسسة، حيث تكون المؤسسات الكبيرة أكثر قدرة على تحمل المخاطر مقارنة بالمؤسسات الصغيرة.

الفرضية الثالثة:

H3: تلعب البيئة التنظيمية دوراً معدلاً في العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية في المملكة العربية السعودية، حيث تؤثر القوانين واللوائح المحلية على فعالية تنفيذ استراتيجيات إدارة المخاطر السيبرانية.

هذه الفرضية تفترض أن البيئة التنظيمية المحلية، بما في ذلك القوانين واللوائح، تؤثر بشكل كبير على كيفية تنفيذ استراتيجيات إدارة المخاطر السيبرانية وفعاليتها في تحسين الأداء المالي.

الفرضية الرابعة:

H4: تؤثر البنية التحتية للمؤسسة المالية كمتغير معدل على العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية.

هذه الفرضية تفترض أن المؤسسات التي تتمتع ببنية تحتية ذات جودة عالية تكون أكثر قدرة على تحويل استراتيجيات إدارة المخاطر السيبرانية إلى تحسينات ملموسة في الأداء المالي.

الفرضية الخامسة:

H5: تساهم الحوكمة المؤسسية كمتغير وسيط في تعزيز العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية، حيث تؤدي الحوكمة الجيدة إلى تحسين تنفيذ استراتيجيات إدارة المخاطر السيبرانية وزيادة الاستقرار المالي.

الفرضية السادسة:

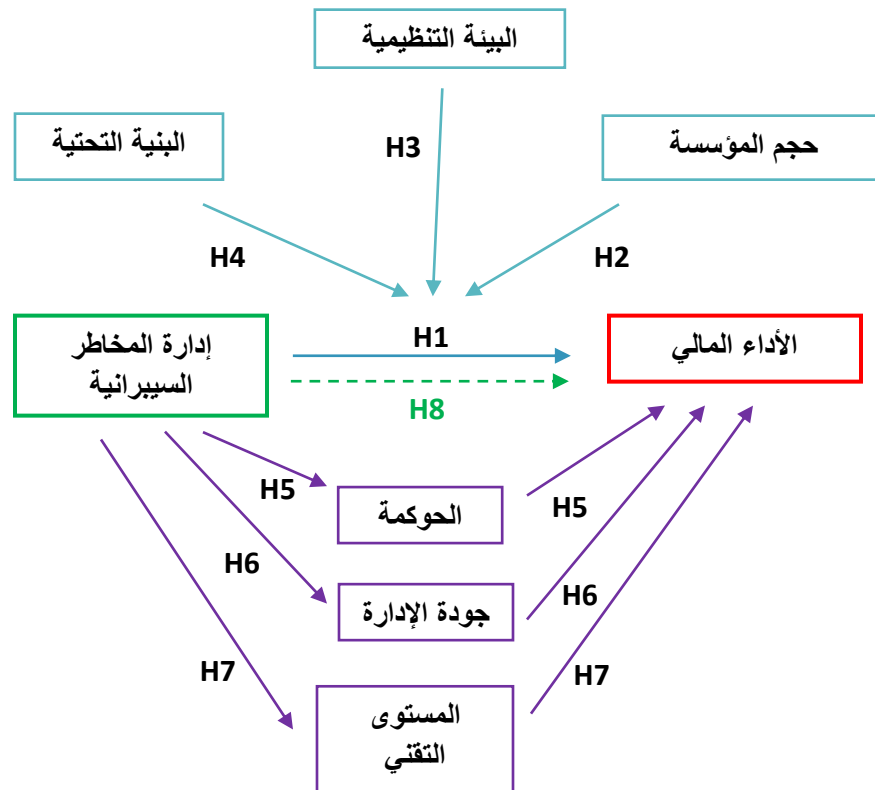
H6: تؤثر جودة الإدارة كمتغير وسيط على العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية، حيث تساهم الإدارة الفعالة في تحسين فعالية استراتيجيات إدارة المخاطر السيبرانية وبالتالي تحسين الأداء المالي.

الفرضية السابعة:

H7: يؤثر المستوى التقني للمؤسسة المالية كمتغير وسيط على العلاقة بين إدارة المخاطر السيبرانية والأداء المالي.

