

The Impact of Applying Cybersecurity Standards on Reducing Risks in Commercial Banks in Riyadh During the Year 2025

Mr. Hassan Khidhr Alhallafi*, Mr. Almotasim Khalil Alabbas, Ms. Mona Jeza Almutairi

Faculty of Management | Midocean University | Comoros

Received:

29/10/2025

Revised:

09/11/2025

Accepted:

30/11/2025

Published:

28/02/2026

* Corresponding author:

mohp2@hotmail.com

Citation: Alhallafi, H.

KH., Alabbas, A. KH., &

Almutairi, M. J. (2026). The

Impact of Applying

Cybersecurity Standards

on Reducing Risks in

Commercial Banks in

Riyadh During the Year

2025. *Journal of Economic,*

Administrative and Legal

Sciences, 10(2), 1 – 10.

<https://doi.org/10.26389/AJSRP.F011125>

[AJSRP.F011125](https://doi.org/10.26389/AJSRP.F011125)

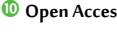
2026 © AISRP • Arab

Institute for Sciences &

Research Publishing

(AISRP), United States, all

rights reserved.

 Open Access



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) [license](https://creativecommons.org/licenses/by-nc/4.0/)

Abstract: This study aimed to analyze the impact of applying cybersecurity standards on reducing risks in commercial banks in Riyadh, within the context of the accelerating digital transformation that has made information protection and operational continuity a strategic necessity for the financial sector. The study employed a quantitative method and relied on an electronic questionnaire as the primary tool for data collection from a purposive sample of employees working in cybersecurity, risk management, and information technology departments in commercial banks. Three main dimensions of cybersecurity standards were examined — personnel security, information control security, and physical security — and their effects on the overall level of risk were measured using multiple regression analysis through the SPSS software. The results indicated that the application of cybersecurity standards effectively contributed to reducing operational, informational, and compliance risks, with information control security having the strongest impact, followed by personnel security and physical security. The study recommended integrating cybersecurity frameworks within digital transformation strategies in Saudi banks and enhancing employee training and awareness to achieve a safer and more sustainable banking environment aligned with Saudi Vision 2030.

Keywords: Cybersecurity Standards, Risk Reduction, Commercial Banks, Information Security, Personnel Security, Physical Security, Digital Transformation, Saudi Vision 2030.

أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر في البنوك التجارية بمدينة الرياض خلال العام 2025

أ. حسن خضر الحلافي*, أ. المعتصم خليل العباس، أ. منى جزا المطيري

كلية الإدارة | جامعة ميدوشن | جزر القمر

المستخلص: هدفت هذه الدراسة إلى تحليل أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر في البنوك التجارية بمدينة الرياض، في ظل التحول الرقمي المتسارع الذي جعل حماية المعلومات واستمرارية العمليات ضرورة استراتيجية للقطاع المالي. استخدمت الدراسة المنهج الكمي، واعتمدت على الاستبانة الإلكترونية أداة لجمع البيانات من عينة قصدية من العاملين في إدارات الأمن السيبراني وإدارة المخاطر وتقنية المعلومات في البنوك التجارية. وتناولت الدراسة ثلاثة أبعاد رئيسة لمعايير الأمن السيبراني، هي: أمن الأفراد، وأمن ضبط المعلومات، والأمن المادي، وقيست أثارها على المخاطر الكلية باستخدام تحليل الانحدار المتعدد عبر برنامج SPSS. وأظهرت النتائج أن تطبيق معايير الأمن السيبراني أسهم بفاعلية في خفض مستوى المخاطر التشغيلية والمعلوماتية والامتثالية، وأن يُعد أمن ضبط المعلومات كان الأكثر تأثيراً، يليه أمن الأفراد ثم الأمن المادي. وأوصت الدراسة بضرورة دمج الأطر الأمنية ضمن استراتيجيات التحول الرقمي للبنوك السعودية، وتعزيز التدريب والوعي الأمني للعاملين بما يحقق بيئة مصرفية أكثر أماناً واستدامة، انسجاماً مع رؤية السعودية 2030.

الكلمات المفتاحية: معايير الأمن السيبراني، الحد من المخاطر، البنوك التجارية، أمن المعلومات، أمن الأفراد، الأمن المادي، التحول الرقمي، رؤية السعودية 2030.

1. الإطار العام

1.1 المقدمة

يشهد العالم المعاصر تسارعًا رقميًا غير مسبوق جعل البيانات تمثل أصلًا استراتيجيًا ومحورًا رئيسًا لاتخاذ القرار من خلال منصات ذكاء الأعمال والتحليلات المتقدمة. أصبح الأمن السيبراني عنصرًا حاكمًا لاستدامة الأعمال وضمان الثقة في البيانات الرقمية، حيث يمثل خط الدفاع الأول لحماية تدفقات المعلومات والحفاظ على موثوقيتها وسريتها وتكاملها. إن دمج ممارسات الأمن السيبراني ضمن نظم ذكاء الأعمال يساهم في رفع جودة البيانات، ويحد من مخاطر التسرب والوصول غير المصرح به، كما يعزز قدرة المؤسسات على الاستجابة السريعة للهجمات والاختلالات التشغيلية.

تسعى المملكة العربية السعودية، من خلال برامج رؤية 2030، إلى بناء اقتصاد رقمي آمن ومتوازن يجمع بين الابتكار وحوكمة البيانات. ويأتي قطاع البنوك في مقدمة القطاعات التي تتأثر بمدى نضج الممارسات السيبرانية، نظرًا لاعتماده الكبير على التقنيات الرقمية وأنظمة التحليل الذي في إدارة العمليات واتخاذ القرار. ومن هذا المنطلق، يمثل التكامل بين الأمن السيبراني وذكاء الأعمال ركيزة أساسية لتمكين التحول الرقمي الآمن في المؤسسات المالية، من خلال ضمان التدفق الآمن للمعلومات، وتحسين جودة التحليل والتقارير، ورفع كفاءة القرارات الاستراتيجية.

ومع تصاعد حجم التهديدات الإلكترونية، تزايد أهمية توظيف تقنيات الذكاء الاصطناعي والتعلم الآلي ضمن بيئات ذكاء الأعمال لتعزيز قدرات الرصد والإنذار المبكر، وتحليل الأنماط السلوكية للهجمات، وتفسير الأحداث الأمنية في وقتٍ قياسي. وتعمل هذه التقنيات على دعم القرارات الأمنية من خلال توفير نماذج تحليلية دقيقة ومتعددة الأبعاد، تساهم في تحسين الشفافية والجاهزية المؤسسية. في المقابل، يبرز تحدي الخصوصية وحوكمة البيانات بوصفه أحد أهم العوامل المؤثرة في نجاح هذه الأنظمة، مما يستلزم تشفيرًا متقدمًا وضبطًا محكمًا لعمليات الوصول إلى المعلومات الحساسة.

