انعكاسات مخاطر التحول الرقمي على عملية المراجعة.
(دراسة ميدانية)

Reflections of Digital Transformation Risks on The Audit Process.
(A Field Study)

د. ولاء نصرالدين جاد
مدرس المحاسبة
المعهد العالي لعلوم الحاسب ونظم المعلومات (CIS)

المستخلص:

قامت العديد من المؤسسات في عصر التقدم التكنولوجي وتطوره السريع بتبني التحول الرقمي بشكل متزايد للحفاظ علي ميزتها التنافسية في ظل تطور المشهد التجاري، حيث يشمل التحول الرقمي دمج التقنيات الرقمية في جميع جوانب المؤسسة، مما يغير بشكل جوهري كيفية عملها وقيمتها للمعنيين بها، وبينما يجلب هذا التحول فوائد عديدة، يتسبب أيضًا في مجموعة من المخاطر، ومع تحول المشهد التقليدي للمراجعة والذي كان في السابق يعتمد بشكل رئيسي على الورق والعمل اليدوي، الي الأرضية الرقمية المعقدة وترقية المؤسسات لعملياتها، يواجه المراجعين تحديات وتعقيدات جديدة لضمان نزاهة وأمان وموثوقية المعلومات المالية، ونتيجة لذلك أصبح فهم وتخفيف اثر المخاطر المرتبطة بالتحول الرقمي أمرًا حيويًا للمراجعين للحفاظ على مصداقية وفعالية عمليات المراجعة الخاصة بهم.

ويهدف هذا البحث إلى استكشاف المخاطر المتعددة المضمنة في رحلة التحول الرقمي والانغماس في تأثيرها العميق على عملية المراجعة، ومحاولة الوصول الي أفضل الممارسات والاستراتيجيات للتخفيف من هذا التأثير.

الكلمات المفتاحية: التحول الرقمي، المخاطر الرقمية، عملية المراجعة، مخاطر المراجعة، سلامة البيانات، التنظيم، الامتثال، المراجعة المستمرة، تحليلات البيانات، إدارة المخاطر.

Abstract:

In the era of rapid technological advancements and its swift, organizations are increasingly embracing digital transformation to stay competitive and agile in the evolving business landscape. While this shift brings numerous benefits, it also introduces a myriad of risks that can significantly impact the auditing process. The traditional audit landscape, once predominantly paper-based and manual, is now navigating through a complex digital terrain. As organizations digitize their processes, auditors face new challenges and complexities in ensuring the integrity, security, and reliability of financial information. Understanding and mitigating the risks associated with digital transformation have become imperative for auditors to maintain the credibility and effectiveness of their assurance processes. This paper aims to (1) Explore the multifaceted risks embedded in the digital transformation journey, (2) Delves into their profound impact on the auditing process, (3) Recommend Best Practices and Mitigation Strategies.

Keywords: *Digital Transformation, Digital Risks, Audit Process, Audit Risks, Data Integrity, Regulatory, Compliance, Continuous Auditing, Data Analytics, Risk Management.*

١ – المقدمة

وفقاً لتعريف (Gartner, 2016) التحول الرقمي هو "عملية الانتقال إلى الأعمال الرقمية لتغيير نموذج الأعمال وتوفير مصادر وفرص جديدة، ويّري التحول الرقمي على انه الأرضية الأساسية بين العالم الحالي والعالم المستقبلي للأعمال، ويتفق كل من خبراء التقنيات الرقمية وصناع القرارات على أهمية اعتماد أنظمة أكثر مرونة لتقليص الفجوة بين العمل المكتبي ونظيره الافتراضي حيث لم يعد هناك مكان لبيئات العمل البطيئة في ظل التطورات السريعة في عالم الأعمال اللحظي خاصة بعد تصاعد جائحة كوفيد التي تطلبت وسائل أسرع للعمل، وعلي الرغم مما يقدمه التحول الرقمي من تقدم كبير، إلا أن هناك عدة مخاطر مرتبطة به، بما في ذلك احتمال هجمات القرصنة، وانتهاكات البيانات، وفشل التكنولوجيا، بالإضافة إلى ذلك، يمكن أن يؤدي التحول الرقمي أيضًا إلى اضطرابات تعرقل سير الأعمال إذا لم يكن لدي المؤسسة القوي اللازمة للتعامل معه، ونتيجة لذلك، فمن المهم أن يتم إدارة التوقعات ووضع طموحات واقعية لعملية التحول الرقمي، حيث انه عندما لا تأخذ المؤسسات في اعتبارها المخاطر الضمنية له، يمكن أن تنتهي بارتكاب أخطاء مكلفة.

من ناحية أخرى، فإن تزايد تعقيد الأعمال وثورة البيانات قد أطلقا تحديات جديدة، ووفقاً لـ (McAllum, 2016) يحدث اضطراب في مجتمع البشر بمعدل ١٠ مرات أسرع وبنسبة ٣٠٠ مرة مقارنة بفترة الثورة الصناعية، وبالتالي يُلاحَظ تأثير التحول الرقمي بمقدار يُقارَب ٣٠٠٠ مرة أكثر في العصر الجديد، ونظرًا لأن مهنة المراجعة تؤدي دورًا أساسيًا في عالم الأعمال لتحقيق نزاهة ودقة البيانات المالية، فإنها تواجه العديد من التحديات نتيجةً لوتيرة التحول الرقمي السريع (Babayeva, 2022).

٢ – مشكلة البحث

وفقا لدراسة (Nurhajati, 2016)تعرفعملية المراجعة على انها عملية تقويم ومراجعة أنظمة المؤسسات وعملياتها من قبل فريق مستقل، وتهدف عملية المراجعة إلى تحسين الكفاءة والفعالية واكتشاف المخاطر والتحكم فيها، والمؤسسات

التي تستخدم التحول الرقمي في عملياتها تصبح أكثر تنافسية وربحية وأكثر مرونة في مواجهة منافسيها، حيث يهدف التحول الرقمي في المؤسسات وفقاً لتقرير (Gartner, 2016) إلى تقديم أفضل الخدمات والمنتجات للعملاء بطرق حديثة ومبتكرة وبشكل مختصر، مما يتطلب تغييرًا في الإجراءات التنظيمية، وفهمًا للجمهور ومعرفة بثقافة الأعمال والعملاء وكذلك التعرف على المخاطر الكامنة في عملية التحول الرقمي.

وتكمن المشكلة الرئيسية للبحث في محاولة الإجابة عن التساؤل الآتي:

"ما هي انعكاسات مخاطر التحول الرقمي على عملية المراجعة وكيف يمكن إدارتها؟"

ويتفرع من هذا التساؤل عدة تساؤلات فرعية كالتالي:

١- كيف تُثير البنية التحتية للسحابة المتعددة والسحابة الهجينة تحديات في استجابة عملية المراجعة؟

٢- ما هي المخاطر المرتبطة بالاعتماد المتزايد على أنظمة سلسلة التوريد الرقمية، وكيف تؤثر هذه المخاطر على فعالية الأساليب التقليدية لعمليات المراجعة؟

٣- كيف يسبب إنترنت الأشياء (IoT) المخاطر لعملية المراجعة، وما هي التدابير التي يمكن اتخاذها للتعامل مع هذه المخاطر؟

٤- ما هي المخاطر الجديدة التي قد يدخلها الاعتماد المتزايد على الأتمتة والتحليلات في عمليات المراجعة خاصة فيما يتعلق بدقة البيانات والتحيزات الخوارزمية وإمكانية وجود أنشطة احتيال غير مكتشفة؟

٥- بأي الطرق تؤثر مخاطر استخدام تكنولوجيا Blockchain على عمليات وأساليب المراجعة التقليدية، وكيف يمكن للمراجعين التكيف لتخفيف هذه المخاطر؟

٦- كيف يزيد استخدام الذكاء الاصطناعي في المراجعة من مخاطر المراجعة، وما هي الاستراتيجيات التي يمكن تنفيذها لضمان عملية مراجعة عادلة ومسؤولة؟

٧- ما هي المخاطر المرتبطة ب Big Data في المراجعة، وما هي التدابير التي يجب أن يتخذها المراجعين لمعالجة هذه المخاطر؟

٣- أهداف البحث

يتمثل الهدف الرئيسي للبحث في رصد تأثير مخاطر التحول الرقمي على عملية المراجعة وذلك من خلال تحقيق الأهداف الفرعية التالية:

١. دراسة كيف تُثير البنية التحتية للسحابة المتعددة والسحابة الهجينة تحديات في استجابة عملية المراجعة؟
٢. التعرف على المخاطر المرتبطة بالاعتماد المتزايد على أنظمة سلسلة التوريد الرقمية، وكيف تؤثر هذه المخاطر على فعالية الأساليب التقليدية لعمليات المراجعة؟
٣. دراسة كيف يسبب إنترنت الأشياء (IoT) المخاطر لعملية المراجعة، وما هي التدابير التي يمكن اتخاذها للتعامل مع هذه المخاطر؟
٤. التعرف على المخاطر التي قد يدخلها الاعتماد المتزايد على الأتمتة والتحليلات في عمليات المراجعة خاصة فيما يتعلق بدقة البيانات والتحيزات الخوارزمية وإمكانية وجود أنشطة احتيال غير مكتشفة؟
٥. دراسة كيفي تؤثر مخاطر استخدام تكنولوجيا Blockchain على عمليات وأساليب المراجعة التقليدية، وكيف يمكن للمراجعين التكيف لتخفيف هذه المخاطر؟
٦. معرفة كيف يزيد استخدام الذكاء الاصطناعي في المراجعة من مخاطر المراجعة، وما هي الاستراتيجيات التي يمكن تنفيذها لضمان عملية مراجعة عادلة ومسؤولة؟
٧. التعرف على المخاطر المرتبطة ب Big Data في المراجعة، وما هي التدابير التي يجب أن يتخذها المراجعين لمعالجة هذه المخاطر؟
٨. تحديد أفضل الممارسات والاستراتيجيات اللازمة لتجنب مخاطر التحول الرقمي.

٤- أهمية البحث

تكشف الأدبيات الحالية عن فجوة ملحوظة في البحوث المتعلق بالتحديات والمخاطر المعقدة التي يواجها المراجعين في سياق التحول الرقمي، و يظهر هذا العجز بشكل خاص في ندرة الأبحاث التي توضح تأثير مخاطر التحول الرقمي على إجراءات

المراجعة والمعايير والمنهجيات، والغياب الواضح لدليل موحد أو مجموعة من التوصيات المصممة بشكل صريح لمساعدة المراجعين في التنقل بفعالية في وجه التحديات المعقدة التي يطرحها التحول الرقمي، ويحاول هذا البحث ملء الحاجة الملحة للجهود العلمية التي تهدف إلى سد هذه الفجوة الواضحة في الفهم، وبالتالي تزويد الممارسين برؤية تعزز من متانة ممارسات المراجعة في عصر التحول الرقمي الشامل.

٥- المحاور الرئيسية للدراسة

هدفت الباحثة في هذا الجزء إلى تحليل الدارسات السابقة التي تناولت مخاطر التحول الرقمي وتأثيرها على عملية المراجعة وذلك لتحديد الفجوة البحثية الموجودة في الدراسات السابقة، ولمعرفة المتغيرات التي يمكن استخدامها في الدراسة الميدانية.

