Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (2): 181-201
Doi: www.doi.org/10.25130/tjaes.22.SP7.2.10

Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
EISSN: 3006-9149
PISSN: 1813-1719

Cyber Risk Analysis and Its Impact on Bank Management Quality: A Statistical Study Using Advanced Models

Sufian M. Salih* [A], Rawahil Ali Tali [B], Hiba Abdulrazzaq Khudhur [B]
[A] College of Business Economics / Al-Nahrain University
[B] College of Administration and Economics / Wasit University

Keywords:
Cyber risks, quality of bank management, IT companies, telecommunications company, banks.

Article history:

Received	29 Oct. 2025
Received in revised form	02 Nov. 2025
Accepted	02 Dec. 2025
Available online	14 Jun. 2026

*Corresponding author:
Sufian M. Salih
College of Business Economics / Al-Nahrain University

Abstract: This research aims to identify the impact of cyber risks on financial institutions, given the increasing cyber threats faced by banks of all types worldwide. These threats include, for example, data breaches, cyber espionage, and other risks that jeopardize information security and the integrity of electronic systems in banks. The researcher sought to measure and test the correlations and influences between the research variables. To achieve this, the study relied on the contributions of a group of specialized researchers and reputable studies that addressed the investigated variables. The research sample consisted of 270 questionnaires distributed among an IT company, a telecommunications company, and banks. The data obtained using the statistical software SPSS version 23 was analyzed to arrive at the relevant results. The Spearman correlation coefficient was used to measure the correlation between variables, and the t-test was used to determine the significance of this relationship. Multiple regression analysis and the F-test were employed to determine the significance of the regression equation. The R^2 value was used to interpret the extent to which independent variables influence the dependent variable. The study concluded with several key findings, most notably the existence of a statistically significant correlation and influence between cyber risks and the quality of bank management.

The research concluded with a set of recommendations, including the necessity of increasing awareness among financial institutions in general, and banks in particular, regarding the importance of using information security governance principles and standards to enable them to confront challenges and risks.

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (2): 181-201
Doi: www.doi.org/10.25130/tjaes.22.SP7.2.10

تحليل المخاطر السيبرانية وأثرها على جودة إدارة المصارف: دراسة إحصائية باستخدام نماذج متقدمة

سفيان منذر صالح
كلية اقتصاديات الاعمال
جامعة النهرين

رواحل علي طليع
كليه الإدارة والاقتصاد
جامعه واسط

هبه عبد الرزاق خضر
كليه الإدارة والاقتصاد
جامعه واسط

المستخلص

هدف البحث الحالي إلى تحديد تأثير المخاطر السيبرانية على المؤسسات المالية، ونظرًا لتزايد التهديدات الإلكترونية التي تواجهها المصارف بمختلف أنواعها حول العالم. والتي تشمل كمثال على هذه التهديدات والهجمات الإلكترونية (اختراق البيانات، والتجسس الإلكتروني، وغيرها) من المخاطر التي تهدد أمن المعلومات وسلامة الأنظمة الإلكترونية في المصارف. إذ حاول الباحث الوصول إلى قياس علاقات الارتباط والتأثير بين متغيرات البحث واختبارها ولتحقيق ذلك حاولت الدراسة الاعتماد على مساهمات مجموعة من الباحثين المختصين والدراسات الرصينة التي تناولت دراسة المتغيرات المبحوثة. وقد أشملت عينة البحث على (270) استمارة تم توزيعها بين شركة تكنولوجيا المعلومات وشركة الاتصالات والمصارف، وجرى تحليل البيانات التي تم الحصول عليها عبر أداة الدراسة باستعمال البرنامج الإحصائي (SPSSV•23) للوصول الى النتائج المتعلقة بها. واستعمل معامل الارتباط (Spearman) لقياس علاقة الارتباط بين المتغيرات واختبار (t) لمعرفة الدلالة المعنوية لهذه العلاقة، وتحليل الانحدار المتعدد (Multiple Regression Analysis)، واختبار(F) لتحديد معنوية معادلة الانحدار، كما تم استعمال (R2) لتفسير مقدار تأثير المتغيرات المستقلة في المتغير المعتمد. كما توصلت الدراسة إلى مجموعة من النتائج من أهمها وجود علاقة ارتباط وتأثير ذات دلالة معنوية بين المخاطر السيبرانية بين جودة ادارة المصارف.

ثم اختتم البحث بمجموعة من التوصيات وكانت من بين هذه التوصيات ضرورة زيادة الاهتمام بتوعية المؤسسات المالية عامة والمصرفية خاصة بأهمية استخدام مبادئ ومعايير حوكمة أمن المعلومات حتى يتسنى لها مواجهة التحديات والمخاطر.

الكلمات المفتاحية: المخاطر السيبرانية، جودة ادارة المصارف، شركات تكنولوجيا المعلومات، شركة الاتصالات، المصارف.

المقدمة

يشهد العالم اليوم تطورًا متسارعًا في تكنولوجيا المعلومات والاتصالات، الأمر الذي أسهم في تحول جذري في طبيعة إدارة الأعمال وطريقة تقديم الخدمات، خاصة في المؤسسات المالية والمصرفية التي أصبحت تعتمد بشكل واسع على الأنظمة الرقمية والمنصات الإلكترونية في أداء عملياتها اليومية. وقد أدّى هذا التحول الرقمي إلى تعزيز كفاءة العمل المصرفي وتوسيع نطاق الخدمات، لكنه في الوقت نفسه أوجد تحديات جديدة تتمثل في المخاطر السيبرانية التي باتت تشكّل تهديدًا مباشرًا لأمن الأنظمة المصرفية واستقرارها.

وتعد المخاطر السيبرانية من أبرز التحديات التي تواجه المصارف حول العالم، إذ تتنوع الهجمات الإلكترونية لتشمل اختراق البيانات، والبرمجيات الخبيثة، وهجمات حجب الخدمة،

والتجسس الإلكتروني، وغيرها من التهديدات التي تستهدف البنية التحتية المصرفية. ومع الاعتماد المتزايد على التكنولوجيا الرقمية في تقديم الخدمات المصرفية، أصبحت هذه التهديدات تمثل خطرًا لا يقتصر على الجانب التقني فحسب، بل يمتد ليؤثر في جودة الإدارة المصرفية، ورضا العملاء، وإدارة المخاطر، واستمرارية الأعمال.

وقد ساهم إدخال تكنولوجيا المعلومات في القطاع المصرفي في إعادة تصميم الهياكل التنظيمية للمصارف، وتحويلها من هياكل تقليدية إلى هياكل رقمية أكثر مرونة واستجابة. وهذا التحول فرض ضرورة تقييم سياسات وإجراءات أمن المعلومات والتأكد من توافقها مع المواصفات القياسية العالمية مثل ISO/IEC 27001، من خلال عمليات تدقيق ورقابة مستقلة تكشف نقاط الضعف وتقدم توصيات لتحسين منظومة الأمن السيبراني.

وفي هذا الإطار، يلعب التحليل الإحصائي التطبيقي دورًا محوريًا في قياس تأثير المخاطر السيبرانية على جودة إدارة المصارف، عبر استخدام أساليب كمية ونماذج تحليلية متقدمة لتحديد أنماط الهجمات، وقياس آثارها التشغيلية والإدارية، ودراسة العلاقة بين مستوى الأمن السيبراني وأداء المصارف. ويسهم هذا النهج الكمي في تقديم نتائج دقيقة تدعم اتخاذ قرارات استراتيجية تعزز أمن المعلومات وتضمن استمرارية العمليات المصرفية. اشتمل البحث على مقدمة وأربعة مباحث وكما يأتي: إذ تمثل الفصل الأول منهجية البحث والدراسات السابقة فتناول المبحث الأول منهجية البحث في حين شمل المبحث الثاني الدراسات السابقة أما الفصل الثاني يتحدث عن الإطار النظري للبحث إذ شمل المبحث الأول المخاطر الأمن السيبراني وتناول المبحث الثاني عن المخاطر في الأداء المصرف: المخاطر السيبرانية (التوسع - الطبيعة - الأجناس - الابعاد). وتضمن الفصل الثالث الجانب العملي وتناول الفصل الرابع الاستنتاجات والتوصيات إذ تضمن المبحث الأول الاستنتاجات في حين شمل المبحث الثاني التوصيات

الفصل الاول: منهجية البحث والدراسات السابقة

المبحث الأول: منهجية البحث

1. **هدف البحث:** يهدف هذا البحث إلى تحليل أثر المخاطر السيبرانية على جودة إدارة المصارف، وتحديد مدى قدرة المصارف على تبنّي سياسات أمنية فعّالة تضمن حماية أنظمتها الرقمية وتعزيز استمرارية أعمالها، وذلك من خلال تقديم إطار علمي يساعد المؤسسات المصرفية على اتخاذ إجراءات استباقية للتقليل من التهديدات الإلكترونية ورفع مستوى الأمن والجودة التشغيلية.
2. **مشكلة البحث:** تتجلى المشكلة البحثية في الأسئلة الآتية:

على الرغم من التطور الكبير في التقنيات الرقمية التي تعتمد عليها المصارف في تقديم خدماتها، إلا أن هذا التحول قد صاحبه تزايد ملحوظ في مستوى المخاطر السيبرانية التي تهدد أمن المعلومات واستقرار الأنظمة المصرفية. فالهجمات الإلكترونية بمختلف أنواعها—مثل اختراق البيانات، والتجسس الإلكتروني، والبرمجيات الخبيثة—أصبحت تمثل تحديًا حقيقيًا يؤثر في قدرة المصارف على إدارة عملياتها بكفاءة وضمان جودة خدماتها واستمرارية أعمالها.