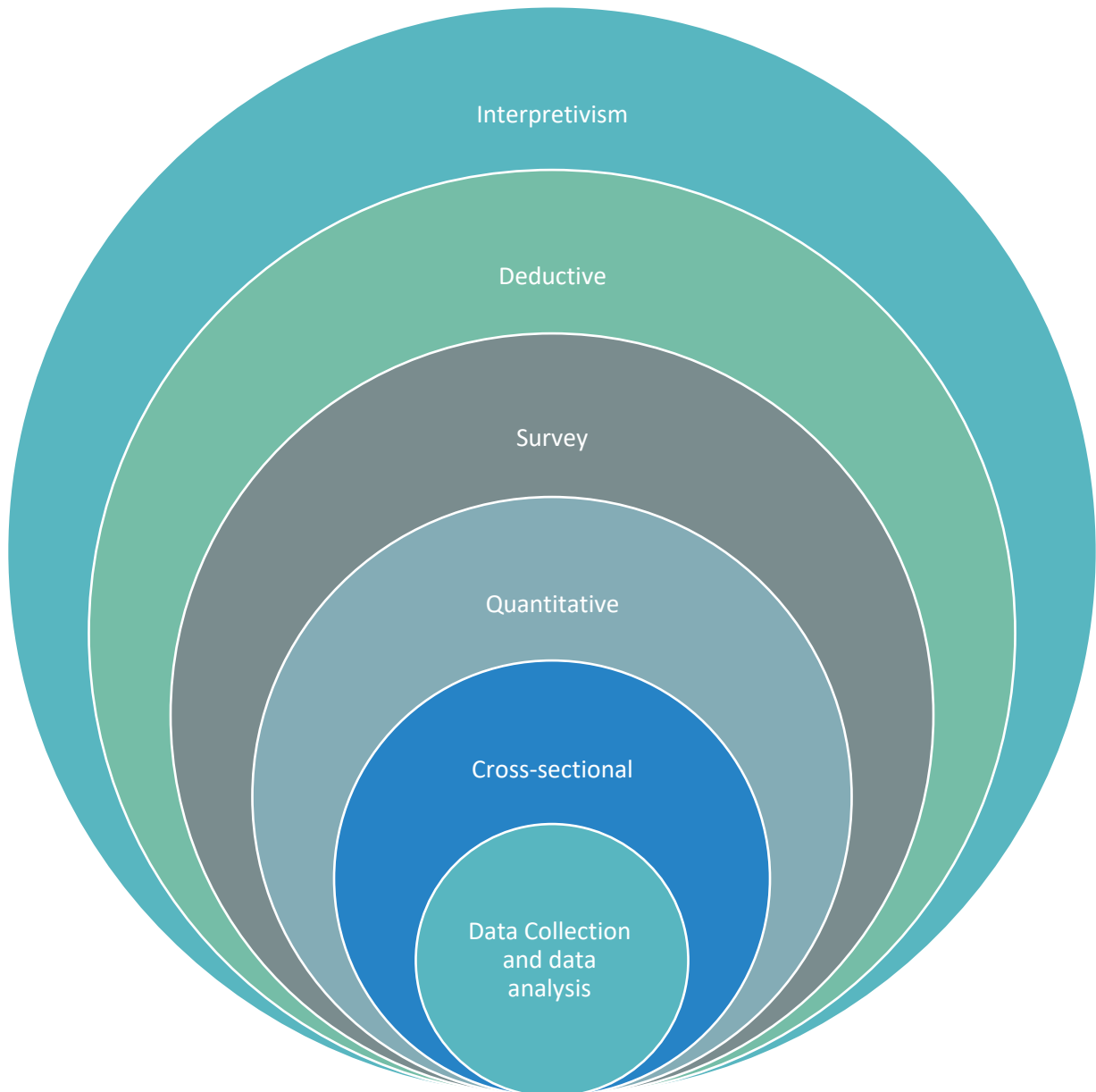
هذه الفرضية تفترض العلاقة الطردية للأمن السيبراني والتقدم التقني للمؤسسة المالية.

١,٧. نموذج الدراسة



١,٨ . منهجية الدراسة

١ . تصميم البحث:



الفصل الأول: الإطار العام للدراسة

تعتبر مراجعة الأدبيات جزءاً أساسياً ومحورياً من الإطار العام لأي دراسة بحثية، فهي تمثل الجسر الذي يربط الباحثين بالمعرفة العلمية الحالية في مجال معين. من خلال هذه المراجعة، يمكن للباحثين ليس فقط فهم الوضع الراهن للمعرفة، بل أيضاً استنباط الدروس المستفادة من الدراسات السابقة وتحديد الفجوات البحثية التي لم تُغطَّ بعد. في هذا السياق، يعد فهم ممارسات إدارة المخاطر السيبرانية كمتغير مستقل وكيفية تأثيرها المباشر على الأداء المالي للمؤسسات المالية، الذي يمثل المتغير التابع، من الأمور الحاسمة في هذا النوع من الدراسات. تحليل البيئة المحلية واستيعاب تأثير المتغيرات المعدلة مثل حجم المؤسسة والبيئة التنظيمية، إلى جانب المتغيرات الوسيطة مثل جودة الإدارة والحوكمة المؤسسية، يمثلان جزءاً أساسياً من فهم هذه العلاقة المعقدة. العلاقات المتشابكة بين هذه المتغيرات تعد بمثابة العمود الفقري للتحليل في الدراسة الحالية، مما يبرز أهمية دراسة تأثير القوانين واللوائح المحلية على فعالية هذه الاستراتيجيات. هذا يعني أن كل مؤسسة تعمل في إطار تنظيمي خاص بها، والذي يمكن أن يعزز أو يعيق تنفيذ استراتيجيات إدارة المخاطر السيبرانية. بالإضافة إلى ذلك، تلعب الحوكمة المؤسسية وجودة الإدارة دوراً وسيطاً يمكن أن يعزز من تأثير ممارسات إدارة المخاطر السيبرانية على الأداء المالي. الأدبيات تشير إلى أن هذه العناصر الوسيطة لا تعمل فقط كعوامل تمكين، بل تساعد في تحويل استراتيجيات إدارة المخاطر السيبرانية إلى نتائج ملموسة تعزز من استقرار المؤسسات المالية وقدرتها على تحقيق أهدافها المالية. الحوكمة الفعالة والإدارة الجيدة هما ما يضمنان أن الاستراتيجيات الموضوعة ليست مجرد خطط على الورق، بل تُترجم إلى ممارسات حقيقية تؤثر إيجاباً على الأداء المالي.