ولتحقيق الهدف من هذه الجزئية قامت الباحثة بتقسيم الدراسات السابقة على أساس المتغيرات التي تتضمنها الدراسة إلى سبع محاور كالتالي:

أ- المحور الأول: مخاطر البنية التحتية للسحابة المتعددة والسحابة الهجينة (Multi-cloud and hybrid cloud infrastructures)

وفقاً لتقرير (Flexera, 2023) أبلغت ٨٧٪ من المؤسسات عن استخدامها لاستراتيجيات سحابية متعددة، و٧٢٪ منها تتخذ نهجًا مختلطًا من خلال الجمع بين استخدام السحابتين العامة والخاصة، ويري (Vehent, 2018) أن هذه الديناميكيات تشكل تحديات لآليات المراجعة التقليدية، التي تجد صعوبة في مراقبة وإدارة التغييرات في البنية التحتية بشكل فعال حيث تواجه المؤسسات صعوبات كبيرة في جذب المهنيين المهرة ذوي الخبرة في البيئات السحابية المتعددة عند توسيع عملياتها.

ويري (Torkura et al., 2021) انه بينما تعمل تكنولوجيا المعلومات على تبسيط عملية المراجعة الخارجية، فإنها تقدم مخاطر يمكن أن تؤثر على نتائجها، تشمل هذه المخاطر التحديات المتعلقة باختفاء البيانات أو الصعوبة في تتبع الأدلة الإلكترونية (المخاطر الكامنة)، والمخاطر المرتبطة بالرقابة، والفشل المحتمل في اكتشاف أو منع الأخطاء أو الانتهاكات الجسيمة في البيانات المالية (مخاطر

الاكتشاف)، ومن الأهمية بمكان أن نلاحظ أن مخاطر المراجعة التقليدية لا تزال قائمة حتى مع دمج تكنولوجيا المعلومات.

وأوضح (Robson & Sowel, 2022) أن البيئات السحابية المتعددة والسحابة الهجينة تتضمن العديد من موفري الخدمات السحابية Cloud Service Providers (CSPs) والمكونات المحلية وهذا التعقيد المتزايد يجعل المراجعة أكثر صعوبة، حيث يحتاج المراجعون إلى فهم وتقييم الأنظمة والتكوينات والتفاعلات المختلفة، ويزداد التعقيد مع اعتماد الحوسبة السحابية، حيث توجد التقنيات المستخدمة خارج شركات المراجعة.

وينصح (Nurhajati, 2016) مستخدمو الحوسبة السحابية بإجراء تقييم للمخاطر التي قد يتعرضون لها عند العمل في البيئة السحابية (والذي يعتمد على نوع الخدمة السحابية ونموذجها المستخدم، ويعتبر تقييم تنفيذ وفعالية الضوابط الأمنية أحد الجوانب الأساسية لمراجعة الأمن في البيئة السحابية المتعددة.

وقدم كل من (Dhirani et al., 2019; Kallinikos et al., 2013; Rittinghouse & Ransome, 2017) رؤى حول التحديات القضائية التي يواجهها مستخدمي البيئة السحابية والتحديات المرتبطة بقيود حركة البيانات وتأثيرها على الامتثال وحوكمة البيانات، فقد تخضع البيانات المخزنة عبر العديد من موفري الخدمات السحابية للوائح إقليمية مختلفة لحماية البيانات، مما قد يؤدي إلى مشكلات الامتثال عند استخدام العديد من موفري الخدمات السحابية، ويتطلب مراجعة إعدادات البيئة السحابية المتعددة والهجينة تقييم ممارسات حوكمة البيانات، بما في ذلك تصنيف البيانات وعناصر التحكم في الوصول وسيادة البيانات عبر موفري الخدمات السحابية المختلفين، واصبح الامتثال للوائح مثل General Data Protection Regulation (GDPR) أو The Health Insurance Portability and Accountability Act (HIPAA) أو المعايير الخاصة بالصناعات أكثر تعقيدا بسبب الطبيعة الموزعة للبيانات.

ويري (Alonso et al., 2023) أن حوكمة البيانات الفعالة ومراجعة الامتثال في البيئات السحابية المتعددة والهجينة تتطلب فهما شاملا للتحديات التي تفرضها البيانات الموزعة، ويجب على المؤسسات الاستفادة من التقنيات والأدوات المناسبة لضمان الشفافية والأمن والالتزام باللوائح ووضع ضوابط أمنية موحدة، ومن خلال معالجة هذه الجوانب يمكن للشركات التنقل بثقة في تعقيدات إدارة البيانات في عصر البيئة السحابية.

وسلطت إرشادات (CSA, 2019; NIST, 2020) الضوء على التعقيدات المرتبطة بكل من تنسيق التحكم في الوصول القائم على الأدوار في البيئات متعددة السحابة، وضرورة فحص تكوين وانتشار عناصر التحكم لتحديد نقاط الضعف والتأكد من توافقها مع أفضل ممارسات الصناعة.

ويري (Agu et al., 2019) كذلك أن المخاطر المتعلقة بالبيئة السحابية تتضمن مخاطر تكامل البيانات وقابلية التشغيل البيني حيث يجب أن تشمل المراجعة فحصا شاملا لتدفقات البيانات، ورسم خرائط لكيفية انتقال المعلومات عبر الأنظمة المختلفة، وهذا يشمل تقييم كفاءة آليات نقل البيانات وتحديد أي اختناقات أو نقاط فشل محتملة ويتضمن ذلك فحص بروتوكولات التشفير وعناصر التحكم في الوصول وآليات المصادقة المعمول بها أثناء نقل البيانات.

وفقاً لدراسة (Forcepoint, 2019; Praveena et al., 2021) يجب أن تؤكد المراجعة أيضا علي أن البيانات ليست آمنة فحسب، بل تصل أيضا إلى وجهتها بدقة، دون خسارة أو تلف، ويمكن أن يساعد استخدام حلول (DLP) Data Loss Prevention في مراقبة ومنع النقل غير المصرح به للبيانات الحساسة.

ويري (Botta et al., 2016) انه من الصعب تحديد وفهم التكاليف الخفية أو غير المتوقعة المرتبطة بالخدمات السحابية، مثل رسوم الخروج أو زيادة التخزين حيث إن تقييم ما إذا كانت المؤسسة تستخدم الخدمات والموارد السحابية الأكثر فعالية

من حيث التكلفة تقدم تحديات لعمليات المراجعة، كما ناقش البحث العوامل التي تؤثر على التكلفة الإجمالية للملكية (TCO) في البيئات السحابية.

ب- المحور الثاني: دراسات متعلقة بمخاطر سلسلة الإمداد الرقمية (Digital supply chains)

وفقاً لكل من (Pasula et al., 2013) هناك نماذج مختلفة لسلسلة التوريد داخل الشركات والتي ويتم تكييفها مع التعقيدات المختلفة للنشاط الذي تشارك فيه، ولا يوجد نموذج مثالي يوفر أفضل النتائج، وتنقسم عمليات إدارة سلسلة التوريد التي حددها The Global Supply Chain Forum الي (إدارة علاقات العملاء؛ إدارة العلاقات مع الموردين؛ إدارة خدمة العملاء؛ إدارة الطلب؛ تنفيذ الطلب؛ إدارة تدفق التصنيع؛ تطوير المنتجات وتسويقها؛ إدارة المرتجعات) كل هذه العمليات هي ملامح مترابطة لسلسلة التوريد داخل جميع أنواع الأعمال ونجاحها يتطلب التعاون بين جميع الوظائف داخل المنشأة.

وفقاً لدراسة (Ageron et al., 2020; Chen et al., 2023) فقد نتج عن تزايد اعتماد منظمات الأعمال على التكنولوجيا الرقمية، العديد من المخاطر المتنوعة والمعقدة، بما في ذلك مخاطر أمن المعلومات والموثوقية والانتهاكات ومخاطر الامتثال ومخاطر السرية والنزاهة وانعدام الثقة، مما يؤثر سلبا على دور سلسلة التوريد وتحقيق أهدافها وبالتالي التأثير على الأهداف العامة للمنظمة.

وقال جوزيف تارانتينو الرئيس والمدير التنفيذي لمؤسسة الاستشارات العالمية Protiviti إن مجالس الإدارة ولجان المراجعة التابعة لها يجب أن تكون على دراية بالعقبات والفرص التي تنتظرها وأن تكون مستعدة لتقديم المشورة لمؤسساتها بسرعة وفاعلية، ووفقاً لشركة Protiviti تم إدراج إدارة مخاطر سلسلة التوريد وارتفاع تكاليف السلع ضمن أكبر عشرة تحديات تجارية لشركات الخدمات غير المالية (www.cfoinnovation.com).

وفقاً لدراسة (Powell, 2022) تولد سلاسل التوريد الرقمية كميات هائلة من البيانات التي يعتمد عليها المراجعون في عملهم، وتؤثر الرقمنة المتزايدة لسلاسل التوريد على تعقيد ونطاق عملية المراجعة بعدة طرق، فمع استخدام التقنيات الرقمية، أصبحت سلاسل التوريد أكثر ترابطا ونتج عن هذا زيادة كبيرة في حجم البيانات وسرعتها والمزيد من البيانات المتنوعة التي يحتاج المراجعون إلى تحليلها، حيث أن هذه البيانات تعتبر عرضة للتلاعب والأخطاء والانتهاكات، لذلك يحتاج المراجعون إلى التأكد من سلامة البيانات التي يقومون بمراجعتها والتحقق من دقتها واكتمالها عن طريق التحقق من مخاطر التلاعب أو الوصول غير المصرح به الذي قد يؤثر على موثوقية نتائج المراجعة.

ويري (Dasaklis et al., 2022; Dutta et al., 2020; Ivanov & Dolgui, 2021; MacCarthy & Ivanov, 2022)) انه يمكن لسلاسل التوريد الرقمية تحسين الشفافية وإمكانية التتبع من خلال توفير معلومات في الوقت الفعلي عن حركة وحالة السلع والخدمات، ومع ذلك، يواجه المراجعون الهديد من التحديات في التحقق من دقة هذه المعلومات أثناء مرورها عبر مختلف الأنظمة الرقمية، وقد يتطلب ضمان سلامة البيانات ودقتها تنفيذ Blockchain أو غيرها من التقنيات المقاومة للعبث والتي تعمل على تعزيز سلامة البيانات في عمليات سلسلة التوريد، ومعالجة المخاوف المتعلقة بالثقة والموثوقية.

ويري (Bansal et al., 2022; Kalia et al., 2021; Kshetri, 2017) أن استخدام بيانات سلسلة التوريد الرقمية خاصة عند التعامل مع المعلومات الحساسة، مثل بيانات العملاء أو الأسرار التجارية، يوجب على المراجعين التأكد من أن تتوافق ممارسات معالجة البيانات مع اللوائح ذات الصلة، مثل اللائحة العامة لحماية البيانات The General Data Protection Regulation (GDPR)، وكذلك التأكد من أن تدابير حماية البيانات المناسبة مطبقة.

ويري (Ivanov & Dolgui, 2021; Pettit et al., 2019) انه لتقييم مرونة واستمرارية سلاسل التوريد الرقمية، يحتاج المراجعون إلى تقييم وجود وفعالية خطط التعافي من الكوارث وأنظمة النسخ الاحتياطي وتدابير التكرار، ويجب عليهم أيضا اختبار استجابة سلسلة التوريد لاضطرابات المحاكاة لقياس قدرتها على التعافي ومواصلة العمليات.

