



## أثر مخاطر الأمن السيبراني في جودة التدقيق الإلكتروني في البنوك الأردنية

أ.د. عماد يوسف الشيخ\*\*

رشا حسن الغزي\*

### الملخص

هدف هذا البحث الى بيان أثر مخاطر الأمن السيبراني بأبعاده (مخاطر أمن المعلومات، المخاطر التكنولوجية والتشغيلية، مخاطر الأداء) في جودة التدقيق الإلكتروني في البنوك الأردنية، تم استخدام المنهج الوصفي التحليلي من خلال توظيف الاستبانة واستخدام عدد من الأساليب الإحصائية كالمتوسط الحسابي والانحراف المعياري ومعامل الانحدار المتعدد، وبرنامج spss لتحليل البيانات واختبار الفرضيات، تمثلت العينة من العاملين في الدوائر (المالية والتدقيق الداخلي وتكنولوجيا المعلومات) في البنوك الأردنية، مع تضمين المدققين الداخليين والمحاسبين والتقنيين في هذه الأقسام، ولهذا فقد قام الباحثان بتوزيع (180) استبانة إلكترونية وتم استرجاع (167) استبانة، جميعها صالحة للتحليل، أظهر نتائج البحث وجود أثر إيجابي ذي دلالة إحصائية عند مستوى معنوية (0.05 < α) لمخاطر الأمن السيبراني بأبعاده في جودة التدقيق الإلكتروني، وأوصى البحث بالاستمرار على العمل في تمكين الضوابط الأمنية السيبرانية اللازمة للحد من تأثير المخاطر على جودة التدقيق الإلكتروني وضرورة التطوير المستمر في برنامج تدريب الموظفين حول مخاطر أمن المعلومات. الكلمات المفتاحية: مخاطر الأمن السيبراني، جودة التدقيق الإلكتروني، البنوك الأردنية.

\* طالبة دكتوراة، جامعة العلوم الإسلامية العالمية. rasha.alghazy1@icloud.com

\*\* كلية المال والأعمال، جامعة العلوم الإسلامية العالمية.

### 1.1 المقدمة:

في ظل عالم يزداد فيه الترابط والرقمنة، يزداد معه أيضاً انتشار واسع للأخطار ومنها خطر الهجمات السيبرانية على كافة القطاعات الاقتصادية، حيث إنّ التطور السريع في مجالات تكنولوجيا المعلومات، واستخدامها في مختلف القطاعات وخاصة في عمليات البنوك سيؤدي إلى التعرض لمخاطر الأمن السيبراني بشكل متزايد، مما قد تنعكس تلك المخاطر بشكل سلبي على الاستقرار المالي لهذا القطاع، حيث قد تعمل على تهديد عملياته المحلية والخارجية وتهديد المتعاملين معه، وبذلك قد تزداد الجرائم السيبرانية وعمليات الاحتيال والنصب، وقد تزداد معه مخاطر الاختراق لبيانات هذا القطاع.

كما أن زيادة استخدام تكنولوجيا الأعمال من قبل البنوك أدى إلى استخدام مجموعة من تكنولوجيا المعلومات التي تتصف بالتعقيد مثل حفظ البيانات على وسائط الكترونية بدلاً من وسائط ورقية، وبذلك قد أصبح من المهم استخدام التقنيات الرقمية، وبما أن أساليب التدقيق تتأثر بيئة نظم المعلومات المحاسبية، فقد أصبح من المهم على مدقي الحسابات تطوير مهاراتهم من أجل مواكبة التطور التكنولوجي السريع، والاستفادة من آثاره الإيجابية، ومواجهة المخاطر والتحديات التي يفرضها، وبالتالي تحسين جودة التدقيق المطلوبة من المدقق بما يكفل تحسين وزيادة موثوقية الرقابة الداخلية، وباعتبار قطاع البنوك من أهم القطاعات الاقتصادية، ونظراً لظهور تحديات متعددة أهمها مخاطر الأمن السيبراني، الأمر الذي أدى إلى زيادة أهمية جودة التدقيق الإلكتروني؛ لضمان سلامة العمليات المالية وحماية معلومات المتعاملين المالية، جاء هذا البحث لمعرفة أثر مخاطر الأمن السيبراني في جودة التدقيق الإلكتروني في البنوك الأردنية.

#### 1.1 مشكلة البحث وأسئلته:

غالباً ما تواجه جودة التدقيق الإلكتروني في البنوك العديد من التحديات التي يمكن إرجاعها إلى طبيعة أعمال التدقيق الإلكترونية التي تقتضي توفر شروط بيئية مناسبة حتى يتمكن المدقق من أداء مهامه بجودة وفاعلية، ويكمن التحدي بمواكبة التغيرات الديناميكية السريعة للمخاطر السيبرانية المتغيرة بسرعة في البنوك الأردنية، ذلك الأمر الذي من شأنه أن يقلل من قدرة

التدقيق الإلكتروني وكفاءته وجودته في ظل وجود مخاطر الأمن السيبراني، خاصة في بيئة معقدة مثل البنوك الأردنية، حيث قد تنشأ اختراقات الأمن السيبراني نتيجة فشل البنوك في حماية المعلومات الخاصة بها سواء بالموظفين والعملاء والموردين والمستثمرين الآخرين وغيرهم، حيث تعد تلك المعلومات ضرورية لأداء البنك في المستقبل، ولذلك فقد أصبح من الضروري اكتساب المهارة العالية والخبرة من قبل مدقق الحسابات ومعرفة أساليب التدقيق المناسبة لتجنب التعرض لمخاطر بيئة نظم المعلومات المحاسبية الإلكترونية، وبالتالي زيادة فعالية وجودة التدقيق الإلكتروني، وقد جاءت مشكلة البحث بالاعتماد على دراسة Saputra and Paranoan التي بينت أن هنالك علاقة إيجابية بين كل من الأمن السيبراني وجودة عمليات التدقيق الداخلي، في حين أشارت دراسة Rosati et al. (2020) إلى أن حوادث الأمن السيبراني لا تؤثر بشكل كبير على جودة التدقيق، وعليه تم صياغة أسئلة البحث على النحو الآتي:

السؤال الرئيس: ما أثر مخاطر الأمن السيبراني بأبعاده (مخاطر أمن المعلومات، المخاطر التكنولوجية والتشغيلية، مخاطر الأداء) في جودة التدقيق الإلكتروني في البنوك الأردنية؟

ويتفرع عنه الأسئلة الفرعية التالية:

السؤال الفرعي الأول: ما أثر مخاطر أمن المعلومات في جودة التدقيق الإلكتروني في البنوك الأردنية؟

السؤال الفرعي الثاني: ما أثر المخاطر التكنولوجية والتشغيلية في جودة التدقيق الإلكتروني في البنوك الأردنية؟

السؤال الفرعي الثالث: ما أثر مخاطر الأداء في جودة التدقيق الإلكتروني في البنوك الأردنية؟

## 2.1 أهمية البحث:

### 1. الأهمية العلمية:

يسعى هذا البحث من الناحية العلمية إلى تقديم مساهمة في تبيان أثر المخاطر الأمنية السيبرانية ومدى تأثيرها في جودة التدقيق الإلكتروني في البنوك التي تمارس نشاطاتها في بيئة تكنولوجية وتقنية، مما يعزز جودة عملية التدقيق الإلكتروني ويجعلها أكثر انسجاماً وتوافقاً مع البيئة الرقمية، ومما يزيد من الأهمية العلمية لهذا البحث ندرة الدراسات بالبيئة الأردنية التي عمدت إلى البحث في أثر مخاطر الأمن السيبراني في جودة التدقيق الإلكتروني في البنوك الأردنية، حيث

سيشكل هذا البحث تراكمًا إضافيًا علميًا للباحثين في هذا المجال، يساعد في تطبيقه على أنظمة وقطاعات مختلفة ومؤسسات خاصة وحكومية مالية وغير مالية.

## 2. الأهمية العملية:

سعى هذا البحث إلى التعرف على أثر مخاطر الأمن السيبراني لتدقيق البنوك في الأردن، فكلما كانت الأنظمة مستقرة وآمنة ساعدت في تحسين أداء المدقق في عمليات التدقيق الفني والمالي، وبالتالي ينعكس بشكل إيجابي في تحسين كفاءة وجودة التدقيق.

كما تكمن أهمية البحث من الناحية العملية من الدور الهام الذي تؤديه البنوك الأردنية في دعم الاقتصاد الأردني بشكل عام من حيث إسهاماتها في التنمية النقدية والاقتصادية، وبالتالي ازدياد احتياجاتها مع زيادة التطور التكنولوجي، والحجم الكبير من العمليات التي يجب على البنوك تنفيذها بدقة عالية جداً ومواجهة مخاطر الأمن السيبراني التي قد تتعرض لها بشكل مستمر، وحيث إنّ الأمن السيبراني يعتبر من المواضيع الحيوية التي تتسم بالحدثة والأهمية في آن معاً، أصبح من الواجب عليها توفير حلول وأدوات للحد من مخاطر الأمن السيبراني وبالتالي زيادة جودة وفعالية التدقيق.

## 3.1 أهداف البحث:

هدف البحث وبشكل أساس إلى بيان أثر مخاطر الأمن السيبراني في جودة التدقيق الإلكتروني في البنوك الأردنية المدرجة في بورصة عمان، وعليه فإن الهدف الرئيس يتمثل في مجموعة من الأهداف وهي:

الهدف الرئيس: التعرف إلى أثر مخاطر الأمن السيبراني بأبعاده (مخاطر أمن المعلومات، المخاطر التكنولوجية والتشغيلية، مخاطر الأداء) في جودة التدقيق الإلكتروني في البنوك الأردنية. ويتفرع عنه الأهداف الفرعية التالية:

- 1- التعرف إلى أثر مخاطر أمن المعلومات في جودة التدقيق الإلكتروني في البنوك الأردنية.
- 2- التعرف إلى أثر المخاطر التكنولوجية والتشغيلية في جودة التدقيق الإلكتروني في البنوك الأردنية.
- 3- التعرف إلى أثر مخاطر الأداء في جودة التدقيق الإلكتروني في البنوك الأردنية.

## 4.1 فرضيات البحث:

## الفرضية الرئيسية:

H01: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر الأمن السيبراني بأبعاده (مخاطر أمن المعلومات، المخاطر التكنولوجية والتشغيلية، مخاطر الأداء) في جودة التدقيق الإلكتروني في البنوك الأردنية. ويتفرع عنها الفرضيات الفرعية التالية:

## الفرضية الفرعية الأولى:

H01.1: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر أمن المعلومات في جودة التدقيق الإلكتروني في البنوك الأردنية.

## الفرضية الفرعية الثانية:

H01.2: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) للمخاطر التكنولوجية والتشغيلية في جودة التدقيق الإلكتروني في البنوك الأردنية.

## الفرضية الفرعية الثالثة:

H01.3: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر الأداء في جودة التدقيق الإلكتروني في البنوك الأردنية.

## 2. الدراسات السابقة وما يميز الدراسة الحالية:

دراسة محمود وآخرون (2025): هدفت هذه الدراسة إلى التعرف على أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين في جمهورية مصر العربية، حيث تكون مجتمع الدراسة من المستثمرين في الجمهورية المصرية وتكونت عينة الدراسة من (75) مفردة صحيحة، واستخدمت الدراسة المنهج الاستقرائي والاستنباطي والتجريبي، حيث تقوم على مجموعة من الحالات الافتراضية مع تدعيم تلك الحالات بمجموعة من الأسئلة الاستقصائية لتجميع البيانات اللازمة، التي سيتم تحليلها احصائياً لاختبار فروض الدراسة.