ومع أن العديد من المصارف تبنّت أنظمة معلومات حديثة، إلا أن ضعف تطبيق سياسات الأمن السيبراني أو عدم توافقها مع المعايير الدولية كـ ISO/IEC 27001 قد يجعلها أكثر عرضة للثغرات والاختراقات، مما ينعكس سلبًا على ثقة العملاء وسمعة المصرف وأدائه التشغيلي.

وبناءً على ذلك تتحدد مشكلة البحث في السؤال الآتي:

"إلى أي مدى تؤثر المخاطر السيبرانية في جودة إدارة المصارف، وما هو دور السياسات الأمنية والتدابير الوقائية في الحد من هذه المخاطر وتعزيز استمرارية الأعمال المصرفية؟"

3. **أهمية البحث:** يسعى البحث إلى تحقيق الفائدة لكل من المؤسسات المصرفية والعملاء وصناع القرار ومن خلال تسليط الضوء على أهمية الأمن السيبراني ودوره في الوصول لجودة الإدارة المصرفية
4. **فرضية البحث:** أن فرضية البحث تتلخص بالآتي:

أ. توجد علاقة ذات دلالة بين المخاطر السيبرانية وجودة إدارة المصارف.
ب. توجد علاقة ذات دلالة بين أنواع الهجمات الإلكترونية وكفاءة العمليات المصرفية.
ج. تساهم السياسات الأمنية الفعّالة في الحد من آثار المخاطر السيبرانية.
د. تؤثر المخاطر السيبرانية في استمرارية أعمال المصارف بدرجة معنوية.

5. **حدود البحث:**

الحدود البشرية: موظفي شركة لمديرين الماليين والمحاسبين القائمين على التعامل مع نظم المعلومات المحاسبية الالكترونية. وموظفين في إدارة تكنولوجيا المعلومات وتكنولوجيا المعلومات من متخصصين ومراجعي نظم المعلومات الالكترونية ومديري الإدارات. والمراجعين الخارجيين الذين يعتمدون بمراجعة أنظمة تلك الشركات والمصارف.

الحدود المكانية: شركات العاملة في مجال الأمن السيبراني (تكنلوجيا المعلومات والاتصالات) والمتعاونة بعقود مع المصارف، والمصارف العاملة في العراق.

الحدود التطبيقية: تم توزيع الاستبيانات من خلال كوكل فورم واستمرت فترة بين تحليل النتائج واستخلاص النتائج من 5/11 /2025 الى فترة 10/22 /2025

المبحث الثاني: الدراسات السابقة

دراسة آمنة محمد منصور لعام 2021 بعنوان تأثير الأمن السيبراني على الرقابة الداخلية وانعكاساتها على الوحدة الاقتصادية: دراسة استطلاعية للآراء عينة من المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي هدفت الدراسة إلى التعرف على أهمية الأمن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية باعتماد إطار حوكمة تقنية المعلومات (COBITS)، ومن أهم النتائج التي توصلنا إليها البحث أن هناك تقبل واتفاق بشكل عام على وجود علاقة بين أبعاد ومتطلبات الأمن السيبراني على الأطر الحديثة للرقابة الداخلية وقيمة الوحدة الاقتصادية وأوصت الباحثة المستمرة قيام الوحدة الاقتصادية بتبني وسائل فاعلة للتقويم المستمر للرقابة الداخلية للحفاظ على أمن المعلومات باعتماد الأطر الحديثة للرقابة الداخلية لتلافي وسائل اختراق النظم الإلكترونية ومحاولات التلاعب في معلوماتها.

دراسة حنان هارون فريد لعام 2022 بعنوان الدور المقترح لمراجع الحسابات في الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية: هدف الدراسة هو إظهار دور المراجعات في الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره على دلالة القوائم المالية، حتى تتمكن المراجعات من مواكبة التغير السريع في بيئة الأعمال، وخلصت الدراسة إلى وجود تأثير معنوي لأهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني ووجود تأثير معنوي للمقترحين لمراجع الحسابات وأثره على القوائم المالية.

دراسة هبة جمال علي لعام 2023 بعنوان منهج إجرائي مقترح لقياس مدى استجابة المراجعات الخارجية للمخاطر السيبرانية في منشأة العميل: هدف الدراسة إلى إجراء لمنهج إجرائي مقترح

لقياس مدى استجابة المراجعات الخارجية للمخاطر السيبرانية في منشأة العميل بالبيئة المصرية، وتوصلت الدراسة إلى أن تقييم مخاطر الأمن السيبراني يعتمد على عمليات المراجعة التي تدرس وتقيم مجموعة من الضوابط المحددة مسبقًا في مجموعة متنوعة من الموضوعات المتعلقة بالأمن السيبراني وتكتشف الدراسة وجود تأثير طردي معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجية ووجود ارتباط طردي معنوي بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجية، وتوصلت الدراسة إلى عدد من النتائج والتوصيات أهمها.

قام (أبو زيادة (2011) بدراسة المعرفة مدى تطبيق إدارة الجودة الشاملة في المصارف التجارية الفلسطينية من وجهة نظر موظفي الوظائف الإشرافية فيها، وأثر هذا التطبيق على ارتفاع التنظيمي، وخلصت الدراسة إلى أن المصارف المبحوثة تطبق مبادئ الجودة الشاملة فيها بشكل متوسط، وذلك حسب الترتيب التالي من الأكثر إلى الأقل تطبيقا: التركيز على المعتمدين، وتدريب الموظفين وتأهيلهم، والقدرة على الاتصال الفعال (بدرجة عالية)، ثم المتاع الإدارة العليا بمشاركة الموظفين وتحفيزهم والتحسين والتطوير المستمر والتخطيط الاستراتيجي، بهدف اتخاذ القرارات بناء على بيانات (بدرجة متوسطة)، كما تبين وجود أثر ذي دلالة إحصائية ثلاثية الأبعاد للجودة الشاملة على الأداء التنظيمي المرتبط بالموارد البشرية

هدفت دراسة (أسير (2009) إلى تقييم النظام المصرفي السوري والكشف عن مدى توافقه مع متطلبات إدارة الجودة الشاملة، وأعلن عدم تلاؤم الخطط والسياسات المصرفية مع متطلبات هذه الإدارة بسبب تقادم القوانين والتشريعات ومركزية العمل، وعدم مقارنة الأداء مع المصارف التنافسية والمعيارية، فضلا عن غياب الخطط الاستراتيجية، وغياب الجودة كفلسفة في العمل، كما بينت الدراسة أن ثقافة التداول في المصارف البحوث غير داعمة لفعالية الجودة الشاملة، إذ إن مكافحة القيادية القائمة لا تدعم الموظف، وإن معايير تقييم الموظفين معايير تقليدية لا تنطوي على جودة الخدمات، كما تبين أن العادات والتقاليد سياسات كالعمل الجماعي في أدنى مستوى فضلا عن غياب الوعي بأهمية الجودة لدى الموظفين وضعف البرامج التدريبية التي لا تتلاءم مع فلسفة الجودة الشاملة.

