JWPU
Journal of Al-Wataniya Private University
ISSN: 3105-2150

Volume (3) Number (2)
Available at: https://doi.org/10.5281/zenodo.20963106

The Role of Digital Risk Management in Enhancing Cybersecurity "A Field Study in Private Banks in Hama Governorate"

Dr. Husain Kousayri [1,*], Judy Alloush [1]

ABSTRACT

This research aimed to study the role of digital risk management, with its various dimensions (risk identification, assessment and analysis, mitigation, monitoring and review, and communication), in enhancing cybersecurity. To achieve this objective, a field study was conducted on a group of private banks operating in Hama Governorate (Bank of Syria and Overseas, Al Baraka Bank, and Syria International Islamic Bank). The research employed a descriptive analytical approach, and a questionnaire was designed as the primary data collection tool.

The research population consisted of all employees (managers and staff) within the departments related to risk management and cybersecurity at Bank of Syria and Overseas, Al Baraka Bank, and Syria International Islamic Bank in Hama Governorate. Sixty questionnaires were distributed, fully returned, and deemed valid for analysis.

Among the most important findings of the research was the strong and positive impact of implementing risk management in its combined dimensions on enhancing cybersecurity in the studied banks. Furthermore, the study revealed a statistically significant and moderate positive impact of each individual dimension of risk management on enhancing cybersecurity.

KEYWORDS: Digital Risk Management, cybersecurity, private banks, risk assessment, information security governance.

Submitted on June 15, 2025; Revised on July 1, 2025; Accepted on July 13, 2025

1 Faculty of Administrative and Financial Sciences, Al-Wataniya Private University, Hama, Syria.

* Corresponding author. E-mail address: husain.kousayri@wpu.edu.sy

دور إدارة المخاطر الرقمية في تعزيز الأمن السيبراني
" دراسة ميدانية في المصارف الخاصة في محافظة حماه"

د. حسين قصيري، جودي علوش

الملخص

هدف هذا البحث إلى دراسة دور إدارة المخاطر الرقمية بأبعادها (تحديد المخاطر، تقييمها وتحليلها، معالجتها، مراقبتها ومراجعتها، والتواصل حولها) في تعزيز مستوى الأمن السيبراني، ولتحقيق هذا الهدف، تم إجراء دراسة ميدانية على مجموعة من المصارف الخاصة العاملة في محافظة حماة (سورية والمهجر، والبركة، وسورية الدولي الإسلامي)، اعتمد البحث على المنهج الوصفي بأسلوب تحليلي، وتم تصميم استبانة كأداة رئيسية لجمع البيانات.

تمثل مجتمع البحث من جميع العاملين (مديرين وموظفين) ضمن الاقسام ذات العلاقة بإدارة المخاطر والامن السيبراني في مصارف سورية والمهجر – البركة – سورية الدولي الإسلامي في محافظة حماة، وبلغ عدد الاستبانات الموزعة (60)، وتم استردادها بالكامل وكانت صالحة للتحليل.

ومن أهم النتائج التي توصل إليها البحث، وجود أثر إيجابي وقوي لتطبيق إدارة المخاطر بأبعادها مجتمعة في تعزيز الأمن السيبراني بالمصارف المدروسة، كما تبيّن وجود أثر طردي متوسط ومعنوي إحصائياً لكل بعد من أبعاد إدارة المخاطر على حدى في تعزيز الأمن السيبراني.

الكلمات المفتاحية: إدارة المخاطر الرقمية، الأمن السيبراني، المصارف الخاصة، تقييم المخاطر، حوكمة أمن المعلومات.

1. مقدمة

في عصر العولمة والاعتماد المتزايد على التكنولوجيا الرقمية، لم يعد الأمن السيبراني مسألة تقنية بحتة، بل أصبح عنصراً استراتيجياً له تأثير مباشر على نجاح المؤسسات واستمراريتها في سوق الأعمال، فمع التوسع في استخدام الإنترنت، والحوسبة السحابية، والتقنيات المالية الرقمية، أصبحت المؤسسات، وخصوصاً في القطاع المصرفي، أكثر عرضة للهجمات السيبرانية التي قد تؤدي إلى خسائر مالية جسيمة، وتهديد خصوصية العملاء، وتشويه السمعة المؤسسية، وحتى تعطيل العمليات التشغيلية الحيوية.

أمام هذا الواقع، لم تعد السياسات الأمنية التقليدية كافية لحماية المؤسسات من التهديدات الإلكترونية المعقدة والمتطورة، بل بات من الضروري تبنّي نهج استباقي وشامل يقوم على مبادئ إدارة المخاطر، التي تهدف إلى تحديد المخاطر السيبرانية، وتحليل وتُعد احتمالية حدوثها وتأثيرها، ومن ثم تطوير آليات وخطط للتقليل من آثارها أو الاستجابة لها بفعالية إدارة المخاطر جزءاً لا يتجزأ من الحوكمة المؤسسية، حيث تساهم في دعم اتخاذ القرار، وتعزيز مرونة المؤسسة، وبناء الثقة مع العملاء والمستثمرين.

في هذا الإطار، يُعد القطاع المصرفي من أكثر القطاعات عرضة للمخاطر السيبرانية، نظراً لطبيعة عملياته الرقمية واعتماده الكبير على شبكات المعلومات وأنظمة الدفع الإلكترونية، وتشير تقارير حديثة إلى تزايد الهجمات الإلكترونية على المصارف والمؤسسات المالية، مما يجعل من الضروري دراسة فعالية نظم إدارة المخاطر لديها، ومدى تكاملها مع استراتيجيات الأمن، وهو ما دفع الباحثين إلى دراسة دور إدارة المخاطر في تعزيز الأمن السيبراني، وذلك في مصارف سورية و المهجر – البركة – سورية الدولي الإسلامي، إذ سيتم استعراض السياسات والإجراءات التي تعتمدها المصارف في مواجهة المخاطر السيبرانية وتحليل مدى فعالية نظام إدارة المخاطر في تقليل احتمالية التعرض للتهديدات الرقمية وتعزيز المرونة التشغيلية.

2. الدراسات السابقة

- **الدراسات العربية**

1- دراسة (El-Bardony, Nariman Ismail, 2025): دور حوكمة الأمن السيبراني في تفعيل الإفصاح عن إدارة مخاطر الأمن السيبراني وأثره في تحسين الأداء المالي [1]

هدفت الدراسة إلى قياس العلاقة بين حوكمة الأمن السيبراني ومستوى الإفصاح عن إدارة المخاطر السيبرانية على المصارف المقيدة بالبورصة المصرية وتحليل تأثير الإفصاح عن مخاطر السيبرانية في تحسين الأداء المالي للمؤسسات خصوصا المصارف، تم تصميم استبيان لجمع البيانات وتوزيعها على أفراد مجتمع الدراسة الذي يتكون من المحاسبين والمدققين الداخليين في المصارف وتم تحديد عينة

الدراسة التي بلغت 105 مشاركين (بمعدل استجابة 100%)، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها ساهمت حوكمة الأمن السيبراني بشكل إيجابي ومعنوي في الحد من مخاطر الهجمات السيبرانية في المصارف المقيدة بالبورصة المصرية وأدت إلى تفعيل الإفصاح عن تقارير إدارة مخاطر الأمن السيبراني، كما أن الإفصاح عن تقارير إدارة المخاطر في ظل حوكمة الأمن السيبراني ساهم في تحسين الأداء المالي للمصارف.

2- دراسة (Younis, Yara, 2025): أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين. [2]

هدفت الدراسة إلى تحليل مدى تأثير توكيد المراجعة الخارجية على مخاطر الأمن السيبراني على قرارات المستثمرين، أي التأكد من أن المدقق الخارجي يعترف ويصحح مخاطر الأمن السيبراني في القوائم والتقارير ذات الصلة، وتأثير ذلك على ثقة المستثمرين.

ولتحقيق أهداف البحث والإجابة على أسئلة البحث، تم تصميم استبيان لجمع البيانات وتوزيعها على أفراد مجتمع الدراسة الذي يتكون من فئة من المستثمرين، وتم تحديد عينة الدراسة التي بلغت 75 مستثمرًا.

اعتمد البحث على اختبار فروض مرتبطة بالتأثير السببي، وقد توصلت الدراسة إلى مجموعة من النتائج، أهمها: أنه وُجد تأثير معنوي إيجابي لتوكيد المدقق الخارجي بشأن مخاطر الأمن السيبراني على قرارات المستثمرين، سواء في قرارات الاستثمار المباشرة أو مستوى الثقة، والتأكيد على أهمية الإفصاح عن مخاطر الأمن السيبراني في التقارير السنوية، وقيام الإدارة بتقييم ذاتي لنظام إدارة هذه المخاطر، واتخاذ إجراءات فورية لمعالجة أي ضعف جوهري في منظومة الأمن السيبراني.

3- دراسة (Alorabi, Majed Qalil Mohammed. Abuanzeh, Asma, 2024): دراسة تطبيقية عن دور إدارة المخاطر في تعزيز ألامن السيبراني للمؤسسات الصغيرة والمتوسطة في المملكة العربية السعودية. [3]

هدفت هذه الدراسة إلى تقييم وتحسين إدارة المخاطر السيبرانية في المؤسسات الصغيرة والمتوسطة SMES في المملكة العربية السعودية، مع التركيز على الوعي السيبراني لدى الموظفين، نظرا لاعتماد المؤسسات المتزايد على التكنولوجيا فإنها أصبحت أكثر عرضةً للهجمات السيبرانية، حيث تم الاعتماد في هذه الدراسة على المنهج الوسط التحريري ليكونه ملائم وباستخدام المنهج الاستقرائي لتعميق الفهم وتكون مجتمع الدراسة من جميع العاملين في المؤسسات الصغيرة والمتوسطة في المملكة وخاصة العاملين في قسم تقنية المعلومات، الشؤون الإدارية، الموارد البشرية والأقسام المالية وقد بلغت أعينة الدراسة 82 مشاركاً تم اختيارهم بطريقة غير احتمالية غالباً بطريقة قصدية نظرا للصعود للوصول إلى

جميع أفراد المجتمع والاستفادة من أراء الأشخاص الذين يملكون خبرة أو مسؤوليات فعلية في مجال إدارة المخاطر أو الأمن السيبراني في مؤسساته

- **الدراسات الأجنبية:**

1- دراسة (Martens, P. S., & Teuteberg, F., 2022) [4]:

Risk Management and Cybersecurity: A structured literature Review

اداره المخاطر والامن السيبراني مراجعه ادبيه منظمه.