ومن أهم ما توصلت إليه الدراسة وجود أثر لتوكيد المراجع الخارجي على المخاطر السيبرانية في قرارات المستثمرين، وأهمية قيام الإدارة بالتقييم الذاتي لنظام إدارة مخاطر الأمن السيبراني

لتحديد ما إذا كان هناك أوجه ضعف جوهرية في هذا النظام، واتخاذ ما يلزم من إجراءات للتغلب على نقاط الضعف.

وبناءً عليه أوصت الدراسة وجوب زيادة الاهتمام بأهمية الإفصاح عن الهجمات والاختراقات السيبرانية، ووضع عقوبات في حال عدم الإفصاح عن أي هجمات واختراقات، واتخاذ إجراءات تنظيمية لتعزيز الإفصاح في الوقت المناسب عن الاختراقات السيبرانية.

دراسة الخروف (2025): هدفت هذه الدراسة إلى التعرف على أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي في تدقيق شركات التكنولوجيا المالية في الأردن، ولتحقيق أهداف الدراسة فقد تم تصميم وتطوير استبانة وتحكيمها وتوزيعها على عينة الدراسة المكونة من (199) محاسباً قانونياً، وتم استخراج مقاييس الإحصاء الوصفي والمتوسط الحسابي والانحراف المعياري وتحليل الانحدار الخطي.

أظهرت النتائج أنه يوجد أثر ذو دلالة إحصائية لمتغير مقومات الأمن السيبراني في جودة التدقيق الخارجي بأبعادها (المسؤولين عن رقابة الجودة، المتطلبات الأخلاقية والاستقلالية، قبول الارتباط الجديد والاستمرار في الارتباط، موارد الارتباط البشرية، تنفيذ الارتباط، التفتيش، التوثيق) في شركات التكنولوجيا المالية في الأردن، كما أظهرت النتائج أن جميع أبعاد المتغير التابع مرتبطة بشكل إيجابي بأبعاد المتغير المستقل وتتأثر بدرجة عالية بمقومات الأمن السيبراني، كما أظهرت النتائج عدم وجود أثر لمتطلبات البنك المركزي في تحسين أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي بأبعادها ومنفردة في شركات التكنولوجيا المالية في الأردن باستثناء بعد التفتيش الذي أظهر أثر في تحسين العلاقة.

وعليه توصل الباحث إلى مجموعة من التوصيات أهمها: استمرار المدققين الخارجيين المزاولين بتدقيق الأنظمة والبرامج وتطبيق المعايير الملزمة وإصدار التقارير حول كفاية أنظمة الأمن السيبراني وإكساب المدققين الخارجيين المزاولين المزيد من المعرفة بالأمن السيبراني وإجراءات الحماية حول الهجمات السيبرانية والاطلاع عليها مما يساهم في رفع جودة التدقيق.

في ضوء النتائج أوصت الدراسة عدداً من التوصيات أهمها تشجيع البنوك على تبني استراتيجيات حديثة لاستخدام الذكاء الاصطناعي ولغة تقارير الأعمال الموسعة، مثل تطبيقات

التعلم الآلي والنظم الخبيرة والشبكات العصبية، لزيادة الشفافية وتحسين جودة الإفصاح المحاسبي عن الاستدامة.

دراسة Kanyongo and Wadesango (2025): تناولت هذه الدراسة تأثير الأمن السيبراني على استراتيجية التخفيف من المخاطر التي تتبناها البنوك التجارية الزيمبابوية في الأسواق الناشئة، وتضمنت الأهداف استكشاف العلاقة بين الفضاء الإلكتروني والتهديدات السيبرانية، وتحديد أسباب وتحديات هذه التهديدات، واقتراح الحلول، وقد تم تبني نهج بحثي كمي باستخدام الاستبانات لجمع البيانات من عينة من 25 مستجيباً.

وقد أشارت النتائج إلى أن المخاطر السيبرانية الرئيسية شملت التصيد الاحتيالي والقرصنة والاحتيال المحاسبي الداخلي، وكانت التحديات الرئيسية التي تم تحديدها هي عدم كفاية الإشراف من قبل المديرين، وعدم كفاية تشفير البيانات، والاعتماد على خدمات الطرف الثالث، والافتقار إلى المعايير والبنية الأساسية الوطنية، مما يعوق الجهود المبذولة لمكافحة التهديدات السيبرانية، كما أشارت النتائج إلى أن تعزيز الأمن السيبراني أمر بالغ الأهمية للبنوك الزيمبابوية. وقد كان من أهم التوصيات المقدمة لبنك نيومان (NB) تنفيذ مراقبة صارمة لأنشطة الموظفين المتعلقة بسرية العملاء، وإجراء عمليات تدقيق منتظمة للأمن السيبراني، وزيادة وعي العملاء، وتبني تدابير مثل المصادقة متعددة العوامل، وميزات تسجيل الخروج التلقائي، وجدران الحماية القوية للتخفيف من المخاطر السيبرانية بشكل فعال.

دراسة Iskandar and Deniswara (2025): هدفت هذه الدراسة إلى الكشف عن الدور الحاسم للأمن السيبراني وتكامله مع عملية التدقيق في تعزيز أمن المعلومات والبيانات في مواجهة الهجمات السيبرانية وتهديدات البيانات المتزايدة في إندونيسيا، وذلك باستخدام النظرية الموحدة الموسعة لقبول واستخدام التكنولوجيا (UTAUT).

وعلى الرغم من أهمية هذا التكامل، لا تزال نماذج البحث التي تستكشف العلاقة بين الأمن السيبراني والتدقيق غير مدروسة بشكل كافٍ، ولسد هذه الفجوة، اعتمد البحث منهجية كمية للتواصل مع المدققين الخارجيين في شركات المحاسبة العامة في منطقة جاكارتا الكبرين وإلى جانب إطار UTAUT، اعتمدت هذه الدراسة المخططات السلبية من نموذج الجاهزية التكنولوجية (TR) لتقييم تصور المدقق لاستخدام التكنولوجيا الجديدة، وقد جُمعت البيانات من خلال استبانات وحُللت باستخدام SmartPLS.

ومن أهم النتائج التي أظهرتها الدراسة أن النية السلوكية للمدققين لاستخدام الأمن السيبراني تتأثر بشدة بتوقعات الأداء، وتوقعات الجهد، وظروف التسهيل، وانعدام الأمن، حيث لا يكون للتأثير الاجتماعي وعدم الراحة أي تأثير يُذكر من خلال تطوير إطار عمل موسع لـ UTAUT. توصلت الدراسة إلى ضرورة استعداد المدققين الخارجيين لتبني الأمن السيبراني ضمن عملية التدقيق الخاصة بهم لتحسين أداء التدقيق وأمن البيانات.

دراسة Saputra and Paranoan (2024): هدفت هذه الدراسة إلى تقديم الأدلة التجريبية الخاصة بتحليل تأثيرات الأمن السيبراني والرقمنة وتصورات البيانات على الجودة المرتبطة بعمليات التدقيق البيئي الداخلي، ولتحقيق أهداف الدراسة فقد تم إجراء الدراسة على رؤساء لجان التدقيق الداخلي والمسؤولين عن تصميم وتنفيذ برامج التدقيق الداخلي لـ 300 فندق مصنف 4 و 5 نجوم في مدينة بالي في إندونيسيا من خلال أدوات المسح الآلي للبيانات كأداة بحث وبالاعتماد على أسلوب التقييم الكمي الذي يعتمد بالدرجة الأولى على الفلسفة الوضعية التي تستند على فحص قابلية الاختبار وإيجاد الحلول البسيطة أكثر من الحلول المعقدة في البحث من أجل تحقيق أكبر درجة ممكنة من التعميم.

ومن أهم النتائج التي توصلت إليها الدراسة، أن هنالك علاقة إيجابية بين كل من الأمن السيبراني والرقمنة وتصورات البيانات على جودة عمليات التدقيق الداخلي الذي يعتبر (التدقيق الداخلي) أكثر تفصيلاً وتركيزاً على العمليات في الفنادق المصنفة 4 و 5 نجوم في بالي، ويمكن لهذه الفنادق الاستفادة من عمليات التدقيق الداخلي كأداة لتقييم المخاطر البيئية، وحيث إنّ المدقق الداخلي يسعى كأحد مهامه إلى التحقق من الامتثال للأنظمة والقوانين، فهم يحتاجون إلى تتبع البيانات لأغراض تقييم الامتثال، وبالتالي الحاجة إلى وجود أنظمة قادرة على توفير البيانات والاطلاع عليها وتتبعها بطريقة غير معقدة للمدقق الداخلي ولكن هذا يحتاج إلى بنية تحتية قوية متوافقة مع هذه الأنظمة لحماية البيانات من مخاطر الأمن السيبراني، وبالتالي أوصت هذه الدراسة إلى ضرورة توفير بيانات ومعلومات وقرارات موثوقة من خلال الرجوع إلى المعايير الخاصة بالأمن السيبراني.

دراسة البواعنة (2023): هدفت هذه الدراسة إلى التعرف على أثر مخاطر الأمن السيبراني بأبعاده الأربعة (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية،

مخاطر الهجمات السيبرانية) في استخدام البطاقات المصرفية، حيث تكون مجتمع الدراسة من البنوك الإسلامية التي تعمل في الأردن والبالغ عددها أربعة بنوك منها ثلاث بنوك أردنية وبنك أجنبي، حيث استخدمت الدراسة استراتيجية المسح الشامل، واستخدمت المنهج الوصفي التحليلي، حيث تم جمع البيانات من خلال استبانة تم إعدادها وتوزيعها إلكترونياً على موظفي الإدارة العليا والوسطى والدنيا في البنوك الإسلامية العاملة في الأردن، حيث تم استخدام تحليل الانحدار الخطي البسيط والمتعدد لاختبار فرضيات الدراسة وذلك من خلال برمجية SPSS. وقد كان من أهم ما توصلت إليه الدراسة وجود أثر لمخاطر الأمن السيبراني بأبعاده الأربعة (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) بشكل منفرد أو مجتمع على استخدام البطاقات المصرفية للبنوك عينة الدراسة.

حيث أوصت الدراسة على ضرورة زيادة الوعي لموظفي وعملاء البنوك بالمخاطر المترتبة على الهجمات السيبرانية، وأهمية اتخاذ الاحتياطات اللازمة، كما أوصت بتحديث التطبيقات والأنظمة الأمنية وإجراء اختبارات للتأكيد على سلامتها.

دراسة (Ngo and Tick (2021): هدفت هذه الدراسة إلى التعرف على العلاقة بين مخاطر الأمن السيبراني وجودة التدقيق الخارجي الذي يتم بذله بشكل إضافي وخاص من قبل المدقق الخارجي للشركات التي واجهت هجمات أمن سيبرانية من خلال فرض رسوم تدقيق أعلى من المعتاد لمواجهة خطر عدم القدرة على اكتشاف المخاطر المتعلقة بالأمن السيبراني والمؤثرة على البيانات المالية. وتحقيقاً لهدف الدراسة، فقد تم إجراء الدراسة على عينة مكونة من 100 شركة عالمية متنوعة الحجم، من الشركات: الصغيرة، والمتوسطة، والكبيرة الحجم بالاعتماد على البيانات المقدمة من Wharton Research Data Service، للفترة من العام 2005 ولغاية العام 2014، واعتمد الباحثان في دراستهم على البحث الكمي لاستكشاف العلاقات والاتجاهات ضمن البيانات التي تم جمعها وعرضها ووصفها وفحصها.