على المستوى العربي، تزايد الأدلة الميدانية التي تؤكد الأثر الإيجابي لتطبيق معايير الأمن السيبراني على كفاءة إدارة المخاطر، إلا أن درجة هذا الأثر تتباين باختلاف البنية التحتية ومستوى الالتزام المؤسسي. كما تكشف التحليلات الحديثة عن مجموعة من المتطلبات الرئيسية لدمج الأمن السيبراني مع ذكاء الأعمال، تشمل بنية البيانات المتكاملة، والأدوات التحليلية المتقدمة، والسياسات التنظيمية الصارمة، والمهارات البشرية المؤهلة للتعامل مع التقنيات الحديثة. وتُظهر المقارنات القطاعية أن المؤسسات التي تتمتع ببنية سيبرانية قوية تحقق استفادة أعلى من نظم ذكاء الأعمال من حيث سرعة الوصول إلى المعلومات، وجودة التقارير، وفعالية اتخاذ القرار.

رغم التقدم البحثي الكبير في هذا المجال، إلا أن هناك فجوة تطبيقية واضحة في القطاع المصرفي السعودي؛ إذ تتركز معظم الدراسات السابقة على قطاعات التعليم العالي أو المؤسسات الحكومية، بينما تقل الدراسات الميدانية التي تتناول العلاقة بين تطبيق معايير الأمن السيبراني ومستوى المخاطر الكلية في البنوك التجارية. ومن هنا، تسعى هذه الدراسة إلى سد هذه الفجوة من خلال بناء نموذج تطبيقي يقيس أثر تطبيق أبعاد الأمن السيبراني — المتمثلة في أمن الأفراد، وضبط المعلومات، والأمن المادي — على مؤشرات المخاطر الكلية كما تُدركها الإدارات المعنية في البنوك التجارية بمدينة الرياض. ويهدف هذا النموذج إلى تقديم تصور علمي يساهم في تعزيز الثقة الرقمية واستقرار العمليات المالية، دعمًا لأهداف التحول الرقمي ضمن رؤية المملكة 2030.

1.2 مشكلة الدراسة وتسؤلاتها

مع تسارع التحول الرقمي في القطاع المصرفي، أصبحت البنوك تعتمد بصورة متزايدة على أنظمة ذكاء الأعمال وتحليل البيانات في إدارة عملياتها اليومية واتخاذ قراراتها الاستراتيجية. ورغم ما يوفره هذا التحول من فرص لتعزيز الكفاءة التشغيلية وتحسين جودة القرارات، فإنه أوجد تحديات متنامية تتعلق بسلامة المعلومات وحمايتها من المخاطر السيبرانية المتصاعدة. إذ أصبحت الاختراقات، وتسرب البيانات، وضعف ضوابط الوصول من أبرز العوامل التي تهدد الاستقرار المؤسسي والموثوقية التشغيلية داخل المؤسسات المالية.

تتضح المشكلة في أن تطبيق معايير الأمن السيبراني، رغم أهميته المتزايدة، ما يزال يواجه فجوة في التطبيق والقياس داخل القطاع المصرفي السعودي. فالكثير من الجهود تركز على الجوانب التقنية أو الامتثال العام، بينما تفتقر البنوك إلى نماذج قياس كمية دقيقة تُظهر العلاقة الفعلية بين مستوى تطبيق المعايير السيبرانية — بأبعادها المتعلقة بأمن الأفراد وضبط المعلومات والأمن المادي — وبين مستوى المخاطر الكلية في بيئات العمل المصرفية.

كما يلاحظ أن معظم الدراسات العربية ركزت على قطاعات أخرى مثل التعليم أو المؤسسات الحكومية، في حين ظل القطاع المصرفي، وخاصة في مدينة الرياض، أقل تناوُلًا من حيث تحليل أثر تطبيق الأمن السيبراني على منظومة المخاطر المؤسسية. ومن ثم، تمثل مشكلة الدراسة في وجود قصور بحثي وتطبيقي يتمثل في غياب النماذج التجريبية التي تقيّم بصورة كمية ومتكاملة أثر تطبيق معايير الأمن السيبراني على الحد من المخاطر الكلية في البنوك التجارية.

تسعى الدراسة الحالية إلى معالجة هذا القصور من خلال بناء نموذج علمي تطبيقي يقيس العلاقة بين أبعاد الأمن السيبراني ومستوى المخاطر الكلية في البيئة المصرفية السعودية، بما يساهم في دعم صانعي القرار لتحديد مجالات الاستثمار السيبراني الأكثر تأثيراً على خفض المخاطر وتعزيز استقرار العمليات، بما يتوافق مع مستهدفات التحول الرقمي ورؤية المملكة 2030.

بناء على ما سبق هدفت الدراسة الحالية إلى الإجابة عن السؤال الرئيس التالي:

ما أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر الكلية في البنوك التجارية بمدينة الرياض؟

يتفرع منه كل من الأسئلة الفرعية التالية:

- 1- ما أثر أمن الأفراد في الحد من المخاطر في البنوك التجارية بمدينة الرياض؟
- 2- ما أثر أمن ضبط المعلومات في الحد من المخاطر في البنوك التجارية بمدينة الرياض؟
- 3- ما أثر الأمن المادي في الحد من المخاطر في البنوك التجارية بمدينة الرياض؟

1.3 أهداف الدراسة

يهدف هذا البحث إلى قياس وتحليل أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر في البنوك التجارية بمدينة الرياض، وذلك من خلال مجموعة من الأهداف التفصيلية، هي:

1. تحليل أثر أمن الأفراد في الحد من المخاطر في البنوك التجارية بمدينة الرياض.
2. تحليل أثر أمن ضبط المعلومات في خفض مستوى المخاطر في البنوك التجارية بمدينة الرياض.
3. تحليل أثر الأمن المادي في تعزيز استقرار بيئة العمل المصرفي والحد من المخاطر في البنوك التجارية بمدينة الرياض.
4. بناء نموذج تفسيري يربط بين تطبيق معايير الأمن السيبراني ومستوى المخاطر الكلية في البنوك التجارية، بما يساهم في سدّ الفجوة التطبيقية في البيئة المصرفية السعودية.