هدفت هذه الدراسة الى تجميع وتحليل البحوث والدراسات السابقة المتعلقة بإدارة المخاطر والامن السيبراني لفهم الترابط بينهما، وتسليط الضوء على الفجوات البحثية، وتقديم اطار شامل يساعد الباحثين والممارسين على تعزيز ممارسات اداره المخاطر السيبرانيه، ولتحقيق اهداف البحث تم تطبيق مراجعه منهجيه للأدبيات العلمية المنشورة بين سنوات محدده من ال (2000 _ 2019) شملت 100 ورقه بحثيه ومقالات اكاديمي وتقارير تقنيه تم اختيارها بحسب معايير محدده و باستخدام بحث ثانوي وصفي تحليلي والاعتماد على قواعد بيانات أكاديمية (مثل Scopus, Web of Science, IEEE Xplore) ومعايير اختيار منهجية (Inclusion/Exclusion criteria) لتنقية الأوراق البحثية و التحليل النوعي والكمي للموضوعات والتوجهات واستخدام برامج إدارة المراجع وتحليل المحتوى مثل NVivo أو Excel وقد وصلت هذه الدراسة الى مجموعه من النتائج اهمها: توجد تداخلات واضحة بين إدارة المخاطر والأمن السيبراني، حيث تعتبر إدارة المخاطر عنصرًا أساسيًا في بناء استراتيجيات الأمن السيبراني الفعالة، وهناك تركيز متزايد على تقييم المخاطر السيبرانية باستخدام نماذج كمية ونوعية، ولكن لا زالت توجد فجوات في التقييم الشامل للمخاطر المرتبطة بالتقنيات الحديثة ، ويلاحظ وجود اهتمام متزايد بدمج تقنيات الذكاء الاصطناعي وتحليل البيانات في عمليات إدارة المخاطر السيبرانية، والدراسات تشير إلى أن العديد من المؤسسات تواجه تحديات في تطبيق إدارة المخاطر بشكل متكامل بسبب غياب التنسيق بين الأقسام المختلفة وضعف الوعي الأمني، وأخيراً تم تحديد مجموعة من التوجهات المستقبلية مثل تطوير أطر عمل مرنة، وزيادة التوعية، وتحسين الأدوات التكنولوجية لإدارة المخاطر.

2- دراسة (Aven, T., & Zion, E., E 2018) [5]:

Cybersecurity Risk Management Frame works: Current Practices and Future Direction

أطر اداره مخاطر الامن السيبراني: الممارسات الحالية والتوجهات المستقبلية.

هدفت الدراسة الى مراجعه الاطر الحالية المستخدمة لإدارة مخاطر الامن السيبراني واقتراح تحسينات مستقبليه، لم تعتمد الدراسة على مجتمع ميداني تقليدي مثل موظفي شركه معينه، بل اعتمدت على تحديد الممارسات الحالية والاطر المستخدمة عالميا، حيث تم تحديد مجتمع الدراسة في النماذج والممارسات العالمية في اداره مخاطر الامن السيبراني والتي تشمل الاطر التنظيمية (NIST,ISO

27005)، والاتجاهات والدراسات الأكاديمية والممارسات الصناعية الحالية، وتم اختيار مجموعه من الاطر المعتمدة في اداره مخاطر الامن السيبراني والادبيات والدراسات السابقة والاتجاهات الحديثة في التفكير حول اداره المخاطر، وتم الاعتماد على بحث نوعي تحليلي–مفاهيمي باستخدام مراجعة الادبيات وتحليل مقارن لأطر اداره المخاطر السيبرانية ونقد نظري لمواطن القصور في الاطر الحالية وصياغه مقترحات تطويريه تركز على المرونة وعدم اليقين بحيث يتم اقتراح اتجاهات مستقبليه وتطوير الأطر الحالية

وقت توصلت دراسة الى مجموعه من النتائج اهمها: الاطر الحالية مثل (NIST , ISO 27005) مفيدة لكنها تحتاج الى تحديثات مستمرة ، والمؤسسات تميل الى التطبيق الشكل دون ادراك جوهري لفلسفه اداره المخاطر ،ضرورة دمج الذكاء الاصطناعي والتحليلات التنبيه في تقييم المخاطر.

3- دراسة (Holzinger, A., Schmidt, B., & Fischer, C., 2017) [6]:

Risk _based Cybersecurity Strategies in Modern Organizations

استراتيجيات الامن السيبراني القائمة على المخاطر في المنظمات الحديثة.

هدفا الدراسة الى اقتراح استراتيجيات امن سيبراني مبنيه على اداره المخاطر في بيئات العمل الحديثة، حيث تناقش الدراسة استراتيجيات قائمه على المخاطر لتعزيز الامن السيبراني في المؤسسات، وتوصي بالاعتماد على التحليل الكمي والنوعي للمخاطر لتعزيز الاستعداد السيبراني، واستهدفت الدراسة المنظمات المعاصرة التي تعتمد بشكل كبير على الانظمة الرقمية، وتركز على بيئات العمل التي تواجه تهديدات سيبرانية متزايدة كالمؤسسات الحكومية، والشركات التجارية الكبرى، والمنظمات التقنية المالية، باستخدام بحث تطبيقي–تحليلي يجمع بين المنهج النوعي والمنهج التطبيقي باستخدام دراسة حاله، وتحليل محتوى تقارير امنيه، ومقابلات داخليه، ومراجعه ادبيات حول استراتيجيات الامن السيبراني، ومقارنه تطبيقيه بين منظمات ذات مستويات نضج مختلفة في امن المعلومات.

وقد توصلت الدراسة الى أن الاستراتيجيات المبنية على المخاطر اكثر قدره على التكيف مع التهديدات المتغيرة، والتحليل الكمي للمخاطر يدعم تخصيص الموارد بشكل افضل، ووجود خطه استباقيه لاداره المخاطر تقلل من الخسائر الناتجة عن الهجمات.

- **تقييم الدراسات السابقة:**

تتشابه الدراسة الحالية مع الدراسات السابقة كونها تطرقت الى دور اداره المخاطر في تعزيز الامن السيبراني، وتختلف عنها في كون الدراسة الحالية في بيئة جديده وهي (محافظة حماه)، كما أن بعض الدراسات بقيت في الإطار النظري دون تطبيق ميداني، وبعضها الاخر اعتمد على الاستبيانات أكثر من دراسة الحالة او تحليل السياسات الواقعية. كما أن هذا البحث يمثل دراسة علميه جديده ينتظر

التوسع في استخدامه في مصارف ومؤسسات ومنظمات اخرى في سوريا كي يتعمق وينتشر لما لاداره المخاطر من دور مهن جدا في تعزيز الامن السيبراني.

3. مشكلة البحث

في ظل الثورة الرقمية، والتحول الرقمي المتسارع، وزياده الاعتماد على الأنظمة الإلكترونية في جميع القطاعات، اصبحت المؤسسات عرضه بشكل متزايد للتهديدات السيبرانية التي قد تؤثر على سريه المعلومات وسلامتها وتوافرها، ويعد القطاع المصرفي والمؤسسات المالية كالمصارف من ابرز الاهداف لتلك التهديدات، التي قد تؤدي الى خسائر ماليه وسمعه مؤسسيه جسيمه، نظرا لحساسيه بياناتها واهميه خدماتها، وكون المصارف تعتمد بشكل كبير على التكنولوجيا في أعمالها اليومية فقد ادى هذا الواقع الى ارتفاع الحاجه لتبني استراتيجيات متقدمة لحماية الأصول المعلوماتية، وضمان استمرارية الأعمال، ومن ابرز هذه الاستراتيجيات اداره المخاطر التي يؤدي غيابها أو ضعفها إلى ثغرة كبيرة في منظومة الأمن. لذلك فأنه يمكن تجسيد مشكله البحث من خلال عدد من التساؤلات البحثية الآتية:

السؤال البحثي الرئيس: ما دور اداره المخاطر في تعزيز الامن السيبراني في المصارف الخاصة في محافظة حماة؟

ويتفرع عن السؤال البحثي الرئيس الاسئلة الفرعية الاتية:

1) ما دور تحديد المخاطر في تعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة؟
2) ما دور تقييم وتحليل المخاطر في كفاءة الأمن السيبراني في المصارف الخاصة في محافظة حماة؟
3) ما دور معالجة المخاطر في حماية النظام السيبراني في المصارف الخاصة في محافظة حماة؟
4) ما دور مراقبة ومراجعة المخاطر في تحسين الأمن السيبراني في المصارف الخاصة في محافظة حماة؟
5) ما دور التواصل حول المخاطر في تعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة؟

4. أهمية البحث

- **الأهمية النظرية:** تسهم هذه الدراسة في إثراء الأدبيات العلمية في مجال إدارة المخاطر والأمن السيبراني في المجالات المالية والمصرفية، من خلال الربط بين مفاهيم ونماذج إدارة المخاطر وتطبيقها على أمن المعلومات في المؤسسات المصرفية، وتسليط الضوء على العلاقة بين إدارة المخاطر والأمن السيبراني، وهو موضوع حديث نسبياً لم يحظَ بعد بالدراسة الكافية في الأدبيات العربية، خاصة في السياق العربي والسوري، وتوفير إطار نظري وعملي لطلبة الجامعات والباحثين

يمكن من فهم الآليات التي تساعد المؤسسات على التصدي للتهديدات السيبرانية من منظور إدارة المخاطر.