الفصل الثاني الإطار النظري للبحث

المبحث الأول: المخاطر السيبرانية (المفهوم، الطبيعة، الأنواع، الابعاد) وفق ISO 27001

أولاً. مفهوم المخاطر السيبرانية: يمثل الأمن السيبراني حزمة عمليات وإجراءات تتوخى تأمين وحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو السرقة والوصول غير المصرح به، وكذلك من التعطيل أو العرقلة في الخدمات التي تقدمها، بحسب التعريف المعطى له، في التقرير الصادر عن الاتحاد الدولي للاتصالات، هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين، يمكن تعريف الأمن السيبراني، انطلاقا من أهدافه، بأنه النشاط الذي يؤمن حماية الموارد البشرية، والمالية للدولة، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع إلى ما كان عليه،

بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج وبحيث، لا تتحول الأضرار إلى خسائر دائمة (الجبور، 2021: 32)

أما المخاطر السيبرانية فيقصد بها المخاطر التشغيلية على أصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية وسلامة ونظم المعلومات ومقارنة بفئات المخاطر التي يغطيها التأمين فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسئولية مع مخاطر كل من الممتلكات والخصوم وكذلك المخاطر الكارثية والتشغيلية، ومما لاشك فيه أن تكنولوجيا المعلومات والاتصالات تتيح إمكانات هائلة وغير مسبوقة لإنتاجية أفضل في جميع القطاعات وللتواصل عبر القارات إلا أن البنية التحتية لهذه التقنيات تمثل ارتباطاً بين مصالح متعددة وخدمات مختلفة ودول عديدة الأمر الذي يجعل من الأخطار في المجال السيبراني أخطاراً عالمية فلا يمكن لأي جهة أن تضمن بقاءها في منأى عن الأخطار ما دامت سلامة الآخرين معرضة للخطر.(البغدادي، 2023: 1461)

ثانيا طبيعة المخاطر السيبرانية: مما لا شك فيه أن تكنولوجيا المعلومات والاتصالات، تتيح إمكانات هائلة وغير مسبوقة، لإنتاجية أفضل في جميع القطاعات، وللتواصل عبر القارات. إلا أن البنية التحتية لهذه التقنيات تمثل ارتباطا بين مصالح متعددة، وخدمات مختلفة، ودول عديدة، الأمر الذي يجعل من الاخطار في المجال السيبراني، أخطارا عالمية. فلا يمكن لأي جهة، أن تضمن بقاءها في منأى عن الاخطار، ما دامت سلامة الآخرين معرضة للخطر (ليبتون، 2020: 3).

1. **المخاطر التقنية:** تترافق طبيعة التقنيات والاتصالات، مع اخطار خاصة مرتبطة بهندستها الخاصة، وبالبيئة التي تعمل في اطارها، أي الفضاء السيبيري. وإذا كانت التقنية والرقمنة، تتحكم بتوسع تقنيات المعلومات والاتصالات، وبالولوج إلى الفضاء السيبيري، ورسم حدوده، بما جعل البعض يعتبرونها، قادرة على لعب دور القانون في تنظيم الفضاء السبيراني، وضبط الأعمال المخلة بأمنه وصولا إلى انكارهم على المشرع، حق الاضطلاع بمهمة هذا التنظيم (الربيعية، 2021: 32)

إلا أن هذا الأمر لا يستقيم، فقد أثبتت هذه التقنية أنها ليست قادرة على ضبط التصرف الانساني وتأمين سلامة الأفراد والمؤسسات والدول التي أصبحت أكثر اعتمادا عليها.

فقد عمدت أكثر الدول تقدما إلى لفت الانتباه إلى هشاشة الوضع، فضلا عن الخلل العضوي الذي يعترى البرمجيات والتجهيزات على السواء، والذي يشكل نقاط ضعف يمكن استغلالها بسهولة من قبل الخبراء في خرق الأنظمة المعلوماتية، وإلى حجم المخاطر الذي يرتبها هذا الأمر (Stallings، 2020 :72).

2. **المخاطر القانونية:** تتمثل المخاطر القانونية بشكل أساسي، في غياب الهيكل التشريعي والتنظيمي المناسب للتعامل مع نتائج الأعمال القانونية وغير القانونية منها، والتي تتم في الفضاء السيبراني. فالنشاط الاقتصادي والتجاري وغيره، يتطلب تحديدا واضحا للحقوق والواجبات بما يساهم في تعزيز الثقة بقدرات تكنولوجيا المعلومات والاتصالات، في مجال الخدمات عبر الفضاء الإلكتروني (البغدادي، 2023: 1461).

وعلية، فأن المخاطر القانونية تتمثل في: غياب الأمن القانوني، وتناقض الأحكام والقوانين وتنازع الانظمة القانونية من جهة، وفي اتساع امكانات انتشار الجريمة الإلكترونية من جهة أخرى. إذ يرتفع نسبة هذه المخاطر، مع انعدام أو ضعف التعاون بين الدول المختلفة في ملاحقة مرتكبى تتلاءم الاعتداءات الإلكترونية التي لا تقتصر على الأفراد فحسب بل تمتد لتطول أمن الدول واستقرارها (جبور، 2012: 15)

ثالثاً. أنواع المخاطر السيبرانية: يتمثل تأثير الهجمات السيبرانية من خلال المساس بالجوانب الرئيسية الثلاثة لأمن المعلومات والتي تتمثل في السرية والنزاهة واستمرارية الأداء من خلال: (Stallings، 2020 :72):

1. السرية: حيث تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل الشركة إلى أطراف ثالثة كما في حالة حدوث اختراق البيانات.
2. النزاهة: والتي تتعلق بإساءة استخدام الأنظمة كما هو الحال بالنسبة للاحتيال
3. استمرارية الأداء: والتي تتلخص في تعطل أو التوقف عن ممارسة الأعمال وتتمثل خطوط الدفاع الثلاثة للحد من المخاطر السيبرانية في:

رابعاً. أبعاد الأمن السيبراني: يمكن أن تتعرف المنظمة على كيفية إدارة حماية المعلومات من خلال ثلاثة أبعاد (السرية، السلامة، التوفر) أو كما وصفتها هيئة معايير معالجة البيانات الاتحادية الفيدرالية FIPS، معايير معالجة المعلومات بأحجار الزاوية لحماية المعلومات وذلك من خلال تطبيق نظم إدارة حماية المعلومات، أو باستعمال معايير ايزو 27001 كدليل لتطوير ISMS إدارة امن المعلومات.

يمتد الأمن السيبراني ليشمل جميع المجالات الاقتصادية والاجتماعية والسياسية والقانونية لكافة المجتمعات المعاصرة واستنادا لما سبق فأن الأمن السيبراني يرتبط ارتباطا وثيقاً بسلامة مصادر الثروة والتقدم فالوقت الراهن والتي تشمل القدرة على الاتصال والتواصل والبيانات والمعلومات التي يستند عليها الإنتاج والإبداع والقدرة على المنافسة لذلك تتمثل محددات الأمن السيبراني في الآتي (عبد الرحمن، 2020: 48):

1. **البعد العسكري:** إن بدء استخدام الإنترنت قد تم في بيئة عسكرية ثم تطور الأمر ليشمل البعد الأكاديمي لها بهدف تطوير القدرات العسكرية والإنجازات العلمية التي تضمن تقدم دولة على أخرى خاصة في مجال تطوير الأسلحة النووية ومن أبرز الأمثلة التي يمكن عرضها في هذا المجال لتوضيح الأبعاد العسكرية للأمن السيبراني وخطورة الهجمات السيبرانية ما حدث في جورجيا وكوريا الجنوبية وإيران مثال على بعض الهجمات والاختراقات والتي انتهت بالصراع المسلح لاحق أو بانقطاع الاتصال بالفضاء السيبراني داخل الدولة أو التشويش على الإدارات الحكومي (Clarke & Knake, 2022: 54).
2. **البعد الاجتماعي**: تسمح طبيعة الفضاء السيبراني المفتوحة عبر وسائل التواصل الاجتماعية لكل مواطن بالتعبير عن تطلعاته السياسية وطموحاته الاجتماعية، كذلك تعد فرص ميسرة للاطلاع على الأفكار والمعلومات المتباينة مما يسمح بتبادل الخبرات وتحقيق التعاون والتقارب بين المجتمعات المختلفة كما أنه لا يمكن تجاهل الدور الفضاء السيبراني في تبادل المعلومات في المجالات العلمية والثقافية والخدمية وفي أوقات الأزمات والكوارث.... إلخ إذ لا تقف الأبعاد الاجتماعية عند هذه الحدود فقط بل تتعداها إلى صيانة القيم الجوهرية في المجتمع كالانتماء والمعتقدات فضلا عن العادات والتقاليد.
3. **البعد السياسي:** تتمثل الأبعد السياسية للأمن السيبراني في حق الدولة في حماية نظامها السياسي ومصالحها في وقت تؤثر التقنيات على موازين القوى داخل المجتمع نفسه حيث أصبح من حق المواطن الاطلاع على خلفيات ومبررات القرارات السياسية داخل بلادة والاطلاع على نظيرتها في الدول الأخرى بالمقابل يحاول العاملون في الشأن السياسي الإفادة مما تقدمه هذه التقنيات والترويج لسياساتهم في العالم (Schneier, 2020: :8).