وفقاً لدراسة (Ivanov et al., 2019; Larson, 2001) تؤثر رقمنة سلسلة التوريد على إدارة المخزون وإعداد التقارير المالية من خلال توفير المزيد من البيانات في الوقت الفعلي حول مستويات المخزون ومعلومات المعاملات ويحتاج المراجعون إلى التحقق من دقة واكتمال سجلات المخزون والبيانات المالية من خلال مقارنتها بالعدد المادي والمستندات الداعمة.

وفقاً لمنشورات (IIA, 2022) غالبا ما تتضمن سلاسل التوريد الرقمية العديد من البائعين ومقدمي الخدمات الخارجيين، ويحتاج المراجعون إلى تقييم المخاطر المرتبطة بهذه الكيانات الخارجية، مثل الاستقرار المالي والامتثال للوائح والالتزام ببروتوكولات الأمان، ويمكن أن يكون للفشل أو الاختراق في أي مرحلة من مراحل سلسلة التوريد آثار متتالية على عملية المراجعة، ويجب على المراجعين ضمان الإشراف والمراقبة الكافيين لهؤلاء البائعين.

ويري كل من (MacCarthy & Ivanov, 2022) أن المراجعين يحتاجوا إلى النظر في المشهد التنظيمي وتقييم ما إذا كانت سلسلة التوريد الرقمية تلتزم بالقوانين ذات الصلة، مثل خصوصية البيانات أو حماية المستهلك أو اللوائح الخاصة بالصناعة حيث يمكن أن يؤدي عدم الامتثال إلى مخاطر قانونية للمنظمة الخاضعة للمراجعة.

ويري (Sabri, 2019) إن سلاسل التوريد ازدادت تعقيداً بسبب العولمة، والاستعانة بمصادر خارجية، والشبكات المعقدة، وعدم اليقين والتقلب في القدرات اللوجستية، والانتشار السريع لوحدات حفظ المخزون (SKUs) وتكوينات المنتجات، ومع ذلك، يواصل العديد من المصنعين وتجار التجزئة استخدام النهج القديم لتجزئة

سلسلة التوريد وهو ما يمثل عائقا أكثر من كونه مساعدة في تقليل التعقيد وتحسين الهامش.

ت- المحور الثالث: دراسات متعلقة بمخاطر إنترنت الأشياء (Internet of things (IoT))

وفقاً لدراسة (Diego & Francisco, 2021; Griffin, 2017) يعد إنترنت الأشياء ابتكارا جديدا يفتقر إلى بعض التطبيقات الفعالة ولكن ازداد استخدامه في السنوات الماضية خاصة في الشركات الكبيرة التي يمكنها تحمل تكاليف الأجهزة والبرامج لجعل جمع البيانات أسهل وأقل استهلاكا للوقت، ولذلك يتم توظيف محللي البيانات بأعداد كبيرة للمساعدة في سد الاحتياجات اللازمة لفهم جميع البيانات التي يتم جمعها.

ناقش (Diego & Francisco, 2021) انتشار أجهزة إنترنت الأشياء وكيف توسع نطاق عمليات المراجعة، وشددوا على حاجة المراجعين إلى التكيف مع التعقيد المتزايد لبيئات تكنولوجيا المعلومات، بما في ذلك الزيادة الكبيرة في الأجهزة المترابطة.

ذكر (Flexera, 2023; Vehent, 2018) التعقيدات التي أدخلها إنترنت الأشياء في سياق الأمن السحابي، وقد سلط (Torkura et al., 2021) الضوء على التحديات التي يفرضها العدد المتزايد من أجهزة إنترنت الأشياء، مشدداً على ضرورة أن يأخذ المراجعون في الاعتبار مجموعة أوسع من الأجهزة في تقييماتهم، وأشار تقرير (ENISA, 2018) الي حاجة المراجعين إلى تقييم الضوابط الأمنية المحيطة بأجهزة إنترنت الأشياء وضمان موثوقية البيانات التي يقومون بمراجعتها وإنشاء إجراءات فعالة للتحقق من صحة البيانات لضمان دقة واكتمال المعلومات المالية.

وفقاً لدراسة (Peng et al., 2020) ينطبق إنترنت الأشياء على أي نظام أو تطبيق أو جهاز أو منصة متصلة بالشبكة العنكبوتية، مما يجعل المجتمع أكثر ترابطاً من أي وقت مضى وهذا بالطبع يخلق فرصاً جديدة وبالتالي مخاطر جديدة مثل الافتقار إلى الوجود المادي ونقل وتخزين البيانات غير الآمن، بالإضافة إلى ذلك،

تكون الكميات الهائلة من البيانات التي تم إنشاؤها بواسطة أجهزة إنترنت الأشياء هدفا مغرياً لمجرمي الإنترنت.

وفقاً لورقة عمل نشرتها شركة الاستشارات العالمية Protiviti يجب أن يكون تركيز المراجعين على مستوى "الحل" للسلسلة المستمرة " وإيجاد أفضل الممارسات الداخلية للتعرف على ومواجهة المخاطر الجديدة التي يمثلها إنترنت الأشياء (Griffin, 2017)، حيث يمكن أن تؤدي الاختراقات الأمنية إلى المساس بسلامة وسرية المعلومات المالية التي يحتمل أن تؤثر على إجراءات المراجعة.

أكد (Torkura et al., 2021) على الحاجة إلى المراقبة المستمرة واكتشاف التهديدات للتخفيف من المخاطر المرتبطة بقابلية أجهزة إنترنت الأشياء للهجمات السيبرانية وتقييم التدابير الأمنية، وشددت (ICAEW, 2017) في تقريرها على أهمية بقاء المراجعين على اطلاع بالتقنيات الناشئة ونواقل الهجوم المرتبطة بها.

ث- المحور الرابع: دراسات متعلقة بمخاطر الأتمتة والتحليلات (Automation and analytics)

تعرف الأتمتة وفقاً لقاموس هارفرد للأعمال على إنها عملية إنشاء وتطبيق تقنيات لإنتاج السلع والخدمات وتقديمها بأقل قدر من التدخل البشري، يؤدي تنفيذ تقنيات وعمليات الأتمتة إلى تحسين كفاءة وموثوقية و/أو سرعة العديد من المهام التي كان يؤديها البشر سابقاً، ويتم استخدام الأتمتة في عدد من المجالات مثل التصنيع والنقل والمرافق والتقنيات العسكرية والعمليات ومؤخراً تكنولوجيا المعلومات.

أضاف كل من (Mökander et al., 2021; NIST SP 800-37, 2018) في دراستهم أن هناك خطر من اعتماد المراجعين بشكل كبير على الأتمتة وأدوات التحليل دون ممارسة الحكم المهني المناسب، في حين أن هذه الأدوات يمكن أن توفر رؤى قيمة، إلا أنه يجب استخدامها كمساعدات وليس كبدائل للحكم البشري، وأكدوا على الحاجة إلى نهج متوازن يجمع بين الأتمتة والحكم البشري من أجل عملية مراجعة شاملة وموثوقة.

أوضحت دراسة (Mökander et al., 2021) أن استخدام أدوات المراجعة الآلية في المجالات الحساسة، مثل اكتشاف الاحتيال، يثير العديد من المخاوف الأخلاقية، فإذا لم يتم تطوير هذه الأدوات أو مراقبتها بشكل كاف، فمن المحتمل أن تؤدي إلى اتهامات كاذبة أو انتهاك للخصوصية، علاوة على ذلك، قد تكون هناك آثار أخلاقية من حيث الشفافية والإفصاح إذا كان أصحاب المصلحة غير مدركين لاستخدام الأدوات الآلية في عملية المراجعة، كما شدد على أهمية عمليات التطوير والرصد القوية للتخفيف من مخاطر الاتهامات الكاذبة أو انتهاكات الخصوصية، كما تدعو المبادئ التوجيهية الأخلاقية إلى الشفافية والإفصاح لدعم نزاهة عملية المراجعة.

يري (A. Hasan et al., 2022; Kordzadeh & Ghasemaghaei, 2022) أن الأتمتة والتحليلات يمكن أن تؤدي إلى إدخال تحيزات في عملية المراجعة إذا كانت الخوارزميات المستخدمة تستند إلى بيانات تاريخية متحيزة أو افتراضات معيبة، بالإضافة إلى ذلك، قد يقوم المراجعون أنفسهم بإدخال تحيزات غير مقصودة أثناء تصميم وتنفيذ الأنظمة الآلية، مما يؤدي الي صعوبة تفسير النتائج الناتجة عن أنظمة المراجعة الآلية والتحقق من صحتها، خاصة عندما تكون الخوارزميات المستخدمة معقدة ولا يمكن فهمها بسهولة، ولذلك فإن التدريب التوعوي والمبادئ التوجيهية الأخلاقية من الأمور المهمة للتخفيف من التحيزات غير المقصودة.

وفقاً لدراسة (Bansal et al., 2022; PwC, 2017) يمكن أن تستبعد الأتمتة في المراجعة، دون قصد، البيانات أو المعاملات المهمة عندما لا تكون الخوارزميات المستخدمة مصممة لالتقاط أنواع معينة من المعاملات التي تقع خارج المعايير التي حددها النظام الآلي، بالإضافة إلى ذلك، إذا لم يتم تحديث الأتمتة بانتظام للتكيف مع التغييرات في العمليات أو اللوائح التجارية، فقد يتم تفويت البيانات ذات الصلة.

يري (CPA, 2020; Mokander et al., 2021; PwC, 2017) أن الاعتماد على المراجعة الآلية يمكن أن يؤثر على عملية إبلاغ نتائج المراجعة إلى

العملاء وأصحاب المصالح، فقد لا توفر التقارير الآلية دائماً السياق أو التفسيرات اللازمة وراء نتائج المراجعة، مما يؤدي إلى سوء الفهم أو سوء التفسير، ولهذا يجب على المراجعين التأكد من أن تظل عملية التواصل شفافة وشاملة ويمكن الوصول إليها، حتى عند استخدام الأتمتة.

ج- المحور الخامس: دراسات متعلقة بمخاطر سلسة الكتل (Blockchain)

وفقاً لتقرير (Deloitte, 2017) ودراسة (Han et al., 2023) يمكن تصنيف مخاطر Blockchain الي ثلاث فئات: (١) المخاطر المعيارية: تعرض تقنيات Blockchain المؤسسات لمخاطر مشابهة لتلك المرتبطة بالعمليات التجارية الحالية ولكنها تقدم فروقاً دقيقة تحتاج الكيانات إلى حسابها.

(٢) مخاطر نقل القيمة: تتيح Blockchain نقل القيمة من نظير إلى نظير دون الحاجة إلى وسيط مركزي ويعرض نموذج العمل الجديد هذا الأطراف المتفاعلة لمخاطر جديدة كانت تدار سابقا من قبل وسطاء مركزيين، (٣) مخاطر العقود الذكية: يمكن للعقود الذكية تشفير التعاقدات التجارية والمالية والقانونية المعقدة على Blockchain ، مما يؤدي إلى المخاطر المرتبطة برسم الخرائط الفردية لهذه الترتيبات one-to-one mapping وتحويلها من الإطار المادي إلى الإطار الرقمي، ووفقاً لدراسة (Lombardi et al., 2022; Politou et al., 2021) يتطلب مراجعة العقود الذكية فهماً قوياً للغة البرمجة الأساسية واحتمال حدوث أخطاء في الترميز أو نقاط الضعف التي قد تؤدي إلى أخطاء مالية أو انتهاكات أمنية، ولذلك يتم حث المراجعين على معالجة نقاط الضعف في الترميز، وتقييم وتعزيز التدابير الأمنية لمنع الوصول غير المصرح به، واستكشاف سبل التحقق الخارجي، وتنفيذ إجراءات اختبار قوية للتخفيف من العواقب التي لا رجعة فيها لتنفيذ العقود الذكية.