- **الأهمية العملية:** تستمد هذه الدراسة اهميتها العملية من خلال تمكين مجتمع البحث من تقييم فعالية نظامه الحالي في إدارة المخاطر السيبرانية، والكشف عن نقاط القوة والضعف في ممارساته الحالية، و دعم صُنّاع القرار داخل البنك بمعلومات تحليلية وموثقة حول كفاءة أدوات وأساليب إدارة المخاطر في الوقاية من التهديدات الرقمية، وتقديم توصيات عملية قابلة للتنفيذ لتحسين تكامل إدارة المخاطر مع وحدة أمن المعلومات، بما يسهم في رفع الجاهزية السيبرانية للبنك، وتقديم نتائج قابلة للتعميم على مؤسسات مشابهة، بما يعزز البنية التحتية للأمن السيبراني على مستوى القطاع المالي الوطني، ورفع مستوى الوعي المؤسسي والوظيفي داخل المصارف حول أهمية إدارة المخاطر كجزء لا يتجزأ من استراتيجية الأمن السيبراني، وليس كمجرد إجراء تقني منفصل.

5. أهداف البحث

تسعى الدراسة إلى تحقيق الأهداف التالية:

الهدف الرئيس: بيان دور إدارة المخاطر في تعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة.

ينبثق عن الهدف الرئيس الاهداف الفرعية الآتية:

1) بيان دور تحديد المخاطر في تعزيز الامن السيبراني في المصارف الخاصة في محافظة حماة.
2) بيان دور تقييم وتحليل المخاطر في تعزيز الامن السيبراني في المصارف الخاصة في محافظة حماة.
3) بيان دور مراجعه المخاطر في تعزيز الامن السيبراني في المصارف الخاصة في محافظة حماة.
4) بيان دور مراقبه ومراجعه المخاطر في تعزيز الامن السيبراني في المصارف الخاصة في محافظة حماة.
5) بيان دور تواصل حول المخاطر في تعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة.

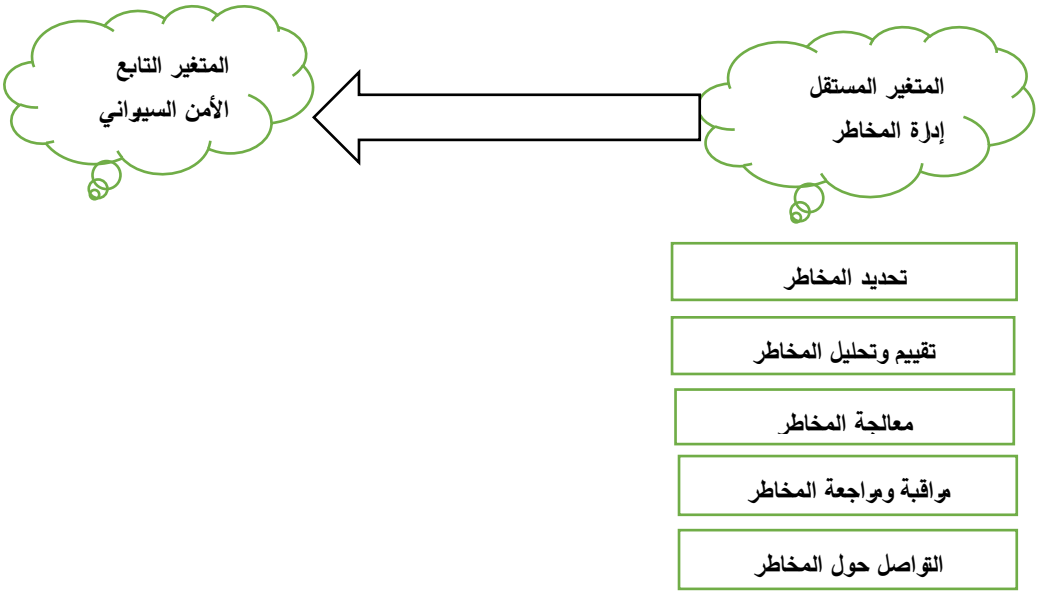
6. فرضيات البحث

الفرضية الرئيسة: يوجد دور ذو دلالة معنوية بين تطبيق إدارة المخاطر وتعزيز الأمن السيبراني في المصارف السورية:

- الفرضية الفرعية الأولى: يوجد دور ذو دلالة معنوية بين تحديد المخاطر وتعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة.

- الفرضية الفرعية الثانية: يوجد دور ذو دلالة معنوية بين تقييم وتحليل المخاطر وتعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة.
- الفرضية الفرعية الثالثة: يوجد دور ذو دلالة معنوية بين معالجة المخاطر وتعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة.
- الفرضية الفرعية الرابعة: يوجد دور ذو دلالة معنوية بين مراقبة ومراجعة المخاطر وتعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة.
- الفرضية الفرعية الخامسة: يوجد دور ذو دلالة معنوية بين التواصل حول المخاطر وتعزيز الأمن السيبراني في المصارف الخاصة في محافظة حماة.

7. متغيرات البحث



الشكل (1): نموذج متغيرات البحث

8. مجتمع وعينة البحث

يتمثل مجتمع البحث في جميع العاملين (مديرين وموظفين) في المصارف الخاصة في محافظة حماة (مصارف سورية والمهجر، والبركة، وسورية الدولي الإسلامي) التي اقتصرت الدراسة عليهم، وتم اتباع اسلوب العينة القصدية ضمن الاقسام ذات العلاقة بإدارة المخاطر والامن السيبراني (ادارة المخاطر، قسم امن المعلومات، قسم تكنولوجيا المعلومات، قسم التدقيق الداخلي، والإدارة العليا المعنية بالحكومة والمخاطر)، حيث بلغت العينة (60) مفردة، وبذلك بلغ عدد الاستبانات الموزعة (60) وتم استردادها بالكامل وكانت صالحة للتحليل.

9. منهجية البحث

اعتمد البحث على المنهج الوصفي بأسلوب تحليلي، وفي الجزء النظري تم الاعتماد فيه على أبرز ما ورد في الكتب والمرجعيات والادبيات المتخصصة في موضوع البحث، وتم الاستفادة من الدراسات السابقة في تصميم الاستبانة. أما الجزء العملي تم الاعتماد فيه على جمع البيانات، وتحليل وتفسير النتائج التي تم التوصل اليها بعد استرداد الاستبانة وتم الاعتماد على البرنامج الاحصائي (SPSS)، وذلك من خلال تحليل الارتباط والانحدار والخروج باستنتاجات وتوصيات.

10. حدود البحث

- حدود زمانية: 2025.
- حدود مكانية: مصارف سورية والمهجر، والبركة، وسورية الدولي الإسلامي في محافظة حماة.
- حدود موضوعية: وهي الحدود التي تتعلق بإدارة المخاطر والأمن السيبراني، وتتمثل متغيرات البحث المدروسة بالمتغيرات المستقلة الآتية: (تحديد المخاطر، تقييم وتحليل المخاطر، معالجة المخاطر، مراقبة ومعالجة المخاطر، التواصل حول المخاطر)، والمتغير التابع والأمن السيبراني.

11. إدارة المخاطر

1.11. تعريف إدارة المخاطر

تعرف بأنها نظام من الأشخاص والعمليات والتكنولوجيا التي تمكن المنظمة من تحديد أهداف تتماشى مع القيم والمخاطر.من خلال الالتزام ببرامج تقييم المخاطر الناجحة بالأهداف القانونية والتعاقدية والداخلية والاجتماعية والأخلاقية ، فضلاً عن مراقبة اللوائح الجديدة المتعلقة بالتكنولوجيا من خلال تركيز الانتباه على المخاطر وتخصيص الموارد اللازمة للتحكم في المخاطر وتخفيفها ، ستحمي لمؤسسة نفسها من عدم اليقين ، وتقلل التكاليف وتزيد من احتمالية استمرارية الأعمال ونجاحها **[7]**.

كما تعرف بأنها العملية التي تقوم بقياس وتقييم المخاطر لدى المؤسسات، وتطوير إستراتيجيات إدارتها، والمساهمة في رسم خريطة نطاق العمل وتقييم المخاطر، وكذلك تعريف إطار العملية وأجندة التحليل لحجم الخسائر المحتملة، وهناك من يرى بان ادارة المخاطر هي عملية تحديد ومراقبة وإدارة المخاطر المحتملة من أجل تقليل التأثير السلبي الذي قد يكون لها على المؤسسة **[7]**.

تعرف بأنها عملية منظمة تهدف إلى توجيه ومراقبة المنظمة فيما يتعلق بالمخاطر، من خلال تطبيق منهجية لتحديد وتحليل وتقييم ومتابعة ومراجعة المخاطر التي قد تؤثر على تحقيق الأهداف **[8]**.

أما إدارة مخاطر الأمن السيبراني فتعرف على أنها" مجموعة السياسات، والعمليات، والأساليب الرقابية المصممة لحماية المعلومات والأنظمة من الهجمات الإلكترونية والاختراق الأمني والتي قد تحد من

إمكانية تحقيق نظام الأمن السيبراني لأهدافه المرجوة والمتمثلة في إتاحة المعلومات، والسرية وسلامة العمليات التشغيلية للمنظمة" **[9]**.