ومن أهم النتائج التي توصلت إليها الدراسة، أن هنالك ضغوطات مستمرة على المدقق الخارجي بسبب تزايد مخاطر وحدة الهجمات السيبرانية وأثرها على البيانات المالية، ووجود علاقة إيجابية بين رسوم التدقيق والهجوم السيبراني، مما يعني زيادة جودة التدقيق الخارجي بسبب مخاطر الهجوم السيبراني.

أوصت الدراسة بضرورة إجراء المزيد من الدراسات على فترات زمنية أطول وبمعلومات أكثر شمولية.

دراسة Rosati et al. (2022): هدفت هذه الدراسة إلى التعرف على علاقة حوادث الأمن السيبراني في جودة التدقيق وتم تناول أربعة أبعاد للمتغير التابع والمتمثلة بجودة الاستحقاقات التي يتم تطبيقها وتسجيلها في الشركة، إدارة الأرباح، الاستمرارية، وإعادة صياغة البيانات المالية بعد عملية التعرض لهجوم سيبراني. وتحقيقاً لأهداف الدراسة، فقد اعتمد الباحثون على البيانات لجميع الحوادث السيبرانية المسجلة لدى منظمة تبادل معلومات حقوق الخصوصية (Privacy Rights Clearinghouse) وهي منظمة غير ربحية في الولايات المتحدة الأمريكية تهدف لجمع البيانات حول الاختراقات السيبرانية التي تمت في الولايات المتحدة الأمريكية للفترة من العام 2005 ولغاية العام 2014، وتكونت مجموعة البيانات التي تم الحصول عليها من قبل الباحثين على 4041 من الحوادث السيبرانية لعدة شركات مختلفة مدرجة في السوق المالي واستبعاد الشركات المالية والشركات التي لم يتم تدقيقها من شركات التدقيق الأربع الكبار Big4، لعدد 329 شركة.

ومن أهم النتائج التي توصلت إليها الدراسة، أن حوادث الأمن السيبراني لا تؤثر بشكل كبير على جودة التدقيق، وأن شركات التدقيق لديها قدرة كبيرة للتعامل مع التقارير المالية التي يتم تدقيقها حتى في ظل عدم وجود التشريعات التنظيمية الكافية، ولكن هذه النتيجة قد لا يكون من المناسب تعميمها لا سيما أن الدراسة على شركات التدقيق الأربع الكبار الذين يمتازون بجودة تدقيق على كل الأحوال، وبهذا توصي الدراسة بأن يتم عمل دراسات على الشركات الأخرى غير الأربع الكبار.

ومن خلال مراجعة الدراسات السابقة تبين بأن البحث الحالي تميز بما يلي:

- الربط بين مخاطر الأمن السيبراني بأبعاده (مخاطر أمن المعلومات، المخاطر التشغيلية والتكنولوجية، مخاطر الأداء) وبين جودة التدقيق الإلكتروني.
- تم إجراء هذا البحث على القطاع المصرفي في البنوك التجارية، حيث يعد هذا القطاع من أهم القطاعات الأساسية التي تدعم التنمية الاقتصادية والقومية الأردنية.

-استخدم هذا البحث أحدث الدراسات العلمية المنشورة في المجالات العلمية المحكمة والمصادر الأصلية المتخصصة والرجوع إلى التطبيقات والتجارب العملية للبنوك فيما يتعلق بمخاطر الأمن السيبراني والتدقيق الإلكتروني.

-قدم البحث نتائج يمكن أن تساهم في مساعدة البنوك في فهم تأثير الأخطار السيبرانية على إجراءات التدقيق الإلكتروني، مما يساهم في تحسين وزيادة جودة التدقيق الإلكتروني، وتعزيز موثوقية وشفافية المعلومات المالية وغير المالية.

### 3. الإطار النظري:

#### 1.3 مخاطر الأمن السيبراني:

##### 1.1.3 مفهوم الأمن السيبراني:

يعتبر الأمن السيبراني محورياً أساسياً في السياسة الأمنية للدول والمنظمات على حد سواء، وأصبحت الدول تهتم بوسائل الدفاع السيبراني باعتبارها أولوية في سياساتها الدفاعية، حيث باتت تلك الدول تعتبر الأطر القانونية والهيكل التنظيمية والوسائل التكنولوجية جزءاً من منظومة الأمن لديها بهدف حماية بيانات الأفراد والمنظمات من الاستخدام غير المصرح به (كريمة، 2024).

وقد شاع استخدام مفهوم الأمن السيبراني باعتباره المرادف لأمن المعلومات، وذلك بسبب انتشار مفهوم فضاء الأمن السيبراني المرتبط بتكنولوجيا المعلومات والاتصالات، عن طريق البنى التحتية المختلفة للاتصالات والأنظمة المعلوماتية، ولكن من المعلوم أن مفهوم الأمن السيبراني أشمل وأعم من مفهوم أمن المعلومات (براهيمي وحديدي، 2025).

وعُرف الأمن السيبراني من قبل البنك المركزي الأردني (2018) بأنه "الحفاظ على سرية وتكاملية وتوافرية المعلومات وأصول المعلومات التابعة للشركة ضمن الفضاء السيبراني من أي تهديد عن طريق مجموعة من الوسائل والسياسات وأفضل الممارسات بهذا الخصوص".

في حين عرف المركز الوطني للأمن السيبراني (2019) الأمن السيبراني على أنه "الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني، والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها دون تصريح، أم سوء استخدام، أم نتيجة إخفاق في إتباع الإجراءات الأمنية أم التعرض للخداع الذي يؤدي لذلك".

ويرى Peng & Krivacek (2020): أن الأمن السيبراني هو القواعد والإجراءات الوقائية المطلوبة لضمان حماية المنظمة من تهديدات الجرائم الإلكترونية، بالإضافة إلى حمايتها من الوصول غير المصرح به لنظم الاتصالات والمعلومات.

### 2.1.3 أبعاد مخاطر الأمن السيبراني:

يعد الأمن السيبراني أحد أهم المجالات التي تسعى إلى توفير الحماية اللازمة للأنظمة الإلكترونية والمعلومات من الخروقات والتهديدات السيبرانية، حيث يؤدي الأمن السيبراني دوراً حيوياً في الحفاظ على سلامة البيانات المخزنة، ومن بين المخاطر السيبرانية التي تتعرض لها المنظمة (الشيخ وأحمد، 2023):

- 1- الاختراق السيبراني: حيث يعتبر أحد أكبر المخاطر تأثيراً على المنظمة بسبب تمكن المهاجمين من اختراق الحواجز الأمنية والوصول إلى البيانات المحاسبية الحساسة.
- 2- الفيروسات والبرامج الخبيثة: يمكن للفيروسات والبرامج الخبيثة الدخول إلى الأنظمة وتعطيلها والتسبب بتلف البيانات المخزنة.
- 3- الهجمات الإلكترونية الموزعة: يقوم مهاجمو الأجهزة المتصلة بالإنترنت بالاستيلاء عليها واستخدامها لتوجيه هجمات متعددة.

إن التعامل الصحيح مع مخاطر الأمن السيبراني يوفر فرصة لتحقيق أهداف المنظمة وصولاً إلى رؤيتها الاستراتيجية، كما يساعد ذلك التعامل الجيد مع تلك المخاطر في تطوير وتحسين مسارها، واستخدام مواردها بكفاءة وفعالية أعلى، ولتحقيق كل ذلك لا بد من توافر عدد من الأبعاد للتعامل معها وفقاً لأفضل الممارسات العالمية الخاصة بالمخاطر السيبرانية وهي كالآتي (Kanyongo & Wadesango, 2025):

- 1- مخاطر أمن المعلومات: إن استخدام تكنولوجيا المعلومات له الكثير من الميزات والقيم المضافة على مستوى المنظمة، كما أن استخدام التقنية أصبحت أحد أساسيات العمل الإداري، وهذا يتطلب السعي المستمر لتوقع مخاطر أمن المعلومات والاستعداد الجيد لها من خلال الحلول والبدائل التي تضمن استمرارية العمل وخاصة عند التعرض لمثل هذه المخاطر، وقد عُرِفَت مخاطر أمن المعلومات باعتبارها التهديدات والأخطار المرتبطة باستخدام تكنولوجيا المعلومات، بالإضافة إلى أنها أي تهديد أو نشاط عن طريق جهة غير مصرح لها.
- 2- المخاطر التكنولوجية والتشغيلية: إن القيام بالمهام والنشاطات اليومية من خلال أنظمة المعلومات والاتصالات يعرض المنظمة للعديد من المخاطر التي قد تؤثر بصورة مباشرة على سير العمل،

وقد عُرفت المخاطر التكنولوجية والتشغيلية على أنها المخاطر التي تنشأ عند ممارسة البنك لأنشطته المختلفة عبر الإنترنت والحاسوب، من حدث يؤثر على الأصول المعلوماتية أو الحاسوب أو موارد الاتصالات أو البيانات المالية التي تنتج عنها مخاطر الخسارة المالية أو الإضرار بسمعة البنك أو تعطّل أعماله.

3- مخاطر الأداء: إن القيام بالنشاطات المختلفة يحتاج إلى مجموعة من الأدوات والتقنيات التكنولوجية اللازمة للخروج بالنتائج المرجوة من هذه النشاطات، كما أن هذه الأدوات وتلك التقنيات تتعرض للمخاطر المعروفة باسم مخاطر الأداء، حيث عُرفت مخاطر الأداء على أنها المخاطر المرتبطة بفشل الأدوات والتقنيات والبنية الأساسية التكنولوجية في تحقيق أهدافها والمهام المنوطة بها.

### 2.3 جودة التدقيق الإلكتروني:

#### 1.2.3 مفهوم جودة التدقيق:

لا يمكن أن تُعتبر الجودة هدفاً نهائياً، وعلى المنظمات الأخذ بها كثقافة مُنظمة آلية معتمدة لأداء المهام، بهدف تحسين العمليات والنشاطات بصورة مستمرة، مع ضرورة إجراء المراجعة الدورية للأداء، الأمر الذي ينعكس إيجاباً على كفاءة وفعالية الأداء (أكساس وقادري، 2021).

ويمكن النظر إلى مفهوم الجودة على أنه إيصال المنتجات سواءً كانت سلعة أم خدمات إلى المُستخدمين والمُستهلكين بوقت وكلفة وجهد أقل؛ على أن تتضمن أعلى مستوى إشباع وحسب رغبات المُستهلكين (المولى، 2018).

ويُعرف مفهوم الجودة بأنه مجموعة من الخصائص والصفات للمنتجات القادرة على تلبية رغبات المُستفيدين (الحاج والعلوص، 2023).

كما يُنظر إلى الجودة باعتبارها مجموعة المواصفات التي تحددها المنظمة التي يجب أن تتضمنها المنتجات (يوسف، 2024).