يشير تقرير (Deloitte, 2018) أن دور ومهارات المراجعين قد تتغير مع ظهور تقنيات وإجراءات جديدة قائمة على Blockchain، على سبيل المثال، ستحتاج طرق الحصول على أدلة مراجعة مناسبة وكافية إلى النظر في كل من دفاتر الأستاذ

العامة التقليدية المستقلة وكذلك دفاتر أستاذ سلسلة الكتل، بالإضافة إلى ذلك، هناك احتمالية لمزيد من التوحيد والشفافية في الإبلاغ والمحاسبة، مما قد يمكن المراجعين من استخراج البيانات وتحليلها بشكل أكثر كفاءة.

تظهر دراسة (Appelbaum et al., 2018) أن ثبات Blockchain وعدم إمكانية عكس المعاملات يجعل من الصعب تصحيح الأخطاء أو الأنشطة الاحتيالية بمجرد تسجيلها على Blockchain ، وقد يواجه المراجعون العديد من المخاطر والتحديات المحتملة عند التحقق من صحة ودقة السجلات المالية القائمة على Blockchain، حيث يعمل نظام Blockchain بطريقة لامركزية على عكس الأنظمة المركزية التقليدية، مما يجعل من الصعب تحديد الأطراف المسؤولة ومحاسبتها، ويشكل هذا النقص في الرقابة مخاطر على موثوقية أدلة مراجعة الحسابات واكتمالها وكذلك تحديث وتصحيح الأخطاء في السجلات المالية.

وفقاً لكل من (Deloitte, 2017; Graham, 2023; Gürcan, 2020) تمثل مراجعة المعاملات والعقود عبر الحدود التي تتم على شبكات Blockchain العالمية تحديات بما في ذلك:

• المسائل القضائية: يمكن أن يكون تحديد اللوائح القضائية التنظيمية التي تنطبق على معاملات محددة أمراً معقداً، لا سيما في الشبكات الدولية اللامركزية.

• الامتثال للوائح المحلية: يجب على المراجعين التأكد من أن المعاملات التي تتم على شبكات Blockchain العالمية تتوافق مع اللوائح المحلية ذات الصلة في كل دولة.

• الاختلافات اللغوية والثقافية: قد يواجه المراجعون حواجز لغوية واختلافات في الممارسات والمعايير المحاسبية عبر الحدود.

• تحويلات العملة: قد تنطوي المعاملات عبر الحدود على عملات متعددة، مما يتطلب من مراجعي الحسابات مراعاة تقلبات أسعار الصرف وقضايا التقييم المحتملة.

ح- المحور السادس: دراسات متعلقة بمخاطر الذكاء الاصطناعي (Artificial Intelligence)

تبحث المؤسسات بشكل متزايد عن طرق لوضع تقنيات الذكاء الاصطناعي (AI) للعمل على تحسين إنتاجيتها وربحيتها ونتائج أعمالها، ومع ذلك، في حين أن هناك العديد من الفوائد التجارية للذكاء الاصطناعي، إلا أن هناك أيضا بعض الحواجز والعيوب التي يمكن أن تسبب أضراراً جسيمة للبنية التحتية للشركة وسمعتها، فعلى سبيل المثال تسبب الانهيار السريع لعام ٢٠١٠ (The flash crash) الذي استمر لمدة ٣٦ دقيقة في خسارة سوق الأسهم الأمريكية ٩٪ من قيمتها.

يري (Issa et al., 2016) انه على الرغم من قيام Big 4 بالمزيد من الاستثمارات لاستخدام الذكاء الاصطناعي في عملية الممارسات الاستشارية والتوكيد، هناك صحوة تدريجية لحقيقة العواقب غير المقصودة التي قد تنشأ.

يري (Contag et al., 2017) أن التطورات التكنولوجية متاحة لضمان تحسين جودة أدلة المراجعة، ومع ذلك، نظراً لأن المؤسسات والمراجعين يعتمدون أكثر فأكثر على الذكاء الاصطناعي، فهناك العديد من الافتراضات الأساسية التي قد يقومون بها، أحد هذه الافتراضات هو الاعتقاد بأن هذه الأنظمة دقيقة دائماً، الافتراض الثاني هو أن أنظمة الذكاء الاصطناعي ستتصرف دائماً ضمن القيود المرغوبة، الافتراض الثالث هو أن الاختلاف عن القيود المرغوبة سيكون قابلاً للاكتشاف والتصحيح.

وفقاً لاستطلاع أجراه المنتدى الاقتصادي العالمي(WEF, 2020) (World Economic Forum survey) عام ٢٠١٥ على ٨٠٠ مدير تنفيذي وجد أن ٧٥٪ من هؤلاء المديرين التنفيذيين يعتقدون أنه بحلول عام ٢٠٢٥، ٣٠٪ من عمليات مراجعة المؤسسات سيتم إجراؤها باستخدام الذكاء الاصطناعي.

وفقاً لتقرير (CPA, 2020) يعتمد الذكاء الاصطناعي بشكل كبير على البيانات، ويمكن أن تؤثر جودة وسلامة البيانات المستخدمة في المراجعة بشكل مباشر على نزاهة وموثوقية عمليات المراجعة التي تعتمد على الذكاء الاصطناعي، والنزاهة

هي قدرة المراجع أو غريزته على أن يكون شجاعاً وشفافاً ومسؤولاً وحكيماً وصادقاً، لذلك لا يمكن تقييم النزاهة من خلال نظام أو تقنية مراجعة قائمة على التكنولوجيا، حيث إنها تحتاج الي غرائز المراجع الخاصة، وإذا كانت البيانات المستخدمة لتدريب الذكاء الاصطناعي غير كاملة أو غير دقيقة أو متحيزة، فإن ذلك يؤدي إلى نتائج مراجعة خاطئة (Cheng et al., 2021).

ويري (Griffin, 2017; Joshi, 2021) أن الاعتماد على الذكاء الاصطناعي يمكن أن يؤثر في المراجعة على مستوى الحكم البشري والشك المهني المستخدم عادة في عملية المراجعة، حيث لا يستطيع أن يحل محل مهارات التفكير النقدي والحكمي للمراجعين، وتظل الرقابة البشرية أمر ضروري وحاسم لضمان توافق نتائج الذكاء الاصطناعي مع السياق والظروف المحددة لكل مهمة من مهام المراجعة.

يري (Fedyk et al., 2022; Stancheva, 2018) إن للاعتماد علي الذكاء الاصطناعي في المراجعة تأثير كبير على دقة وموثوقية البيانات المالية، حيث يمكن لخوارزميات الذكاء الاصطناعي تحديد الأنماط والحالات الشاذة والاتجاهات التي قد يكون من الصعب على البشر اكتشافها، وتحسين الكفاءة، والحد من التحيز البشري، والتصدي للتحديات التقليدية، مما يؤدي إلى تحليل أكثر شمولاً ودقة للبيانات المالية، غير أنه يشدد أيضاً على حاجة المراجعين إلى النظر بعناية في قيود خوارزميات الذكاء الاصطناعي وممارسة الحكم المهني لضمان دقة وأهمية استنتاجات المراجعة.

وفقاً لتقرير (Deloitte, 2023; Eprs, 2023) يتمثل أحد تحديات الذكاء الاصطناعي في ضمان توافق معايير استخدام أنظمة الذكاء الاصطناعي مع لوائح ومعايير المراجعة ومواكبة التطور السريع للتكنولوجيا والمشهد التنظيمي، ولذلك تحتاج شركات المراجعة إلى إنشاء آلية للمراقبة المستمرة وتحديث نماذج الذكاء الاصطناعي مع الامتثال للقوانين واللوائح المتغيرة وقد يتضمن ذلك التعاون مع الهيئات التنظيمية وخبراء الصناعة للبقاء على اطلاع بالتحديثات ذات الصلة.

وفقاً لتقرير (CPA, 2020) يمكن لأتمتة إجراءات المراجعة من خلال الذكاء الاصطناعي إعادة تحديد الأدوار والمسؤوليات الوظيفية للمراجعين بما فيه من آثار عميقة، ومن اجل تلاشي ذلك التأثير يتم تشجيع المراجعين على تبني المهارات التحليلية المحسنة، والتركيز على الحكم والرقابة، والتكيف مع التغيرات التكنولوجية المستمرة.

ويري (A. Hasan et al., 2022) أن بعض خوارزميات الذكاء الاصطناعي، مثل الشبكات العصبية للتعلم العميق، معقدة ويصعب شرحها أو تفسيرها، ويشكل هذا الافتقار إلى الشفافية المزيد من تحديات لعملية المراجعة، حيث يكافح المراجعون لفهم كيفية وصول نماذج الذكاء الاصطناعي إلى استنتاجاتها، وتتطلب معالجة هذه المخاطر تطوير نماذج ذكاء اصطناعي يمكن تفسيرها وتزويد المراجعين بالأدوات والتقنيات اللازمة لتقييم موثوقية وشفافية عمليات المراجعة القائمة على الذكاء الاصطناعي.

يري (A. R. Hasan, 2022; Munoko et al., 2020) أن قضية المسؤولية والمساءلة موضوعا مركزياً في الخطاب القانوني والأخلاقي حول الذكاء الاصطناعي في المراجعة، ويعد تحديد المسؤولية في حالة الأخطاء أو التحيزات أو العواقب غير المقصودة لقرارات الذكاء الاصطناعي أمراً بالغ الأهمية، ويجب أن تتطور الأطر القانونية لمواجهة هذه التحديات، كما يجب وضع خطوط واضحة للمساءلة.

خ- المحور السابع: دراسات متعلقة بمخاطر البيانات الضخمة (Big Data)

أوضحت دراسة (Brown-Liburd et al., 2015) انه بالاستناد إلى معيار المراجعة الدولي رقم ١١٠٥ (Professional skepticism) الشك المهني يجب أن تكون أدلة المراجعة كافية ومناسبة، وهذا يعتمد فقط على حكم المراجع، مما يخلق تحدياً لمهنة المراجعة حول كيفية استخراج القيمة من البيانات الضخمة وضمان أن تستند أحكام المراجعة إلى معلومات عالية الجودة ذات صلة وموثوقة (PCAOB, 2010).

ويري (Al-Ateeq et al., 2022; Brunsdon & Comber, 2020; Dimitris et al., 2020; Hezam et al., 2023) أن الاعتماد على تحليلات البيانات الضخمة فقط دون إجراءات المراجعة التقليدية العديد من العواقب المحتملة مثل:

• التغاضي عن العوامل النوعية: قد لا تلتقط تحليلات البيانات الضخمة جميع الجوانب النوعية التي يمكن للمراجعين البشريين أخذها في الاعتبار.