1.4 فرضيات الدراسة

تؤكد الدراسات الحديثة أن تطبيق معايير الأمن السيبراني يشكل عاملاً محورياً في تقليل مستوى المخاطر التشغيلية والمعلوماتية، إذ يساهم في تعزيز موثوقية البيانات، وضمان استمرارية الأعمال، وحماية الأنظمة من التهديدات المتزايدة (Harry & Michael, 2024; Bucharest & Springer, 2022).

كما أظهرت نتائج الحربي، (2024) وعبد الرحمن، (2024) أن التكامل بين الأمن السيبراني وذكاء الأعمال يؤدي إلى تحسين جودة التحليل واتخاذ القرار، ما يقلل من فرص التعرض للمخاطر. ومن جانب آخر، بيّنت دراسات مثل العتوم، (2020) أن تطبيق المعايير الأمنية وفق أبعادها الفنية والبشرية والمادية يساهم في رفع جاهزية المؤسسات وتقليل الثغرات الأمنية، مما يدعم فرضية وجود أثر جوهري للأمن السيبراني في خفض مستوى المخاطر الكلية داخل البيئة المصرفية.

H01: لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لتطبيق معايير الأمن السيبراني بأبعاده الثلاثة (أمن الأفراد، أمن ضبط المعلومات، الأمن المادي) في الحد من المخاطر الكلية في البنوك التجارية بمدينة الرياض.

تشير نتائج الزهراني، (2023) وأحمد العتيبي، (2023) إلى أن وعي الأفراد بسياسات الأمن السيبراني والتزامهم بالإجراءات الوقائية يمثلان خط الدفاع الأول في مواجهة التهديدات الرقمية. فالتدريب المستمر على استخدام الأنظمة الآمنة، والتزام الموظفين بمعايير السرية والخصوصية، يساهمان في تقليل الأخطاء البشرية التي تشكل أحد أبرز أسباب الاختراقات والتهديدات. كما أوضحت دراسة الدوسري، (2024) أن بناء كوادر بشرية تمتلك مهارات في كلّ من الأمن السيبراني وتحليل البيانات يعزز قدرة المؤسسات على التنبؤ بالمخاطر والاستجابة السريعة لها، وهو ما يبرر أهمية متغير أمن الأفراد في الحد من المخاطر المصرفية، وعليه يمكن صياغة الفرضية الفرعية التالية:

● **H01-1:** لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لأمن الأفراد في الحد من المخاطر في البنوك التجارية بمدينة الرياض.

أظهرت دراسات الحربي، (2024) وعبد الرحمن، (2024) أن أمن المعلومات يمثل محور التكامل بين الأمن السيبراني وذكاء الأعمال، حيث يؤدي وجود سياسات صارمة للتحكم في الوصول وتشفير البيانات إلى ضمان جودة المعلومات ودقتها وتقليل احتمالات التسرب أو التلاعب. كما بيّنت دراسة Al-Rabaie & Abualkishik (2024) أن تطبيق المعايير الدولية مثل ISO/IEC 27001 و NIST يساهم في تنظيم الوصول إلى البيانات وضبط استخدامها ضمن بيئة آمنة، مما يعزز كفاءة إدارة المخاطر في المؤسسات التي تعتمد على البيانات المكثفة كالقطاع المصرفي. هذه النتائج تدعم الفرضية القائلة بأن أمن ضبط المعلومات يلعب دوراً جوهرياً في تقليل المخاطر التشغيلية والتقنية، وعليه يمكن صياغة الفرضية الفرعية التالية:

● 2-01H: لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لأمن ضبط المعلومات في الحد من المخاطر في البنوك التجارية بمدينة الرياض.

تشير الدراسات إلى أن فعالية الأمن السيبراني لا تكتمل دون وجود إجراءات حماية مادية قوية تشمل مراكز البيانات، والخوادم، وأنظمة المراقبة الفيزيائية. فقد

شدت دراسات (Harry & Michael, 2024) و (Radanliev et al, 2022)) على أن البنية التحتية المادية الآمنة تمثل الأساس في استمرارية العمليات وتقليل الانقطاعات الناتجة عن الحوادث أو الأعطال أو الاختراقات المادية. كما أظهرت دراسة العتيبي، (2023) أن المؤسسات التي تدمج الأمن المادي ضمن استراتيجيتها الأمنية تحقق مستويات أعلى من الجاهزية والاستجابة للأزمات. وبناءً على ذلك، يُتوقع أن يساهم تعزيز الأمن المادي في البنوك التجارية بمدينة الرياض في الحد من المخاطر التشغيلية والفنية بشكل ملموس، وعلى يمكن صياغة الفرضية الفرعية التالية:

● 3-01H: لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) للأمن المادي في الحد من المخاطر في البنوك التجارية بمدينة الرياض.

1.5 حدود الدراسة

تقتصر هذه الدراسة مكانياً على البنوك التجارية بمدينة الرياض في المملكة العربية السعودية، حيث جرى تنفيذ البحث وجمع البيانات من العاملين في إدارات الأمن السيبراني، وإدارة المخاطر، وتقنية المعلومات. أما زمنياً، فقد أجريت الدراسة خلال العام الأكاديمي ٢٠٢٥م، وهو الإطار الزمني الذي شمل إعداد الأداة وجمع البيانات وتحليلها إحصائياً.

2. الأطار النظري

2.1 المخاطر المصرفية

2.1.1 مفهوم المخاطر المصرفية وأنواعها

تعدّ المخاطر المصرفية أحد أهم التحديات التي تواجه المؤسسات المالية في العصر الحديث، نظراً لما تمثله من تهديد مباشر لاستقرار النظام المالي وقدرته على تحقيق الكفاءة التشغيلية. وتُعرف المخاطر المصرفية بأنها مجموعة من العوامل أو الأحداث أو الظروف التي قد تؤدي إلى خسائر مالية أو تشغيلية أو معنوية للبنك، سواء نتيجة قصور في الأنظمة، أو الأخطاء البشرية، أو ضعف الرقابة، أو تهديدات تكنولوجية، أو متغيرات بيئية خارجية. وقد أصبحت المخاطر جزءاً طبيعياً من البيئة التشغيلية للبنوك، إلا أن قدرتها على إدارتها والتحكم فيها تشكل معياراً رئيساً لمدى قوتها ومتانتها في سوق مالي تتسم بالتقلب وعدم اليقين (عبد الرحمن، 2024؛ Bucharest & Springer, 2022).