في ضوء هذه الاعتبارات، يسعى هذا البحث إلى تقديم إسهام علمي جديد من خلال استكشاف العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي في المؤسسات المالية السعودية. سيكون التركيز على دور المتغيرات المعدلة والوسيطة في هذا السياق، حيث يتطلع البحث إلى سد الفجوات المعرفية الحالية في الأدبيات، وتقديم رؤى جديدة قد تساهم في تحسين استراتيجيات إدارة المخاطر السيبرانية بما يتناسب مع الخصوصيات المحلية للسوق السعودي. من خلال هذا النهج، يأمل البحث في تقديم توصيات عملية يمكن أن تدعم المؤسسات المالية في تعزيز أدائها المالي وتحقيق استدامة أكبر في مواجهة التحديات المستقبلية.

الفصل الثاني: الإطار النظري

الإطار النظري يُعتبر العمود الفقري لأي بحث علمي، فهو يوفر الأساس الذي تُبنى عليه الدراسة ويوجه الباحثين نحو فهم أعمق للعلاقات بين المتغيرات المختلفة قيد الدراسة. من خلال الإطار النظري، يُمكن للباحثين توضيح كيف تؤثر هذه المتغيرات على بعضها البعض، وتقديم تفسير شامل للعلاقات التي تربط بينها. في سياق هذه الدراسة، يهدف الإطار النظري إلى تحليل العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية في المملكة العربية السعودية، مع تسليط الضوء على تأثير المتغيرات المعدلة والوسيط.

إدارة المخاطر السيبرانية تُعد جزءاً لا يتجزأ من الاستراتيجيات الشاملة التي تتبناها المؤسسات المالية. فهي تهدف إلى تقليل المخاطر المالية والتشغيلية الناتجة عن الهجمات السيبرانية التي قد تواجهها هذه المؤسسات. الدراسات الحديثة تؤكد أن إدارة المخاطر السيبرانية الفعالة يمكن أن تسهم بشكل كبير في تحسين الأداء المالي للمؤسسات، من خلال تقليل التعرض للهجمات الإلكترونية وتقليل التكاليف المرتبطة باستعادة البيانات والأضرار الناجمة عن تلك الهجمات (Dionne (2013). أشار في بحثه إلى أن "إدارة المخاطر السيبرانية هي عنصر حاسم في استدامة الأداء المالي، حيث تعزز قدرة المؤسسات على الصمود أمام التهديدات السيبرانية المتزايدة."

تُعد مراجعة الأبحاث جزءاً جوهرياً من الإطار النظري، حيث توفر للباحثين نظرة شاملة على ما تم إنجازه في هذا المجال وتساعد في تحديد الفجوات التي لم يتم تناولها بعد (Fraser, Simkins, & Narvaez (2014). في دراستهم حول إدارة المخاطر المؤسسية، أشاروا إلى أن "تطوير فهم شامل للمخاطر السيبرانية وممارسات إدارتها هو أمر أساسي لتحقيق أداء مالي مستدام".

- المتغير المستقل:

تسعى الدراسة إلى فهم تأثير إدارة المخاطر السيبرانية على الأداء المالي للمؤسسات المالية. تشمل هذه الممارسات استراتيجيات متنوعة مثل الوقاية من الهجمات السيبرانية، والتعافي من الكوارث السيبرانية، وإدارة الأمن السيبراني اليومي.

- المتغير التابع:

الأداء المالي، يُقاس من خلال مؤشرات مثل الربحية، الاستقرار المالي، ونمو الإيرادات وتحمل التكاليف. وقد أكدت العديد من الدراسات أن الأداء المالي يتأثر بشكل مباشر بفعالية ممارسات إدارة المخاطر السيبرانية (Lundqvist, 2015). أوضح في بحثه أن "الفعالية في تطبيق استراتيجيات إدارة المخاطر السيبرانية تساهم في تعزيز الأداء المالي من خلال تحسين قدرة المؤسسات على التعامل مع التهديدات السيبرانية وتقليل الخسائر."

- المتغيرات المعدلة:

مثل حجم المؤسسة والبيئة التنظيمية، تلعب دورًا مهمًا في تحديد مدى فعالية العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي. حجم المؤسسة يمكن أن يكون له تأثير كبير على كيفية تطبيق استراتيجيات إدارة المخاطر السيبرانية. المؤسسات الكبيرة، بفضل مواردها الكبيرة، قد تكون أكثر قدرة على تنفيذ استراتيجيات معقدة وفعالة.

المتغيرات الوسيطة مثل الحوكمة المؤسسية وجودة الإدارة تلعب دورًا حيويًا في تحويل ممارسات إدارة المخاطر السيبرانية إلى نتائج ملموسة في الأداء المالي. McShane, Nair, & Rustambekov (٢٠١١) أكدوا في بحثهم أن "الحوكمة المؤسسية الجيدة تعزز من فعالية استراتيجيات إدارة المخاطر السيبرانية، حيث تدعم الإدارة القوية تطبيق هذه الاستراتيجيات بشكل فعال مما يساهم في تحسين الأداء المالي". الإدارة الجيدة تساهم في توجيه الموارد بشكل فعال وتطبيق السياسات التي تعزز من قدرة المؤسسة على مواجهة المخاطر السيبرانية بكفاءة.