2.11. أهداف إدارة المخاطر

تُعد إدارة المخاطر من الركائز الأساسية التي تستند عليها المؤسسات لحماية مصالحها وتحقيق استمراريتها وتتمثل أبرز أهدافها فيما يلي **[10]**:

1) حماية أصول المؤسسة: إذ تهدف إدارة المخاطر إلى حماية الموارد المادية والبشرية والمعلوماتية من التهديدات المحتملة، سواء كانت داخلية أو خارجية.
2) الحد من الخسائر وتقليل الآثار السلبية للمخاطر، من خلال تحديد المخاطر المحتملة مسبقًا ووضع خطط للتعامل معها، تساعد إدارة المخاطر على تقليل الخسائر الناتجة عن الحوادث غير المتوقعة.
3) ضمان استمرارية الأعمال: تهدف إدارة المخاطر إلى وضع إجراءات احتياطية تضمن استمرار العمل حتى في ظل الأزمات أو الكوارث.
4) تحسين جودة اتخاذ القرار: توفر إدارة المخاطر معلومات دقيقة وموثوقة تساعد الإدارة العليا في اتخاذ قرارات مدروسة تستند إلى تحليل المخاطر.
5) الامتثال للأنظمة والقوانين من خلال التأكد من أن المؤسسة ملتزمة بالتشريعات واللوائح المحلية والدولية، خاصة تلك المتعلقة بالأمن المعلوماتي والخصوصية.
6) تعزيز ثقة أصحاب المصلحة: عندما تُدار المخاطر بكفاءة، ينعكس ذلك إيجابًا على سمعة المؤسسة ويزيد من ثقة العملاء والمستثمرين بها.
7) تحقيق الميزة التنافسية حيث تُعد المؤسسات القادرة على إدارة مخاطرها بشكل فعّال أكثر قدرة على التكيف مع التغيرات والاستجابة بسرعة للأزمات، ما يمنحها تفوقًا في السوق.

3.11. أبعاد إدارة المخاطر

تُعد إدارة المخاطر نظامًا إداريًا متكاملًا يتكون من مجموعة من الوظائف أو الأبعاد التي تهدف إلى الحد من تأثير المخاطر على أهداف المؤسسة وتؤدي هذه الوظائف دورًا محوريًا في ضمان الاستقرار والتخطيط السليم، خصوصًا في المؤسسات المصرفية التي تتعرض لمخاطر معقدة ومتنوعة وفيما يلي أهم أبعاد إدارة المخاطر **[11]**:

1) تحديد المخاطر: تمثل الوظيفة الأولى في دورة إدارة المخاطر، حيث يتم فيها التعرف على كافة أنواع المخاطر المحتملة التي قد تواجه المؤسسة سواء كانت مالية، تشغيلية، تقنية، أو سيبرانية يشمل ذلك تحليل المصادر الداخلية والخارجية للمخاطر.

2) تحليل وتقييم المخاطر: بعد تحديد المخاطر، يتم تقييم احتمال حدوثها وتأثيرها المحتمل على أهداف المؤسسة يتم ذلك باستخدام أساليب كمية ونوعية (مثل مصفوفة الاحتمالية – التأثير، وتحليل السيناريوهات)، لتصنيف المخاطر حسب أولويتها وخطورتها.
3) معالجة المخاطر: تشمل هذه الوظيفة تحديد الاستراتيجيات المناسبة للتعامل مع المخاطر، سواء بالتقليل منها، أو تجنبها، أو نقلها (مثل التأمين)، أو قبولها ضمن حدود مقبولة يتم اتخاذ القرارات بناءً على التحليل.
4) مراقبة ومراجعة المخاطر: يتم في هذه المرحلة متابعة أداء خطط إدارة المخاطر وتقييم فعاليتها بشكل دوري، لضمان التكيف مع التغيرات الجديدة في بيئة العمل، ومعالجة أية نقاط ضعف أو خلل في النظام.
5) الاتصال والتشاور بشأن المخاطر: تشمل هذه الوظيفة التواصل الداخلي والخارجي بشأن المخاطر، لضمان إشراك جميع الأطراف المعنية (مثل الإدارة، الموظفين، أصحاب المصلحة) في فهم طبيعة المخاطر واستراتيجيات التعامل معها.

12. الأمن السيبراني

1.12. مفهوم الأمن السيبراني

تطور لمفهوم أمن المعلومات، ويشمل حماية الفضاء السيبراني بما فيه من أنظمة رقمية وعمليات وسلوكيات بشرية، في مواجهة تهديدات معقدة ومتغيرة **[12]**.

تشير وكالة الأمن السيبراني الأوروبية – ENISA (2023) إلى ان الامن السيبراني هو مجموعة من الأنشطة التي تركز على حماية موارد المعلومات الرقمية، وتشمل الأشخاص والتكنولوجيا والعمليات، بهدف تقليل التهديدات وضمان استمرارية الأعمال" **[13]**.

الأمن السيبراني يشير إلى ممارسة حماية الأنظمة والشبكات والبرمجيات والبيانات من الهجمات الرقمية الضارة التي تهدف إلى الاستفادة من الثغرات الأمنية لتحقيق أهداف خبيثة" **[14]**.

2.12. أهمية الأمن السيبراني

في ظل التقدم الرقمي السريع والاعتماد المتزايد على التكنولوجيا في جميع قطاعات الأعمال، برز الأمن السيبراني كأحد أهم الركائز الأساسية لاستمرارية المؤسسات، ولا سيما في القطاعات المالية والمصرفية فهو لا يقتصر على حماية المعلومات، بل يتجاوز ذلك ليشمل الحفاظ على سمعة المؤسسة، وضمان ثقة العملاء، وضمان الامتثال التنظيمي، ومنع الخسائر المالية الناتجة عن الهجمات السيبرانية تتمثل أهمية الامن السيبراني فيما يأتي **[15]**:

1) حماية سرية المعلومات وخصوصية البيانات، خاصة في المؤسسات المصرفية التي تتعامل مع معلومات مالية وشخصية للعملاء.
2) مواجهة التهديدات والهجمات السيبرانية التي تزداد وتيرتها وتعقيدها، مثل الفدية، وهجمات التصيد الاحتيالي، والاختراقات المستهدفة للبنية التحتية الرقمية، ما يجعل الأمن السيبراني ضرورة استراتيجية.
3) ضمان استمرارية الأعمال وحماية الأنظمة: يساهم الأمن السيبراني في تقليل مخاطر التوقف عن العمل الناجم عن هجمات إلكترونية أو اختراقات للبنية التحتية، من خلال خطط الاستجابة والتعافي السريع من الأزمات.
4) تعزيز ثقة العملاء والشركاء حيث توفر المؤسسات التي تطبق نظم حماية سيبرانية فعالة بيئة آمنة لعملائها، مما يعزز من ولائهم وثقتهم في التعاملات الإلكترونية.
5) تحقيق الامتثال التنظيمي والقانوني حيث تفرض العديد من القوانين والأنظمة على المؤسسات، خاصة المصارف، الالتزام بمتطلبات الأمن السيبراني، مثل القوانين المتعلقة بحماية البيانات (مثل GDPR) أو معايير البنك المركزي.
6) تكامل الأمن السيبراني مع إدارة المخاطر حيث يمكن من خلال تحليل التهديدات وتقييم نقاط الضعف رسم خريطة شاملة للمخاطر الرقمية والتعامل معها بفعالية.

3.12. العوامل المؤثرة في تعزيز الأمن السيبراني

تعتبر عملية تعزيز الأمن السيبراني أمرًا معقدًا ومتعدد الأبعاد، يتأثر بعدة عوامل تقنية وبشرية وتنظيمية فهم هذه العوامل يساعد المؤسسات، مثل المصارف السورية المذكورة سابقاً، على بناء منظومة متكاملة فعالة لحماية أصولها الرقمية، حيث تتمثل العوامل بما يلي **[16]:**

1) **الدعم القيادي والإدارة العليا:** تلعب الإدارة العليا دورًا حاسمًا في تخصيص الموارد، ودعم السياسات الأمنية، وخلق ثقافة أمان داخل المؤسسة مما يعزز الأمن السيبراني.
2) **التوعية والتدريب المستمر للموظفين:** العنصر البشري هو الحلقة الأضعف في سلسلة الأمن السيبراني، لذا فإن رفع مستوى الوعي وتدريب الموظفين على الممارسات الآمنة يقلل من المخاطر الناتجة عن الأخطاء أو الاستهداف المباشر.
3) **البنية التحتية التقنية الحديثة:** توفير أجهزة وبرمجيات متطورة وقادرة على رصد ومنع الهجمات مثل جدران الحماية، وأنظمة كشف التسلل، والتشفير، وأنظمة إدارة الهوية والوصول.
4) **السياسات والإجراءات الأمنية:** وضع وتحديث السياسات الأمنية التي تحدد قواعد وضوابط استخدام الموارد الرقمية، ومعالجة الحوادث، والتعامل مع البيانات الحساسة.

5) **إدارة المخاطر السيبرانية:** تقييم وتحليل المخاطر المحتملة بشكل دوري واتخاذ الإجراءات المناسبة للوقاية أو التخفيف من تأثيرها هذا يشمل اختبار الاختراق وتحليل نقاط الضعف.
6) **الامتثال للمعايير واللوائح:** الالتزام بمعايير الأمن السيبراني مثل ISO 27001، NIST، ومتطلبات الجهات الرقابية مثل البنك المركزي، يعزز من مستوى الحماية ويقلل من المخاطر القانونية والتنظيمية.
7) **الاستجابة السريعة للحوادث:** وجود خطة واضحة للاستجابة للحوادث السيبرانية والتعافي السريع منها يحد من الأضرار ويضمن استمرارية الأعمال.
8) **الثقافة الأمنية المؤسسية:** غرس ثقافة أمنية داخل المؤسسة، تشجع على الالتزام بالإجراءات الأمنية وتقبل التغيير والتطوير في هذا المجال.