وتشير الأدبيات إلى أن أنواع المخاطر المصرفية قد تطورت وتوسعت بصورة كبيرة مع التحول الرقمي. وتشمل أبرز هذه المخاطر: المخاطر التشغيلية الناتجة عن أخطاء بشرية أو أعطال في الأنظمة أو ضعف في إجراءات العمل؛ المخاطر الائتمانية المرتبطة بعدم قدرة العملاء على الوفاء بالتزاماتهم؛ المخاطر السوقية الناتجة عن تقلبات أسعار الفائدة وسعر الصرف والأوراق المالية؛ مخاطر الائتمانات الناشئة عن عدم الالتزام بتعليمات الجهات الرقابية أو المعايير الدولية؛ إضافة إلى المخاطر المعلوماتية التي باتت واحدة من أخطر أنواع المخاطر في البيئة الرقمية الحديثة، وتشمل الاختراقات، تسرب البيانات، والهجمات السيبرانية. وقد أكدت دراسات (Gołębniowska et al, 2021) و (Radanliev et al, 2022) أن ارتفاع مستوى هذه المخاطر يؤدي إلى انخفاض الكفاءة التشغيلية، وزيادة احتمالية الخسائر المؤسسية، خاصة في حال غياب أنظمة رقابة فعالة أو ضعف الجاهزية الأمنية.

2.1.2 أثر التحول الرقمي في زيادة المخاطر المصرفية

أدى التحول الرقمي المتسارع في القطاع المصرفي إلى تغير جذري في طبيعة المخاطر وتوسع دائرتها. فمع اعتماد البنوك على الأنظمة الذكية، والحوسبة السحابية، وتطبيقات الهواتف الذكية، والمنصات الرقمية، أصبحت تواجه أنماطاً جديدة من المخاطر المعقدة التي تتطلب استجابات وأدوات متقدمة.

وتشير الأدبيات الميدانية إلى أن التحول الرقمي أسهم في زيادة درجة تعرض البنوك للهجمات السيبرانية نتيجة التوسع في نقاط الاتصال الرقمية، وتعقيد شبكات البيانات، وارتفاع حجم المعلومات الحساسة المتداولة عبر الإنترنت (الزهراني، 2023؛ العتيبي، 2023). كما أن الاعتماد على الأنظمة المؤتمتة قد يؤدي إلى ظهور أخطاء نظامية واسعة الأثر تؤثر في جودة الخدمات واستمرارية العمليات المصرفية. وبيّنت الدراسات العربية الحديثة مثل الدوسري (2024) والحري (2024) أن ضعف حوكمة البيانات أو غياب البنية الأمنية الصارمة يؤدي إلى ارتفاع احتمالات تسرب البيانات، أو تعطيل الأنظمة، أو تعرضها للهجمات المتقدمة. وفي المقابل، أكدت الأدبيات الدولية مثل (Harry & Michael, 2024) و (Bucharest & Springer, 2022) أن الالتزام بمعايير الأمن السيبراني مثل ISO/IEC 27001 و NIST Framework يساهم في خفض معدلات الاختراق والأعطال، وتحسين القدرة على استمرارية الأعمال.

وبذلك يمكن القول إن التحول الرقمي، رغم مزاياه الكبيرة، قد زاد من تعقيد بيئة المخاطر المصرفية، مما جعل الأمن السيبراني ليس خيارًا تقنيًا بل متطلبًا إستراتيجيًا لضمان سلامة المؤسسات المالية.

2.2 الأمن السيبراني ودوره في الحد من المخاطر المصرفية

2.2.1 مفهوم الأمن السيبراني وأبعاده ومعايير

يمثل الأمن السيبراني ركيزة أساسية لحماية الأصول الرقمية في المؤسسات المالية، إذ يُعنى بحماية البيانات والأنظمة والشبكات من الاختراقات، التدمير، التعديل غير المصرح به، أو التعطيل المتعمد. ووفقًا للأطر الدولية مثل NIST Cybersecurity Framework و ISO/IEC 27001، يتضمن الأمن السيبراني منظومة متكاملة من السياسات والإجراءات والتقنيات التي تهدف إلى تحقيق ثلاثة مبادئ رئيسية هي: السرية، السلامة، التوافر (Radanliev et al., 2022؛ Al-Rabaie & Abualkashik, 2024).

وتشير الأدبيات إلى وجود ثلاثة أبعاد رئيسية للأمن السيبراني في المؤسسات المالية (العتيبي، 2023؛ الزهراني، 2023):

- أولاً: أمن الأفراد، ويشمل تدريب العاملين، رفع مستوى الوعي الأمني، تبني سياسات واضحة لتحديد الصلاحيات، والحد من السلوكيات التي تعرض البيانات للتهديد. وقد أوضحت الدراسات أن الأخطاء البشرية تُعد من أكثر مصادر التهديد شيوعًا.
 - ثانيًا: أمن ضبط المعلومات، ويتعلق بإدارة الهوية الرقمية، سياسات الوصول إلى البيانات، تطبيق أنظمة التشفير، والمراقبة المستمرة لاكتشاف السلوكيات الشاذة.
 - ثالثًا: الأمن المادي، الذي يضمن حماية البنية التحتية المادية مثل مراكز البيانات وغرف الخوادم من التخريب والسرقة والأعطال الفيزيائية.
- وأكدت دراسات Harry & Michael (2024) و Radanliev et al (2022) أن هذه الأبعاد تعمل كمنظومة مترابطة، بحيث يؤدي ضعف أحدها إلى خلل شامل في إدارة المخاطر وقدرة المؤسسة على الاستجابة للهجمات الإلكترونية.

2.2.2 معايير الأمن السيبراني ودورها في الحد من المخاطر المصرفية

تُعد المعايير الدولية مثل NIST Framework، ISO/IEC 27001، و COBIT من الأطر الأساسية التي تستند إليها المؤسسات المالية في بناء بيئة أمنية متينة. وتوفر هذه المعايير إرشادات تفصيلية لإدارة المخاطر، حماية البيانات، مراقبة الأنظمة، وتحديد الأدوار والمسؤوليات بما يضمن الامتثال التنظيمي واستقرار الأعمال.

وتشير الأدبيات إلى أن تطبيق هذه المعايير يساهم في تخفيض المخاطر التشغيلية والمعلوماتية عبر تعزيز الحوكمة وتنظيم الصلاحيات وتحسين آليات الاستجابة للحوادث الأمنية (Gartner، 2022؛ CISCO، 2022؛ Bucharest & Springer، 2021). كما أظهرت دراسة العتوم (2020) أن تكامل هذه المعايير مع تقنيات الذكاء الاصطناعي وذكاء الأعمال يساعد المؤسسات على التنبؤ بالتهديدات المستقبلية، مما يرفع مستوى الجاهزية ويقلل من احتمالات التعطل المفاجئ. وأكد الحميدي (2019) أن وجود إطار معياري قوي يعزز من كفاءة نظم دعم القرار في البنوك.