• الأخطاء الجوهرية: قد يؤدي الاعتماد فقط على البيانات الضخمة إلى التغاضي عن أخطاء كبيرة أو أنشطة احتيالية غير واضحة في البيانات.

نشرت لجنة التجارة الفيدرالية (FTC, 2022) Federal Trade Commission في أغسطس ٢٠٢٢، إشعاراً مسبقاً تحت عنوان Trade Regulation Rule on Commercial Surveillance and Data Security لاستقصاء أراء العامة حول القواعد المقترحة لممارسات المراقبة التجارية وأمن البيانات، بما في ذلك تلك المتعلقة بقاعدة الضمانات الخاصة بها من بين أمور أخرى، وطرح الإشعار المسبق لوضع القواعد المقترحة أسئلة متعددة حول جمع بيانات المستهلك واستخدامها والاحتفاظ بها بما في ذلك ما إذا كان:

• يجب أن تقتصر المؤسسات على جمع بيانات المستهلك أو الاحتفاظ بها أو استخدامها أو نقلها فقط بالقدر اللازم لتقديم الخدمة المحددة التي يسعى إليها مستهلك فردي معين صراحة أو تلك المتوافقة مع تلك الخدمة المحددة.

• ينبغي فرض قواعد جديدة لتنظيم التجارة لتقييد الفترة الزمنية التي تجمع فيها المؤسسات بيانات المستهلك أو تحتفظ بها، بغض النظر عن الأغراض المختلفة التي تضع تلك البيانات من أجلها.

• ينبغي أن يطلب من المؤسسات أن تشهد بأن ممارساتها في مجال المراقبة التجارية تفي بمعايير واضحة فيما يتعلق بجمع بيانات المستهلك أو استخدامها أو الاحتفاظ بها أو نقلها أو تسييلها.

وفقاً لدراسة (Small & Whitepaper, 2019) للاعتماد بشكل كبير على موفري البيانات الخارجيين للمراجعة القائم على البيانات الضخمة العديد الآثار مثل:

• عدم وجود رقابة: قد يكون للمراجعين سيطرة محدودة على جودة وسلامة البيانات التي تم الحصول عليها من أطراف ثالثة.

• قضايا الامتثال للبيانات: قد يؤدي الاعتماد على مزودي البيانات التابعين لجهات خارجية إلى إثارة مخاوف بشأن ملكية البيانات والخصوصية والامتثال للوائح.

يري كل من (Fadlallah et al., 2023; Walshe, 2021) أن التطور السريع لتقنيات البيانات الضخمة يمكن أن يؤثر على مدى كفاية وأهمية معايير المراجعة الحالية بطرق مختلفة كالتالي:

• المبادئ التوجيهية التي عفا عليها الزمن: قد لا تعالج معايير المراجعة التقليدية بشكل كاف التعقيدات والمخاطر المرتبطة بتحليلات البيانات الضخمة.

• فجوات المهارات: قد يفتقر المراجعون إلى المهارات والمعرفة اللازمة للاستفادة من أحدث تقنيات البيانات الضخمة بشكل فعال.

• تحديات توحيد المعايير: مع تطور التكنولوجيات، يمكن أن يصبح توحيد ممارسات مراجعة الحسابات عبر الصناعات أكثر صعوبة.

٦- منهجية الدراسة:

تتحقق أهداف هذا البحث من خلال المزج بين المنهجين الاستقرائي والاستنباطي كما يأتي:

أ- المنهج الاستقرائي:

اعتمدت الباحثة على استقراء التعليمات والإصدارات الدولية وكذلك دراسة خلاصة ما توصلت إليه الأبحاث العلمية المتعلقة بموضوع التحول الرقمي وتأثيره على المراجعة.

ب- المنهج الاستنباطي:

لغرض الدراسة قامت الباحثة بإجراء دراسة ميدانية للوقوف على رأي كلٍ من مراقبي الحسابات والمستخدمين بشأن مخاطر التحول الرقمي ومدي تأثيرها على عملية المراجعة وذلك باستخدام طريقة دلفي وهي تقنية تسمح للخبراء بالتعامل بشكل منهجي مع مشكلة أو مهمة معقدة (Ismail & Taliep, 2023) وتتألف من سلسلة من الاستبيانات التي ترسل إما عن طريق البريد أو عن طريق النظم المحوسبة إلى فريق من الخبراء المختارين مسبقا، والغرض من هذه الاستبيانات هو استنباط وتطوير ردود فردية على المشاكل المطروحة.

٧- متغيرات وفروض البحث

أ- **متغيرات الدراسة:**

- **المتغيرات المستقلة:**

- مخاطر البنية التحتية للسحابة المتعددة والسحابة الهجينة.
- مخاطر سلسلة الإمداد الرقمية.
- مخاطر إنترنت الأشياء.
- المخاطر الأتمتة والتحليلات.
- مخاطر سلسة الكتل.
- مخاطر الذكاء الاصطناعي.
- مخاطر البيانات الضخمة.

- **المتغير التابع:**

- عملية المراجعة.

ب- فروض الدراسة: -

يمكن صياغة فروض الدراسة كالآتي:

١- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر البنية التحتية للسحابة المتعددة والسحابة الهجينة وعملية المراجعة.

٢- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر سلسلة الإمداد الرقمية وعملية المراجعة.

٣- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر إنترنت الأشياء وعملية المراجعة.

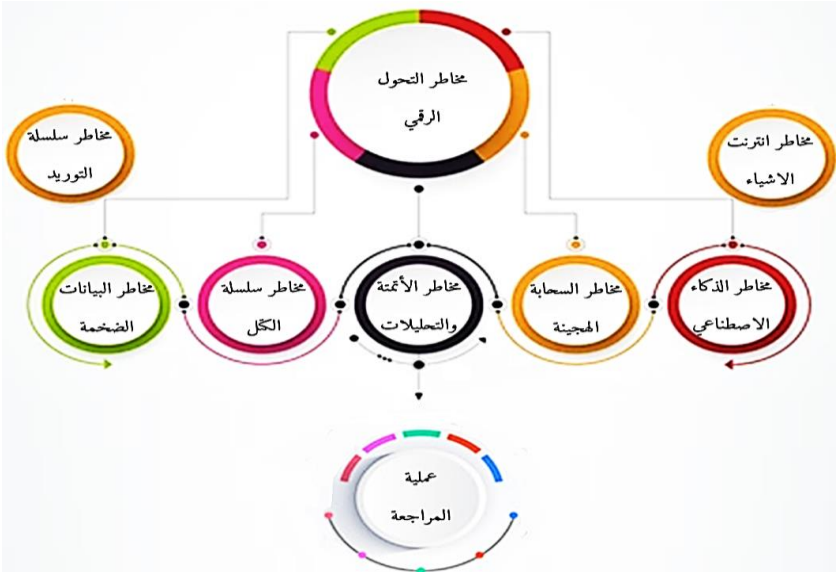
٤- توجد علاقة طردية ذات دلالة إحصائية بين المخاطر الأتمتة والتحليلات وعملية المراجعة.

٥- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر سلسة الكتل وعملية المراجعة.

٦- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر الذكاء الاصطناعي وعملية المراجعة.

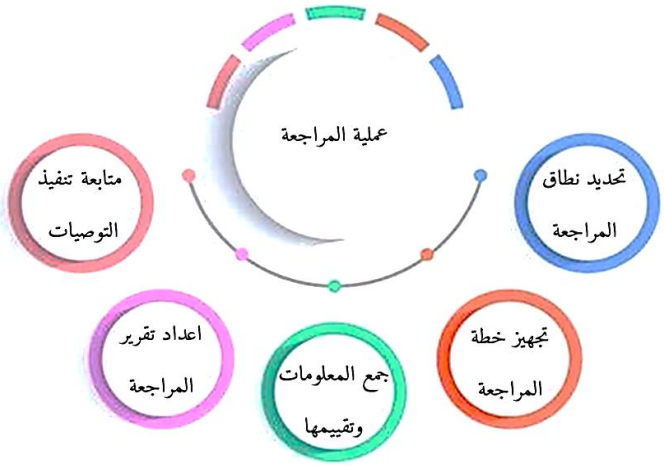
٧- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر البيانات الضخمة وعملية المراجعة.

ويمكن تلخيص العلاقة بين المتغيرات في الشكل رقم (١)



شكل رقم (١): متغيرات الدراسة

المصدر: من إعداد الباحثة



شكل رقم (٢) عملية المراجعة

المصدر: من إعداد الباحثة

٨- اختبارات الفروض ونتائج الدراسة

أ- مجتمع الدراسة

اعتمدت الباحثة في اختيار مجتمع الدراسة على خبرة أفراده في مجال المحاسبة والمراجعة من مهنيين وأكاديميين بمحافظة الجيزة وتمثل مجتمع الدراسة في الفئات التالية:

- **الفئة الأولي:** ٣٨ مراقب حسابات مقيد بسجلات البنك المركزي في نطاق محافظة الجيزة والمنشور أسمائهم على الموقع الالكتروني للبنك.
- **الفئة الثانية:** ١٦ أستاذ واستاذ مساعد عامل داخل الجامعات الحكومية بمحافظة الجيزة والمنشور أسماءهم على الموقع الالكتروني لكلية التجارة، جامعة القاهرة.

ب- عينة الدراسة

قامت الباحثة بتحديد مجتمع الدراسة والذي تضمن مراقبي الحسابات المقيدين بسجلات البنك المركزي وأساتذة المحاسبة في الجامعات الحكومية داخل نطاق محافظة الجيزة وذلك لسهولة التواصل معهم، وتم إرسال قوائم الاستقصاء التي اعتمدت عليها الدراسة لتجميع البيانات إلى مفردات العينة والبالغ عددها وفقاً لمعادلة ستيفن ثامبسون الإحصائية (٥٠) مفردة.

$$n=\frac{N\times p(1-p)}{\left[\left[N-1\times\left(d^2\div z^2\right)\right]+p(1-p)\right]}$$

N: حجم المجتمع والمكون من (٣٨ مراقب حسابات + ١٦ أستاذ واستاذ مساعد فعال) داخل نطاق محافظة الجيزة.

Z: الدرجة المعيارية المقابلة لمستوي الدلالة ٩٥٪

D: نسبة الخطأ وتساوي ٤٪

P: نسبة توافر الخاصية والمحايدة وتساوي ٠.٥٠

وبعد عملية الفرز والتنظيم تبين أن مجموع الاستمارات التي تمت الإجابة عليها هي (٤٤) استمارة كما هو مبين في الجدول التالي: -

جدول (١)

بيان مفردات العينة

م	البيان	العدد	النسبة
١	حجم العينة	٥٠	١٠٠٪
٢	عدد الاستمارات المجاب عنها	٤٤	٨٨٪

المصدر: من إعداد الباحثة

وفقاً للجدول السابق كانت نسبة الاستمارات المجاب عنها تساوي ٨٨٪ من حجم العينة وهي نسبة تصلح للاستخدام في التحليل الإحصائي.