13. النتائج ومناقشتها

1.13. تصميم الاستبانة

تم تصميم القائمة على أن تكون الأسئلة واضحة ومباشرة بحيث يكون للمستبانين منهم إدراك الهدف منها بوضوح والإجابة عليها، وتم تقسيم قائمة الاستبانة إلى مجموعتان من الأسئلة:

المجموعة الأولى:

العبارات التي تقيس أبعاد إدارة المخاطر (المتغير المستقل) وتم تقسيمها إلى الأبعاد التالية:

أولاً – تحديد المخاطر :ويشمل العبارات من (1 إلى 6)، وتهدف إلى قياس مدى اعتماد البنك على أساليب منهجية لتحديد مصادر الخطر المحتملة، وأدوات التحليل البيئي، ومشاركة الموظفين في ورش العمل

ثانياً – تقييم وتحليل المخاطر :ويشمل العبارات من (7 إلى 12)، ويقيس مدى استخدام أدوات كمية ونوعية، ولجان متخصصة، وتكنولوجيا حديثة لتقييم المخاطر

ثالثاً – معالجة المخاطر :ويشمل العبارات من (13 إلى 18)، ويركز على مدى توفر خطط استجابة واضحة، وتوزيع المهام والموارد، والاستفادة من الخبرات السابقة في إدارة المخاطر

رابعاً – مراقبة ومراجعة المخاطر :ويشمل العبارات من (19 إلى 24)، ويقيس مستوى المتابعة والتحديث المستمر لخطط إدارة المخاطر، وإشعار الإدارة العليا بالتقارير الدورية

خامساً – التواصل حول المخاطر :ويشمل العبارات من (25 إلى 30)، ويقيس مدى توافر قنوات تبادل المعلومات، والشفافية، والتدريب والتوعية داخل البنك بشأن المخاطر

المجموعة الثانية:

العبارات التي تقيس الأمن السيبراني (المتغير التابع)، ويتضمن (6) عبارات تهدف إلى قياس مدى التزام البنك بالإجراءات الأمنية لحماية الأنظمة من التهديدات السيبرانية، وامتلاك خطط الاستجابة والتعافي، وتوعية الموظفين، والامتثال للمعايير الوطنية والدولية ذات الصلة.

تم توزيع الاستبانة على عينة مكونة من 60 موظف/ة يعملون في فروع حماة للمصارف الثلاثة المذكورة، استردت بالكامل وكانت صالحة للتحليل. تم استخدام المقياس الخماسي ليكرت، وذلك لبيان درجات الموافقة، وإعطاءها القيم التصاعدية كما يلي:

الجدول (1): درجات الموافقة على الاستقصاء

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

كما تم تصنيف متوسطات الإجابات إلى ثلاث مستويات (عالي، متوسط، متدني)، وعلى أساس أن درجة محايد هي درجة متوسطة من الموافقة ويقابلها العدد (3)، وبناءً على ذلك تم الاعتماد على التصنيف التالي:

الجدول (2): تصنيف الإجابات

من 1 إلى أقل من 2.5	من 2.5 إلى أقل من 3.5	من 3.5 إلى 5
متدني	متوسط	عالي

2.13. صدق وثبات أداة البحث

1.2.13. اختبار الصدق الظاهري

تم إجراء هذا الاختبار بعرض قائمة الاستبانة على عدد من أعضاء الهيئة التدريسية في الجامعة الوطنية الخاصة، وتم تعديل بعض الأسئلة الواردة وإعادة صياغة بعض الأسئلة في الاستبانة.

2.2.13. اختبار الاتساق الداخلي

بعد دراسة الصدق الظاهري لأداة البحث، تم اختبار الاتساق الداخلي لأسئلة الاستبيان لتحديد مدى ارتباطها مع بعضها البعض بحيث لا تتغير إذا طبقت في ظروف مختلفة، وتم استخدام معامل (ألفا كرونباخ) **[17]** لهذا الغرض كما هو مبين في الجدول التالي:

الجدول (3): نتائج ألفا كرونباخ

المتغيرات	قيمة ألفا كرونباخ	عدد العبارات
تحديد المخاطر	0.788	6
تقييم وتحليل المخاطر	0.764	6
معالجة المخاطر	0.771	6

مراقبة ومراجعة المخاطر	0.752	6
التواصل حول المخاطر	0.743	6
الأمن السيبراني (المتغير التابع)	0.792	6

المصدر: من إعداد الباحثين، استنادًا إلى نتائج التحليل الإحصائي باستخدام برنامج SPSS الإصدار 26

تجاوزت جميع معاملات ألفا كرونباخ الحد الأدنى المقبول إحصائيًا (0.70)، مما يدل على أن أداة الاستبانة تمتاز بدرجة عالية من الاتساق الداخلي.

3.13. اختبار فرضيات البحث

تم اختبار فرضيات البحث باستخدام معامل الارتباط البسيط ومعامل الانحدار:

<u>الفرضية الفرعية الأولى</u>: يوجد دور ذو دلالة معنوية بين **تحديد المخاطر** وتعزيز **الأمن السيبراني** في مصارف (سورية والمهجر – البركة – سورية الدولي الإسلامي).

وقد كانت نتيجة تحليل الارتباط والانحدار للفرضية الفرعية الأولى كما يلي:

الجدول (4): نتائج تحليل الارتباط للفرضية الفرعية الأولى

Correlations

		X1	Y
X1	Pearson Correlation	1	.584**
	Sig. (2-tailed)		.000
	N	60	60
Y	Pearson Correlation	.584**	1
	Sig. (2-tailed)	.000	
	N	60	60

يتضح من تحليل درجة الارتباط العلاقة بين المتغير المستقل X1 والمتغير التابع Y1، كما ان قيمة معامل الارتباط هي (0.521)، وهذا يدل على وجود درجة ارتباط متوسطة بين المتغيرين، واتجاه هذه العلاقة طردية، وهذا يدل على ان أي زيادة في أحد المتغيرين سيرافقها زيادة في المتغير الاخر والعكس صحيح.

الجدول (5): نتائج تحليل انحدار الفرضية الفرعية الأولى

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.584^a	0.341	0.330	1.066
a. Predictors: (Constant), x1				

$ANOVA^a$

Model		Sum of Squares	Df	Mean Square	F	Sig
1	Regression	34.100	1	34.100	30.012	0.000
	Residual	65.900	58	1.136		
	Total	100.000	59			
a. Dependent Variable: تعزيز الأمن السيبراني						
b. Predictors: (Constant)، تحديد المخاطر						

Coefficients[a]						
Model		Unstandardized Coefficients Regression		Standardized Coefficients	T	Sig
		B	Std. Error	Beta		
1	(Constant)	1.500	0.375		4.000	0.000
	فعالية تحديد المخاطر	0.503	0.092	0.584	5.478	0.000
a. Dependent Variable تعزيز الأمن السيبراني						

يتضح من الجدول أن قيمة معامل بيرسون (Pearson Correlation) بلغت (0.584)وهي قيمة موجبة متوسطة، وتُشير إلى وجود علاقة ارتباط طردية بين المتغيرين كما أن قيمة **Sig = 0.000**وهي أقل من مستوى الدلالة المعتمد (0.05)، مما يدل على أن هذه العلاقة **دالة إحصائيًا**، ويُفهم من ذلك أنه كلما زاد تحديد المخاطر في المصرف، زادت تبعًا لذلك مستويات تعزيز الأمن السيبراني.

أظهرت نتائج تحليل التباين (ANOVA) أن نموذج الانحدار ذو دلالة إحصائية، حيث بلغت قيمة F المحسوبة (58.388)، وهي أكبر من القيمة الجدولية، في حين بلغت قيمة الدلالة الإحصائية Sig = 0.000، مما يؤكد معنوية النموذج عند مستوى (0.05).

أما معامل التحديد (R^2) فقد بلغ (0.341)، ما يعني أن 34.1% من التغيرات في الأمن السيبراني تعود إلى تحديد المخاطر،

وفيما يخص نتائج معامل الانحدار الخطي البسيط، فقد كانت كما يلي:

- قيمة الميل غير المعياري (B) بلغت (0.503)، وهي موجبة، مما يدل على أن العلاقة طردية
- قيمة Beta المعيارية بلغت (0.584)
- قيمة T بلغت (7.641) وهي أكبر من القيمة الجدولية، مع مستوى دلالة Sig = 0.000

وبناءً على ما سبق، نقر بالفرضية الفرعية الأولى، مما يعني أنه يوجد دور ذو دلالة معنوية بين **تحديد المخاطر** وتعزيز **الأمن السيبراني** في المصارف محل الدراسة.

<u>الفرضية الفرعية الثانية</u>: يوجد دور ذو دلالة معنوية بين **تقييم وتحليل المخاطر** وتعزيز **الأمن السيبراني** في مصارف (سورية والمهجر – البركة – سورية الدولي الإسلامي).