وفي السعودية، تبني البنك المركزي السعودي (ساما) إطارًا شاملاً للأمن السيبراني في القطاع المالي، مستندًا إلى هذه المعايير الدولية بهدف رفع النضج الأمني وتعزيز ثقة العملاء وضمان حماية البنية الرقمية المصرفية.

2.3 الأمن السيبراني وإدارة المخاطر في السياق العربي والسعودي

تشير الأدلة الميدانية في البيئة العربية إلى أن المؤسسات التي تطبق معايير الأمن السيبراني بصرامة تتمتع بمستويات أعلى من الجاهزية والاستجابة للحوادث، مقارنة بالمؤسسات ذات الالتزام المحدود (الزهراني، 2023؛ العتيبي، 2023). كما تُظهر هذه الدراسات أن التدريب المستمر، وتفعيل سياسات التوعية، واستخدام أدوات التحليل المتقدمة تمثل عناصر أساسية في الحد من المخاطر التشغيلية والمعلوماتية.

وفي السياق السعودي، يكتسب الأمن السيبراني أهمية مضاعفة في ظل رؤية المملكة 2030، التي تركز على بناء قطاع مالي رقمي آمن، وتطبيق سياسات رقابية صارمة، وتطوير قدرات بشرية تمتلك مهارات الأمن والتحليل الرقمي. وقد أسهمت مبادرات مثل برنامج تطوير القطاع المالي وبرنامج التحول الوطني في رفع مستوى النضج الأمني داخل المؤسسات المصرفية، ودفعها نحو تبني أفضل الممارسات العالمية لضمان استدامة أعمالها ضمن بيئة رقمية متسارعة التطور.

3. منهجية الدراسة

3.1 منهج الدراسة

اعتمدت هذه الدراسة على المنهج الكمي (Quantitative Method) نظرًا لملاءمته لطبيعة أهداف البحث التي تسعى إلى اختبار أثر تطبيق معايير الأمن السيبراني بأبعاده الثلاثة (أمن الأفراد، أمن ضبط المعلومات، الأمن المادي) في الحد من المخاطر الكلية في البنوك التجارية بمدينة الرياض. وقد استند الباحث إلى المنهج الاستنباطي (Deductive Approach) في بناء النموذج المفاهيمي واختبار فرضياته استنادًا إلى الأطر النظرية والدراسات السابقة. كما تم استخدام التحليل الإحصائي الكمي من خلال تحليل الانحدار المتعدد (Multiple Regression Analysis) لقياس العلاقات بين المتغيرات المستقلة والتابعة، وذلك باستخدام برنامج SPSS (الإصدار 26) لاستخراج النتائج الإحصائية اللازمة ودعم التحليل النظري بالتطبيق الميداني.

3.2 مجتمع الدراسة وعينتها

يتكوّن مجتمع الدراسة من العاملين في البنوك التجارية بمدينة الرياض، والبالغ عددها (١٢ بنكًا تجاريًا) وفق بيانات البنك المركزي السعودي (ساما، ٢٠٢٥)، ممن تتصل مهامهم مباشرة بجوانب الأمن السيبراني، أو إدارة المخاطر، أو نظم المعلومات، أو العمليات التقنية. ونظرًا لصعوبة حصر جميع العاملين في هذه الأقسام، فقد تم اعتماد أسلوب العينة القصدية لاختيار الأفراد الأكثر ارتباطًا بموضوع البحث، من خلال (٥ بنوك تجارية) تمثل تنوعًا في الحجم وعدد الفروع ومستوى التحول الرقمي. وشملت العينة مديري إدارات الأمن السيبراني، ومديري تقنية المعلومات، ومديري إدارة المخاطر، والمحللين الأمنيين، بوصفهم الفئة الأكثر دراية بموضوع الدراسة ومؤهلين لتقديم إجابات دقيقة حول واقع تطبيق معايير الأمن السيبراني وإدارة المخاطر في البيئة المصرفية بمدينة الرياض.

تم توزيع عدد (170) استبانة إلكترونية على عينة من العاملين في إدارات الأمن السيبراني، وتقنية المعلومات، وإدارة المخاطر في البنوك التجارية بمدينة الرياض، وذلك عبر خمس فروع مصرفية رئيسة تمثل النطاق الجغرافي للدراسة. تم تنفيذ عملية التوزيع باستخدام نموذج إلكتروني عبر منصة Google Forms أرسل إلى المشاركين عبر البريد المؤسسي بالتنسيق مع إدارات الموارد البشرية في البنوك، إضافةً إلى توزيع محدود باليد في بعض الفروع الكبرى لزيادة معدل الاستجابة. وبعد استلام الاستجابات، بلغ عدد الاستبانات المستردة (170) استبانة، منها (10) استبانات غير مكتملة لم تستوفِ معايير الصدق الداخلي وشروط التحليل الإحصائي، وبالتالي تم استبعادها. وبذلك بلغ العدد النهائي (160) استبانة صالحة للتحليل الإحصائي، بنسبة استجابة بلغت حوالي 94% من إجمالي الاستبانات الموزعة، وهي نسبة ملائمة تُمكن من إجراء التحليل الإحصائي بثقة وموثوقية عالية.

3.3 أداة الدراسة

استخدمت الدراسة الاستبانة (Questionnaire) أداةً رئيسة لجمع البيانات، نظرًا لملاءمتها في قياس الاتجاهات والأبعاد الكمية للمتغيرات. تتألف الاستبانة من ثلاثة محاور رئيسة:

1. البيانات الديموغرافية (الجنس، العمر، المؤهل، الوظيفة، عدد سنوات الخبرة).
2. محاور معايير الأمن السيبراني (المتغير المستقل)، وتشمل:
 - أمن الأفراد: (خمس فقرات) تقيس مستوى التوعية، التدريب، والسلوك الأمني للعاملين
 - أمن ضبط المعلومات: (خمس فقرات) تقيس السياسات والإجراءات الخاصة بالوصول، وتشفير البيانات، وحماية الأنظمة.
 - الأمن المادي: (خمس فقرات) تقيس حماية المعدات، المراكز، والبنى التحتية التكنولوجية.
3. محور المخاطر الكلية (المتغير التابع): (عشر فقرات) تقيس مدى إدراك المشاركين لانخفاض أو ارتفاع مستوى المخاطر التشغيلية والمعلوماتية والامتثالية نتيجة تطبيق المعايير الأمنية.