4. **البعد الاقتصادي:** يرتبط الأمن السيبراني ارتباطا وثيقاً بالاقتصاد فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية التي تبحث عن إدارة تكلفة إنتاجها بأفضل الشروط إلا أن هذا الواقع يطرح مسائل مختلفة تتعلق بحماية مقدم الخدمة أو حماية المستهلك على الإنترنت.
5. **البعد القانوني:** يرتب النشاط الفردي والحكومي في الفضاء السيبراني نتائج قانونية تتطلب اهتماما لحل النزاعات التي يمكن أن تنشأ عنها ونظراً لنشأة مجتمع المعلومات وتطوره السريع فقد أضيف إلى قائمة الحقوق الأساسية والحريات المعترف بها في الدساتير والتشريعات الدولية حقوقاً أخرى كحق النفاذ إلى الشبكة العالمية للمعلومات كما توسعت بعض المفاهيم لتشمل أساليب ممارسة واستخدام تقنيات المعلومات والاتصالات كالحق في إنشاء المدونات الإلكترونية والحق في إنشاء التجمعات على الإنترنت والحق في حماية ملكية البرامج المعلوماتية. (البغدادي، 2023: 1461)

المبحث الثاني: تهديدات الامن السيبراني للمصارف واليات مواجهاتها/ ومعوقات تحقيقها لضمان استمرارية الاعمال ISO27001

أولاً. الايزو 27001: يعد التخطيط الإقليمي عنصرًا حاسمًا في تطوير القطاعات الحيوية، بما في ذلك القطاع المصرفي، إذ يؤثر بشكل مباشر على استراتيجيات الأمن السيبراني وإدارة المخاطر. وفي ظل العولمة الرقمية وتوسع الخدمات المصرفية الإلكترونية، أصبح من الضروري دمج التخطيط الإقليمي مع تطبيق معيار ISO/IEC 27001 لضمان حماية البيانات المالية وتعزيز استدامة العمليات المصرفية على المستوى الوطني والإقليمي. في ظل التطور السريع في مجال الخدمات المصرفية الرقمية والاعتماد المتزايد على الأنظمة الإلكترونية، أصبحت حماية المعلومات والبيانات الحساسة أمرًا بالغ الأهمية. تتعرض المؤسسات المالية، وخاصة المصارف، لتهديدات متزايدة مثل الهجمات السيبرانية، الاحتيال المالي، وتسريب البيانات، مما قد يؤثر سلبًا على ثقة العملاء واستقرار الأنظمة المصرفية (علي، 2022: 58):

لذلك، يعد معيار ISO/IEC 27001 أحد أهم المعايير الدولية المعتمدة في مجال إدارة أمن المعلومات(ISMS) ، إذ يوفر إطارًا متكاملاً لتحديد المخاطر، وحماية الأصول المعلوماتية، وتحقيق الامتثال للتشريعات المصرفية والتنظيمية. يساعد هذا المعيار المصارف على تطوير سياسات وإجراءات أمنية صارمة تضمن حماية البيانات المالية، وتأمين المعاملات المصرفية، وتعزيز استمرارية الأعمال (Calder, 2022: 11)

يهدف تطبيق معيار ISO 27001 في المصارف إلى تقليل المخاطر الأمنية، وضمان سرية وسلامة وتوافر المعلومات، مما يساهم في تحسين الأداء المؤسسي وتعزيز ثقة العملاء والشركاء. ومن خلال تنفيذ هذا النظام، يمكن للمصارف حماية بياناتها من الاختراقات، والامتثال للوائح التنظيمية مثل مكافحة غسل الأموال (AML) واعرف عميلك(KYC) ، فضلا عن تحسين جاهزيتها لمواجهة أي تهديدات مستقبلية (ISACA, 2022:24)

ثانياً. مفهوم تكاملية التخطيط الإقليمي في أمن المعلومات المصرفي: إن تكاملية التخطيط الإقليمي تعني التعاون بين الجهات المختلفة ضمن إطار جغرافي معين لضمان تحقيق الأهداف المشتركة، مثل (علي، 2022: 58):

- تنسيق السياسات الأمنية بين المصارف والمؤسسات المالية الإقليمية.

❖ إنشاء بنية تحتية تكنولوجية موحدة تعزز أمن المعلومات.
❖ الامتثال للقوانين واللوائح الإقليمية الخاصة بحماية البيانات المالية.
❖ تعزيز التعاون بين القطاعين العام والخاص في إدارة المخاطر المصرفية.

ثالثاً. دور التخطيط الإقليمي في تطبيق ISO 27001 في المصارف (علي، 2022: 58):

1. **التوافق مع السياسات والتشريعات الإقليمية:** تتطلب المصارف العاملة في مناطق متعددة الامتثال لمعايير الأمن السيبراني التي تختلف من دولة إلى أخرى. إذ يساعد التخطيط الإقليمي على توحيد هذه السياسات وضمان الامتثال لمعايير مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا أو معايير البنك المركزي المحلي.
2. **تطوير بنية تحتية أمنية موحدة:** انشاء مراكز بيانات إقليمية تتمتع بأعلى معايير الأمان لحماية الأنظمة المصرفية. تطوير شبكات اتصال آمنة بين المصارف المركزية والتجارية لتعزيز تبادل المعلومات بأمان.
3. **إدارة المخاطر والأزمات على المستوى الإقليمي:** إنشاء مراكز استجابة للطوارئ الأمنية (SOC Centers) - Security Operation للتعامل مع الهجمات السيبرانية بشكل مشترك.
4. وضع خطط استمرارية الأعمال على مستوى المنطقة لتقليل تأثير الهجمات الإلكترونية على الخدمات المصرفية.
4. تعزيز التعاون بين المؤسسات المالية الإقليمية من خلال:

❖ تبادل المعلومات حول التهديدات الأمنية المحتملة بين البنوك.
❖ تنظيم ورش عمل ومؤتمرات إقليمية حول الأمن السيبراني في المصارف.

5. تنفيذ تمارين محاكاة الاختراقات السيبرانية لاختبار فعالية أنظمة الأمن المصرفي.

رابعاً. فوائد دمج التخطيط الإقليمي مع ISO 27001 في المصارف (عبد الرحمن، 2020: 48)

1. تحسين كفاءة تطبيق ضوابط أمن المعلومات من خلال التنسيق المشترك.
2. تقليل مخاطر الهجمات السيبرانية عبر إنشاء شبكات أمان مصرفية إقليمية.
3. ضمان الامتثال التنظيمي وفقًا للقوانين المحلية والدولية لحماية البيانات المصرفية.
4. تعزيز استمرارية الأعمال والاستجابة الفعالة للأزمات الأمنية عبر الحدود.
5. خفض تكاليف تطبيق المعيار من خلال تبادل الموارد والخبرات بين المؤسسات المالية الإقليمية.

نظام إدارة أمن المعلومات (ISMS) وفقًا لمعيار ISO/IEC 27001 هو إطار عمل معترف به عالميًا يهدف إلى حماية المعلومات من التهديدات المحتملة، مثل الاختراق، الفقدان، أو التعديل غير المصرح به.

خامساً. متطلبات تطبيق ISO 27001 في المصارف (Calder، 2020 :45)

1. **تحديد نطاق نظام إدارة أمن المعلومات (ISMS):** تحديد الأصول المصرفية الهامة، مثل: بيانات العملاء والحسابات المصرفية، أنظمة الدفع والتحويل الإلكتروني، الخوادم وقواعد البيانات، القنوات الرقمية (التطبيقات والمواقع الإلكترونية)، تحديد الجهات ذات العلاقة، مثل الموظفين، العملاء، الجهات التنظيمية، والشركاء التقنيين.
2. **تحليل وإدارة المخاطر**: تقييم التهديدات المحتملة مثل: الهجمات السيبرانية (الاختراق، التصيد الاحتيالي، الفدية الإلكترونية)، الاحتيال المالي والتلاعب في المعاملات، فقدان البيانات بسبب أخطاء

داخلية أو فشل تقني، الامتثال للقوانين واللوائح (مثل مكافحة غسل الأموالAML). من خلال وضع استراتيجيات للحد من المخاطر، مثل:

- ❖ تشفير البيانات المالية والحساسة، تطبيق مصادقة متعددة العوامل (MFA) لحماية الوصول،
- ❖ تنفيذ بروتوكولات كشف الاحتيال والاختراق.