العلاقة بين المتغيرات المختلفة في هذه الدراسة تمثل محور التحليل النظري. يسعى الباحث إلى فهم كيف تؤثر ممارسات إدارة المخاطر السيبرانية على الأداء المالي، وكيف يمكن للمتغيرات المعدلة والوسيطة أن

تعزز أو تقلل من هذا التأثير. فهم هذه العلاقات بشكل دقيق يمكن أن يساعد في تقديم توصيات أكثر فعالية للمؤسسات المالية لتحسين استراتيجياتها في إدارة المخاطر السيبرانية وتحقيق أداء مالي مستدام.

الإطار النظري لهذه الدراسة يوفر قاعدة علمية متينة لتحليل العلاقة بين ممارسات إدارة المخاطر السيبرانية والأداء المالي في المؤسسات المالية السعودية. من خلال استعراض الأدبيات السابقة واستخدام المفاهيم النظرية ذات الصلة، يسعى البحث إلى تقديم إسهام علمي جديد يمكن أن يساعد المؤسسات المالية على تحسين استراتيجياتها في إدارة المخاطر السيبرانية وتحقيق أداء مالي مستدام في بيئة متغيرة ومتطلبة. بناءً على هذا الإطار، يمكن للمؤسسات أن تطور استراتيجيات مرنة وقادرة على التكيف مع الظروف المحلية والدولية، مما يعزز من قدرتها على الصمود في وجه التهديدات السيبرانية المتزايدة.

الفصل الثالث: متغير مستقل [إدارة المخاطر السيبرانية]

إدارة المخاطر السيبرانية تلعب دورًا حيويًا في حماية الأصول الرقمية للمؤسسات المالية، وهي تتفاعل مع العديد من المتغيرات الأخرى مثل البيئة التنظيمية، حجم المؤسسة، وجودة الإدارة، مما يؤثر بشكل كبير على فعالية استراتيجيات إدارة المخاطر السيبرانية.

١. البيئة التنظيمية وتأثيرها

كما ذكر (von Solms & van Niekerk (2013 فإن البيئة التنظيمية لا تقتصر على وضع القوانين والسياسات فحسب، بل تمتد أيضًا إلى كيفية تطبيق هذه القوانين وتفاعل المؤسسات معها. وذكر أن "البيئة التنظيمية المعقدة قد تفرض تحديات على المؤسسات في كيفية تأمين أصولها الرقمية، لكنها في الوقت نفسه توفر إطارًا لتحسين تلك الاستراتيجيات". هذا يشير إلى أن القوانين الصارمة يمكن أن تحفز المؤسسات على تحسين إجراءات الأمن السيبراني لديها.

٢. حجم المؤسسة والبنية التحتية للأمن السيبراني

أوضح (von Solms (2013 أن المؤسسات الكبيرة غالبًا ما تمتلك بنية تحتية قوية للأمن السيبراني، وهو ما يمكن أن يُعزى إلى حجم مواردها وقدرتها على الاستثمار في تقنيات متقدمة. ومع ذلك، حذرت الورقة من أن هذه المؤسسات قد تكون أهدافًا رئيسية للهجمات السيبرانية نظرًا لحجم البيانات التي تحتفظ

بها وأهمية أصولها الرقمية. على النقيض، المؤسسات الأصغر قد لا تملك الموارد اللازمة لتطوير نظام أمني معقد، مما يجعلها أكثر عرضة للمخاطر السيبرانية.

٣. جودة الإدارة والحوكمة المؤسسية

تناولت الدراسة أيضًا دور الحوكمة المؤسسية في تعزيز الأمن السيبراني، مشيرة إلى أن جودة الإدارة لها تأثير مباشر على كيفية تطبيق استراتيجيات الأمن السيبراني (von Solms (2013. شددوا على أن "الإدارة القوية تساهم في بناء ثقافة أمنية داخل المؤسسة، مما يساعد في تقليل المخاطر وتجنب الأزمات السيبرانية". هذا يعني أن الإدارة التي تضع الأمن السيبراني كأولوية تستطيع توجيه المؤسسة نحو ممارسات أكثر أمانًا وتحقيق نتائج مالية أفضل.

٤. تأثير إدارة المخاطر السيبرانية على الأداء المالي

أشار (von Solms (2013 إلى أن إدارة المخاطر السيبرانية ليست مجرد مجموعة من الإجراءات التقنية، بل هي عملية شاملة تهدف إلى حماية الأصول الرقمية للمؤسسة وتأمينها ضد التهديدات المتزايدة. وذكر أن "الاستثمار في الأمن السيبراني يمكن أن يؤدي إلى تحسين الأداء المالي للمؤسسات من خلال تقليل الخسائر المحتملة الناتجة عن الهجمات السيبرانية". هذا الرأي يدعم ما تم ذكره في الأدبيات الأخرى حول أهمية الاستثمارات في التكنولوجيا والتدريب لتحسين الكفاءة التشغيلية والربحية.

إدارة المخاطر السيبرانية تشكل عنصرًا أساسيًا في الاستراتيجيات الشاملة للمؤسسات المالية، حيث تساهم في حماية الأصول الرقمية وتعزيز الاستقرار المالي. من خلال التركيز على البيئة التنظيمية، حجم المؤسسة، وجودة الإدارة، يمكن للمؤسسات تحسين استراتيجياتها الأمنية وبالتالي تحسين أدائها المالي. الأدبيات الحديثة.