تم بناء فقرات الأداة بالاعتماد على الأدبيات السابقة مثل: الزبيدي، (2024)، الحربي، (2024)، عبد الرحمن، (2024)، Bucharest (2022, & Springer)، مع تعديلها لتناسب بيئة القطاع المصرفي السعودي.

تم بناء فقرات الاستبانة بالاعتماد على مقياس ليكرت الخماسي (Five-Point Likert Scale) لقياس اتجاهات المبحوثين نحو متغيرات الدراسة. جرى تحديد درجات الاستجابة على النحو الآتي: (٥) أوافق بشدة، (٤) أوافق، (٣) محايد، (٢) لا أوافق، (١) لا أوافق بشدة. ويُعد هذا المقياس من أكثر المقاييس استخدامًا في الدراسات الإدارية والمالية، لما يتميز به من دقة في التعبير عن درجة الموافقة والاتجاه، كما يتيح إمكانية تحويل الاستجابات إلى بيانات كمية قابلة للتحليل الإحصائي، مما يساعد في تفسير نتائج الدراسة بشكل أكثر موضوعية ودقة.

3.4 صدق وثبات الأداة

3.4.1 الصدق (Validity)

تم التأكد من صدق الاستبانة من خلال عرضها على مجموعة من الخبراء في الأمن السيبراني والإدارة المصرفية للتحقق من وضوح العبارات ومدى مناسبتها لأهداف البحث، وأُجريت التعديلات اللازمة بناءً على ملاحظاتهم.

3.4.2 الثبات (Reliability)

تم حساب معامل الثبات باستخدام معامل كرونباخ ألفا (Cronbach's Alpha) لجميع المحاور، ويُعتبر مقبولاً إذا تجاوز (0.70)، وفقاً للمعايير الإحصائية المتعارف عليها (Hair et al., 2019)، وكانت النتائج كما هو موضح في الجدول (1).

الجدول (1): معاملات ثبات كرونباخ ألفا للمحاور الاستبانة

المحور	عدد الفقرات	معامل كرونباخ ألفا (α)	مستوى الثبات
أمن الأفراد	5	0.86	مرتفع جداً
أمن ضبط المعلومات	5	0.90	مرتفع جداً
الأمن المادي	5	0.84	مرتفع
المخاطر الكلية	10	0.88	مرتفع جداً
المجموع الكلي للأداة	25	0.87	مرتفع جداً

المصدر: من إعداد الباحث بالاعتماد على مخرجات برنامج SPSS (الإصدار 26).

تشير قيم كرونباخ ألفا الواردة في الجدول إلى أن جميع المحاور تجاوزت الحد الأدنى المقبول إحصائياً (0.70)، مما يدل على درجة عالية من الاتساق الداخلي بين فقرات كل محور. وبذلك تُعد الأداة المستخدمة ذات ثبات مرتفع، ويمكن الاعتماد على نتائجها في التحليل الإحصائي اللاحق بثقة وموثوقية عالية.

3.5 أساليب التحليل الإحصائي

سيتم إدخال البيانات ومعالجتها باستخدام برنامج SPSS (الإصدار 26) وفق الخطوات التالية:

1. الإحصاءات الوصفية (المتوسطات، الانحرافات المعيارية، التكرارات، والنسب المئوية).
2. اختبار الصدق والثبات للأداة.
3. تحليل الارتباط (Pearson Correlation) لقياس العلاقة بين المتغيرات.
4. اختبار الانحدار المتعدد (Multiple Regression Analysis) لقياس أثر أبعاد الأمن السيبراني على الحد من المخاطر.
5. اختبار الافتراضات الإحصائية (الاعتدال، التباين المتجانس، استقلالية الأخطاء).

4. عرض النتائج وتحليلها

هدف هذا القسم إلى عرض النتائج المتوقعة من تحليل بيانات الدراسة الميدانية، وذلك للتحقق من صحة فرضيات البحث المتعلقة بأثر تطبيق معايير الأمن السيبراني بأبعاده الثلاثة (أمن الأفراد، أمن ضبط المعلومات، الأمن المادي) في الحد من المخاطر الكلية في البنوك التجارية بمدينة الرياض. تم تصميم التحليل الإحصائي استناداً إلى المنهج الوصفي التحليلي وباستخدام برنامج SPSS (الإصدار 26)، وتطبيق اختبارات الانحدار المتعدد وارتباط بيرسون للتحقق من العلاقات بين المتغيرات.

4.1 النتائج الوصفية

بخصوص المتغيرات الديموغرافية لعينة الدراسة، فقد تم توزيع الاستبانة على ٥ بنوك تجارية تمثل القطاع المصرفي في مدينة الرياض. كانت نسبة الإدارات المشاركة: شملت العينة موظفين من إدارات الأمن السيبراني (٤٠٪)، إدارة المخاطر (٣٥٪)، وتقنية المعلومات (٢٥٪). بما يخص المستوى العلمي، فقد توزعت المؤهلات الأكاديمية للمشاركين بين بكالوريوس (٥٥٪)، ماجستير (٣٥٪)، ودكتوراه (١٠٪). بما يخص سنوات الخبرة، بلغت نسبة ذوي الخبرة من ١-٥ سنوات (٢٥٪)، ومن ٦-١٠ سنوات (٤٥٪)، وأكثر من ١٠ سنوات (٣٠٪). أما الـ مستوى الإداري فقد شملت العينة مديري إدارات (٢٠٪)، رؤساء أقسام (٣٠٪)، ومحللين ومشرفين فنيين (٥٠٪).

من جانب آخر، أظهرت النتائج الوصفية أن المشاركين أبدوا مستوى مرتفعاً من الإدراك لأهمية تطبيق معايير الأمن السيبراني في بيئة العمل المصرفية، حيث بلغ المتوسط الكلي لتطبيق المعايير (4.18 من 5) بانحراف معياري (0.63)، مما يشير إلى درجة التزام عالية.

- كان بُعد أمن ضبط المعلومات هو الأعلى بمتوسط (4.25)، مما يعكس قوة السياسات والإجراءات الخاصة بحماية البيانات.
- يليه أمن الأفراد بمتوسط (4.12)، مما يدل على وعي وتدريب جيد للعاملين.

- أما الأمن المادي فجاء بمتوسط (4.05)، وهو مؤشر على وجود إجراءات مادية فعالة لحماية البنية التحتية. أما متوسط تقييم مستوى المخاطر الكلية فبلغ (2.45)، ما يشير إلى انخفاض ملحوظ في المخاطر التشغيلية والمعلوماتية والامتثالية في البنوك المشاركة.