3. **تنفيذ السياسات والإجراءات الأمنية:** تطوير سياسات أمن المعلومات الداخلية، مثل: سياسة حماية بيانات العملاء، سياسة إدارة كلمات المرور والتحكم في الوصول، سياسة النسخ الاحتياطي واستعادة البيانات، سياسة الاستجابة للحوادث الأمنية

1. نموذج سياسة أمن المعلومات في المصارف (Information Security Policy) (عبد الرحمن، 2020: 48):

أ. **الهدف**: تحدد هذه السياسة المبادئ والتوجيهات لضمان سرية وسلامة وتوافر المعلومات المصرفية، والامتثال لمتطلبات معيار ISO/IEC 27001 لحماية بيانات العملاء والأنظمة المصرفية من التهديدات الأمنية.

ب. نطاق التطبيق: تنطبق هذه السياسة على:

- ❖ جميع الموظفين والمتعاقدين في المصرف.
- ❖ جميع الأنظمة والتطبيقات وقواعد البيانات المصرفية.
- ❖ جميع البيانات المتعلقة بالعملاء والمعاملات المالية.

ج. المبادئ الأساسية:

- ❖ السرية (Confidentiality): حماية المعلومات من الوصول غير المصرح به.
- ❖ السلامة (Integrity): ضمان دقة البيانات وعدم تعديلها بطرق غير مصرح بها.
- ❖ التوافر (Availability): ضمان الوصول إلى المعلومات والأنظمة عند الحاجة إليها.

2. نموذج سياسة التحكم في الوصول (Access Control Policy) (Stallings, 2020 :142)

أ. **الهدف**: تحديد آليات التحكم في الوصول لضمان أن الأفراد المخوّلين فقط هم من يمكنهم الوصول إلى الأنظمة المصرفية والبيانات الحساسة.

ب. قواعد التحكم في الوصول

- ❖ استخدام المصادقة متعددة العوامل (MFA) لجميع الأنظمة المصرفية.
- ❖ تطبيق مبدأ الحد الأدنى من الصلاحيات (Least Privilege) لمنح الوصول فقط عند الحاجة.
- ❖ مراجعة صلاحيات المستخدمين كل 6 أشهر لضمان عدم وجود صلاحيات زائدة.
- ❖ تسجيل جميع محاولات تسجيل الدخول والخروج من الأنظمة الحساسة.

3. نموذج سياسة إدارة الحوادث الأمنية (Incident Management Policy) (White, 2022 :45)

أ. **الهدف:** توفير إطار عمل موحد للاستجابة للحوادث الأمنية لضمان تقليل تأثيرها واستعادة الأنظمة المصرفية بسرعة.

ب. إجراءات الاستجابة للحوادث: الإبلاغ عن الحوادث: يجب على جميع الموظفين الإبلاغ فورًا عن أي حادث أمني إلى فريق أمن المعلومات.

- ❖ تحليل الحادث: يتم تحليل الحادث لتحديد مصدره وتأثيره.
- ❖ الاستجابة والتخفيف: يتم عزل الأنظمة المتضررة ومنع الانتشار.
- ❖ الإبلاغ القانوني: يتم إخطار الجهات التنظيمية وفقًا للمتطلبات المحلية.

❖ تحليل ما بعد الحادث: يتم إجراء مراجعة لاستخلاص الدروس وتحسين الإجراءات المستقبلية.

سادساً. أبعاد الأداء المصرفي: تتمثل أبعاد الأداء المصرفي من خلال الآتي (إبراهيم الكرسانة، 2006: 4):

1. **الفاعلية**: الفاعلية المصرفية تعني قدرة المصرف على تحقيق أهدافه المالية والإدارية والتشغيلية بأعلى مستوى من الكفاءة والجودة، وبأقل الموارد والتكاليف، مع ضمان الاستمرارية وتقليل المخاطر.

هي مؤشر على مدى نجاح المصرف في إدارة موارده، وخدماته، وتقنياته، وموظفيه، وعلاقته بالزبائن، مقارنةً بما هو مخطط له. هي قدرة المصرف على تحقيق أهدافه المالية والإدارية من خلال الاستخدام الأمثل للموارد، وتحسين جودة الخدمات، وتعزيز الأداء التشغيلي، والحد من المخاطر. ويتم قياس الفاعلية المصرفية عادةً من خلال مؤشرات مالية وتشغيلية وإدارية، تُظهر مدى نجاح المصرف في تنفيذ استراتيجياته وتحقيق نتائج ملموسة بعد تطبيق الأنظمة أو السياسات المعتمدة.

2. **الكفاءة**: الكفاءة المصرفية تعني قدرة المصرف على استغلال موارده المالية والبشرية والتكنولوجية بأفضل صورة ممكنة من أجل تحقيق أعلى مخرجات بأقل التكاليف والجهد والوقت.

وهي مقياس يوضح مدى قدرة المصرف على العمل بكفاءة داخل بيئة تنافسية وتقديم خدمات مالية ذات جودة عالية مع خفض الهدر والتكاليف التشغيلية.

3. **الإنتاجية**: الإنتاجية المصرفية تعني قدرة المصرف على تحقيق أكبر قدر ممكن من المخرجات (الخدمات المصرفية، المعاملات، الأرباح) باستخدام كمية محدودة من المدخلات (الموظفين، الوقت، التكاليف، التكنولوجيا).

هي مؤشر أساسي لمدى تحسن أداء المصرف وكفاءته وجودة خدماته داخل السوق المصرفي.

الفصل الثالث الجانب العملي (الدراسة الميدانية):

اولاً. مجتمع وعينة الدراسة: يتكون مجتمع الدراسة من شركات العاملة في مجال الامن السيبراني (تكنلوجيا المعلومات والاتصالات) والمتعاونة بعقود مع المصارف، والمصارف العاملة في العراق، وقد تم اختيار عينة عشوائية المجتمع الدراسة من تلك الشركات والمصارف بلغ عددها خمس شركات لتكنولوجيا المعلومات (تصميم المواقع والبرامج الخاصة المصرفية) بواقع 70 استمارة، وسبع شركات اتصالات(تجارة أدوات الاتصالات الذكية التي تدخل بالأمور المالية) بواقع 90 استمارة، وأربعة مصارف (مختارة) بواقع 110 استمارة، وقد تم توزيع استمارات الاستبيان داخل تلك الشركات والمصارف على الفئات الآتية من خلال الكوكل فورم:

1. المديرين الماليين والمحاسبين بعدّهم القائمين على التعامل مع نظم المعلومات المحاسبية الالكترونية.
2. الموظفين في إدارة تكنولوجيا المعلومات IT من متخصصين ومراجعي نظم المعلومات الالكترونية ومديري الإدارات.
3. المراجعين الخارجين الذين يقومون بمراجعة أنظمة تلك الشركات والمصارف.

ويمكن توضيح التوزيع النسبي المفردات العينة من خلال الجدول الآتي:

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (2): 181-201
Doi: www.doi.org/10.25130/tjaes.22.SP7.2.10

جدول (1): التوزيع النسبي لاستمارات الاستقصاء على مفردات العينة

مفردات العينة	العدد	النسبة
شركات تكنولوجيا	70	%26
شركة الاتصالات	90	%34
المصارف	110	%40
الإجمالي	270	%100

ثانياً. إدخال ومعالجة البيانات: قام الباحث بمراجعة استمارات الاستبيان للتأكد من اكتمالها وصلاحيتها لإدخال البيانات والتحليل الإحصائي، وتم استبعاد الاستمارات التي لا تتوافر فيها الشروط اللازمة، ويوضح الجدول الآتي عينة الدراسة ومعدلات الإجابة الصحيحة القابلة للتحليل من بين مفردات العينة.