ويعتبر De Angelo (1981) أول من أشار إلى مفهوم جودة التدقيق بأنه مدى قدرة المدقق على اكتشاف الخروقات الموجودة في النظام المحاسبي والتقرير عنه. ويرى المعهد الأمريكي للمحاسبين القانونيين AICPA (2018) أن جودة التدقيق تعني أن يطبق المدقق المتطلبات المهنية للتدقيق والمتضمنة قواعد وأداب السلوك المهني؛ لما تقدمه المعايير من ضمانة تدل على مستويات الجودة المقبولة عند مراجعة القوائم المالية.

وتُعرف جودة التدقيق على أنها مستوى الامتثال للمعايير الشخصية والعامة، بالإضافة إلى الالتزام بمعايير التقرير من المدقق، علاوةً على توافر الموضوعية والنزاهة والاستقلالية والكفاءة اللازمة للقيام بمهام التدقيق (معمرى وآخرون، 2020).

ويمكن تعريف جودة التدقيق على أنها جودة التدقيق باعتبارها مستوى التأكيد الذي يوفره المدقق عن طريق عملية التدقيق بعد إتباع الإجراءات اللازمة وإطلاق الأحكام الصحيحة (El Badlaoui et al., 2021).

وعُرفت جودة التدقيق على أنها قدرة المدقق على المنح بين معايير التدقيق ومعايير التقرير من جهة والمعايير الوطنية من جهة أخرى، الأمر الذي يسهل على المستخدمين قراءة تقرير المدقق بصورة شمولية (عبد الصمد وبن أزواو، 2022).

وتُعرف جودة التدقيق بأنها قدرة المدقق على اكتشاف الأخطاء والتحريفات في القوائم المالية، والإبلاغ عنها ضمن تقريره الذي يصدر في نهاية أعمال التدقيق (بولعراس وسليمان، 2022).

كما تُعرف على أنها مجموعة الخصائص النوعية للتدقيق، التي تصدر من منظمات دولية راعية للمهنة، وتعمل على إشباع حاجات المستخدمين من تقرير المدقق (سعيد وحسين، 2022).

وعرفت دراسة عويّنة ونقاز (2022) بأنها أداء مهام عملية التدقيق، من قبل مدقق يمتاز بكفاءة وفاعلية عالية، ويستند إلى الأحكام والمعايير المهنية، قاصداً إشباع حاجات الأطراف المستفيدة من خدمات التدقيق.

ويرى المعيار الدولي رقم (220) أن جودة التدقيق ما هي إلا قيام المدقق بالمهام والنشاطات التدقيقية بما يتلاءم مع معايير التدقيق المتعارف عليها (حميداتو، 2023).

وتُعرف جودة التدقيق بأنها مقدار العناية المهنية التي يبذلها المدقق في التعامل مع مراحل عملية التدقيق، شريطة القيام بالإبلاغ عن الثغرات والأخطاء المكتشفة لإدارة المنظمة محل التدقيق وتقديم مجموعة من الحلول التي تكون قادرة على التعامل معها ضمن معايير التدقيق المتبعة (Hidayat et al., 2024).

كما يُقصد بمفهوم جودة التدقيق أنه القدرة على اكتشاف التحريفات أو الانحرافات الموجودة فعلاً في القوائم المالية، التي تكون جوهرية والإبلاغ عنها بواسطة التقرير المالي الذي يصدره المدقق (الفضلي والعامري، 2025).

### 2.2.3 مفهوم التدقيق الإلكتروني :

مع دخول عصر التكنولوجيا إلى مستويات متقدمة جداً بات التحول من نظام تدقيق تقليدي إلى نظام تدقيق إلكتروني ضرورة للنهوض بعملية التدقيق، لا سيما مع اتساع البقعة الجغرافية للكثير من المنظمات وكبر حجم بعضها الآخر، الأمر الذي أدى إلى الاستخدام الحتمي لتكنولوجيا المعلومات في مختلف مستوياتها الإدارية والوظيفية، بما في ذلك التدقيق من أجل تحقيق أهدافه وفقاً لآلية دقيقة وموثوقة وبجهد ووقت وتكلفة أقل (مومني وفراج، 2020).

ويُنظر إلى التدقيق الإلكتروني باعتباره تدقيقاً يقوم على استخدام تقنيات تكنولوجيا المعلومات في مراحل العملية التدقيقية، لما لهذه التقنيات من مساهمة إيجابية عند التخطيط لعملية التدقيق والرقابة عليها وتوثيقها، بهدف حماية أصول المنظمة محل التدقيق واستخدام مواردها بكفاءة وفعالية وتحقيق أهدافها الموضوعية مسبقاً (عبد الله ومصطفى، 2017).

كما يشير التدقيق الإلكتروني إلى استخدام الحاسوب في مراحل العملية التدقيقية من بداية جمع البيانات والمعلومات وتحليلها إلى إصدار التقرير الخاص بالعملية، مع ضرورة المحافظة على المعلومات والبيانات لتحقيق الكفاءة في الأنظمة التكنولوجية المستخدمة (العجمي والعلي، 2019).

كما يمكن تعريف مفهوم التدقيق الإلكتروني على أنه عملية تطبيق نظم التدقيق من خلال استخدام تكنولوجيا المعلومات؛ بمعنى الانتقال الكامل من تشغيل البيانات بشكل تقليدي إلى التشغيل الإلكتروني؛ لضمان المساهمة الفاعلة في إنجاز التدقيق بالطريقة المثلى وبوقت وجهد وكلفة أقل مع الحفاظ على جودة عملية التدقيق (يخلف وطرشي، 2020).

وترى دراسة بن بوعلي (2021) أن المقصود بالتدقيق الإلكتروني هو آلية ومنهجية تعتمد على الأنظمة الحاسوبية في جمع وتقييم الأدلة بصورة موضوعية، بالإضافة إلى فحص النظام المحاسبي ونظام الرقابة الداخلية؛ لتحديد مدى التوافق بين نتائج النشاطات والعمليات الاقتصادية والمعايير المقررة مسبقاً، وتوصيل نتائج التدقيق للأطراف ذات العلاقة.

ويمكن تعريف التدقيق الإلكتروني بأنه عملية تقييم وجمع المعلومات التي تمكننا من تحديد مدى مساهمة استخدام الحاسوب في حماية أصول المنظمة وسلامة بياناتها، مما يؤثر بصورة إيجابية على تحقيق أهدافها الموضوعية مسبقاً بفاعلية، علاوةً على الاستخدام الأمثل لمواردها المتاحة بكفاءة وفعالية (Khandelwal et al., 2022).

كما يُنظر إلى مفهوم التدقيق الإلكتروني بأنه عملية تنطوي على استخدام النظم والتكنولوجيات الحديثة بهدف تحليل البيانات والمعلومات وفحص العمليات المحاسبية والمالية والإدارية داخل المنظمة، حيث هذا النوع من التدقيق على الأنظمة المؤتمتة بدلاً من العمليات التقليدية (Almubaydeen et al, 2024).

وترى دراسة ملياني وسعود (2024) أن التدقيق الإلكتروني يعتبر أحد أنواع التدقيق ويقوم على استخدام التكنولوجيا بما يتلاءم والتكنولوجيا الموجودة في المنظمة محل التدقيق، لتقديم رأي في محايد عن مدى عدالة القوائم المالية.

### 3.2.3 أهداف التدقيق الإلكتروني:

التدقيق الإلكتروني يستطيع أن يحل محل التدقيق التقليدي لما يحققه من أهداف تتمثل فيما يلي (يخلف وطرشي، 2020):

- 1- سهولة الحصول على البيانات والتقارير المالية وغير المالية ومعرفة المخاطر والأخطاء والمخالفات في المالية بصورة فورية؛ وبالتالي رفع مستوى دقة واكتمال النتائج عبر تحليل شامل للبيانات.
- 2- التحقق من مصداقية ومصادقة الإدارة على التراخيص التي تتعلق بمشروعية وملكية البرامج والتقنيات المستخدمة في المنظمة.
- 3- القدرة على توفير تدابير احترازية قادرة على حماية أجهزة الحواسيب والبرامج والتقنيات وخطوط الاتصالات والمعلومات والبيانات من الوصول لغير المصرح لهم بذلك؛ وبالتالي حماية أصول المنظمة المعلوماتية من شتى أنواع المخاطر مثل: التخريب أو التلف أو السرقة.

### 4. منهجية البحث:

**1.4 منهج البحث:** تمثل المنهج الرئيسي في الدراسة بالمنهج الوصفي التحليلي، وهو أحد المناهج الاحصائية الأكثر شيوعاً في الدراسات والأبحاث الكمية، إذ يقوم على وصف حيثيات الظواهر والأحداث المتعلقة بالدراسة بدقة وسردها بصورة كمية ونوعية (النجار وآخرون، 2020).

**2.4 مجتمع البحث وعينته:** تكون مجتمع البحث من البنوك الأردنية، البالغ عددها (15) بنكاً، منها (12) بنكاً تجارياً، (3) بنوك إسلامية، ونظراً لصغر حجم مفردات المجتمع فقد تم تضمين جميع البنوك الأردنية في عينة البحث.

**3.4 وحدة المعاينة والتحليل:** ركزت الدراسة على الأفراد العاملين في الدوائر (المالية والتدقيق الداخلي وتكنولوجيا المعلومات) في البنوك الأردنية، مع تضمين المدققين الداخليين والمحاسبين والتقنيين في هذه الأقسام، وقد تم اختيار هؤلاء الأفراد بشكل عشوائي. ولهذا فقد قام الباحثان بتوزيع (180) استبانة إلكترونية وتم استرجاع (167) استبانة، جميعها صالحة للتحليل. وقد استخدمت الاستبانة أسلوب القياس الخماسي في تعبير أفراد وحدة المعاينة والتحليل عن آرائهم على فقرات الاستبانة، وتم تحديد قيم عديدة للإجابات على الفقرات كما يأتي: 5: موافق بشدة، 4: موافق، 3: موافق بدرجة متوسطة، 2: غير موافق، 1: غير موافق بشدة (Sekaran & Bougie, 2016). واعتمدت الدراسة ثلاثة مستويات للأهمية النسبية ووفقاً لقيم المتوسط الحسابي للإجابات على الاستبانة، وهي منخفض ومتوسط ومرتفع، بحيث تقيس هذه المستويات مستوى الاهتمام الذي توليه البنوك الأردنية بمتغيرات الدراسة.

**5.4 اختبار صدق المحتوى:** تم عرض الاستبانة الأولية على مجموعة من المحكمين الأكاديميين والإداريين المختصين بمواضيع الدراسة والبالغ عددهم (٥)؛ بهدف التحقق من وضوح وملاءمة مفردات وفقرات الاستبانة، ودقتها لقياس ما وضعت لأجله، وإمكانية فهمها واستيعابها من الفئات التي شملتها الدراسة. وقد تم الالتزام بالتعديلات والملاحظات التي أوردتها المحكمون على الاستبانة، لتظهر الاستبانة بصورتها النهائية. وعليه تعتبر أداة الدراسة صالحة لقياس ما وضعت لأجله.

**5.4 اختبار ثبات أداة البحث:** يهدف اختبار ثبات أداة البحث إلى التحقق من أن جميع فقرات أداة البحث تساهم في الغرض العام الذي يتم قياسه، وذلك من خلال ضمان اتساقها مع بعضها البعض. ويعد معامل ألفا كرونباخ (Alpha Cronbach Coefficient) من أكثر الطرق الإحصائية استخداماً في هذا المجال، حيث يُحدد هذا المعامل ثبات أداة البحث، فإذا تجاوزت قيمة المعامل 0.70 فهذا مؤشر على ثبات الأداة (Sekaran & Bougie, 2016). ويوضح الجدول (1) قيم معامل ألفا كرونباخ لثبات أداة البحث.