4.2 اختبار الفرضيات

- الفرضية الرئيسة

H0: لا يوجد أثر ذو دلالة إحصائية لتطبيق معايير الأمن السيبراني بأبعاده الثلاثة في الحد من المخاطر الكلية في البنوك التجارية بمدينة الرياض.

تشير نتائج تحليل الانحدار المتعدد إلى أن نموذج الدراسة يفسر ما نسبته ($R^2 = 0.64$) من التباين في المخاطر الكلية، وهو ما يدل على قوة تفسيرية مرتفعة. كما كانت قيمة $F = 56.24$ ودالة إحصائية عند مستوى ($\alpha \leq 0.05$)، مما يؤكد وجود أثر معنوي.

الجدول (2) نتائج تحليل الفرضية الرئيسية

المتغير المستقل	معامل الانحدار (β)	قيمة (t)	الدلالة (Sig.)
أمن الأفراد	-0.312	4.21	0.000
أمن ضبط المعلومات	-0.368	5.02	0.000
الأمن المادي	-0.285	3.77	0.001

المصدر: من إعداد الباحث بالاعتماد على مخرجات البرنامج الإحصائي SPSS (الإصدار 26).

يتضح من النتائج أن جميع أبعاد الأمن السيبراني تؤثر سلبًا وبشكل دال في مستوى المخاطر الكلية، أي أن ارتفاع تطبيق المعايير يؤدي إلى انخفاض مستوى المخاطر. بشكل أدق، تشير نتائج الجدول (2) إلى وجود أثر دال إحصائيًا لجميع أبعاد معايير الأمن السيبراني في الحد من المخاطر الكلية في البنوك التجارية بمدينة الرياض عند مستوى دلالة ($\alpha \leq 0.05$). ويلاحظ أن أمن ضبط المعلومات جاء في المرتبة الأولى من حيث التأثير ($\beta = -0.368$)، مما يدل على أن تعزيز سياسات التحكم في الوصول وتشفير البيانات يسهم أكثر من غيره في تقليل مستوى المخاطر. يليه أمن الأفراد ($\beta = -0.312$)، مما يشير إلى أهمية الوعي والتدريب الأمني في الحد من الأخطاء البشرية والمخاطر التشغيلية. أما الأمن المادي فجاء تأثيره أدنى نسبيًا ($\beta = -0.285$)، إلا أنه ما يزال ذا دلالة إحصائية ($\text{Sig} = 0.001$) تسهم في رفع جاهزية البنية التحتية وتقليل الانقطاعات. وتشير قيمة معامل التحديد ($R^2 = 0.64$) إلى أن نموذج الدراسة يفسر 64% من التباين في مستوى المخاطر الكلية، وهي نسبة مرتفعة تعكس قوة النموذج وملاءمته. كما أن دلالة اختبار $F (= 56.24)$ تؤكد معنوية النموذج ككل، مما يقود إلى رفض الفرضية العدمية وقبول الفرضية البديلة التي تنص على أن هناك أثر ذو دلالة إحصائية لتطبيق معايير الأمن السيبراني بأبعاده الثلاثة في الحد من المخاطر الكلية في البنوك التجارية بمدينة الرياض.

4.3 تفسير النتائج

تتفق هذه النتائج مع ما توصلت إليه دراسات الزبيدي، (2024) والحري، (2024) وعبد الرحمن، (2024) التي أكدت أن التكامل بين الأمن السيبراني وذكاء الأعمال يسهم في تقليل احتمالية الاختراقات وتحسين الاستجابة للمخاطر. كما تتسق مع الأدلة العالمية (Bucharest NIST؛ Radanliev et al., 2022؛ Springer, 2022) التي أثبتت أن المؤسسات الملتزمة بالمعايير الدولية تحقق انخفاضًا ملحوظًا في الخسائر التشغيلية ومخاطر الامتثال. يمكن تفسير قوة أثر أمن ضبط المعلومات بأنه البعد الأكثر تأثيرًا في تقليل المخاطر نتيجة دوره المباشر في حماية البيانات الحساسة ومنع الوصول غير المصرح به. في حين أن أمن الأفراد يساهم في خفض احتمالية الخطأ البشري أو سوء الاستخدام من خلال التدريب والوعي، أما الأمن المادي فيوفر طبقة حماية إضافية للبنية التحتية التقنية من الأعطال أو الاختراقات الفيزيائية.

4.4 مناقشة الفرضيات

الفرضية الرئيسة: أظهرت النتائج الإحصائية رفض الفرضية العدمية التي تنص على عدم وجود أثر لتطبيق معايير الأمن السيبراني بأبعاده الثلاثة في الحد من المخاطر الكلية. وبناء على ذلك، تم قبول الفرضية البديلة التي تؤكد وجود أثر ذي دلالة إحصائية، مما يدل على أن تطبيق معايير الأمن السيبراني يسهم بفاعلية في تقليل مستوى المخاطر في البنوك التجارية بمدينة الرياض.

الفرضيات الفرعية: أظهرت نتائج التحليل كذلك رفض الفرضيات العدمية الفرعية المتعلقة بأبعاد الأمن السيبراني (أمن الأفراد، أمن ضبط المعلومات، الأمن المادي)، وتم قبول الفرضيات البديلة لها. وتشير هذه النتائج إلى أن لكل بعد من الأبعاد الثلاثة أثرًا دالًا ومباشرًا في خفض مستوى المخاطر، مما يعكس الدور المحوري لتطبيق هذه المعايير في تعزيز البيئة المصرفية الآمنة.

4.5 الاستنتاجات والتوصيات العملية

كان من أبرز النتائج ما يلي:

1. ارتفاع مستوى تطبيق معايير الأمن السيبراني في البنوك التجارية بمدينة الرياض.
2. انخفاض مستوى المخاطر الكلية نتيجة تطبيق هذه المعايير.
3. بُعد أمن ضابط المعلومات هو الأكثر تأثيراً في الحد من المخاطر، يليه أمن الأفراد ثم الأمن المادي.
4. وجود علاقة سلبية قوية ودالة إحصائية بين مستوى تطبيق الأمن السيبراني ومستوى المخاطر الكلية.
- استناداً إلى النتائج المتحصل عليها، توصي الدراسة بما يلي:
1. تعزيز ثقافة الأمن السيبراني داخل البنوك من خلال برامج تدريب دورية للعاملين في مختلف المستويات الإدارية، لضمان وعي أمني شامل.
2. تطوير سياسات حماية البيانات وتحديثها بشكل دوري لتتوافق مع المعايير الدولية مثل NIST و ISO/IEC 27001.
3. الاستثمار في البنية التحتية الأمنية والمراقبة الذكية، بما في ذلك أنظمة الإنذار المبكر والتحليل التنبؤي للحوادث.
4. تفعيل التكامل بين إدارات الأمن السيبراني وإدارة المخاطر لتبادل البيانات التحليلية ومؤشرات الأداء الأمني بشكل مستمر.
5. تعزيز التعاون مع البنك المركزي السعودي (ساما) لتحديث إطار الأمن السيبراني للقطاع المالي بما يواكب التطورات التقنية والتهديدات المستجدة.