الفصل الرابع: متغير تابع [الأداء المالي]

الأداء المالي للمؤسسات المالية هو المتغير التابع الذي يعكس مدى نجاح المؤسسات في تحقيق أهدافها الاقتصادية وضمان استدامتها في سوق تنافسي يتسم بالتحديات المستمرة. هذا الأداء يعبر عنه من خلال مجموعة من المؤشرات المالية مثل الربحية، الاستقرار المالي، نمو الإيرادات، والعائد على الأصول والعائد على حقوق الملكية. يعتبر الأداء المالي حجر الزاوية في تقييم كفاءة وفعالية المؤسسات المالية، ويشكل جزءًا أساسيًا من استراتيجيات الإدارة العليا التي تسعى إلى تعزيز قيمة المؤسسة وضمان استمراريتها.

أبعاد الأداء المالي:

• الربحية:

الربحية هي واحدة من أبرز المؤشرات المالية التي تقيس قدرة المؤسسة على تحقيق الأرباح من عملياتها التشغيلية. (Altman & Sabato (2007) تعد الربحية من أهم مؤشرات الصحة المالية للمؤسسات المالية، حيث تعكس كفاءة الإدارة في استخدام الموارد لتحقيق العوائد". الربحية تعكس قدرة المؤسسة على تحويل إيراداتها إلى أرباح صافية بعد خصم جميع التكاليف والنفقات. تعتمد الربحية بشكل كبير على قدرة المؤسسة على إدارة تكاليفها بشكل فعال، بالإضافة إلى استراتيجيات التسعير والإيرادات.

• الاستقرار المالي:

يشير الاستقرار المالي إلى قدرة المؤسسة على الوفاء بالتزاماتها المالية واستدامة عملياتها في ظل الظروف الاقتصادية المتقلبة (Merton (1974، في نظريته حول هيكل رأس المال، أشار إلى أن "الاستقرار المالي يعتبر مؤشرًا حاسمًا على قدرة المؤسسة على الصمود في وجه الأزمات الاقتصادية". الاستقرار المالي يساهم في تعزيز الثقة لدى المستثمرين والعملاء، مما يؤدي إلى تحسين القدرة على الحصول على التمويل وتقليل تكاليف الاقتراض.

• نمو الإيرادات:

نمو الإيرادات يعكس قدرة المؤسسة على توسيع قاعدة عملائها وزيادة مبيعاتها بمرور الوقت Penrose (1959) في دراستها حول نمو المؤسسات، أوضحت أن "نمو الإيرادات يرتبط بشكل مباشر بقدرة

المؤسسة على الابتكار واستغلال الفرص في السوق". نمو الإيرادات المستدام يشير إلى نجاح المؤسسة في توسيع حصتها السوقية وزيادة إيراداتها من خلال استراتيجيات فعالة للتسويق وتطوير المنتجات.

• العائد على الأصول والعائد على حقوق الملكية:

يمثل العائد على الأصول والعائد على حقوق الملكية مقياسين رئيسيين للأداء المالي، حيث يعكسان كفاءة الإدارة في استخدام الأصول المتاحة لتحقيق العوائد (Ross et al. (2008). أوضحوا أن "العائد على الأصول والعائد على حقوق الملكية هما مؤشرين مركزيين في تقييم أداء المؤسسات المالية، حيث يساعدان في تحديد مدى كفاءة استخدام الموارد المتاحة لتحقيق الأرباح."

• الأداء المالي للمؤسسات المالية

يمثل مقياسًا مركزيًا لنجاحها وقدرتها على البقاء في بيئة تنافسية مليئة بالتحديات. إدارة المخاطر السيبرانية كمتغير مستقل تؤثر بشكل كبير على الأبعاد المختلفة للأداء المالي، من الربحية إلى الاستقرار المالي، ومن نمو الإيرادات إلى العائد على الأصول وحقوق الملكية. من خلال استثمار المؤسسات في الأمن السيبراني وتبني استراتيجيات فعالة لإدارة المخاطر، يمكنها حماية نفسها من الخسائر المحتملة وتحقيق أداء مالي مستدام. الأدبيات الحديثة تؤكد أن الامتثال الفعال لسياسات الأمن السيبراني وتدريب الموظفين على هذه السياسات يمكن أن يعزز من الأداء المالي، مما يبرز أهمية مواصلة تطوير هذه الاستراتيجيات في ظل التهديدات السيبرانية المتزايدة.

الفصل الخامس: العلاقة بين متغيرات البحث

العلاقة بين المتغيرات في هذه الدراسة تتمحور حول فهم التأثيرات المتبادلة بين إدارة المخاطر السيبرانية (المتغير المستقل) والأداء المالي (المتغير التابع) للمؤسسات المالية، مع الأخذ بعين الاعتبار الأبعاد المختلفة لكل منهما والتفاعل مع المتغيرات الوسيطة والمعدلة التي تشمل حجم المؤسسة، البيئة التنظيمية، وجودة الإدارة. هذه العلاقات المتشابكة تؤثر بشكل كبير على كيفية تأثير إدارة المخاطر السيبرانية على الأداء المالي، وبالتالي فهمها بدقة يمكن أن يقدم قيمة حول كيفية تحسين استراتيجيات إدارة المخاطر السيبرانية لتعزيز الأداء المالي.