الجدول 1: نتائج اختبار ثبات أداة البحث

| الرقم | البعد (المتغير)                | عدد الفقرات | قيمة كرونباخ ألفا |
|-------|--------------------------------|-------------|-------------------|
| 1     | مخاطر أمن المعلومات            | 8           | 0.915             |
| 2     | المخاطر التكنولوجية والتشغيلية | 8           | 0.951             |
| 3     | مخاطر الأداء                   | 8           | 0.960             |
| 4     | مخاطر الأمن السيبراني          | 24          | 0.977             |
| 5     | جودة التدقيق الإلكتروني        | 10          | 0.958             |

يوضح الجدول (1) أن أداة البحث تتميز بدرجات عالية نسبياً من الثبات، حيث تبين أن جميع قيم معامل ألفا كرونباخ تجاوزت القيمة (0.70)، إذ تراوحت القيم بين (0.915 - 0.977) (Sekaran & Bougie, 2016).

#### 6.4 اختبار صلاحية نموذج البحث:

يهدف اختبار صلاحية نموذج البحث إلى التحقق من ملاءمة وموثوقية بيانات البحث لإجراء الاختبارات الإحصائية، وللتحقق من ذلك تم إجراء اختبار التعدد الخطي (Multicollinearity)، حيث تعتبر مشكلة التعدد الخطي من المشاكل المرتبطة بنماذج الانحدار للمتغيرات المستقلة، وتنشأ هذه المشكلة عند وجود ارتباط خطي قوي (تام أو شبه تام) بين متغيرين مستقلين أو أكثر، مما يؤثر سلباً على دقة القياسات، ويجعل تقدير المعلمات مستحيلاً، ويعود ذلك إلى تضخيم قيمة معامل التحديد  $R^2$  إلى ما يفوق قيمته الحقيقية (Guajarati, 2004). وللتحقق من وجود هذه المشكلة تم قياس معامل تضخم التباين (VIF)، حيث تشير قيمة (VIF) التي تزيد عن 10 إلى وجود مشكلة التعدد الخطي، بينما تشير القيمة التي تقع ضمن النطاق من 1 إلى 10 إلى عدم وجود هذه المشكلة (Guajarati, 2004).

الجدول 2: اختبار صلاحية نموذج البحث باستخدام معامل تضخم التباين

| المتغير                        | معامل تضخم التباين VIF | التباين المسموح به Tolerance |
|--------------------------------|------------------------|------------------------------|
| مخاطر أمن المعلومات            | 4.794                  | 0.209                        |
| المخاطر التكنولوجية والتشغيلية | 6.879                  | 0.145                        |
| مخاطر الأداء                   | 7.116                  | 0.141                        |

يوضح الجدول (2) أن البيانات خالية من مشكلة التعدد الخطي، حيث ظهرت جميع القيم ضمن النطاق المحدد، إذ تراوحت قيم معامل تضخم التباين (VIF) بين (4.794-7.116)، وتراوحت قيم التباين المسموح به (Tolerance) بين (0.141 - 0.209) (Guajarati, 2004).

### 5. التحليل الإحصائي:

1.5 وصف الخصائص الشخصية والوظيفية للمبحوثين: تم تحليل الخصائص الشخصية والوظيفية لأفراد عينة البحث، والمتمثلة في العاملين في الدوائر (المالية والتدقيق الداخلي وتكنولوجيا المعلومات) في البنوك الأردنية، بالإضافة إلى المدققين الداخليين والمحاسبين والتقنيين في هذه الأقسام، من خلال تطبيق مقاييس الإحصاء الوصفي كالتكرارات والنسب المئوية، وشملت هذه الخصائص: التخصص الأكاديمي، والمؤهل الأكاديمي، والمستوى الوظيفي، وسنوات الخدمة. ويهدف هذا الجزء من الدراسة إلى تقديم نظرة عامة على السمات الشخصية والمهنية السائدة بين الأفراد العاملين في البنوك الأردنية.

وقد تبين أن أعلى نسبة من عينة الدراسة كانت من فئة التخصص الأكاديمي (المحاسبة)، التي بلغت (43.5%)، وهذا مرتبط بحاجة البنوك لتخصص المحاسبة بهدف القيام بالواجبات والمهام في عمليات البنك، وخاصة في إنجاز عمليات المحاسبة والمساهمة في عمليات التدقيق الإلكتروني. كما أن أعلى نسبة منهم حاصلون على المؤهل الأكاديمي (بكالوريوس)، التي بلغت (61.7%)، وهذا يشير إلى ارتفاع المستوى العلمي والمعرفي للعاملين في البنوك الأردنية. وقد شكّلت فئة (الموظفون) أعلى نسبة من عينة الدراسة التي بلغت (44.9%)، تلاها فئة (رئيس قسم) ونسبة (30.5%)، وهذا مرتبط بحاجة البنوك وأقسامها المتعددة وعملياتها المتنوعة والمستمرة لوجود هذه المسميات. ويمتلك النسبة الأكبر منهم سنوات خدمة من الفئة (من 5 – أقل من 10 سنوات) التي بلغت (38.3%)، وهذا مرتبط بسياسات البنوك الأردنية في استقطاب أصحاب الخبرات للعمل لديها، كما يرتبط بوجود نسبة عالية من الموظفين بين أفراد عينة البحث.

2.5 وصف متغيرات البحث: اشتملت الاستبانة على قسمين، يختص كل جزء بالمتغيرات الرئيسة للبحث (مخاطر الأمن السيبراني، وجودة التدقيق الإلكتروني)، وقد تم قياس هذه الأجزاء من خلال (34) فقرة موزعة على هذه المتغيرات والأبعاد المخصصة لقياسها، وقد تم استخدام المتوسطات الحسابية والانحرافات المعيارية بالإضافة إلى الرتبة والأهمية النسبية لوصف هذه المتغيرات وتحديد مستوى اهتمام المنظمات المبحوث بها.

الجدول 3: وصف مخاطر الأمن السيبراني وجودة التدقيق الإلكتروني في البنوك الأردنية

| الرقم | البعد والمتغير                 | الأوساط الحسابية | الانحرافات المعيارية | الرتب | مستويات الأهمية النسبية |
|-------|--------------------------------|------------------|----------------------|-------|-------------------------|
| 1     | مخاطر أمن المعلومات            | 4.246            | 0.585                | 2     | مستوى مرتفع             |
| 2     | المخاطر التكنولوجية والتشغيلية | 4.254            | 0.608                | 1     | مستوى مرتفع             |
| 3     | مخاطر الأداء                   | 4.229            | 0.624                | 3     | مستوى مرتفع             |
|       | مخاطر الأمن السيبراني          | 4.243            | 0.580                |       | مستوى مرتفع             |
|       | جودة التدقيق الإلكتروني        | 4.186            | 0.641                |       | مستوى مرتفع             |

يوضح الجدول 3 المستوى المرتفع من اهتمام البنوك الأردنية بمخاطر الأمن السيبراني، حيث بلغ الوسط الحسابي الإجمالي (4.243) والانحراف المعياري (0.580). وتراوحت قيم المتوسطات الحسابية لجميع الأبعاد بين (4.229 – 4.254)، مع أهمية نسبية مرتفعة لجميع الأبعاد، حيث احتلت (المخاطر التكنولوجية والتشغيلية) المرتبة الأولى بوسط حسابي قدره (4.254) وانحراف معياري قدره (0.608)، بينما احتلت (مخاطر الأداء) المرتبة الثالثة والأخيرة بوسط حسابي قدره (4.229) وانحراف معياري قدره (0.624). كما يوضح الجدول 3 المستوى المرتفع من اهتمام البنوك الأردنية بجودة التدقيق الإلكتروني، حيث بلغ الوسط الحسابي الإجمالي (4.186) والانحراف المعياري (0.641).

### 3.5 اختبار فرضيات البحث:

يعرض هذا القسم من البحث نتائج اختبار الفرضيات، التي صيغت وفقاً لمشكلة البحث وأهدافه. وتركز هذه الفرضيات على دراسة تأثير مخاطر الأمن السيبراني في جودة التدقيق الإلكتروني، مع الأخذ في الاعتبار أبعادها مجتمعةً ومنفردةً. لذلك، تمت صياغة فرضية رئيسية،

واختبارها باستخدام الأساليب الإحصائية المناسبة؛ إذ تم اختبار الفرضية الرئيسة باستخدام تحليل الانحدار الخطي المتعدد Multiple Linear Regression وتم اختبار الفرضيات الفرعية باستخدام تحليل الانحدار الخطي البسيط Simple Linear Regression.

1.3.5 نتائج اختبار الفرضية الرئيسة:

تتناول الفرضية الرئيسة تأثير مخاطر الأمن السيبراني في جودة التدقيق الإلكتروني، وتنص على ما يلي: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر الأمن السيبراني بأبعادها (مخاطر امن المعلومات، المخاطر التكنولوجية والتشغيلية، مخاطر الأداء) في جودة التدقيق الإلكتروني في البنوك الأردنية". وكانت النتائج كما يأتي:

الجدول 4: ملخص النموذج وتحليل تباين الانحدار للفرضية الرئيسة

| المتغير التابع          | ملخص النموذج     |                              |                                              | تحليل التباين ANOVA               |                 |                            |
|-------------------------|------------------|------------------------------|----------------------------------------------|-----------------------------------|-----------------|----------------------------|
|                         | معامل الارتباط R | معامل التحديد R <sup>2</sup> | معامل التحديد المعدل Adjusted R <sup>2</sup> | الخطأ المعياري للنموذج Std. Error | درجات الحرية DF | القيمة المحسوبة للاختبار F |
| جودة التدقيق الإلكتروني | 0.905            | 0.820                        | 0.816                                        | 0.275                             | 3               | 246.845                    |
|                         |                  |                              |                                              |                                   |                 | 0.000                      |

يوضح الجدول (4) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة بين مخاطر الأمن السيبراني وجودة التدقيق الإلكتروني، حيث كانت قيمة معامل الارتباط ( $R=0.905$ ). ويتضح أن متغير مخاطر الأمن السيبراني يُفسر (82.0%) من التغير في جودة التدقيق الإلكتروني، مع بقاء العوامل الأخرى ثابتة، حيث كانت قيمة معامل التحديد ( $R^2=0.820$ ).

كما يتضح من الجدول أن النموذج معنوي، حيث إنَّ قيمة F المحسوبة هي (246.845) ومستوى الدلالة هو ( $\text{Sig F}=0.000$ ) وهو أقل من 0.05، مما يشير إلى وجود تأثير ذي دلالة إحصائية لمخاطر الأمن السيبراني في جودة التدقيق الإلكتروني عند مستوى دلالة ( $\alpha \leq 0.05$ ).

لذلك، يتم رفض الفرضية العدمية الرئيسة الأولى، ويتم قبول الفرضية البديلة التي تنص على ما يلي: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر الأمن السيبراني بأبعادها (مخاطر أمن المعلومات، المخاطر التكنولوجية والتشغيلية، مخاطر الأداء) في جودة التدقيق الإلكتروني في البنوك الأردنية".