جدول (2): عدد الاستمارات المرسلة، والواردة والمستبعدة والصحيحة

مفردات العينة	المرسل	الوارد		المستبعد		الصحيح	
		العدد	النسبة	العدد	النسبة	العدد	النسبة
شركات تكنولوجيا المعلومات	70	67	%84	17	%21	50	%63
شركات الاتصالات	90	78	%78	20	%20	58	%58
المصارف	110	98	%82	9	%7.5	89	%74
الإجمالي	270	243	%81	46	%15	197	%66

ثالثاً. أساليب التحليل الإحصائي للبيانات: قام الباحث بتفريغ الإجابات عن الأسئلة بجداول البيانات، وتم تحليلها بهدف تحديد مدى تحقق فروض الدراسة واستخلاص النتائج من خلال تطبيق بعض الأساليب الإحصائية الواردة بمجموعة البرامج الإحصائية للعلوم الاجتماعية (SPSS) وتحديد تم الاستعانة بالأساليب الآتية:

أساليب الإحصاء الوصفي:

❖ الوسط الحسابي.

الصيغة الرياضية:

$$\bar{X} = \frac{\sum_{i=1}^{n}}{}$$

- $\bar{X}$: الوسط الحسابي
- X_i: القيمة رقم (i)
- n: عدد القيم
- $\sum$: مجموع القيم

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (2): 181-201
Doi: www.doi.org/10.25130/tjaes.22.SP7.2.10

❖ الانحراف المعياري.

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(X_i - }{n}}$$

$$s = \sqrt{\frac{\sum_{i=1}^{n}(X_i - }{n-1}}$$

- σ: الانحراف المعياري للمجتمع
- s: الانحراف المعياري للعينة
- $(X_i - \bar{X}$: مربع الفرق بين القيمة والوسط
- $n - 1$: معامل التصحيح للعينة

❖ التكرار والنسبة..

أساليب الإحصاء الاستدلالي:

❖ اختبار المصداقية والاعتمادية.

❖ اختبار " ت ".

❖ اختبار فريدمان.

❖ اختبار كروسكال والاس.

❖ اختبار "كا2"

رابعاً. نتائج الاختبارات الإحصائية لفروض الدراسة:

1. **اختبار الثبات والصدق:** ويطلق عليه معامل ثبات ألفا، وهو مقياس يوضح مدى الاعتماد على نتائج قائمة الاستقصاء، ومدى إمكانية تعميم النتائج على مجتمع الدراسة، وكذلك يوضح ثبات المحتوى المتغيرات الدراسة. وقد بلغت قيمة معامل الثبات للاستمارة ككل 0.98 ومعامل الصدق وهو الجذر التربيعي المعامل الثبات 0.99 مما يدل على ثبات أداة البحث ووجود درجة كبيرة من الاتساق الداخلي بين عبارات قائمة الاستقصاء ككل.
2. **التحليل الوصفي:** تم استخدام تحليل التباين لتوصيف آراء العينة حول مخاطر الأمن السيبراني التي تتعرض لها نظم المعلومات المصرفية الالكترونية من خلال المقاييس الإحصائية (الوسط الحسابي، واختبار " ت "، الانحراف المعياري)، وذلك كما يوضحه الجدول رقم (3) فيما يأتي:

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (2): 181-201
Doi: www.doi.org/10.25130/tjaes.22.SP7.2.10

جدول (3): توصيف الآراء من خلال المقاييس الإحصائية حول المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية

السؤال	العدد	الوسط الحسابي	الانحراف المعياري	T.Test
ادخال غير متعمد لبيانات غير سليمة بواسطة الموظفين(كشف التهديدات والاستجابة IAM)	197	4.29	1.09	0.00
ادخال معتمد لبيانات غير سليمة بواسطة الموظفين	197	2.88	0.93	0.00
تدمير غير متعمد لبيانات بواسطة الموظفينAC	197	4.21	1.16	0.00
تدمير متعمد لبيانات بواسطة الموظفينVM	197	2.94	0.98	0.00
دخول غير مصرح به للبيانات بواسطة الموظفين		4.20	1.16	0.00
تبادل الموظفين لكلمات المرور بدون تشفير(Een)	197	4.08	1.22	0.00
ادخال الفيروسات الحاسب الى النظام المالي المصرفي	197	4.21	1.24	0.00
تدمير او سرقة بعض المعلومات من خلال هكرMP	197	4.08	1.24	0.00
عمل نسخ غير مصرح به من مخرجات النظام BDR	197	4.28	1.16	0.00
عرض بيانات سرية على شاشات العرض ادارة الهوية والتحقق (TDR)	197	4.16	1.10	0.00
كوارث طبيعية مثل الحرائق او انقطاع الطاقة SAT	197	4.16	1.19	0.00
مخاطر خارجية متمثلة في البرنامج الخبيثة والاختراقات...وغيرها بلا تفعيل الجدران الناريةFIW	197	4.40	1.04	0.00
الإجمالي	197	4	1.13	0.00

** دال إحصائيا عند مستوى معنوية 0.05

ويتضح من الجدول السابق أن الوسط الحسابي العام يميل إلى الموافقة على أن العناصر التي تم ذكرها تمثل المخاطر التي تتعرض لها نظم المعلومات المصرفية، وذلك بوسط حسابي عام قيمته (4) - وانحراف معياري عام (1.13).

ومن ثم يشير الانحراف المعياري إلى انخفاض التشتت أي يوجد تجانس في الآراء حول تلك المخاطر، كما يشير اختبار " ت " إلى أن النتائج أقل من مستوى معنوية (0.05) بمعنى أن الفروق معنوية وجميع العناصر - بصفة عامة - تعد من المخاطر التي تتعرض لها نظم المعلومات المصرفية الالكترونية.

3. **اختبار فريدمان:** يوضح هذا الاختبار الأهمية النسبية للعبارات أي معرفة العنصر الأكثر أهمية من وجهة نظر مفردات العينة بشأن المخاطر السيبرانية وفق 27001 التي تتعرض لها نظم المعلومات المصرفية المحاسبية الالكترونية، وذلك من خلال متوسط الرتب إذ يأخذ العنصر الأكثر أهمية من وجهة نظر مفردات العينة أعلى متوسط للرتب ويتضح ذلك من خلال الجدول الآتي:

جدول (4): ترتيب الأهمية النسبية للمخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية

السؤال	متوسط الرتب	مستوى العينة
مخاطر خارجية متمثلة في البرامج الخبيثة والاختراقات...وغيرها	8.25	0.00
ادخال غير متعمد لبيانات غير سليمة بواسطة الموظفين	7.74	
عمل نسخ غير مصرح بها من مخرجات النظام	7.57	
ادخال فيروسات الحاسوب الى النظام المحاسبي	7.40	
تدمير متعمد لبيانات بواسطة الموظفين	7.39	
دخول غير مصرح به للبيانات بواسطة الموظفين	7.28	
كوارث طبيعية مثل الحرائق او انقطاع الطاقة	7.10	
عرض بيانات سرية على شاشات العرض	7.02	
تدمير او سرقة بعض المعلومات	6.69	
تبادل الموظفين لكلمات المرور	6.67	
تدمير معتمد للبيانات بواسطة الموظفين	2.52	
ادخال متعمد لبيانات غير سليمة بواسطة الموظفين	2.35	

دال إحصائيا عند مستوى معنوية 0,05

ويتضح من الجدول السابق ما يأتي:

1. أن مستوى المعنوية أقل من 0.05 مما يدل على وجود اختلاف معنوي في الأهمية النسبية من وجهة نظر مفردات العينة حول مخاطر الأمن السيبراني في نظم المعلومات المصرفية.
2. إن أعلى متوسط للرتب يتمثل في أن المخاطر الخارجية المتمثلة في البرامج الخبيثة والاختراقات السيبرانية المختلفة، تعد من أهم المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية، بينما يتمثل كل من التدمير المتعمد للبيانات والإدخال المتعمد لبيانات غير سليمة من أقل المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية حيث أنها تأخذ أقل مستوى للرتب.

4. **اختبار كروسكال والاس:** ويتم إجراء هذا الاختبار لقياس التباين - الاتفاق والاختلاف - في أراء مفردات العينة حول المخاطر السيبرانية التي تتعرض لها نظم المعلومات المحاسبية الالكترونية، ويتضح ذلك من خلال الجدول الآتي:

نظم المعلومات المصرفية الالكترونية:

جدول (5): قياس التباين في أراء مفردات العينة حول مخاطر

البيان	مفردات العينة	العدد	متوسط الراتب	مستوى المعنوية
مخاطر الامن السيبراني في النظام المصرفي المحاسبي الالكتروني	شركات تكنولوجيا المعلومات	50	98.01	0.491
	شركات الاتصالات	58	91.86	
	المصارف	89	103.10	

ويتضح من الجدول السابق أن مستوى المعنوية للعناصر الممثلة لمخاطر الأمن السيبراني في نظم المعلومات المحاسبية الالكترونية مجتمعة أكبر من (0.05) مما يعني وجود اتفاق في آراء مفردات العينة حول اختلاف الأهمية النسبية للمخاطر التي تتعرض لها نظم المعلومات المصرفية الالكترونية.