إدارة المخاطر السيبرانية وتأثيرها على الأداء المالي

إدارة المخاطر السيبرانية هي عملية أساسية تسعى لحماية الأصول الرقمية للمؤسسات المالية من التهديدات المتزايدة في العصر الرقمي. هذه التهديدات قد تؤدي إلى خسائر مالية جسيمة، سواء من خلال الهجمات المباشرة على أنظمة المعلومات أو من خلال التكاليف المرتبطة باستعادة البيانات المتضررة والتعامل مع الأزمات. العلاقة بين إدارة المخاطر السيبرانية والأداء المالي هي علاقة مباشرة ومعقدة في نفس الوقت، حيث تؤثر على مختلف أبعاد الأداء المالي.

١. تأثير إدارة المخاطر السيبرانية على الربحية:

الربحية تعد من أهم المؤشرات التي تقيس نجاح المؤسسة في تحقيق أهدافها المالية. المؤسسات المالية التي تدير مخاطر السيبرانية بفعالية، من خلال تبني استراتيجيات أمان متقدمة وتدريب الموظفين على الالتزام بسياسات الأمان، تكون أكثر قدرة على حماية أرباحها من التآكل بسبب الهجمات السيبرانية. [Cavusoglu, Mishra, & Raghunathan \(2004\)](#) أشاروا إلى أن "الخسائر الناتجة عن الهجمات السيبرانية قد تؤدي إلى تراجع كبير في الربحية، خاصة إذا كانت المؤسسة غير مستعدة للتعامل مع مثل هذه التهديدات".

على سبيل المثال، إذا تعرضت مؤسسة مالية لهجوم سيبراني أدى إلى اختراق البيانات الحساسة، فقد يتعين عليها دفع تعويضات مالية ضخمة للعملاء، بالإضافة إلى تكاليف استعادة البيانات وتحديث أنظمة الأمان. هذه التكاليف تؤثر بشكل مباشر على صافي الأرباح، وبالتالي فإن المؤسسات التي تستثمر في إدارة المخاطر السيبرانية بشكل جيد يمكن أن تحافظ على ربحيتها حتى في مواجهة مثل هذه التهديدات.

٢. تأثير إدارة المخاطر السيبرانية على الاستقرار المالي:

الاستقرار المالي هو مقياس لقدرة المؤسسة على الوفاء بالتزاماتها المالية والحفاظ على عملياتها دون انقطاع. الاستقرار المالي يتأثر بشكل كبير بإدارة المخاطر السيبرانية، حيث يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل عمليات المؤسسة وتشويه سمعتها في السوق.

الهجمات السيبرانية قد تؤدي إلى فقدان الثقة من قبل المستثمرين والعملاء، مما ينعكس على قدرة المؤسسة على جذب التمويل والحفاظ على علاقاتها التجارية. في المقابل، المؤسسات التي تستثمر في أمنها السيبراني وتتمتع بسمعة جيدة في هذا المجال قد تجد نفسها في وضع أقوى للحفاظ على استقرارها المالي حتى في أوقات الأزمات.

٣. تأثير إدارة المخاطر السيبرانية على نمو الإيرادات:

نمو الإيرادات يعكس قدرة المؤسسة على زيادة حصتها في السوق وزيادة مبيعاتها بمرور الوقت. المؤسسات التي تدير مخاطرها السيبرانية بفعالية تستطيع تعزيز ثقة عملائها، مما يؤدي إلى زيادة ولاء العملاء وزيادة الإيرادات (Smith et al. (2010). أكدوا أن "الهجمات السيبرانية التي تؤدي إلى فقدان بيانات العملاء قد تؤدي إلى انخفاض حاد في الإيرادات، خاصة إذا شعر العملاء بأن بياناتهم ليست محمية بشكل كافٍ".

إذا تمكنت مؤسسة مالية من بناء سمعة قوية في مجال الأمن السيبراني، فإنها قد تجذب عملاء جدد وتحتفظ بعملائها الحاليين، مما يساهم في نمو الإيرادات. من ناحية أخرى، الفشل في إدارة المخاطر السيبرانية قد يؤدي إلى فقدان الثقة وبالتالي تراجع الإيرادات.

٤. تأثير إدارة المخاطر السيبرانية على العائد على الأصول (ROA) والعائد على حقوق الملكية (ROE):

العائد على الأصول (ROA) والعائد على حقوق الملكية (ROE) هما مقياسان لكفاءة استخدام الموارد المالية للمؤسسة لتحقيق الأرباح. الهجمات السيبرانية قد تؤدي إلى تضرر الأصول الرقمية للمؤسسة، مما يؤثر سلبًا على هذه المؤشرات المالية (Puhakainen & Siponen (2010). أشاروا إلى أن "التدريب الفعال على سياسات الأمن السيبراني يمكن أن يحسن من الامتثال ويقلل من المخاطر المالية المرتبطة بالهجمات السيبرانية، مما يعزز من كفاءة استخدام الأصول".

إذا كانت المؤسسة قادرة على حماية أصولها الرقمية بشكل فعال من خلال استراتيجيات أمان متقدمة، فإنها تستطيع تحسين عوائدها على الأصول وحقوق الملكية، مما يعزز من قيمة المؤسسة على المدى الطويل.