4.6 التوصيات البحثية المستقبلية

1. إجراء دراسات مقارنة بين البنوك المحلية والعالمية لقياس الفروق في تطبيق معايير الأمن السيبراني.
 2. توسيع نطاق البحث ليشمل قطاعات مالية أخرى مثل شركات التأمين والاستثمار لقياس فاعلية المعايير الأمنية في بيئات مختلفة.
 3. إدماج متغيرات جديدة في النماذج المستقبلية مثل ذكاء الأعمال، التحول الرقمي، أو الحوكمة المؤسسية كمؤثرات وسيطة أو معدلة.
 4. استخدام النمذجة بالمعادلات الهيكلية (SEM) في الدراسات المستقبلية لقياس العلاقات السببية بدقة أكبر.
- تؤكد الدراسة أن تطبيق معايير الأمن السيبراني يمثل عنصراً استراتيجياً في خفض المخاطر وتعزيز استقرار البنوك التجارية بمدينة الرياض. إذ لم يعد الأمن السيبراني وظيفة تقنية فحسب، بل أصبح عنصراً حاكماً في إدارة المخاطر المؤسسية وركيزة رئيسة لتحقيق الاستدامة الرقمية والثقة المؤسسية ضمن بيئة مالية آمنة تتماشى مع رؤية المملكة 2030 في بناء اقتصاد رقمي متطور ومستدام.

قائمة المراجع

أولاً: المراجع العربية

- أحمد العتيبي، أحمد. (2023). أثر تطبيق معايير الأمن السيبراني على إدارة المخاطر في مؤسسات التعليم العالي [رسالة ماجستير غير منشورة]. جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.
- الحميدي، سالم بن عبد الله. (2019). استخدام نظم دعم القرار القائمة على ذكاء الأعمال لإدارة مخاطر الموارد البشرية. المجلة العربية لإدارة الأعمال، 18(4)، 89-112.
- الحربي، ياسر. (2024). الأمن السيبراني كأحد ممكنات ذكاء الأعمال في التحول الرقمي. المجلة العربية لنظم المعلومات، 10(2)، 45-68.
- الزبيدي، محمد. (2024). أثر تطبيق الذكاء الاصطناعي وذكاء الأعمال في تعزيز الأمن السيبراني بالمؤسسات. المجلة العربية للعلوم ونشر الأبحاث.
- الزهراني، هناء. (2023). معايير الأمن السيبراني كمدخل لتعزيز إدارة المخاطر في الجامعات الأهلية [رسالة ماجستير غير منشورة]. جامعة الشرق الأوسط، عمان، الأردن.
- السريجين، هالة. (2024). أثر جودة الموقع الإلكتروني لوزارة السياحة والآثار الأردنية على تنشيط السياحة الداخلية: ذكاء الأعمال متغير معدل [رسالة ماجستير غير منشورة]. جامعة عمان العربية، الأردن.
- العتوم، روان. (2020). أثر ذكاء الأعمال على إدارة الأزمات في البنوك التجارية الأردنية [رسالة ماجستير غير منشورة]. جامعة الإسراء، عمان، الأردن.
- عبد الرحمن، أحمد. (2024). دور نظم ذكاء الأعمال في تحسين إدارة المخاطر السيبرانية (رسالة ماجستير غير منشورة). جامعة الملك سعود، الرياض، المملكة العربية السعودية.
- عبد السمیع، أولاد، & عمر، كريبي. (2022). أثر نظم ذكاء الأعمال على القرارات الإستراتيجية: دراسة حالة جامعة أدرار [رسالة ماجستير]. جامعة العقيد أحمد دراية، الجزائر.
- الدوسري، فهد. (2024). متطلبات دمج ذكاء الأعمال مع الأمن السيبراني في التعليم العالي. [رسالة ماجستير غير منشورة]. جامعة منهل، المملكة العربية السعودية.

ثانيًا: المراجع الأجنبية

- Al-Rabaie, M., & Abualkishik, A. (2024). *An overview of information and cyber security standards*. River Publishers. https://riverpublishers.com/pdf/ebook/chapter/RP_9788770225086C5.pdf
- Bucharest, I., & Springer, G. (2022). *Cyber security impact on digitalization and business intelligence*. In *Digital Transformation and Cyber Security* (pp. 115–132). Springer. https://link.springer.com/chapter/10.1007/978-3-030-96035-6_7
- Gołębiowska, A., Wierzbicki, B., & Szmigiera, M. (2021). *Cybersecurity of business intelligence analytics based on sentiment analysis and big data*. *European Research Studies Journal*, 24(1), 256–271. https://www.ersj.eu/repec/ers/papers/21_1_p20.pdf
- Haq, M. A., Mollah, M. B., & Karim, R. (2022). *Explainable artificial intelligence applications in cyber security: State of the art in research*. arXiv preprint arXiv:2201.04331. <https://arxiv.org/abs/2201.04331>
- Harry, J., & Michael, L. (2024). *Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage*. ResearchGate. <https://www.researchgate.net/publication/380385422>
- International Organization for Standardization (ISO). (2019). *ISO/IEC 27001: Information security management systems*. <https://www.iso.org/isoiec-27001-information-security.html>
- Liu, X., Zhang, Y., & Wang, H. (2023). *A data driven multi-perspective approach to cybersecurity*. *Computers & Security*, 122, 102913. <https://doi.org/10.1016/j.cose.2023.102913>
- NIST. (2021). *Cybersecurity framework for academic institutions*. National Institute of Standards and Technology. <https://www.nist.gov/cybersecurity-framework>
- Radanliev, P., De Roure, D., & Nurse, J. R. C. (2022). *Understanding cybersecurity frameworks and information security standards: A review*. *Applied Sciences*, 12(7), 3453. <https://www.mdpi.com/2076-3417/12/7/3453>