وبناء على نتائج التحليل السابق فقد ثبت صحة الفرض الأول للدراسة والذي ينص على: "تختلف الأهمية النسبية للمخاطر السيبرانية التي تتعرض لها جودة الادارة المصرفية الالكترونية".

خامساً. نتائج اختبار الفرض الثاني: ينص الفرض الثاني للدراسة على: "يؤدي عدم وجود سياسات وبرامج محددة لأمن المعلومات السيبرانية إلى زيادة المخاط التي تتعرض لها نظم المعلومات المصرفية الالكترونية" أي بمعنى آخر أثر المخاطر السيبرانية.

1. **التحليل الوصفي:** يوضح الجدول الآتي توصيف آراء العينة بشأن أسباب حدوث مخاطر الأمن السيبراني في جودة الادارة المصرفية لنظم المعلومات المصرفية المحاسبية الالكترونية من خلال المقاييس الإحصائية الوسط الحسابي والانحراف المعياري واختبار " ت ":

جدول (6): توصيف الآراء حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية

السؤال	العدد	الوسط الحسابي	الانحراف المعياري	T.Test
1-عدم توافر الخبرة اللازمة والتدريب الكافي للموظفين على مفردان وبنود تحقيق الامن السيبراني وفق الايزو 27001	197	1,22	1,22	** 0,00
2- عدم توافر الحماية الكافية ضد مخاطر الفيروسات من خلال تفعيل برامج المكافحة وتفعيل الجدار الناري	197	4,05	1,22	** 0,00
3- عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمي وفق مصفوفات الاعمال المصرفية IAM	197	4,20	1,25	** 0,00
4- عدم وجود سياسات وبرامج محددة لامن السيبراني وتطبيق متطلباته على نظم المعلومات (المتثال للتشريعات(CR	197	2,28	1,24	** 0,00
5- عدم تطبيق مبادى ومعايير حكومة امن المعلومات DR	197	4,20	1,25	** 0,00
الإجمالي	197	4,19	1,29	

** دال احصائيات عند مستوى معنوية (0,05)

من الجدول السابق أن الوسط الحسابي العام يميل إلى الموافقة حول أسباب المخاطر التي تتعرض لها نظم المعلومات المصرفية الالكترونية، وذلك بوسط حسابي عام (4.19)، وانحراف معياري (1.19)، مما يشير إلى انخفاض التشتت أي يوجد تجانس في الآراء بشأن تلك الأسباب، كما يشير اختبار " ت " إلى أن النتائج أقل من مستوى معنوية (0.05) بمعنى أن الفروق معنوية وجميع

العناصر تعد من ضمن الأسباب التي تؤدي إلى زيادة مخاطر الأمن السيبراني في نظم المعلومات المصرفية المحاسبية.

2. **اختبار فريدمان:** يوضح الجدول الآتي قياس وترتيب الأهمية النسبية لأسباب حدوث مخاطر الأمن السيبراني على جودة ادارة نظم المعلومات المصرفية الالكترونية:

نظم المعلومات المصرفية الالكترونية

جدول (7): ترتيب الأهمية النسبية حول أسباب حدوث مخاطر

السؤال	متوسط الرتب	مستوى العينة
1-عدم وجود سياسات وبرامج محددة لامن نظم المعلومات	3,20	**00,00
2- عدم توافر الخبرة اللازمة والتدريب الكافي للموظفين	3,04	
3- عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمي	3,01	
4- عدم تطبيق مبادى ومعايير حكومة امن المعلومات	2,98	
5- عدم توافر الحماية الكافية ضد مخاطر الفيروسات	2,77	

** دال احصائيات عند مستوى معنوية (0,05)

ويتضح من الجدول السابق ما يأتي:

أ. أن مستوى المعنوية أقل من (0.05) مما يدل على وجود اختلاف معنوي في الأهمية النسبية من وجهة نظر مفردات العينة بشأن أسباب حدوث مخاطر الأمن السيبراني على نظم المعلومات المصرفية الالكترونية.

ب. إن أعلى متوسط للرتب يتمثل في أن عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات يُعد من أهم أسباب حدوث مخاطر الأمن السيبراني في نظم المعلومات المصرفية، بينما يتمثل أقل متوسط للرتب في عدم توافر الحماية الكافية ضد مخاطر الفيروسات.

3. **اختبار كروسكال والاس:** يوضح الجدول الآتي قياس التباين في أراء مفردات العينة حول أسباب حدوث مخاطر الأمن السيبراني في نظم المعلومات المصرفي الالكتروني.

نظم المعلومات المصرفية الالكترونية:

جدول (5): قياس التباين في آراء مفردات العينة حول أسباب حدوث مخاطر

البيان	مفردات العينة	العدد	متوسط الراتب	مستوى المعنوية
أسباب حدوث مخاطر الامن السيبراني على نظم المعلومات المصرفية	شركات تكنلوجيا المعلومات	50	108,16	0,491
	شركات الاتصالات	58	98,94	
	المصارف	89	93,89	

ويتضح من الجدول السابق أن مستوى المعنوية لأسباب حدوث مخاطر الأمن السيبراني على نظم المعلومات المصرفية الالكترونية أكبر من (0.05) مما يعني وجود اتفاق في آراء مفردات العينة حول اختلاف أسباب حدوث مخاطر الأمن السيبراني على نظم المعلومات المصرفية الالكترونية.

Tikrit Journal of Administrative and Economic Sciences, Vol. 22, No. Special Issue, Part (2): 181-201
Doi: www.doi.org/10.25130/tjaes.22.SP7.2.10

وبناء على نتائج التحليل السابق يتضح ثبوت صحة الفرض الثاني للدراسة والذي ينص على: **"يؤدي عدم وجود سياسات وبرامج محددة لأمن المعلومات إلى زيادة المخاطر الاسيبرانية التي تتعرض لها نظم المعلومات المصرفية الالكترونية ".**

سادساً. نتائج اختبار الفرض الثالث: ينص الفرض الثالث للدراسة على: " تعمل المصارف والهيئات المالية العراقية ذات العلاقة على تطبيق حوكمة أمن المعلومات في الحد من مخاطر الأمن السيبراني في نظم المعلومات المصرفية الالكترونية ".

جدول (9): التوزيع التكرار والنسبي، واختبار كا 2، واختبار كروسكال والاس حول مدى قيام العينة بتطبيق حوكمة أمن المعلومات

البيان	التكرار	النسبة	اختبار كا2		اختبار كروسكال والاس		
			مستوى المعنوية	الدلالة الإحصائية	مفردات العينة	متوسط الراتب	مستوى المعنوية
لا	143	72,6	**0,00	معنوي	شركات تكنلوجيا المعلومات	101,69	**0,46
نعم	54	27,4			شركات الاتصالات	99,25	
الاجمالي	197	100			البنوك	95,44	

** دال إحصائيا عند مستوى معنوية (0.05).

ويتضح من الجدول السابق أن أكثر مفردات العينة لا تقوم بتطبيق حوكمة أمن المعلومات ضمن إستراتيجيتها للحد من مخاطر الأمن السيبراني في نظم المعلومات المحاسبية الالكترونية عامة ونظم المعلومات المصرفية خاصة وذلك بنسبة 72.6% من إجمالي حجم العينة، عند مستوى معنوية أقل من (0.05)، مما يدل على وجود فروق ذات دلالة إحصائية في آراء مفردات العينة، كما تبين من اختبار " كروسكال والاس " أن مستوى المعنوية أكبر من (0.05) الأمر الذي يدل على وجود اتفاق بين أراء مفردات العينة بشأن عدم تطبيق الجهات التي يعملون بها في الحوكمة للمعلومات احد اهم بنود تحقيق الامن السيبراني وفق الايزو 27001 ومفرداته. والجدول التالي يوضح التوزيع التكرار والنسبي، واختبار كا 2 واختبار " كروسكال والاس " بشأن قيام عينة الدراسة بتطبيق معايير دولية خاصة بأمن المعلومات.