وقامت الباحثة بتوصيف مفردات العينة وفقاً لكل من طبيعة العمل وذلك من خلال جدول (٢)

- **طبيعة العمل:**

جدول رقم (٢)

توصيف مفردات العينة وفقاً لطبيعة العمل

م	التوزيع	العدد	النسبة	الترتيب
٢	**مراقب حسابات**	٣٢	٧٢.٧٪	١
٣	**أستاذ مساعد**	٩	٢٠.٥٪	٢
	أستاذ دكتور	٣	٦.٨٪	٣
الإجـــــــــــــمالي		٤٤	**%100.0**	

المصدر: من إعداد الباحثة وفقاً لمخرجات برنامج SPSS الإصدار ٢٦

ج- مصادر جمع المعلومات

نظرا للأهمية العلمية والعملية التي يحظى بها الجانب الميداني لنجاح وإنجاز أي دراسة، فقد استهدفنا من خلال هذا المطلب إعطاء فكرة توضيحية لأهم المصادر المستخدمة في جمع البيانات والمعلومات المتعلقة بالجانب الميداني، فضلا عن الأساليب الإحصائية التي تم اتباعها لمعالجة أداة الدراسة وذلك بهدف قياس وتحليل الاختبارات الإحصائية لآراء ومقترحات مفردات العينة.

- **مصادر جمع البيانات الأولية:**

استندت الباحثة في جمع البيانات الأولية الي طريقة دلفي، والنقطة الرئيسية وراء طريقة دلفي هي التغلب على عيوب الطرق التقليدية حيث تكون تفاعلات المجموعة في دلفي مجهولة المصدر، بحيث لا يتم كشف هوية المشاركين أو التوقعات أو ما شابهها من حيث منشئها، ولكن يتم تقديمها للمجموعة بطريقة تمنع أي تعرف علي صاحبها (Günaydın, 1995) ويتم اتباع الخطوات التالية لتجميع البيانات:

(١) اختيار الخبراء: يتم اختيار لجنة خبراء تتألف عادة من ١٠ إلى ٢٠ فردًا بناءً على خبراتهم في المجال ذي الصلة أو الموضوع المعني.

(٢) الاستبيان للجولة الأولى: بدأت العملية من ١٢ إلى ٢٥ أغسطس ٢٠٢٣ بإعداد مجموعة من الأسئلة المفتوحة المتعلقة بموضوع الاهتمام. تم تلقي الاستبيان من قبل الخبراء الذين تم اختيارهم، وقدموا ردودهم الفردية وقاموا بإضافة تعليقات أو رؤى إضافية.

(٣) التجميع والتحليل: تم جمع ردود الخبراء وتلخيصها دون الكشف عن الردود الفردية، وقام الباحث بتجميع المعلومات وتحديد المجالات التي تتفق وتختلف فيها الآراء.

- **مصادر جمع البيانات الثانوية:**

قامت الباحثة في هذا الصدد الوصول إلى مصادر المعلومات والوثائق المتاحة، باعتبار أن هذه الخطوة الرئيسية بدأت قبل انطلاق البحث واستمرت معه حتى النهاية، حيث تعددت هذه الوثائق لتشمل كل من:

١- التقارير الصادرة عن الهيئات والمنظمات المهنية الدولية والمتعلقة بموضوع الدراسة.

٢- البحوث العلمية والمقالات الخاصة بموضوع الدراسة.

٣- إضافة إلى السابق اعتمدت الباحثة كذلك على قنوات أخرى من أجل الحصول على المعلومات، يأتي في مقدمتها الشبكة العنكبوتية وذلك من خلال البحث المستمر وتصفح العديد من المواقع المتخصصة في مجال المحاسبة والمراجعة خصوصا على المستوى الدولي، والتي ساعدتها في توجيه دراستها، وتصور منهجية العمل الميداني.

د. أداة الدراسة

لتحقيق أهداف الدراسة استعانت الباحثة باستمارة الاستقصاء لجمع البيانات اللازمة لقياس وتحليل الاختبارات الإحصائية لآراء مفردات العينة وذلك لما لاحظته من نقص في المعلومات في الميدان العملي الخاص بالموضوع.

١. تصميم استمارة الاستقصاء

قامت الباحثة خلال هذه المرحلة بتصميم عبارات الاستمارة بطريقة بسيطة وفقاً للعبارات التي تم التوصل إليها من مقابلات عينة الدراسة بحيث تسمح هذه العبارات باختبار فرضيات البحث، وهذا للإحاطة بكل جوانب تصميم الاستبيان لرفع نسبة الاتفاق لدى العينة.

وتم كتابة وتوزيع استمارات الاستقصاء يدويا أو باستخدام محركات البحث الإلكترونية، واستعانت الباحثة في تصميم الاستمارة بآراء الأساتذة مشرفي الرسالة، والبحوث والدراسات السابقة في هذا المجال، وقد قامت الباحثة قدر الإمكان خلال فترة إعداد القائمة الابتعاد عن التعقيد في طرح الأسئلة، كما قامت بالعمل على طرح مجموعة من العبارات بشكل متسلسل ومترابط حتى تجذب اهتمام وتركيز الفرد المستقصي، وذلك من أجل الحصول على أكبر قدر من الإجابات الجادة والموضوعية.

هذا فضلا عن الديباجة التي تتصدر الاستمارة، والتي تتضمن عنوان الموضوع محل الدراسة، مع تقديم وجيز لبعض المفاهيم المستخدمة في البحث وذلك لتوفير المعلومات اللازمة لفهم الموضوع بصوره أوضح.

٢. هيكل استمارة الاستبيان

تضمنت استمارة الاستبيان النهائية خمسة وسبعون عبارة (٧٥) رئيسية، توزعت على ثمانية محاور رئيسية، ومن أجل الوصول إلى الإجابة الواضحة والدقيقة للمستقصي منهم، تم صياغة العبارات وفقاً للأنواع المتعارف عليها (النوع المغلق)باتباع مقياس لكرت الخماسي وكانت المحاور الرئيسية للأسئلة كالتالي:

- المحور الأول: تضمن هذا القسم عبارات متعلقة بمخاطر البنية التحتية للسحابة المتعددة والسحابة الهجينة (Multi-cloud and hybrid cloud infrastructures) من رقم ١ إلى رقم ١٠.
- المحور الثاني: تضمن هذا القسم عبارات متعلقة بمخاطر سلسلة الإمداد الرقمية (Digital supply chains) من رقم ١١ إلى رقم ١٨.

- المحور الثالث: تضمن هذا القسم العبارات متعلقة بالمخاطر المتعلقة بإنترنت الأشياء ((Internet of things (IoT)) من رقم ١٩ إلى رقم ٢٧.
- المحور الرابع: تضمن هذا القسم العبارات المتعلقة المخاطر المتعلقة بالأتمتة والتحليلات (Automation and analytics) من رقم ٢٨ إلى ٣٨.
- المحور الخامس: تضمن هذا القسم عبارات متعلقة أسئلة متعلقة بمخاطر بسلسة الكتل من رقم ٣٩ الي ٤٩.
- المحور السادس: تضمن هذا القسم عبارات متعلقة أسئلة متعلقة بمخاطر بالذكاء الاصطناعي (Artificial intelligence) من رقم ٥٠ الي ٥٦
- المحور السابع: تضمن هذا القسم عبارات متعلقة أسئلة متعلقة المخاطر المتعلقة بالبيانات الكبيرة (Big Data) من رقم ٥٧ الي ٦٦.
- المحور الثامن: تضمن هذا القسم عبارات متعلقة بفاعلية عملية المراجعة من رقم ٦٧ الي ٧٥

هـ- حدود الدراسة

تقتصر حدود الدراسة على المتغيرات المستخدمة في البحث حيث لم تتطرق الدراسة لاي متغيرات أخري متعلقة بالتحول الرقمي بخلاف السبع متغيرات المذكورة سابقا، وركزت اهتمامها علي أراء الخبراء والمهنيين ممن لديهم المعلومات الكافية عن الموضوع داخل محافظة الجيزة بجمهورية مصر العربية وذلك خلال فترة البحث مما يتيح المجال لمزيد من الدراسات التي تتناول المزيد من المتغيرات وفقا للتطور المستمر في التحول الرقمي على مر الزمن.

و- نتائج اختبار متغيرات الدراسة

- **الأساليب الإحصائية المستخدمة في اختبار الفروض**

لإتمام متطلبات الدراسة طُلب من المستقصي منهم أن تكون الإجابة على أسئلة قائمة الاستقصاء من بين خمس إجابات وفقاً لمقياس لكرت الخماسي وقامت الباحثة بمراجعة استمارات الاستقصاء للتأكد من صلاحيتها لإدخال البيانات والتحليل الإحصائي، حيث تم استخدام الاستمارات التي تتوافر بها الشروط اللازمة، وتم ترميز المتغيرات والبيانات وتفريغها داخل برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) وقد تم استخدام الأساليب الإحصائية التالية:

- **اختبار المصداقية والثبات (Cronbach's Alpha):** وذلك لقياس مدي ثبات وصدق متغيرات الدراسة.
- **الإحصاءات الوصفية:** والتي اشتملت على كل من المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية والتوزيع التكراري ومعاملات الاختلاف وذلك لتحديد اتجاهات وخصائص عينة البحث نحو فرضيات الدراسة.
- **اختبار ت لعينه مستقله One sample t-test:** لقياس الفرق المعنوي بين متوسط العينة ومتوسط مجتمع الدراسة.
- **معامل الارتباط (Correlation):** لقياس طبيعة وقوة العلاقة بين متغيرات ومحاور البحث.
- **معامل الانحدار (Regression):** لقياس مدي تأثر كل متغير من المتغيرات بالآخر.

▪ **اختبار المصداقية والثبات (Cronbach's Alpha):**

قامت الباحثة باستخدام معامل الثبات Cronbach's Alpha ومعامل الصدق الذاتي لقياس ثبات المحتوي للدراسة ككل وكذلك ثبات المحتوي لمحاور الدراسة وكانت النتائج كما هو موضح في الجدول التالي:

جدول (٥)

معامل الصدق والثبات Cronbach's Alpha

م	متغيرات ومحاور الدراسة	العبارات	معامل الثبات	معامل الصدق
١	مخاطر السحابة المتعددة والسحابة الهجينة	١٠	٠.٨٩٢	0.944
٢	مخاطر سلسلة التوريد الرقمية	٨	٠.٧٧١	0.878
٣	مخاطر إنترنت الأشياء	٩	٠.٨٥٥	0.925
٤	مخاطر الأتمتة والتحليلات	١١	٠.٧٥٣	0.868
٥	مخاطر سلسلة الكتل	١١	٠.٧٧٠	0.877
٦	مخاطر الذكاء الاصطناعي	٧	٠.٧٦٤	0.874
٧	مخاطر البيانات الضخمة	١٠	٠.٨٣١	0.912
٨	فاعلية عملية المراجعة	٩	٠.٨١٧	0.904
ثبات ومصداقية النموذج ككل		**٧٥**	**٠.٩٥٣**	**0.967**

المصدر: من إعداد الباحثة وفقاً لمخرجات برنامج SPSS الإصدار ٢٦

يتضح من الجدول السابق أن معامل الثبات أكبر من ٦٠٪ مما يدل على ثبات عبارات كل متغير من متغيرات الدراسة، وكذلك يتبين أن معامل الصدق الذاتي أكبر من (0.5) مما يدل على صدق العبارات المكونة لكل متغير من متغيرات الدراسة بالإضافة إلى ثبات ومصداقية النموذج ككل.