دور المتغيرات الوسيطة والمعدلة في العلاقة بين إدارة المخاطر السيبرانية والأداء المالي

علاوة على التأثير المباشر لإدارة المخاطر السيبرانية على الأداء المالي، هناك مجموعة من المتغيرات الوسيطة والمعدلة التي يمكن أن تؤثر على هذه العلاقة بشكل كبير. هذه المتغيرات تشمل حجم المؤسسة، البيئة التنظيمية، وجودة الإدارة، وكل منها يلعب دورًا في تحديد فعالية إدارة المخاطر السيبرانية وتأثيرها على الأداء المالي.

١. حجم المؤسسة كمتغير معدل:

حجم المؤسسة يمكن أن يؤثر بشكل كبير على كيفية تطبيق استراتيجيات إدارة المخاطر السيبرانية. المؤسسات الكبيرة قد تواجه أيضًا تحديات أكبر نظرًا لتعقيد بنيتها التحتية وحجم عملياتها. في حين أن المؤسسات الصغيرة قد تكون أكثر مرونة في التكيف مع التهديدات السيبرانية الجديدة، إلا أنها قد تفتقر إلى الموارد اللازمة لتطوير نظام أمني شامل.

٢. البيئة التنظيمية كمتغير معدل:

البيئة التنظيمية التي تعمل فيها المؤسسة تلعب دورًا حاسمًا في تحديد كيفية تطبيق استراتيجيات إدارة المخاطر السيبرانية (von Solms & van Niekerk (2013). أشاروا إلى أن "البيئة التنظيمية يمكن أن توفر إطارًا لتحسين استراتيجيات الأمان السيبراني، لكنها قد تفرض أيضًا تحديات في الامتثال". في بعض الحالات، القوانين واللوائح قد تجبر المؤسسات على تبني ممارسات أمان أكثر صرامة، مما يحسن من قدرتها على مواجهة التهديدات السيبرانية.

من ناحية أخرى، في البيئات التنظيمية الأقل تطورًا، قد تواجه المؤسسات صعوبة في تطبيق استراتيجيات أمان فعالة بسبب نقص الدعم القانوني أو التوجيهات الواضحة.

٣. جودة الإدارة كمتغير وسيط:

جودة الإدارة تلعب دورًا محوريًا في توجيه وتنفيذ استراتيجيات إدارة المخاطر السيبرانية (Rao, Upadhyayula, & Unger (2018). أشاروا إلى أن "الإدارة الفعالة يمكن أن تضمن تخصيص الموارد بشكل صحيح وتبني ثقافة مؤسسية تعزز وعي الموظفين بأهمية الأمان السيبراني". الإدارة الجيدة قادرة على تحديد الأولويات بشكل صحيح وضمان أن المؤسسة تستثمر في المجالات التي ستعزز من قدرتها على حماية أصولها الرقمية.

إدارة الجودة تعزز من فعالية استراتيجيات إدارة المخاطر السيبرانية من خلال التوجيه الاستراتيجي وتطبيق السياسات بشكل صحيح، مما يؤدي في النهاية إلى تحسين الأداء المالي للمؤسسة.

التأثيرات المتبادلة بين المتغيرات

العلاقة بين إدارة المخاطر السيبرانية والأداء المالي للمؤسسات المالية ليست خطية أو بسيطة؛ بل هي علاقة متشابكة تتأثر بعدة عوامل وسياقات تنظيمية. المؤسسات التي تتمتع بإدارة قوية وفعالة، وتعمل في بيئات تنظيمية متطورة، وتملك الموارد المالية اللازمة، تكون أكثر قدرة على تطبيق استراتيجيات أمان سيبراني فعالة، مما يؤدي إلى تحسين أدائها المالي.

على الجانب الآخر، المؤسسات التي تواجه تحديات في الموارد أو تعمل في بيئات تنظيمية أقل دعمًا، قد تجد صعوبة في تحقيق نفس المستوى من الحماية السيبرانية، مما يؤثر سلبيًا على أدائها المالي. هذا يبرز أهمية فهم السياق الكامل للعلاقات بين هذه المتغيرات، وتطوير استراتيجيات مخصصة تتناسب مع طبيعة كل مؤسسة وظروفها الخاصة.

العلاقة بين المتغيرات في هذه الدراسة توضح كيف أن إدارة المخاطر السيبرانية تلعب دورًا محوريًا في تحديد الأداء المالي للمؤسسات المالية. من خلال فهم دقيق للتأثيرات المتبادلة بين إدارة المخاطر السيبرانية والأداء المالي، إلى جانب دور المتغيرات الوسيطة والمعدلة مثل حجم المؤسسة، البيئة التنظيمية، وجودة الإدارة، يمكن للمؤسسات تطوير استراتيجيات أكثر فعالية لحماية أصولها الرقمية وتحسين أدائها المالي. هذه العلاقات المعقدة تؤكد على ضرورة تبني نهج شامل ومتكامل لإدارة المخاطر السيبرانية، يأخذ في الاعتبار جميع العوامل المؤثرة لضمان تحقيق أفضل النتائج الممكنة.