جدول (10): التوزيع التكرار والنسبي كا 2 واختبار " كروسكال والاس " حول مدى قيام عينة الدراسة بتطبيق معايير دولية خاصة بأمن المعلومات

البيان	التكرار	النسبة	اختبار كا2		اختبار كروسكال والاس		
			مستوى المعنوية	الدلالة الإحصائية	مفردات العينة	متوسط الراتب	مستوى المعنوية
لا	94	47,7	**0,00	معنوي	شركات تكنلوجيا المعلومات	96,75	**0,93
نعم	103	52,3			شركات الاتصالات	100,15	
الاجمالي	197	100			البنوك	99,52	

ويتضح من الجدول السابق أن نسبة 52.3% من إجمالي حجم العينة تقوم بتطبيق معايير دولية خاصة بأمن المعلومات (الأمن السيبراني)، وذلك عند مستوى معنوية أقل من (0.05)، مما يدل على وجود فروق ذات دلالة إحصائية في أراء مفردات العينة، كما يتضح من نتائج اختبار " كروسكال والاس " أن مستوى المعنوية أكبر من (0.05) مما يدل على وجود اتفاق بين آراء مفردات العينة بشأن تطبيق معايير دولية خاصة لأمن المعلومات (الأمن السيبراني).

ومن ثم يتضح للباحث ثبوت خطأ الفرض الثالث للدراسة، " تعمل المصارف والهيئات المالية العراقية ذات العلاقة على تطبيق حوكمة أمن المعلومات في الحد من مخاطر الأمن السيبراني في نظم المعلومات المصرفية الالكترونية ".

الفصل الرابع: الاستنتاجات والتوصيات

المبحث الأول: الاستنتاجات

استنتاجات الدراسة النظرية:

1. تتعدد صور المخاطر التي تتعرض لها نظم المعلومات المصرفية الالكترونية ما بين مخاطر داخلية ومخاطر خارجية، وتعد المخاطر الداخلية من أكثر المخاطر تهديدا لنظم المعلومات المحاسبية.
2. 2_تتمثل أسباب حدوث تلك المخاطر في: نقص تدريب الموظفين على استخدام وحماية نظم المعلومات، وسوء اختيارهم، وعدم وجود ضوابط وإجراءات كافية تعمل على معالجة والوقاية من حدوث هذه المخطر.
3. لا تكفي الحلول الالكترونية بمفردها في مواجهة المخاطر المختلفة التي تتعرض لها نظم المعلومات المحاسبية الالكترونية، ومن ثم يجب على الشركات اتباع منهج متكامل الإدارة أمن المعلومات (الأمن السيبراني (بحيث يقوم على تقييم التكنولوجيا المستخدمة وتقييم سلوكيات الأفراد والاهتمام بالجوانب التنظيمية حتى يسهل التنبؤ بالمخاطر وإحباط أي محاولة للقيام بها).

أستنتاجات الدراسة الميدانية: في ضوء استخدام الأساليب الإحصائية الوصفية والاستدلالية تم التوصل إلى النتائج الآتية:

1. يوجد اتفاق معنوى وتجانس في الآراء بين مفردات عينة الدراسة بشأن تعدد المخاطر السيبرانية التي تتعرض لها نظم المعلومات المصرفية الإلكترونية، وتعد المخاطر الخارجية متمثلة في البرامج الخبيثة والاختراقات وغيرها من أكثر المخاطر أهمية أكثرها تكرارا، (بينما بعد التدمير المتعمد للبيانات والإدخال المتعمد لبيانات غير صحيحة من أقل المخاطر أهمية أقلها تكرارا).
2. هنالك اتفاق في آراء مفردات العينة بشأن اختلاف الأهمية النسبة للمخاطر السيبرانية التي تتعرض لها نظم المعلومات المصرفية الإلكترونية.
3. يوجد اتفاق في أراء مفردات العينة حول تعدد أسباب حدوث مخاطر الأمن السيبراني على نظم المعلومات المصرفية الإلكترونية، متمثلا بعدم وجود سياسات وبرامج محددة لأمن المعلومات من أهم تلك الأسباب.
4. يقوم عدد كبير من مفردات العينة بتطبيق المعايير الدولية لحوكمة أمن المعلومات وفق الايزو 27001 بصورة منفردة، إلا أنها لا تعمل على تطبيق حوكمة أمن المعلومات. ضمن استراتيجية المصارف والمؤسسات ذات الاعلاقة - للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية بصوره عامة على الرغم من إدراك مفردات العينة لأهمية تطبيق حوكمة أمن المعلومات والقواند المتحققة منها.

المبحث الثاني: التوصيات

في إطار ما جاء بالجزء النظري، وما أكدته الدراسة الميدانية فيمكن لنا تقديم التوصيات الآتية:

1. زيادة الاهتمام بتوعية المؤسسات المالية عامة والمصرفية بصوره خاصة بأهمية استخدام مبادئ ومعايير حوكمة أمن المعلومات حتى يتسنى لها مواجهة التحديات والمخاطر التي تواجه بيئة تكنولوجيا المعلومات، وفق المتغيرات الدورية والعرضية والفجائية التي تصيب النظام العامل المخطط والمرجو منه تحقيق أهدافه التي رسمت له.
2. الاهتمام بإعداد دورات تدريبية خاصة بتكنولوجيا المعلومات وخاصة فيما يخص بالأمن السيبراني والتعريف على أهم بنوده وفق الايزو 27001 للإلمام بالتطورات الحديثة في هذا المجال، والتعرف على الجرائم المحتملة المرتبطة بها وكيفية مواجهتها ولمتابعة التطورات المتلاحقة في مجال المعايير الدولية لأمن المعلومات.
3. قيام ديوان الرقابة المالية أو وزارة المالية كمثال أو البنك العراقي المركزي، بإلزام المؤسسات المالية والمصارف بتطبيق المعايير الدولية الخاصة بحوكمة أمن المعلومات داخل هذه المؤسسات المالية ذات العلاقة والمتداخلة في مصفوفة أعمالها عامة حتى تزيد درجة الثقة والمصداقية في المعلومات والبيانات التي تقوم تلك المؤسسات بالإفصاح عنها عبر الموقع الإلكتروني لها.
4. قيام وزارة المالية - مركز الدراسات والتخطيط والتدريب - بإعداد دليل قواعد ومعايير حوكمة أمن المعلومات" كمرفقات الدليل قواعد ومعايير حوكمة المؤسسات المالية " حتى يتسنى لهذه المؤسسات معرفة أهمية حوكمة أمن المعلومات وخطورة عدم تنفيذها على سمعتها محليا واقليميا وعالميا.

المصادر

اولاً. المصادر العربية:

1. البغدادي، مروة فتحي السيد، (2023)، اقتصاديات الأمن السيبراني في القطاع المصرفي .مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، المجلد 76.
2. جبر، غريب، (2023)، تهديدات الأمن السيبراني للمصارف الإلكترونية وآلية مواجهاتها .المجلة الأكاديمية للعلوم الاجتماعية، المجلد 1، العدد 1.
3. جبور، منى الأشقر، (2012)، الأمن السيبراني: التحديات ومستلزمات المواجهة .جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، بيروت.
4. الربيعية، محمد بن عبد الله، (2021)، الأمن السيبراني: التحديات والاستراتيجيات .مركز البحوث والدراسات الأمنية، الرياض.
5. عبد الرحمن، محمد، (2020)، أمن المعلومات في البنوك: دفتر معيار .(ISO 27001) دار الجامعة الجديدة، مصر.
6. علي، أحمد محمد، (2022)، دور التخطيط الإقليمي في تعزيز أمن المعلومات المصرفية .مجلة الأمن السيبراني، العدد 12.
7. الكرسانة، إبراهيم، (2006)، طرق أساسية ومعاصرة في الرقابة على البنوك وإدارة المخاطر . صندوق النقد العربي، أبوظبي.
8. ليبتون، ديفيد، (2020)، تهديدات الأمن الإلكتروني تدعو إلى تحرك عالمي .صندوق النقد الدولي.

ثانياً. المصادر الأجنبية:

1. Calder, Alan (2020). ISO 27001 for Banks: A Practical Guide. IT Governance Publishing.
2. Clarke, Richard A. & Knake, Robert K. (2022). The Fifth Domain: Defending Our Country, Our Companies and Ourselves in the Age of Cyber Threats.
3. ISACA (2022). Implementing ISO 27001 in Banks: A Global Perspective. ISACA.
4. Schneier, Bruce (2020). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.
5. Stallings, William (2020). Computer Security: Principles and Practice (4th Edition). Pearson.
6. White, Emily (2022). Penetration Testing and Risk Management in Banking. Journal of Cybersecurity in Finance.