- **نتائج الإحصاء الوصفي**

قامت الباحثة باستخدام الإحصاء الوصفي لقياس مدي اتساق عبارات المحاور الأربعة للدراسة من خلال استخراج قيم كل من المتوسط الحسابي والانحراف المعياري ومعامل الاختلاف لعبارات كل محور من محاور الدراسة على حدي، وكانت النتائج كالتالي:

جدول (٦)

نتائج التحليل الوصفي لمحاور الدراسة

م	المحور	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف	الاتجاه العام
١	مخاطر السحابة المتعددة والسحابة الهجينة	4.1591	٠.55862	0.134	أوافق
٢	مخاطر سلسلة التوريد الرقمية	4.2475	٠.50852	0.119	أوافق بشدة
٣	مخاطر إنترنت الأشياء	4.3099	٠.41486	0.096	أوافق بشدة
٤	مخاطر الأتمتة والتحليلات	4.1942	٠.43308	0.103	أوافق
٥	مخاطر سلسلة الكتل	4.0909	٠.53732	0.131	أوافق
٦	مخاطر الذكاء الاصطناعي	4.1616	٠.47603	0.114	أوافق
٧	مخاطر البيانات الضخمة	4.1667	٠.53315	0.127	أوافق
٨	فاعلية عملية المراجعة	4.2475	٠.55862	0.131	أوافق بشدة

المصدر: من إعداد الباحثة وفقاً لمخرجات برنامج SPSS الإصدار ٢٦

أظهرت إجابات أفراد العينة أن مفردات المحور الأول قد أخذت اتجاها عاما نحو الموافقة وذلك بمتوسط حسابي قدره (٤.١٥٩١) وانحراف معياري قدره (٠.55862) ومعامل اختلاف قدره (١٣ %) أي ما يعادل نسبة اتفاق (٨٧ %)، والموافقة بشدة علي عبارات المحور الثاني وذلك بمتوسط حسابي قدره (4.2475) وانحراف معياري قدره (٠.50852) ومعامل اختلاف قدره (١٢٪) أي ما يعادل نسبة اتفاق (٨٨ %)، والموافقة بشدة علي عبارات المحور الثالث وذلك بمتوسط حسابي قدره (4.3099) وانحراف معياري قدره (٠.41486) ومعامل اختلاف قدره (٩ %) أي ما يعادل نسبة اتفاق (٩١ %)، والموافقة علي عبارات المحور الرابع وذلك بمتوسط حسابي قدره (4.1942) وانحراف معياري قدره (٠.43308) ومعامل اختلاف قدره (١٠ %) أي ما يعادل نسبة اتفاق (٩٠ %)، والموافقة علي عبارات المحور الخامس وذلك بمتوسط

حسابي قدره (4.0909) وانحراف معياري قدره (٠.53732) ومعامل اختلاف قدره (١٣ %) أي ما يعادل نسبة اتفاق (٨٧ %)، %)، والموافقة علي عبارات المحور السادس وذلك بمتوسط حسابي قدره (4.1616) وانحراف معياري قدره (٠.47603) ومعامل اختلاف قدره (١١ %) أي ما يعادل نسبة اتفاق (٨٩ %)، والموافقة علي المحور السابع وذلك بمتوسط حسابي قدره (4.1667) وانحراف معياري قدره (٠.53315) ومعامل اختلاف قدره (١٢٪) أي ما يعادل نسبة اتفاق (٨٨ %)، والموافقة بشدة علي عبارات المحور الثامن وذلك بمتوسط حسابي قدره (4.2475) وانحراف معياري قدره (٠.55862) ومعامل اختلاف قدره (١٣ %) أي ما يعادل نسبة اتفاق (٨٧ %).

وتخلص الباحثة إلى أن:

هناك اتفاق بين أراء أفراد العينة على أن مخاطر التحول الرقمي المتمثلة في مخاطر السحابة المتعددة والسحابة الهجينة، ومخاطر سلسلة التوريد الرقمية، ومخاطر إنترنت الأشياء، ومخاطر الأتمتة والتحليلات، و مخاطر سلسلة الكتل، ومخاطر الذكاء الاصطناعي، ومخاطر البيانات الضخمة تؤثر على فاعلية عملية المراجعة.

- **نتائج اختبار ت لعينة واحدة**

تم إجراء الاختبار لمعرفة الفروق بين متوسطات إجابات محاور العينة عن متوسط القيمة المحايدة وكانت النتائج كالتالي:

جدول (٧)

اختبارOne Sample t test

م	المحور	قيمة t	قيمة sig
١	مخاطر السحابة المتعددة والسحابة الهجينة	16.412	٠.000
٢	مخاطر سلسلة التوريد الرقمية	17.506	٠.000
٣	مخاطر إنترنت الأشياء	16.499	٠.000
٤	مخاطر الأتمتة والتحليلات	21.732	٠.000
٥	مخاطر سلسلة الكتل	17.682	٠.000
٦	مخاطر الذكاء الاصطناعي	17.474	٠.000
٧	مخاطر البيانات الضخمة	19.633	٠.000
٨	فاعلية عملية المراجعة	15.455	٠.000

المصدر: من إعداد الباحثة وفقاً لمخرجات برنامج SPSS الإصدار ٢٦

ويتضح للباحثة من الجدول السابق انه توجد فروق ذات دلالة إحصائية بين متوسطات عبارات العينة والمتوسط الطبيعي للقيمة المحايدة (٣) عند مستوي ثقة ٩٩٪.

- **<u>اختبار فروض الدراسة</u>**

تم استخدام معامل الارتباط (Correlation) ومعامل الانحدار (Regression)، لتحديد مدي ارتباط وفعالية كل متغير من المتغيرات المستقلة لمخاطر التحول الرقمي والمتغير التابع المتمثل في عملية المراجعة.

جدول (٨)

نتائج تحليل الانحدار لفروض الدراسة

الفرض	معامل الارتباط	R2	قيمة F	درجات الحرية	مستوي المعنوية	الدلالة
١	0.930	0.865	128.097	21	0.000	دالة إحصائيا
٢	.960[a]	.922	236.444	43	0.000	دالة إحصائيا
٣	.819[a]	.670	40.619	43	0.000	دالة إحصائيا
٤	.686[a]	.471	17.790	43	٠.000	دالة إحصائيا
٥	−.074	.005	.110	43	0.372	غير دالة إحصائيا
٦	.040[a]	.002	.031	43	0.431	غير دالة إحصائيا
٧	.864[a]	.747	58.905	43	0.000	دالة إحصائيا

المصدر: من إعداد الباحثة وفقاً لمخرجات برنامج SPSS الإصدار ٢٦

ويتضح للباحثة من الجدول السابق انه

- توجد علاقة ارتباط طردية بين المتغير التابع (عملية المراجعة) والمتغير المستقل (مخاطر السحابة المتعددة والهجينة) حيث بلغ معامل الارتباط (٠.٩٣٠) بمستويات معنوية أقل من (0.01)، مما يدل على قوة الارتباط بين متغيرات الفرض الأول والتأكيد على فعاليتها وتأثيرها المباشر بين بعضها البعض.
- توجد علاقة ذات دلالة إحصائية بين المتغير المستقل (مخاطر السحابة المتعددة والهجينة) والمتغير التابع (عملية المراجعة) عند مستوي معنوية اقل من (0.01)، حيث يتضح أن ٨٧٪ من التغير في عملية المراجعة يرجع الي مخاطر السحابة المتعددة والهجينة والباقي يرجع إلى عوامل أخري، **ولهذا يتم قبول الفرض الأول القائل بانه "توجد علاقة طردية ذات دلالة إحصائية بين مخاطر البنية التحتية للسحابة المتعددة والسحابة الهجينة وعملية المراجعة".**
- توجد علاقة ارتباط طردية ذات دلالة إحصائية بين المتغير التابع (عملية المراجعة) والمتغير المستقل (مخاطر سلسلة التوريد الرقمية) حيث بلغ معامل الارتباط (٠.٩٦٠) بمستويات معنوية أقل من (0.01)، مما يدل على قوة الارتباط بين متغيرات الفرض الثاني والتأكيد على فعاليتها وتأثيرها المباشر بين بعضها البعض، و يتضح أن ٩٢٪ من التغير في عملية المراجعة يرجع الي مخاطر السحابة المتعددة والهجينة والباقي يرجع إلى عوامل أخري، ولهذا **يتم قبول الفرض الثاني والقائل بانه "توجد علاقة ذات دلالة إحصائية بين مخاطر سلسلة التوريد الرقمية وعملية المراجعة".**
- توجد علاقة ارتباط طردية ذات دلالة إحصائية بين المتغير التابع (عملية المراجعة) والمتغير المستقل (مخاطر سلسلة التوريد الرقمية) حيث بلغ معامل الارتباط (٠.٨١٩) بمستويات معنوية أقل من (0.01)، مما يدل على قوة الارتباط بين متغيرات الفرض الثالث والتأكيد على فعاليتها وتأثيرها المباشر بين بعضها البعض، حيث يتضح أن ٦٧٪ من التغير في عملية المراجعة يرجع الي مخاطر سلسلة التوريد الرقمية والباقي

يرجع إلى عوامل أخري، ولهذا **يتم قبول الفرض الثالث والقائل بانه "توجد علاقة ذات دلالة إحصائية بين مخاطر مخاطر إنترنت الأشياء وعملية المراجعة".**

- توجد علاقة ارتباط طردية ذات دلالة إحصائية بين المتغير التابع (عملية المراجعة) والمتغير المستقل (مخاطر التحليلات والأتمتة) حيث بلغ معامل الارتباط (٠.٦٨٦) بمستويات معنوية اقل من (٠.٠٠١) مما يدل على قوة الارتباط بين متغيرات الفرض الرابع والتأكيد على فعاليتها وتأثيرها المباشر بين بعضها البعض، حيث يتضح أن ٤٧ % من التغير في عملية المراجعة يرجع الي مخاطر التحليلات والأتمتة والباقي يرجع إلى عوامل أخري، ولهذا **يتم قبول الفرض الرابع والقائل بانه "توجد علاقة ذات دلالة إحصائية بين مخاطر التحليلات والأتمتة وعملية المراجعة"**
- توجد علاقة ارتباط عكسية ضعيفة بين المتغير التابع (عملية المراجعة) والمتغير المستقل (مخاطر سلسلة الكتل) حيث بلغ معامل الارتباط (٠.٠٧٤-) بمستويات معنوية (٠.٧٤٤) مما يدل على ضعف الارتباط بين متغيرات الفرض الخامس والتأكيد على عدم فعاليتها أو تأثيرها المباشر بين بعضها البعض، حيث يتضح أن ٠.٥٪ من التغير في عملية المراجعة يرجع الي مخاطر سلسلة الكتل والباقي يرجع إلى عوامل أخري، ولهذا **يتم رفض الفرض الأصل وقبول الفرض البديل والقائل بانه "لا توجد علاقة ذات دلالة إحصائية بين مخاطر سلسلة الكتل وعملية المراجعة"** ويرجع ذلك الي تفاوت اراء افراد العينة حول حجم المخاطر التي تسببها سلسلة الكتل مقارنة بالفوائد الناتجة عن استخدامها.
- توجد علاقة ارتباط ضعيفة بين المتغير التابع (عملية المراجعة) والمتغير المستقل (مخاطر الذكاء الاصطناعي) حيث بلغ معامل الارتباط (٠.٠٤٠) بمستويات معنوية (٠.٨٦١) مما يدل على ضعف الارتباط بين متغيرات الفرض السادس والتأكيد على عدم فعاليتها وتأثيرها المباشر بين بعضها البعض، حيث يتضح أن ٠.٢٪ من التغير في عملية المراجعة يرجع الي مخاطر الذكاء الاصطناعي والباقي يرجع إلى عوامل أخري، ولهذا **يتم رفض الفرض الأصل وقبول الفرض البديل والقائل بانه "لا توجد علاقة ذات دلالة إحصائية بين مخاطر الذكاء الاصطناعي وعملية المراجعة"** وقد

يرجع ذلك الي أن مخاطر الذكاء الاصطناعي تتركز بشكل رئيسي في القضايا الأخلاقية، مثل الخصوصية والتمييز الآلي، بينما مراجعة الحسابات تركز على دقة المعلومات المالية وامتثال المؤسسة للمعايير المحاسبية.