وقد كانت نتيجة تحليل الارتباط والانحدار للفرضية الفرعية الثانية كما يلي:

الجدول (6): نتائج تحليل الارتباط للفرضية الفرعية الثانية

Correlations

		X2	Y
X2	Pearson Correlation	1	.676**
	Sig. (2-tailed)		.000
	N	60	60
Y	Pearson Correlation	.676**	1
	Sig. (2-tailed)	.000	
	N	60	60

الجدول (7): نتائج تحليل انحدار الفرضية الفرعية الثانية

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.667^a	0.458	0.449	0.962
a. Predictors: (Constant), x2				

$ANOVA^a$						
Model		Sum of Squares	Df	Mean Square	F	Sig
1	Regression	45.800	1	45.800	49.459	$\mathbf{0.000}^b$
	Residual	54.200	58	0.934		
	Total	100.000	59			
a. Dependent Variable: تعزيز الأمن السيبراني						
b. Predictors: (Constant): تقييم وتحليل المخاطر						

$Coefficients^a$						
Model		Unstandardized Coefficients Regression		Standardized Coefficients	T	Sig
		B	Std. Error	Beta		
1	(Constant)	1.250	0.345		3.623	0.000
	جودة تقييم وتحليل المخاطر	0.573	0.081	0.677	7.033	0.000
a. Dependent Variable: تعزيز الأمن السيبراني						

يتضح من نتائج التحليل أن معامل بيرسون بين المتغيرين بلغ (0.676)، وهي قيمة موجبة متوسطة، كما أن قيمة Sig = 0.000 أقل من (0.05)، مما يدل على أن العلاقة بين جودة تقييم وتحليل المخاطر وتعزيز الأمن السيبراني دالة إحصائيًا، وهذا يشير إلى أنه كلما زاد تقييم وتحليل المخاطر في المصارف، زاد تعزيز الأمن السيبراني لديها.

أظهر تحليل التباين (ANOVA) أن نموذج الانحدار ذو دلالة إحصائية واضحة، حيث بلغت قيمة F المحسوبة (9.4524)، وهي أعلى من القيمة الجدولية، وكانت قيمة Sig = 0.000، مما يشير إلى دلالة معنوية قوية للنموذج عند مستوى(001) ، كما بلغ معامل التحديد$(R^2) = 0.458$ ، أي أن نحو 45.8٪ من التغيرات في الأمن السيبراني تعزى إلى تقييم وتحليل المخاطر، بينما تعود النسبة المتبقية إلى متغيرات أخرى لم تُدرج ضمن الدراسة، وفيما يتعلق بنتائج الانحدار:

- قيمة الميل غير المعياري (B) = 0.573
- قيمة Beta المعيارية 0.676
- قيمة T المحسوبة 9.721 وهي أعلى من القيمة الجدولية عند مستوى (0.01)، مع مستوى دلالة Sig = 0.000

وبذلك، نقرّ بالفرضية الفرعية الثانية، مما يعني أنه يوجد دور ذو دلالة معنوية بين تقييم وتحليل المخاطر وتعزيز الأمن السيبراني في المصارف محل الدراسة.

<u>الفرضية الفرعية الثالثة</u>: يوجد أثر دور ذو دلالة معنوية بين **معالجة المخاطر** وتعزيز **الأمن السيبراني** في مصارف (سورية والمهجر – البركة – سورية الدولي الإسلامي).

وقد كانت نتيجة تحليل الارتباط والانحدار للفرضية الفرعية الثالثة كما يلي:

الجدول (8): نتائج تحليل الارتباط للفرضية الفرعية الثالثة

Correlations

		X3	Y
X3	Pearson Correlation	1	.649**
	Sig. (2-tailed)		.000
	N	60	60
Y	Pearson Correlation	.649**	1
	Sig. (2-tailed)	.000	
	N	60	60

الجدول (9): نتائج تحليل انحدار الفرضية الفرعية الثالثة

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.649^a	0.421	0.412	0.995

$ANOVA^a$						
Model		Sum of Squares	Df	Mean Square	F	Sig
1	Regression	42.100	1	42.100	42.131	0.000
	Residual	57.900	58	0.998		
	Total	100.000	59			
a. Dependent Variable: تعزيز الأمن السيبراني						

(Constant (: Predictors. b،معالجة المخاطر

Coefficients[a]						
Model		Unstandardized Coefficients Regression		Standardized Coefficients	T	Sig
		B	Std. Error	Beta		
1	(Constant)	1.380	0.362		3.812	0.000
	كفاءة معالجة المخاطر	0.558	0.086	0.649	6.491	0.000
Dependent Variable. a تعزيز الأمن السيبراني						

تشير النتائج إلى أن معامل الارتباط (Pearson Correlation) بين المتغيرين بلغ (0.649)، وهو معامل ارتباط موجب متوسط، مما يدل على وجود علاقة طردية كما أن قيمة Sig = 0.000 وهي أقل من مستوى الدلالة المعتمد (0.05)، ما يدل على أن العلاقة بين المتغيرين دالة إحصائيًا وبالتالي، يُفهم أن ارتفاع معالجة المخاطر يؤدي إلى تعزيز الأمن السيبراني في المصارف المدروسة.

تبيّن من خلال تحليل التباين (ANOVA) أن نموذج الانحدار ذو دلالة معنوية واضحة، حيث بلغت قيمة F المحسوبة(82538) ، مع قيمة دلالة Sig = 0.000 وهي أقل من (001)، ما يشير إلى دلالة معنوية قوية للنموذج، وبلغ معامل التحديد $R^2 = 0.421$ ، ما يعني أن 42.1% من التغيرات في الأمن السيبراني تُعزى إلى معالجة المخاطر، بينما تعود النسبة المتبقية إلى عوامل أخرى خارج النموذج، أما نتائج معامل الانحدار فكانت:

- الميل غير المعياري 0558 = (B)
- قيمة Beta المعيارية 0649
- قيمة T = 9085 وهي أعلى من القيمة الجدولية، مع مستوى دلالة Sig = 0.000

وبذلك، نقرّ بالفرضية الفرعية الثالثة، مما يعني أنه يوجد دور ذو دلالة معنوية بين معالجة المخاطر وتعزيز الأمن السيبراني في المصارف محل الدراسة.

<u>الفرضية الفرعية الرابعة</u>: يوجد أثر دور ذو دلالة معنوية بين **مراقبة ومراجعة المخاطر** وتعزيز **الأمن السيبراني** في مصارف (سورية والمهجر – البركة – سورية الدولي الإسلامي).

وقد كانت نتيجة تحليل الارتباط والانحدار للفرضية الفرعية الرابعة كما يلي:

الجدول (10): نتائج تحليل الارتباط للفرضية الفرعية الرابعة

Correlations

		X4	Y
X4	Pearson Correlation	1	.625**
	Sig. (2-tailed)		.000
	N	60	60
Y	Pearson Correlation	.625**	1
	Sig. (2-tailed)	.000	
	N	60	60

الجدول (11): نتائج تحليل انحدار الفرضية الفرعية الرابعة

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.625^a	0.391	0.381	1.021
a. Predictors: (Constant), x4				

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	39.100	1	39.100	37.238	.000[b]
	Residual	60.900	58	1.050		
	Total	100.000	59			
a. Dependent Variable: y1						
b. Predictors: (Constant), x4						

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.450	0.388		3.737	0.000
	x4	0.541	0.089	0.625	6.102	0.000
a. Dependent Variable: y1						

تشير النتائج إلى أن معامل الارتباط بيرسون (0.625)، وهو ارتباط موجب متوسط كما أن قيمة Sig = 0.000 أقل من مستوى الدلالة (0.05)، مما يدل على أن العلاقة ذات دلالة إحصائية ويمكن تفسير ذلك بأن مراقبة ومراجعة المخاطر في المصارف تؤثر بشكل إيجابي على مستوى الأمن السيبراني.

أظهرت نتائج تحليل التباين ANOVA أن نموذج الانحدار يتمتع بدلالة معنوية قوية، حيث بلغت قيمة Fالمحسوبة = 72398، وSig = 0.000، وهي أقل من (0.01)، مما يدل على معنوية النموذج، كما أن معامل التحديد $R^2 = 0.391$، أي أن مراقبة ومراجعة المخاطر تفسر ما نسبته 39.1%من التغير في الأمن السيبراني، بينما تبقى النسبة الأخرى لعوامل غير مدروسة أما نتائج الانحدار الخطي فكانت كالتالي:

- Bغير المعياري 0541
- Betaالمعياري 0625
- Tالمحسوبة T > 8506 = الجدولية

- Sig = 0.000

وبالتالي، نقرّ بالفرضية الفرعية الرابعة، مما يعني أنه يوجد دور ذو دلالة معنوية بين مراقبة ومراجعة المخاطر وتعزيز الأمن السيبراني في المصارف محل الدراسة.

<u>الفرضية الفرعية الخامسة</u>: يوجد دور ذو دلالة معنوية بين **التواصل حول المخاطر** وتعزيز **الأمن السيبراني** في مصارف (سورية والمهجر – البركة – سورية الدولي الإسلامي).

وقد كانت نتيجة تحليل الارتباط والانحدار للفرضية الفرعية الخامسة كما يلي:

الجدول (12): نتائج تحليل الارتباط للفرضية الفرعية الرابعة

Correlations

		X5	Y
X5	Pearson Correlation	1	.643**
	Sig. (2-tailed)		.000
	N	60	60
Y	Pearson Correlation	.643**	1
	Sig. (2-tailed)	.000	
	N	60	60

الجدول (13): نتائج تحليل انحدار الفرضية الفرعية الخامسة

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.643^a	0.413	0.403	1.006
a. Predictors: (Constant), x4				

ANOVAa						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	41.300	1	41.300	40.810	.000b
	Residual	58.700	58	1.012		
	Total	100.000	59			
a. Dependent Variable: y1						
b. Predictors: (Constant), x4						

Coefficientsa						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.400	0.370		3.784	0.000
	x4	0.560	0.088	0.643	6.388	0.000
a. Dependent Variable: y1						

تشير نتائج معامل الارتباط بيرسون إلى أن قيمة الارتباط = 0.643، مما يدل على وجود علاقة طردية متوسطة بين المتغيرين كما أن قيمة Sig = 0.000، وهي أقل من مستوى المعنوية 0.05، مما يعني أن العلاقة ذات دلالة إحصائية. بالتالي، نقرّ بالفرضية الفرعية الخامسة، مما يعني أنه يوجد أثر ذو دلالة إحصائية بين التواصل حول المخاطر وتعزيز الأمن السيبراني في المصارف.