جدول استبيان: تأثير إدارة المخاطر السيبرانية على الأداء المالي للمؤسسات المالية						
الرقم	السؤال	الخيار ١	الخيار ٢	الخيار ٣	الخيار ٤	الخيار ٥
الجزء الأول: معلومات عامة						
١	ما هو حجم مؤسستك المالية؟	متناهية الصغر	صغيرة	متوسطة	كبيرة	أخرى
٢	ما هو القطاع الذي تعمل به؟	البنوك	التأمين	الاستثمار	الصحة	أخرى
الجزء الثاني: إدارة المخاطر السيبرانية						
٣	هل تمتلك مؤسستك بنية تحتية للأمن السيبراني؟	نعم	لا	لا أدري	أخرى	الخيار ٥
٤	ما هي التقنيات المستخدمة في مؤسستك لإدارة المخاطر السيبرانية؟	جدار ناري	أنظمة كشف التسلل	تشفير البيانات	النسخ الاحتياطي	اخر ما ينطبق
٥	هل تُجرى تدريبات دورية للموظفين حول سياسات الأمن السيبراني؟					
٦	ما مدى فاعلية برامج التدريب على الأمن السيبراني في مؤسستك؟	ضعيف	جيد	متوسط	ممتاز	
٧	هل تمتلك مؤسستك خطة استجابة للطوارئ السيبرانية؟	نعم	لا			
الجزء الثالث: الأداء المالي						
٨	كيف تقيم تأثير إدارة المخاطر السيبرانية على الربحية في مؤسستك؟	تأثير إيجابي	تأثير إيجابي متوسط	تأثير إيجابي ضعيف	لا يوجد تأثير	تأثير سلبي
٩	هل لاحظت تحسناً في الاستقرار المالي لمؤسستك نتيجة للاستثمارات في الأمن السيبراني؟	زيادة ملحوظة	زيادة طفيفة	لم يؤثر	انخفاض	
الجزء الرابع: تقييم عام						
١٠	كيف تقيم كفاءة إدارة المخاطر السيبرانية في مؤسستك بشكل عام؟	ممتاز	جيدة	متوسطة	ضعيفة	أخرى
١١	ما هي التحديات الرئيسية التي تواجه مؤسستك في مجال إدارة المخاطر السيبرانية؟	نقص الموارد	نقص الكوادر	التحديات التنظيمية	ضعف البنية التحتية	ضعف التدريب
هل لديك أي معلومات أخرى تود المشاركة بها ؟						

- Altman, E. I., & Sabato, G. (2007). Modeling Credit Risk for SMEs: Evidence from the US Market. *Abacus*, 43(3), 332-357.
<https://doi.org/10.1111/j.1467-6281.2007.00234.x>
- Andrew W. Lo (2012). *Adaptive Markets Hypothesis: Financial Evolution at the Speed of Thought*. Princeton University Press.
- Bostrom, N., & Yudkowsky, E. (2014). The Ethics of Artificial Intelligence. In *Cambridge Handbook of Artificial Intelligence*, eds. W. Ramsey & K. Frankish. Cambridge University Press.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), 69-104.
<https://doi.org/10.1080/10864415.2004.11044320>
- Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks*. Carnegie Mellon University, Software Engineering Institute.
- Dionne, G. (2013). Risk Management: History, Definition, and Critique. *Risk Management and Insurance Review*, 16(2), 147-166.
<https://doi.org/10.1111/rmir.12019>
- Eling, M., & Wirfs, J. H. (2015). *Modelling and Management of Cyber Risk: An Empirical Analysis*. Geneva Association Report.
- Hull, J. C. (2012). *Risk Management and Financial Institutions*. John Wiley & Sons.
- Harvard Business Review.
- Hubbard, D. W. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons.
- Kaplan, R. S., & Mikes, A. (2012). *Managing Risks: A New Framework*.
- Lam, J. (2003). *Enterprise Risk Management: From Incentives to Controls*. John Wiley & Sons.
- Lundqvist, S. A. (2015). Why firms implement risk governance—Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, 34(5), 441-466.
<https://doi.org/10.1016/j.jaccpubpol.2015.05.002>

- Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.
- McCarthy, J. D., & Campbell, J. (2012). *Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. CRC Press.
- McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value? *Journal of Accounting, Auditing & Finance*, 26(4), 641-658. <https://doi.org/10.1177/0148558X11409160>
- Merton, R. C. (1974). On the Pricing of Corporate Debt: The Risk Structure of Interest Rates. *Journal of Finance*, 29(2), 449-470. <https://doi.org/10.2307/2978814>
- Mosca, M. (2018). Cybersecurity in the Quantum Era: The Impact of Quantum Computing on Cryptography. *Cryptography*, 2(3), 12.
- Nassim Nicholas Taleb (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House.
- Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management*. Oxford University Press.
- Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757-778. <https://doi.org/10.2307/25750704>
- Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press.
- Shackelford, S. J. (2012). Should Your Firm Invest in Cyber Risk Insurance? *Business Horizons*, 55(4), 349-356.
- Solomon, M. G., & Chapple, M. (2014). *Information Security Illuminated*. Jones & Bartlett Learning.
- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.
- Saidov, Ibrokhim. (2023). Understanding Systemic Cyber Risk. *Society and Innovations*, 4(6), 323-327.
- Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization. *MIS Quarterly*, 34(3), 463-486. <https://doi.org/10.2307/25750688>

- von Solms, R., & van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.
<https://doi.org/10.1016/j.cose.2013.04.004>