الجدول 5: معاملات الانحدار للفرضية الرئيسة

| المتغير المستقل                | المعاملات B | الخطأ المعياري Std. Error | قيمة Beta | قيمة الاختبار t | مستوى الدلالة Sig t للاختبار |
|--------------------------------|-------------|---------------------------|-----------|-----------------|------------------------------|
| مخاطر أمن المعلومات            | 0.418       | 0.077                     | 0.382     | 5.441           | 0.000                        |
| المخاطر التكنولوجية والتشغيلية | 0.033       | 0.092                     | 0.032     | 0.364           | 0.716                        |
| مخاطر الأداء                   | 0.541       | 0.086                     | 0.527     | 6.264           | 0.000                        |

يوضح الجدول 5 نتائج معاملات الانحدار لفرضية الدراسة الرئيسة، حيث تبين أن قيمة معامل الانحدار للبُعد (مخاطر أمن المعلومات) هي ( $B=0.418$ )، وقيمة Beta هي (0.382)، وقيمة T هي (5.441) بمستوى دلالة ( $\text{Sig } T=0.000$ )، وهو أقل من 0.05، وهذا يشير إلى وجود تأثير معنوي لهذا البعد في جودة التدقيق الإلكتروني. وتبين أن قيمة معامل الانحدار للبُعد (المخاطر التكنولوجية والتشغيلية) هي ( $B=0.033$ )، وقيمة Beta هي (0.032)، وقيمة T هي (0.364) بمستوى دلالة ( $\text{Sig } T=0.716$ )، وهو أكبر من 0.05، وهذا يشير إلى عدم وجود تأثير معنوي لهذا البعد في جودة التدقيق الإلكتروني. وتبين أن قيمة معامل الانحدار للبُعد (مخاطر الأداء) هي ( $B=0.541$ )، وقيمة Beta هي (0.527)، وقيمة T هي (6.264) بمستوى دلالة ( $\text{Sig } T=0.000$ )، وهو أقل من 0.05، وهذا يشير إلى وجود تأثير معنوي لهذا البعد في جودة التدقيق الإلكتروني.

#### نتائج اختبار الفرضيات الفرعية للفرضية الرئيسة:

تتناول الفرضيات الفرعية للفرضية الرئيسة تأثير أبعاد مخاطر الأمن السيبراني في جودة التدقيق الإلكتروني، حيث جاء نص هذه الفرضيات ونتائج اختبارها على النحو الآتي:

الفرضية الفرعية الأولى: تتناول الفرضية الفرعية الأولى تأثير مخاطر أمن المعلومات في جودة التدقيق الإلكتروني، وتنص على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية

( $\alpha \leq 0.05$ ) لمخاطر أمن المعلومات في جودة التدقيق الإلكتروني في البنوك الأردنية". وكانت النتائج كما يأتي:

الجدول 6: ملخص النموذج وتحليل تباين الانحدار للفرضية الفرعية الأولى

| المتغير التابع          | ملخص النموذج     |                              |                                              |                                  |                 |                            | تحليل التباين ANOVA          |  |
|-------------------------|------------------|------------------------------|----------------------------------------------|----------------------------------|-----------------|----------------------------|------------------------------|--|
|                         | معامل الارتباط R | معامل التحديد R <sup>2</sup> | معامل التحديد المعدل Adjusted R <sup>2</sup> | الخطأ المعياري للمودج Std. Error | درجات الحرية DF | القيمة المحسوبة للاختبار F | مستوى الدلالة للاختبار Sig F |  |
| جودة التدقيق الإلكتروني | 0.859            | 0.739                        | 0.737                                        | 0.329                            | 1               | 466.205                    | 0.000                        |  |

يوضح الجدول (6) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة بين مخاطر أمن المعلومات وجودة التدقيق الإلكتروني، حيث كانت قيمة معامل الارتباط ( $R=0.859$ ). ويتضح أن متغير مخاطر أمن المعلومات يُفسر (73.9%) من التغير في جودة التدقيق الإلكتروني، مع بقاء العوامل الأخرى ثابتة، حيث كانت قيمة معامل التحديد ( $R^2=0.739$ ).

كما يتضح من الجدول أن النموذج معنوي، حيث إن قيمة F المحسوبة هي (466.205) ومستوى الدلالة هو ( $\text{Sig F}=0.000$ ) وهو أقل من 0.05، مما يشير إلى وجود تأثير ذي دلالة إحصائية لمخاطر أمن المعلومات في جودة التدقيق الإلكتروني عند مستوى دلالة ( $\alpha \leq 0.05$ ). لذلك، يتم رفض الفرضية العدمية الفرعية الأولى، ويتم قبول الفرضية البديلة التي تنص على ما يلي: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر أمن المعلومات في جودة التدقيق الإلكتروني في البنوك الأردنية".

الجدول 7: معاملات الانحدار للفرضية الفرعية الأولى

| المتغير المستقل     | المعاملات B | الخطأ المعياري Std. Error | قيمة Beta | قيمة الاختبار t | مستوى الدلالة Sig t للاختبار |
|---------------------|-------------|---------------------------|-----------|-----------------|------------------------------|
| مخاطر امن المعلومات | 0.942       | 0.044                     | 0.859     | 21.592          | 0.000                        |

يوضح الجدول (7) نتائج معاملات الانحدار لفرضية الدراسة الفرعية الأولى، حيث تبين أن قيمة معامل الانحدار للبعد (مخاطر امن المعلومات) هي ( $B=0.942$ )، وقيمة Beta هي ( $0.859$ )، وقيمة T هي ( $21.592$ ) بمستوى دلالة ( $\text{Sig T}=0.000$ )، وهو أقل من  $0.05$ ، وهذا يشير إلى وجود تأثير معنوي لهذا البعد في جودة التدقيق الإلكتروني.

الفرضية الفرعية الثانية: تتناول الفرضية الفرعية الثانية تأثير المخاطر التكنولوجية والتشغيلية في جودة التدقيق الإلكتروني، وتنص على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) للمخاطر التكنولوجية والتشغيلية في جودة التدقيق الإلكتروني في البنوك الأردنية". وكانت النتائج كما يأتي:

الجدول 8: ملخص النموذج وتحليل تباين الانحدار للفرضية الفرعية الثانية

| المتغير التابع          | ملخص النموذج     |                     |                                     | تحليل التباين ANOVA               |                 |                            |
|-------------------------|------------------|---------------------|-------------------------------------|-----------------------------------|-----------------|----------------------------|
|                         | معامل الارتباط R | معامل التحديد $R^2$ | معامل التحديد المعدل Adjusted $R^2$ | الخطأ المعياري للنموذج Std. Error | درجات الحرية DF | القيمة المحسوبة للاختبار F |
| جودة التدقيق الإلكتروني | 0.841            | 0.707               | 0.705                               | 0.348                             | 1               | 397.660                    |
|                         |                  |                     |                                     |                                   |                 | 0.000                      |

يوضح الجدول (8) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة بين المخاطر التكنولوجية والتشغيلية وجودة التدقيق الإلكتروني، حيث كانت قيمة معامل الارتباط ( $R=0.841$ ). ويتضح أن متغير المخاطر التكنولوجية والتشغيلية يُفسر ( $70.7\%$ ) من التغير في

جودة التدقيق الإلكتروني، مع بقاء العوامل الأخرى ثابتة، حيث كانت قيمة معامل التحديد ( $R^2=0.707$ ).

كما يتضح من الجدول أن النموذج معنوي، حيث إن قيمة F المحسوبة هي (397.660) ومستوى الدلالة هو ( $\text{Sig F}=0.000$ )، وهو أقل من 0.05، مما يشير إلى وجود تأثير ذي دلالة إحصائية للمخاطر التكنولوجية والتشغيلية في جودة التدقيق الإلكتروني عند مستوى دلالة ( $\alpha \leq 0.05$ ). لذلك، يتم رفض الفرضية العدمية الفرعية الثانية، ويتم قبول الفرضية البديلة التي تنص على ما يلي: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) للمخاطر التكنولوجية والتشغيلية في جودة التدقيق الإلكتروني في البنوك الأردنية".

الجدول 9: معاملات الانحدار للفرضية الفرعية الثانية

| المتغير المستقل                | المعاملات B | الخطأ المعياري Std. Error | قيمة Beta | قيمة الاختبار t | مستوى الدلالة Sig t للاختبار |
|--------------------------------|-------------|---------------------------|-----------|-----------------|------------------------------|
| المخاطر التكنولوجية والتشغيلية | 0.886       | 0.044                     | 0.841     | 19.941          | 0.000                        |

يوضح الجدول (9) نتائج معاملات الانحدار لفرضية الدراسة الفرعية الثانية، حيث تبين أن قيمة معامل الانحدار للبعد (المخاطر التكنولوجية والتشغيلية) هي ( $B=0.886$ )، وقيمة Beta هي (0.841)، وقيمة T هي (19.941) بمستوى دلالة ( $\text{Sig T}=0.000$ )، وهو أقل من 0.05، وهذا يشير إلى وجود تأثير معنوي لهذا البعد في جودة التدقيق الإلكتروني.

الفرضية الفرعية الثالثة: تتناول الفرضية الفرعية الثالثة تأثير مخاطر الأداء في جودة التدقيق الإلكتروني، وتنص على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر الأداء في جودة التدقيق الإلكتروني في البنوك الأردنية". وكانت النتائج كما يأتي:

الجدول 10: ملخص النموذج وتحليل تباين الانحدار للفرضية الفرعية الثالثة

| المتغير التابع          | ملخص النموذج     |                              |                                              |                                    |                 |                            | تحليل التباين ANOVA          |  |
|-------------------------|------------------|------------------------------|----------------------------------------------|------------------------------------|-----------------|----------------------------|------------------------------|--|
|                         | معامل الارتباط R | معامل التحديد R <sup>2</sup> | معامل التحديد المعدل Adjusted R <sup>2</sup> | الخطأ المعياري لل نموذج Std. Error | درجات الحرية DF | القيمة المحسوبة للاختبار F | مستوى الدلالة للاختبار Sig F |  |
| جودة التدقيق الإلكتروني | 0.882            | 0.778                        | 0.777                                        | 0.303                              | 1               | 577.833                    | 0.000                        |  |

يوضح الجدول (10) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة بين مخاطر الأداء وجودة التدقيق الإلكتروني، حيث كانت قيمة معامل الارتباط ( $R=0.882$ ). ويتضح أن متغير مخاطر الأداء يُفسر (77.8%) من التغير في جودة التدقيق الإلكتروني، مع بقاء العوامل الأخرى ثابتة، حيث كانت قيمة معامل التحديد ( $R^2=0.778$ ).

كما يتضح من الجدول أن النموذج معنوي، حيث إن قيمة F المحسوبة هي (577.833) ومستوى الدلالة هو ( $\text{Sig F}=0.000$ )، وهو أقل من 0.05، مما يشير إلى وجود تأثير ذي دلالة إحصائية لمخاطر الأداء في جودة التدقيق الإلكتروني عند مستوى دلالة ( $\alpha \leq 0.05$ ).

لذلك، يتم رفض الفرضية العدمية الفرعية الثالثة، ويتم قبول الفرضية البديلة التي تنص على ما يلي: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لمخاطر أمن الأداء في جودة التدقيق الإلكتروني في البنوك الأردنية".