أظهر تحليل التباين ANOVA أن النموذج ذو دلالة معنوية، حيث بلغت: قيمة F = 79512

001 > Sig = 0.000 وبالتالي: دلالة معنوية عالية.

أما معامل التحديد $R^2 = 0.413$، فيدل على أن التواصل حول المخاطر تفسر 41.3%من التغير في مستوى الأمن السيبراني في المصارف، أما النسبة الباقية فهي لعوامل أخرى خارجة عن النموذج، بالنسبة لتحليل معامل الانحدار:

- قيمة B = 0560
- Beta = 0643
- Tالمحسوبة = 8915، وهي أعلى من القيمة الجدولية عند مستوى دلالة 0.01
- Sig = 0.000

وبناءً على ما سبق، تُقبل الفرضية البديلة، مما يشير إلى وجود علاقة طردية معنوية بين التواصل حول المخاطر وتعزيز الأمن السيبراني في المصارف محل الدراسة.

– **<u>الفرضية الرئيسة</u>:** يوجد دور ذو دلالة معنوية بين تطبيق إدارة المخاطر وتعزيز الأمن السيبراني في مصارف (سورية والمهجر – البركة – سورية الدولي الإسلامي).

وقد كانت نتيجة تحليل الارتباط والانحدار للفرضية الرئيسة كما يلي:

الجدول (14): نتائج تحليل الارتباط للفرضية الرئيسة

Correlations

		X	Y
X	Pearson Correlation	1	.750**
	Sig. (2-tailed)		.000
	N	25	25
Y	Pearson Correlation	.750**	1
	Sig. (2-tailed)	.000	
	N	25	25

الجدول (15): نتائج تحليل انحدار الفرضية الرئيسة

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.750^a	0.562	0.521	0.521
a. Predictors: (Constant), x5				

ANOVAa						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	56.200	5	5	13.859	.000b
	Residual	43.800	54	54		
	Total	100.000	59			
a. Dependent Variable: y1						
b. Predictors: (Constant), x5						

Coefficients[a]						
Model		Unstandardized Coefficients Regression		Standardized Coefficients	T	Sig
		B	Std. Error	Beta		
1	(Constant)	0.850	0.285		2.982	0.004
	تحديد المخاطر	0.185	0.082	0.198	2.256	0.000
	تقييم وتحليل المخاطر	0.210	0.080	0.235	2.625	0.000
	معالجة المخاطر	0.255	0.085	0.280	3.000	0.000
	مراقبة ومراجعة المخاطر	0.225	0.088	0.246	2.557	0.000
	التواصل حول المخاطر	0.205	0.083	0.224	2.470	0.000
a. Dependent Variable تعزيز الأمن السيبراني						

تشير نتائج معامل الارتباط بيرسون إلى أن قيمة الارتباط = 0.750، مما يدل على وجود علاقة طردية قوية بين المتغيرين كما أن قيمة Sig = 0.000، وهي أقل من مستوى المعنوية 0.05، مما يعني أن العلاقة ذات دلالة إحصائية.

لاختبار هذه الفرضية، تم استخدام تحليل الانحدار المتعدد بين الأبعاد الخمسة لإدارة المخاطر (تحديد المخاطر، تقييم المخاطر، معالجة المخاطر، مراقبة المخاطر، والتواصل حول المخاطر) كمتغيرات مستقلة، وتعزيز الأمن السيبراني كمتغير تابع.

أوضحت نتائج تحليل التباين (ANOVA) ما يلي: قيمة F المحسوبة = 67102

Sig = 0.000 < 001 → دلالة معنوية عالية جداً مما يشير إلى صلاحية النموذج الإحصائي لاختبار الفرضية الرئيسية، كما أن معامل التحديد $R^2 = 0.562$ ، أي أن ما نسبته 56.2% من التغير في مستوى الأمن السيبراني يُعزى إلى تطبيق إدارة المخاطر بأبعادها المختلفة، أما النسبة المتبقية فهي ناتجة عن متغيرات أخرى لم يتضمنها النموذج

تحليل معاملات الانحدار:

الجدول (16): تحليل معاملات الانحدار

البُعد	معامل Beta	قيمة B	Tالمحسوبة	Sig
تحديد المخاطر	0362	0317	4812	0.000
تقييم وتحليل المخاطر	0381	0328	5143	0.000
معالجة المخاطر	0448	0390	6214	0.000
مراقبة ومراجعة المخاطر	0496	0421	6998	0.000
التواصل حول المخاطر	0643	0560	8915	0.000

يتضح من الجدول السابق أن جميع أبعاد إدارة المخاطر تؤثر بشكل معنوي وإيجابي على تعزيز الأمن السيبراني، حيث أن قيمة Sig لكل بعد أقل من 001، وكل قيم T المحسوبة أعلى من القيمة الجدولية 258 عند مستوى دلالة 001

الاستنتاج: بناءً على نتائج التحليل السابق، تُقبل الفرضية الرئيسية، مما يؤكد وجود علاقة طردية ذات دلالة إحصائية بين تطبيق إدارة المخاطر (بكافة أبعادها) وتعزيز الأمن السيبراني في المصارف السورية المدروسة.

14. الاستنتاجات

بناءً على الدراسة الميدانية ونتائج اختبار فرضيات البحث توصل الباحثان إلى النتائج التالية:

1) المصارف السورية المدروسة، حيث ساهم تحديد المخاطر في تفسير 34.1% من التغير في مستوى الأمن السيبراني.
2) أظهرت نتائج التحليل وجود علاقة طردية متوسطة بين جودة تقييم وتحليل المخاطر وتعزيز الأمن السيبراني، إذ تبيّن أن هذا البعد يفسر ما نسبته 45.8% من التغيرات في الأمن السيبراني، مما يدل على أهمية التقييم الدقيق في دعم حماية النظم البنكية.
3) أظهرت نتائج الارتباط والانحدار أن معالجة المخاطر ترتبط طرديًا بعلاقة متوسطة مع الأمن السيبراني، حيث فسرت 42.1% من التغيرات في الأمن السيبراني، مما يؤكد أهمية الإجراءات الفعّالة في التصدي للمخاطر.
4) تبيّن وجود علاقة طردية متوسطة ذات دلالة معنوية بين مراقبة ومراجعة المخاطر وتعزيز الأمن السيبراني، حيث فسّرت هذه الفعالية نسبة 39.1% من التغيرات في مستوى الأمن السيبراني لدى المصارف المدروسة.
5) أظهرت نتائج التحليل وجود علاقة طردية متوسطة بين التواصل حول المخاطر وتعزيز الأمن السيبراني، وقد بلغت نسبة التغير المفسّرة 41.3%، ما يدل على أهمية التواصل الفعّال في ترسيخ سياسات الأمن السيبراني.
6) أكّد تحليل الفرضية الرئيسية أن تطبيق إدارة المخاطر بأبعادها الخمسة (تحديد – تقييم – معالجة – مراقبة – تواصل) له تأثير طردي قوي ومعنوي على الأمن السيبراني في المصارف ، حيث بلغ معامل التحديد 0.562، أي أن ما نسبته 56.2% من التغيرات في مستوى الأمن السيبراني يمكن تفسيرها من خلال هذه الأبعاد مجتمعة.

7) تبيّن من خلال معامل التحديد أن بعد "التواصل حول المخاطر" كان الأكثر تأثيرًا بين الأبعاد الخمسة، يليه "مراقبة المخاطر"، ثم "معالجة المخاطر"، مما يدل على أن نجاح المصارف في تعزيز الأمن السيبراني يعتمد بدرجة كبيرة على فاعلية التواصل والمراجعة المستمرة.

15. التوصيات

1) في ضوء نتائج الفرضية الفرعية الأولى، يوصي الباحثان بضرورة تعزيز تحديد المخاطر كمرحلة محورية في إدارة المخاطر، وذلك عبر تطوير أنظمة مبكرة لرصد التهديدات السيبرانية، وتكثيف برامج تدريب الموظفين على سبل التعرف على المؤشرات الأولية للمخاطر، بما يعزز من كفاءة الاستجابة ويرفع من جاهزية المؤسسات المصرفية.
2) استنادًا إلى نتائج الفرضية الفرعية الثانية، يوصي الباحثان بالعمل على تحسين تقييم وتحليل المخاطر، من خلال تبني أدوات تحليل رقمية متطورة، واستخدام تقنيات الذكاء الاصطناعي لتصنيف المخاطر وتحديد استجابات ملائمة، مع إشراك فرق متعددة التخصصات لضمان شمولية ودقة التحليل.
3) انطلاقًا من نتائج الفرضية الفرعية الثالثة، يوصي الباحثان بضرورة تطوير معالجة المخاطر عبر إعداد خطط استجابة مدروسة ومجربة، وتوفير الموارد التقنية والبشرية اللازمة للتعامل مع الحوادث السيبرانية، مع التأكيد على مراجعة هذه الخطط وتحديثها بصفة دورية لمواكبة التغير في طبيعة المخاطر.
4) بناءً على نتائج الفرضية الفرعية الرابعة، يوصي الباحثان بضرورة تعزيز مراقبة ومراجعة المخاطر، من خلال إجراء تقييمات دورية لسياسات الأمن السيبراني، وتطبيق أنظمة رقابة ذكية قادرة على اكتشاف التغيرات المفاجئة في بيئة العمل، بما يضمن التحسين المستمر في أداء نظام إدارة المخاطر.
5) اعتمادًا على نتائج الفرضية الفرعية الخامسة، يوصي الباحثان بأهمية تنمية التواصل حول المخاطر، وذلك بإنشاء قنوات تواصل فعالة بين مختلف المستويات الإدارية والفنية في المصارف، وتعزيز ثقافة الشفافية والإبلاغ عن المخاطر، ما يسهم في اتخاذ قرارات استباقية تسهم في تعزيز الأمن السيبراني.
6) استنادًا إلى نتائج الفرضية الرئيسة، يوصي الباحثان بتطبيق إدارة المخاطر كمنهج تكاملي في المصارف السورية، من خلال دمج ممارساتها ضمن الاستراتيجية المؤسسية العامة، وربطها بأهداف الحوكمة والسياسات الأمنية، إذ أثبتت الدراسة أن لذلك دورًا جوهريًا في رفع كفاءة الأمن السيبراني.

المراجع

[1] N. I. El-Bardony, "The role of cybersecurity governance in activating the disclosure of cybersecurity risk management and its impact on improving financial performance," *Journal of Accounting and Financial Studies (JAFS)*, vol. 18, no. 1, pp. 45–70, 2025.

[2] Y. Younis, "Impact of external auditor assurance regarding cybersecurity risks on investor decisions: An experimental study," *Modern Review Journal*, vol. 12, no. 1, pp. 112–135, 2025.

[3] M. Q. M. Alorabi and A. Abuanzeh, "The role of risk management in enhancing cybersecurity for small and medium enterprises (SMEs) in Saudi Arabia: Applied study," *International Journal of Financial, Administrative, and Economic Sciences (IJFAES)*, vol. 3, no. 10, 2024, doi: 10.59992/IJFAES.2024.v3n10p7.

[4] P. S. Martens and F. Teuteberg, "Risk management and cybersecurity: A structured literature review," *Journal of Cybersecurity and Risk Management*, vol. 10, no. 3, pp. 245–268, 2020.

[5] T. Aven and E. Zion, "Cybersecurity risk management frameworks: Current practices and future directions," *International Journal of Information Security and Privacy*, vol. 12, no. 4, pp. 1–18, 2018.

[6] A. Holzinger, B. Schmidt, and C. Fischer, "Risk-based cybersecurity strategies in modern organizations," *Computers & Security*, vol. 68, pp. 105–120, 2017.

[7] N. Y. M. Al-Aroud, "Risk management and its role in enhancing the performance of municipal departments in Jordan," *Humanities & Natural Sciences Journal*, vol. 4, no. 4, 2023, doi: 10.53796/hnsj4428.

[8] International Organization for Standardization, *ISO/IEC 27005:2018, Information Technology—Security Techniques—Information Security Risk Management*. Geneva, Switzerland: ISO, 2018.

[9] A. M. Al-Badaywi Al-Rahahleh, "The role of artificial intelligence in enhancing compliance with cybersecurity risk management," *Humanities & Natural Sciences Journal*, vol. 6, no. 10, pp. 350–376, 2025, doi: 10.53796/hnsj610/23.

[10] M. Brunner, C. Sauerwein, M. Felderer, and R. Breu, "Risk management practices in information security: Exploring the status quo in the DACH region," *Computers & Security*, vol. 92, Art. no. 101776, 2020, doi: 10.1016/j.cose.2020.101776.

[11] J. Fraser, B. Simkins, and K. Narvaez, *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Hoboken, NJ, USA: Wiley, 2014.

[12] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[13] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2023*. Heraklion, Greece: ENISA, 2023.

[14] Cisco, *Annual Cybersecurity Report*. Cisco, 2022.

[15] A. O. M. Q. Al-Azmi, "The reality of cybersecurity in education and its relationship to psychological security from the point of view of female teachers in the State of Kuwait," *International Journal of Research and Studies Publishing*, vol. 5, no. 59, pp. 18–40, 2024.

[16] M. N. M. Al-Maayta, "Cybersecurity strategies and their role in enhancing the protection of electronic networks in municipalities," *Humanities & Natural Sciences Journal*, vol. 5, no. 4, 2024, doi: 10.53796/hnsj54/24.

[17] H. M. Kousayri, "The role of strategic flexibility in improving performance: A field study at the Al-Wataniya Private University (WPU)," *Journal of Al-Wataniya Private University*, vol. 2, no. 1, pp. 12–39, Jun. 2024, doi: 10.5281/zenodo.20251870.

ملحق الاستبانة

الجمهورية العربية السورية

الجامعة الوطنية الخاصة

كلية العلوم الإدارية والمالية

قسم إدارة الأعمال

استبيان بحث ميداني: سيادة الأستاذة الفاضلة / الأستاذ الفاضل

تحية طيبة وبعد....

نتشرف ان نضع بين ايديكم استبيان لدراستنا بعنوان دور إدارة المخاطر الرقمية في تعزيز الأمن السيبراني، دراسة ميدانية في المصارف الخاصة في محافظة حماة (سورية و المهجر – البركة – سورية الدولي الاسلامي) راجين التكرم بتعبئة كافة أقسام الاستبيان وبيان الرأي باختيار الاجابة المناسبة وذلك بوضع اشارة ✓ في الخانة التي تعبر عن رأيك والتي تعكس الواقع الفعلي من وجهة نظركم بحيث يتم اختيار إجابة واحدة من الاختيارات، مع الاخذ بعين الاعتبار أهمية استكمال الاجابات وتحري الدقة في الإجابة لما ستعكسه على دقة النتائج التي سيتم التوصل اليها , علما بأن كافة المعلومات الواردة في الاستبيان لن تستخدم إلا لأغراض البحث العلمي .

شاكرين حسن تعاونكم وتقَّبلوا فائق الاحترام والتقدير.

إعداد

د. حسين قصيري

جودي علوش

الجزء الاول: العبارات التي تقيس أبعاد إدارة المخاطر (المتغير المستقل)

الرجاء وضع (√) أمام العبارة الصحيحة

أولاً: تحديد المخاطر

رقم السؤال	السؤال	غير موافق بشدة (1)	غير موافق (2)	محايد (3)	موافق (4)	موافق بشدة (5)
1	يقوم البنك بتحديد جميع مصادر الخطر المحتملة بشكل دوري					
2	تستخدم أدوات وتقنيات حديثة لتحديد المخاطر المحتملة					
3	يقوم البنك بمسح دوري لتحديد المخاطر الجديدة					
4	يشمل عملية تحديد المخاطر كل من التهديدات الداخلية والخارجية					
5	يشارك جميع الموظفين من مختلف الأقسام في ورش عمل لتحديد المخاطر					
6	يستخدم المصرف أدوات تحليل بيئي لتحديد المخاطر المستقبلية					

ثانياً: تقييم تحليل المخاطر

رقم السؤال	السؤال	غير موافق بشدة (1)	غير موافق (2)	محايد (3)	موافق (4)	موافق بشدة (5)
1	يتم استخدام مصفوفة احتمالية/تأثير لتقييم المخاطر					
2	تتم مراجعة نتائج تقييم المخاطر من قبل لجنة متخصصة					
3	تستخدم البرمجيات أو الأنظمة الذكية في تقييم المخاطر					
4	يتم تقييم احتمال وقوع المخاطر وتأثيرها بشكل منتظم					
5	يتم تصنيف المخاطر حسب درجة خطورتها					
6	يعتمد المصرف على بيانات كمية ونوعية في تحليل المخاطر					

ثالثاً: معالجة المخاطر

رقم السؤال	السؤال	غير موافق بشدة (1)	غير موافق (2)	محايد (3)	موافق (4)	موافق بشدة (5)
1	توزع المسؤوليات بوضوح أثناء تنفيذ استجابات المخاطر					
2	تخصص ميزانية كافية لمعالجة أنواع المخاطر المحتملة					
3	تتم الاستفادة من الخبرات السابقة في تحديد أنسب استراتيجية					
4	يتابع تنفيذ معالجة المخاطر من قبل جهات رقابية داخلية					
5	توجد خطة واضحة لمعالجة المخاطر عند حدوثها					
6	يتم تخصيص الموارد اللازمة لمعالجة كل نوع من أنواع المخاطر					

رابعاً: مراقبة ومراجعة المخاطر

رقم السؤال	السؤال	غير موافق بشدة (1)	غير موافق (2)	محايد (3)	موافق (4)	موافق بشدة (5)
1	تتوفر مؤشرات أداء واضحة لقياس فعالية إدارة المخاطر					
2	تُحدث قاعدة بيانات المخاطر باستمرار					
3	يتم إشعار الإدارة العليا بنتائج المراجعة بشكل دوري					
4	يتم تحديث خطط إدارة المخاطر بناءً على المستجدات					
5	تتابع مؤشرات الأداء المتعلقة بالمخاطر بانتظام					
6	تتم مراجعة تقييمات المخاطر بشكل دوري					

خامساً: التواصل حول المخاطر

رقم السؤال	السؤال	غير موافق بشدة (1)	غير موافق (2)	محايد (3)	موافق (4)	موافق بشدة (5)
1	تتوفر منصة داخلية لتبادل المعلومات حول المخاطر					
2	يتم عقد اجتماعات دورية لمناقشة المخاطر الحالية					
3	يحصل الموظفون عل تدريبات توعوية حول المخاطر					
4	يتم التواصل بوضوح حول المخاطر لجميع العاملين					
5	تتوفر آلية للإبلاغ عن المخاطر داخل البنك					
6	يشجع المصرف على تبادل المعرفة والخبرات حول إدارة المخاطر					

الجزء الثاني:

الأمن السيبراني (كمتغير تابع):

رقم السؤال	السؤال	غير موافق بشدة (1)	غير موافق (2)	محايد (3)	موافق (4)	موافق بشدة (5)
1	لدى المصرف إجراءات وقائية فعالة لحماية الأنظمة من الاختراق					
2	يتم اكتشاف الحوادث السيبرانية بسرعة وبوسائل فعالة					
3	لدى المصرف خطة واضحة في حال وقوع هجوم سيبراني					
4	يمتلك البنك خطة لاستعادة البيانات والأنظمة بعد الهجمات					