الجدول 11: معاملات الانحدار للفرضية الفرعية الثالثة

| المتغير المستقل | المعاملات B | الخطأ المعياري Std. Error | قيمة Beta | قيمة الاختبار t | مستوى الدلالة للاختبار Sig t |
|-----------------|-------------|---------------------------|-----------|-----------------|------------------------------|
| مخاطر الأداء    | 0.906       | 0.038                     | 0.882     | 24.038          | 0.000                        |

يوضح الجدول (11) نتائج معاملات الانحدار لفرضية الدراسة الفرعية الثالثة، حيث تبين أن قيمة معامل الانحدار للبُعد (مخاطر الأداء) هي ( $B=0.906$ )، وقيمة Beta هي (0.882)، وقيمة T

هي (24.038) بمستوى دلالة (Sig T=0.000)، وهو أقل من 0.05، وهذا يشير إلى وجود تأثير معنوي لهذا البعد في جودة التدقيق الإلكتروني.

النتائج: تشير النتائج المستخلصة من الدراسة إلى وعي استباقي متقدم لدى البنوك الأردنية بطبيعة المخاطر في العصر الرقمي، وتأثيرها الكبير المباشر على الوظائف الرقابية الهامة والأساسية. ويمكن مناقشة هذه النتائج على النحو التالي:

1- أظهر التحليل أن البنوك الأردنية تولي اهتماماً مرتفعاً بمخاطر الأمن السيبراني بكافة أبعاده، مما يعكس نضجاً في الفهم الاستراتيجي لهذه المخاطر. وهذا المستوى المتقدم من الاهتمام يمثل تحولاً نوعياً نحو ثقافة وقائية متكاملة. فهذا الإدراك العميق ينبع من إدراك البنوك أن استقرارها المالي وسمعتها في السوق أصبحا مرتبطين ارتباطاً وثيقاً بمناعتها الرقمية. وأن ترتيب الأبعاد، بتصدر المخاطر التكنولوجية والتشغيلية يلها مخاطر أمن المعلومات ثم مخاطر الأداء، يكشف عن تسلسل منطقي في الأولويات لدى إدارات البنوك. فالتركيز على المخاطر التكنولوجية والتشغيلية يؤكد أن قوة البنية التحتية ومثانتها تشكل حجر الأساس الذي تقوم عليه آلية استراتيجية أمنية، وهو انعكاس مباشر للتحويل الرقمي المتسارع في تقديم الخدمات، حيث إن أي خلل تقني يمكن أن يضعف العمليات المصرفية. أما الاهتمام المرتفع بمخاطر أمن المعلومات، فيعكس التركيز المتزايد على سرية بيانات العملاء وسلامتها، التي تشكل جوهر الثقة في النظام المصرفي، وإدراك البنوك لهذه المخاطر ينسجم مع متطلبات الأطر التنظيمية الصادرة عن البنك المركزي، وتهدف إلى حماية الاستقرار المالي. ويشير وضع مخاطر الأداء في المرتبة الأخيرة مع الاهتمام المرتفع بها إلى فهم دقيق لطبيعة هذه المخاطر. فمخاطر الأداء، المرتبطة بالكفاءات البشرية ومدى فاعلية تنفيذ السياسات، تعتبر بمثابة أحد مستويات الدفاع، الذي يتطلب استثماراً طويلاً الأجل في بناء القدرات وتطوير المهارات. والاهتمام المرتفع بها يعكس الاعتراف بأنه لا يمكن بناء ثقافة أداء عالي دون تأمين البنية التحتية والمعلومات التي يعتمد عليها الأداء.

2- أظهر التحليل أن البنوك الأردنية تولي اهتماماً مرتفعاً بجودة التدقيق الإلكتروني، وهذا الاهتمام المرتفع يمثل ترجمة عملية للإدراك المتقدم للمخاطر السيبرانية. ففي ظل البيئة الرقمية المعقدة، لم يعد التدقيق التقليدي اليدوي كافياً لضمان دقة وموثوقية التقارير المالية؛ لذلك فإن توجه البنوك نحو تدقيق إلكتروني عالي الجودة هو بمثابة تحول استباقي نحو رقابة ذكية تعتمد على تحليل البيانات في الوقت الفعلي. وهذا الاهتمام يعكس فهماً كبيراً للعلاقة

التبادلية بين الأمن السيبراني والتدقيق الإلكتروني. فمن ناحية، يشكل التدقيق الإلكتروني أداة محورية للكشف عن الثغرات والمخالفات في الأنظمة. ومن ناحية أخرى، فإن نجاح عملية التدقيق الإلكتروني وجودة مخرجاتها تعتمدان بشكل كبير على أمن وسلامة الأنظمة التي يتم تدقيقها. فالبيانات الخاطئة أو غير السليمة تؤدي إلى استنتاجات تدقيقية خاطئة، مما يفسر سبب اقتران زيادة الوعي بالمخاطر السيبرانية بزيادة الاستثمار في أدوات وتقنيات التدقيق الإلكتروني لتعزيز دقته وموثوقيته.

3- أظهرت الدراسة أن مخاطر الأمن السيبراني تؤثر في جودة التدقيق الإلكتروني. وهذا يؤكد أن الأمن السيبراني والتدقيق الإلكتروني وجهان لعملة واحدة في المؤسسات المالية، فكلما ارتفع مستوى هذه المخاطر، زادت التحديات التي تواجه عملية التدقيق، مما يستلزم تطوير آليات تدقيق أكثر تطوراً وقدرة على التكيف. وتعتبر هذه العلاقة علاقة تفاعلية، فوجود مخاطر سيبرانية عالية يخلق بيئة تدقيق غير مستقرة، مما يحفز على تطوير ضوابط أمنية أكثر كفاءة، وبدورها توفر بيئة مستقرة تمكن من إجراء تدقيق إلكتروني موثوق عالي الجودة. وبالتالي، فإن إدارة المخاطر السيبرانية بشكل فعال تسهم في حماية البنك، وتمثل استثماراً استراتيجياً في تعزيز وظيفة الرقابة والتدقيق، مما ينعكس إيجاباً على حوكمة البنك ومصداقيته. وقد توافقت هذه النتيجة مع نتيجة دراسة محمود وآخرين (2025)، والخروف (2025)، وNgo and Tick (2021). بينما اختلفت هذه النتيجة مع نتيجة دراسة Rosati et al. (2022).

4- يؤكد التأثير المعنوي لمخاطر أمن المعلومات في جودة التدقيق الإلكتروني على أن سلامة البيانات هي أساس التدقيق الإلكتروني. فالمخاطر المرتفعة في هذا الجانب تعني احتمالية التلاعب بالبيانات أو تسريبها، مما يحد من الثقة في أدلة التدقيق الإلكترونية ويجعل نتائجها عرضة للتشكيك. لذلك، فإن تعزيز أمن المعلومات يمثل حوكمة متقدمة لبيئة التدقيق الرقمي، ويضمن أن المعلومات التي يتم تحليلها هي نفسها المعلومات التي تعكس الواقع الفعلي.

5- يسلط تأثير المخاطر التكنولوجية والتشغيلية على جودة التدقيق الإلكتروني الضوء على أن التدقيق الإلكتروني هو تطبيق يعمل ضمن بنية تقنية. ففشل الأنظمة، أو ضعف تكاملها، أو انقطاع الخدمة، كلها أحداث تؤدي إلى تعطيل إجراءات التدقيق أو فقدان البيانات أثناء التحليل. كما أن العمليات التشغيلية غير المصممة بشكل جيد، مثل عدم وجود بروتوكول واضح

للتعامل مع البيانات أو ضعف التنسيق بين قسم تكنولوجيا المعلومات والتدقيق، تخلق فجوات تشغيلية تؤثر سلباً على سلاسة وكفاءة عملية التدقيق وموثوقية نتائجها. وتوافقت هذه النتيجة مع نتيجة دراسة Saputra and Paranoan (2024).

6- يشير أثر مخاطر الأداء على جودة التدقيق الإلكتروني على أن جودة التدقيق الإلكتروني لا تعتمد فقط على التكنولوجيا، بل أيضاً على كفاءة العنصر البشري في توظيف هذه التكنولوجيا. فالمدققون يحتاجون إلى مهارات رقمية متطورة تمكنهم من استخدام أدوات التدقيق المتقدمة وفهم مخرجاتها. كما أن وضوح السياسات، وفعالية التنسيق بين الإدارات، وتوافر الوقت والموارد اللازمة، كلها عوامل أدائية تحدد مدى قدرة عملية التدقيق على اكتشاف الأخطاء الجوهرية. وأي قصور في هذا الجانب، حتى مع وجود أنظمة تقنية ممتازة، قد يؤدي إلى بقاء التحريفات دون كشف، مما يجعل الأداء الفعال بمثابة القاعدة الأساسية التي تضمن تحقيق القيمة المضافة المرجوة من التدقيق الإلكتروني. وقد توافقت هذه النتيجة مع نتيجة دراسة Iskandar and Deniswara (2025).

**التوصيات:** بناءً على مناقشة النتائج السابقة، يمكن تقديم التوصيات التالية موجّهة لمختلف المستويات في البنوك الأردنية بهدف تعزيز التكامل بين الأمن السيبراني وجودة التدقيق الإلكتروني:

- 1- تبني البنوك الأردنية أطر عمل متقدمة للأمن السيبراني تهدف إلى حماية الأصول، وتركز على ضمان استمرارية الأعمال حتى في ظل نجاح هجوم سيبراني. ويتطلب ذلك إجراء اختبارات اختراق دورية ومحاكاة سيناريوهات هجمات متطورة لتقييم قدرة البنية التحتية على التحمل والتعافي السريع، مع توثيق الدروس المستفادة وتحديث خطط الاستجابة للحوادث باستمرار.
- 2- تطوير البنوك الأردنية مؤشرات أداء رئيسية متقدمة لمخاطر الأداء السيبراني تقيس فعالية العنصر البشري والتنظيمي.
- 3- على الإدارات العليا في البنوك الأردنية اعتبار المخاطر السيبرانية جزءاً لا يتجزأ من إطار إدارة المخاطر المؤسسية الشامل، ويجب أن يتم رفع تقارير دورية ومنتظمة إلى مجلس الإدارة حول حالة المخاطر السيبرانية وتأثيرها المحتمل على الاستقرار المالي والسمعة، مع تخصيص ميزانيات كافية ومرنة للاستجابة للمتغيرات في هذا المجال.
- 4- استثمار البنوك الأردنية في أدوات التدقيق المستمر والتحليلات المتقدمة مثل (أدوات ذكاء الأعمال، وتعلم الآلة)، لتحليل كامل قاعدة البيانات (وليس العينات فقط) والكشف عن الأنماط غير الطبيعية والاحتمالات المحتملة بشكل آني.

- 5- التعاون بين إدارات تكنولوجيا المعلومات وإدارات التدقيق في البنوك الأردنية لضمان أن أي نظام أو أداة تدقيق إلكتروني يتم تطويرها أو شراؤها تتضمن أعلى معايير الأمن السيبراني منذ مرحلة التصميم الأولى، ويشمل ذلك التشفير القوي للبيانات، وإدارة الهويات والصلاحيات بدقة، وتأمين واجهات برمجة التطبيقات المستخدمة في تبادل البيانات.
- 6- تشكيل البنوك الأردنية لجان أو فرق عمل تنسيقية دائمة تضم ممثلين عن إدارة أمن المعلومات، وإدارة المخاطر التشغيلية، وإدارة التدقيق الداخلي، وعقد اجتماعات دورية لمناقشة المخاطر المستجدة، وتبادل المعرفة حول الثغرات المكتشفة، وتقييم تأثير الخطط الأمنية على خطط التدقيق، والعمل معاً على تطوير سيناريوهات اختبار مشتركة.
- 7- تصميم البنوك الأردنية برامج تدريبية مستمرة للمدققين الداخليين لرفع كفاءتهم في المجالات التقنية والأمنية (مثل تحليل البيانات، وأمن الشبكات)، وتقديم برامج توعوية وتدريبية متخصصة للأمن السيبراني حول أساسيات التدقيق والمتطلبات الرقابية، مما يساهم في خلق مدققين تقنيين وخبراء أمن سيبراني ملمين بالرقابة.
- 8- تبني البنوك الأردنية أطر مرجعية موحدة لمواجهة المخاطر التكنولوجية والتشغيلية وإدارة أمن المعلومات، مما يضمن أن عمليات التدقيق الإلكتروني تتم وفق معايير جودة قوية ومعترف بها دولياً.

## المراجع:

### المراجع العربية:

- أكساس، إيمان وقادري، أحمد معراج (2021). واقع تبني التسويق الداخلي في المؤسسات الجزائرية ودوره في تعزيز مفهوم الجودة "دراسة حالة مؤسسة قديلة للمياه المعدنية". *مجلة نماء للاقتصاد والتجارة*، 5(2)، 107-123.
- براهيمي، فائزة وحديدي، آدم (2025). مساهمة الأمن السيبراني في الحد من مخاطر نظم المعلومات الحاسوبية الرقمية في المصارف الإسلامية. *المجلة الجزائرية للمالية الإسلامية*، 3(1)، 1-15.
- بن بوعل، خديجة (2021). دور التدقيق الإلكتروني في الحد من ممارسة المحاسبة الإبداعية في المؤسسات الاقتصادية الجزائرية. *مجلة المحاسبة التدقيق والمالية*، 3(2)، 77-90.
- البنك المركزي الأردني (2018)، *تعليمات التكيف مع المخاطر السيبرانية*، <https://www.cbj.gov.jo/>.
- البواعنة، سهل محمد (2023). *أثر مخاطر الأمن السيبراني في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن*، رسالة دكتوراه غير منشورة، جامعة العلوم الإسلامية العالمية، الأردن.
- بولعراس، حمزة وسليمان، عصام (2022). مساهمة جودة التدقيق الخارجي في الحد من إدارة الأرباح بالمستحقات والأنشطة الحقيقية - دراسة آراء مجموعة من المهنيين والأكاديميين. *الأفاق للدراسات الاقتصادية*، 7(2)، 50-68.

الحاج، محمد عبدالله رمضان والعلوص، محمد الهلول (2021). مفهوم إدارة الجودة الشاملة كمدخل لتطوير العمل الإداري بالاتحاد الليبي للألعاب. *مجلة العلوم الرياضية والمرتبطة*، 4(34)، 258-269.

حميداتو، صالح (2023). معايير التدقيق الدولية والبيئة الجزائرية. *الآفاق للدراسات الاقتصادية*، 8(1)، 49-69.

الخروف، فادي جمال (2025). أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي: الدور المعدل لمتطلبات البنك المركزي لتدقيق شركات التكنولوجيا المالية في الأردن، رسالة دكتوراه غير منشورة، جامعة العلوم الإسلامية العالمية، الأردن.

سعيد، قيثان سليمان حمة وحسين، سهلا مهيدي حمة (2022). دور الذكاء الاصطناعي في تحقيق جودة التدقيق الخارجي: دراسة استطلاعية من وجهة نظر مراقبي الحسابات في إقليم كردستان العراق. *المجلة العلمية لجامعة جيهان- السليمانية*، 6(1)، 353-385.

الشيخ، صالح سامي صالح وأحمد، عماد يوسف (2023). أثر إطار عمل (COSO) للرقابة الداخلية في الحد من مخاطر المحاسبة السحابية: الدور الوسيط للأمن السيبراني في البنوك التجارية الأردنية. *مجلة جدار للدراسات والبحوث*، 9(2)، 79-115.

عبد الصمد، نجوى وبن أزواو، ليلي (2022). متطلبات الرقابة على جودة التدقيق في الجزائر: مراجعة أولية. *مجلة دفاتر اقتصادية*، 13(1)، 334-350.

عبدالله، فيصل نجم الدين، ومصطفى، شيرزاد أحمد (2017). مدى استخدام تكنولوجيا المعلومات في عملية التدقيق الخارجي. *مجلة زانكو للعلوم الإنسانية*، 21(6)، 139-156.

العجمي، محمد والعلي، طالب (2019). دور التدقيق الإلكتروني في رفع كفاءة التدقيق الخارجي. *مجلة جامعة دمشق للعلوم الاقتصادية والسياسية*، 35(5)، 138-159.

عويضة، عيسى ونقاز، أحمد (2022). جودة خدمة التدقيق الخارجي على إعانات الدولة للجمعيات في الجزائر- دراسة تطبيقية. *مجلة البحوث الاقتصادية المتقدمة*، 7(1)، 273-289.

الفضلي، زهراء عبد الحمزة، والعامري، سميه علي (2025). دور الذكاء الاصطناعي في تحقيق جودة التدقيق في ظل التحول الرقمي. *مجلة الريادة والأعمال*، 6(2)، 140-155.

كريمة، أحمد المختار السيد (2024). دور الأمن السيبراني في مكافحة الفساد. *مجلة القرطاس*، 2(25)، 145-165.

محمود، يارا محمود، حافظ، سماح طارق، الجوهرى، إبراهيم السيد (2025). أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين. *المجلة العلمية للدراسات والبحوث المالية والتجارية*، جامعة دمياط، 6(14)، 827-860.

المركز الوطني للأمن السيبراني (2019). *قانون الأمن السيبراني الأردني*. <https://pm.gov.jo/ar/Pages/NewsPaper>

- معمرى، أسامة ومفتاح، حمزة وعمورة، جمال (2020). متطلبات تحسين جودة التدقيق وتفعيل الرقابة عليها في شركات أو مكاتب التدقيق وفق المعيار الدولي للتدقيق 220. *مجلة دراسات متقدمة في المالية والمحاسبة*، 3(2)، 52-36.
- ملياني، وائل وسعود، وسيلة (2024). دور التدقيق الإلكتروني في تحسين جودة التدقيق الخارجي – وجهة نظر عينة من المهنيين والأكاديميين. *مجلة البحوث في العلوم المالية والمحاسبية*، 9(1)، 109-129.
- المولى، مثنى عبدالوهاب (2018). أوجه التشابه والاختلاف بين مفهوم الجودة ومفهوم التميز لدى منظمات الأعمال. *مجلة كلية المعارف الجامعية*، 27(1)، 638-658.
- مومني، يوسف وفراج، الطيب (2020). مساهمة التدقيق الإلكتروني في تحسين جودة المعلومات المحاسبية – دراسة ميدانية لعينة من المهنيين في الجزائر. *مجلة آفاق للبحوث والدراسات*، 3(2)، 307-323.
- يخلف، صفية، وطوشي، محمد (2020). دور التدقيق الإلكتروني في تحسين جودة ممارسة مهنة التدقيق الداخلي وأثرها على تعظيم القيمة للأطراف المستفيدة من حوكمة الشركات. *مجلة البشائر الاقتصادية*، 6(2)، 763-779.
- يوسف، سمر يوسف طه (2024). دور تقنية نشر وظيفة الجودة (QFD) في تحسين مفهوم الوحدة المحاسبية في الشركات الصناعية. *المجلة العلمية للبحوث التجارية*، 4(55)، 871-896.

### المراجع الأجنبية:

- Almubaydeen, T. H., Alnaji, I., Alkabbji, R., Zahran, S., & Kanan, M. (2024). The effect of electronic auditing in improving the quality of accounting information in the Jordanian industrial companies listed on the Amman stock exchange. In *Artificial Intelligence and Economic Sustainability in the Era of Industrial Revolution 5.0* (pp. 1269-1280). Cham: Springer Nature Switzerland.
- DeAngelo, L. E. (1981). Auditor size and audit quality. *Journal of accounting and economics*, 3(3), 183-199.
- El Badlaoui, A., Cherqaoui, M., & Taouab, O. (2021). Output indicators of audit quality: A framework based on literature review. *Universal Journal of Accounting and Finance*, 9(6), 1405-1421.
- Hidayat, I., Abbas, D., Hamdani, H., & Saad, A. (2024). The mediator role of the quality auditing in the relationship between the non -financial factors of audit fees. *JRAK*, 16(2), 245-256.
- Iskandar, N. & Deniswara, k. (2025). Toward Secure Auditing: A Study On Auditor Resdiness in Cybersecurity Implementation Using Extended Utaut Framwwork, *Journal of Theoretical and Applied Information Technology*, 103 (4).

- Kanyongo, G. & Wadesango, N. (2025). Impact Of Cybersecurity On Risk Mitigation Strategy By Commercial Banks In Emerging Markets: A legal Perspective Case Study, *Journal of The Authors*, 7 (1), 28 -37. <https://doi.org/10.1080/22495/dgrv7ilp3>
- Khandelwal, A., Minuk, L., Liu, Y., Arnold, D. M., Heddle, N. M., Barty, R., ... & Callum, J. (2022). Plasma transfusion practices: A multicentre electronic audit. *Vox Sanguinis*, 117(10), 1211-1219.
- Ngo, Tran Nguen Bao & Tick, Andrea (2021). Cyber-security risks assessments by external auditors. *Interdisciplinary Description of Complex Systems*, 19(3), 375-390. <https://doi.org/10.7906/indexs.19.3.3>
- Peng, J., & Krivacek, G. (2020). The growing role of cybersecurity disclosures. *ISACA Journal*, 2020, 1-7.
- Rosati, Pierangelo, Gogolin, Fabian & Lynn, Theo (2022). Cyber-security incidents and audit quality. *European Accounting Review*, 31(3), 701-728. DOI: 10.1080/09638180.2020.1856162
- Saputra, Komang Adi Kurniawan & Paranoan Selmita (2024). Do cyber security, digitalization and data visualization affect the quality of internal environmental audit?. *AABF*, 18(2), 158-174.

## The Impact of Cybersecurity Risks on the Quality of E-Auditing in Jordanian Banks

### Abstract

This research aimed to examine the impact of cybersecurity risks, across its dimensions (information security risks, technological and operational risks, and performance risks), on the quality of e-auditing in Jordanian banks. The descriptive-analytical methodology was employed using a questionnaire, along with a number of statistical methods such as arithmetic means, standard deviations, and multiple regression coefficients, with SPSS software used for data analysis and hypothesis testing. The sample consisted of employees working in the finance, internal audit, and information technology departments of Jordanian banks, including internal auditors, accountants, and technical staff in these divisions. Accordingly, the researchers distributed (180) electronic questionnaires, of which (167) were retrieved, all of which were valid for analysis.

The research results showed a statistically significant positive impact at a significance level of ( $\alpha \leq 0.05$ ) of cybersecurity risks across its dimensions on the quality of e-auditing. The research recommended continuing efforts to strengthen the necessary cybersecurity controls to mitigate the impact of risks on the quality of e-auditing, and the necessity of continuous development in employee training programs regarding information security risks.

**Keywords:** Cybersecurity Risks, E-Auditing Quality, Jordanian