- توجد علاقة ارتباط قوية ذات دلالة إحصائية بين المتغير التابع (عملية المراجعة) والمتغير المستقل (مخاطر البيانات الضخمة) حيث بلغ معامل الارتباط (٠.٨٦٤) بمستويات معنوية اقل من (٠.٠٠١) مما يدل على قوة الارتباط بين متغيرات الفرض السابع والتأكيد على فعاليتها وتأثيرها المباشر بين بعضها البعض، حيث يتضح أن ٧٥٪ من التغير في عملية المراجعة يرجع الي مخاطر الذكاء الاصطناعي والباقي يرجع إلى عوامل أخري، ولهذا **يتم قبول الفرض الأصل والقائل بانه "توجد علاقة ذات دلالة إحصائية بين مخاطر Big Data وعملية المراجعة"**

جدول (٩)

معاملات خط الانحدار للفروض الدراسة

		B	Std. Error	Beta		
1	(Constant)	.475	.329		1.444	.164
	مخاطر السحابة المتعددة	.888	.078	.930	11.317	.000
2	(Constant)	.255	.256		.993	.332
	مخاطر سلسلة التوريد الرقمية	.946	.062	.960	15.377	.000
3	(Constant)	.521	.576		.905	.376
	مخاطر إنترنت الأشياء	.858	.135	.819	6.373	.000
4	(Constant)	.366	.905		.405	.690
	مخاطر التحليلات والأتمتة	.882	.209	.686	4.218	.000
5	(Constant)	4.549	1.157		3.931	.001
	مخاطر سلسلة الكتل	-.091	.275	-.074	-.332	.744
6	(Constant)	4.006	.914		4.381	.000
	مخاطر الذكاء الاصطناعي	.039	.222	.040	.177	.861
7	(Constant)	.140	.528		.264	.794
	مخاطر Big Data	.968	.126	.864	7.675	.000
a. Dependent Variable: عملية المراجعة						

المصدر: من إعداد الباحثة وفقاً لمخرجات برنامج SPSS الإصدار ٢٦

ويمكن استنتاج معادلات نموذج الانحدار من الجدول السابق كالتالي:

م١: عملية المراجعة = 475. + (0.888) مخاطر السحابة المتعددة والسحابة الهجينة.

وبتفسير النموذج السابق يتضح أن كل تغير قدره وحدة واحدة في مخاطر السحابة المتعددة يؤثر على مخاطر عملية المراجعة بمقدار (0.888).

م٢: عملية المراجعة = 0.255+ (0.946) مخاطر سلسلة التوريد الرقمية.

وبتفسير النموذج السابق يتضح أن كل تغير قدره وحدة واحدة في مخاطر السحابة المتعددة يؤثر على مخاطر عملية المراجعة بمقدار (0.946).

م٣: عملية المراجعة = 0.521+ (0.858) مخاطر إنترنت الأشياء.

وبتفسير النموذج السابق يتضح أن كل تغير قدره وحدة واحدة في مخاطر إنترنت الأشياء يؤثر على مخاطر عملية المراجعة بمقدار (0.858).

م٤: عملية المراجعة = ٠.٣٦٦ + (٠.٨٨٢) مخاطر التحليلات والأتمتة.

وبتفسير النموذج السابق يتضح أن كل تغير قدره وحدة في مخاطر التحليلات والأتمتة يؤثر على عملية المراجعة بمقدار (٠.٨٨٢).

م٥: عملية المراجعة = ٤.٥٤٩ + (- ٠.٠٩١) مخاطر سلسلة الكتل.

وبتفسير النموذج السابق يتضح أن كل تغير قدره وحدة واحدة في مخاطر سلسلة الكتل يؤثر على مخاطر عملية المراجعة بمقدار (-٠.٠٩١).

م٦: عملية المراجعة = ٤.٠٠٦ + (٠.٣٩) مخاطر الذكاء الاصطناعي.

وبتفسير النموذج السابق يتضح أن كل تغير قدره وحدة واحدة في مخاطر الذكاء الاصطناعي يؤثر على مخاطر عملية المراجعة بمقدار (٠.٣٩).

م٧: عملية المراجعة = ٠.١٤٠ + (٠.٩٦٨) مخاطر البيانات الضخمة.

وبتفسير النموذج السابق يتضح أن كل تغير قدره وحدة واحدة في مخاطر البيانات الضخمة يؤثر على عملية المراجعة بمقدار (٠.٩٦٨).

- **نتائج الدراسة النظرية**

قامت الباحثة خلال هذا الفصل بتجميع البيانات اللازمة لإثبات فرضيات الدراسة والمتعلقة بمحاولة الوصول إلى انعكاسات مخاطر التحول الرقمي علي عملية المراجعة، ومن أجل ذلك الهدف صممت الباحثة الفروض بالطريقة التي رأت أنها تناسب الدراسة، حيث كانت توجد العديد من المخاطر المتعلقة بالتحول الرقمي التي تؤثر علي عملية المراجعة ولذلك فقد جاء ترتيب المحاور وعباراتها ليصب في مصلحة تلك الرؤية من أجل الوصول إلي النتيجة النهائية التي تتفق أو تختلف مع فروض الدراسة، وكانت نتيجة الدراسة النظرية هي:

١. **اتضح ان المخاطر المتعددة المضمنة في رحلة التحول الرقمي متعددة ومنها:**

- التحديات في التحقق من صحة البيانات المالية في البيئة الرقمية بسبب توزيع البيانات بين السحابة العامة والخاصة.
- تعقد البيانات المستمدة من البيئة الرقمية.
- مخاطر التحقق من هويات الأطراف المشاركة للتأكد من صحة البيانات المالية.
- عدم وجود معايير موحدة او مبادئ التوجيهية واضحة للتعامل مع تقنيات التحول الرقمي.

٢. **تؤدي المخاطر المرتبطة بالتحول الرقمي الي**

- تحديات في تحقيق التوازن بين استخدام التقنيات الذكية والتفاعل البشري في عملية مراجعة الحسابات.
- فقدان بعض جوانب التفاعل الإنساني الذي يحدث في عملية المراجعة.
- تقديم تقارير مالية مضللة أو تفتقر إلى الدقة مما يؤثر على عملية المراجعة.
- احتياج مراجعي الحسابات إلى تكوين استراتيجيات فعالة لمواجهة هذه المخاطر وضمان استمرارية فعالية عمليات المراجعة في الظروف المتغيرة.

٣. من أفضل الممارسات والاستراتيجيات اللازمة لتجنب مخاطر التحول الرقمي وتأثيره على عملية المراجعة.

- يحتاج المراجعون لمواجهة تحديات التحول الرقمي إلى دمج تحليلات البيانات في منهجياتهم ويتضمن ذلك الاستفادة من أدوات التحليلات المتقدمة لتحليل مجموعات البيانات الكبيرة وتحديد الحالات الشاذة أو الأنماط التي تشير إلى المخاطر.
- اعتماد نهج المراجعة المستمر يسمح للمراجعين بمراقبة المعلومات المالية في الوقت الحقيقي. تساعد هذه الطريقة الاستباقية في تحديد المشكلات على الفور وتعزز الفعالية العامة لعملية المراجعة.
- يجب على المراجعين التعاون بشكل وثيق مع متخصصي تكنولوجيا المعلومات لاكتساب فهم عميق للبنية التحتية التكنولوجية وتقييم المخاطر المرتبطة بها بشكل فعال، يضمن هذا التعاون اتباع نهج شامل للمراجعة في العصر الرقمي.
- يتطلب تنفيذ أنظمة المراجعة الآلية من المراجعين تكييف مناهج المراجعة الخاصة بهم لدمج التقنيات الجديدة والتأكد من قدرتهم على إدارة نتائج الأتمتة والتحقق من صحتها بشكل فعال باستخدام طرق بديلة أو الشبكات اليدوية.
- يجب على المراجعين الامتثال للوائح حماية البيانات وحماية المعلومات الحساسة من الوصول أو الكشف غير المصرح به ويعد التشفير وضوابط الوصول والتخزين الآمن للبيانات من التدابير الأساسية لمعالجة هذه المخاوف ويجب أن يكون المراجعون على دراية جيدة باللوائح والمعايير المطبقة.
- يمكن للمراجعين تحديد أهداف ومعايير المراجعة بوضوح وضمان مواءمة عملية اختيار البيانات مع أهداف المراجعة وتجنب التحيز غير الضروري واستخدم تقنيات أخذ العينات العشوائية كلما أمكن ذلك لتقليل التحيز في اختيار البيانات وتحليلها أثناء مراجعة البيانات الضخمة.

- تلعب حوكمة البيانات دورا حاسما في تقليل المخاطر المرتبطة بمخاطر التحول الرقمي من خلال مراجعة ضوابط الوصول إلى البيانات لضمان تنفيذ ضوابط وصول صارمة أن الموظفين المصرح لهم فقط يمكنهم التعامل مع بيانات المراجعة الحساسة وتحليلها والحفاظ على دقتها واكتمالها وموثوقيتها.
- المبادئ التوجيهية الواضحة بشأن الاحتفاظ بالبيانات وحذفها تقلل من مخاطر تخزين البيانات غير الضرورية أو القديمة.

- **نتائج الدراسة الميدانية**

توصلت الباحثة من خلال الدراسة الميدانية إلى تطابق النتائج النظرية مع نتائج الدراسة الميدانية ويمكن إيجاز تلك النتائج في التالي:

- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر البنية التحتية للسحابة المتعددة والسحابة الهجينة وعملية المراجعة.
- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر سلسلة الإمداد الرقمية وعملية المراجعة.
- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر إنترنت الأشياء وعملية المراجعة.
- توجد علاقة طردية ذات دلالة إحصائية بين المخاطر الأتمتة والتحليلات وعملية المراجعة.
- توجد علاقة طردية ذات دلالة إحصائية بين مخاطر البيانات الضخمة وعملية المراجعة.
- لا توجد علاقة طردية ذات دلالة إحصائية بين مخاطر سلسة الكتل وعملية المراجعة.
- لا توجد علاقة طردية ذات دلالة إحصائية بين مخاطر الذكاء الاصطناعي وعملية المراجعة.

٩- التوصيات

تستخلص الباحثة من النتائج السابقة العديد من التوصيات التي تعمل كدليل استراتيجي للمراجعين والمؤسسات على حد سواء، حيث تقدم خارطة طريق للتنقل في التضاريس المعقدة لمخاطر التحول الرقمي، وتعد كل توصية خطوة ملموسة نحو حماية سلامة عملية المراجعة في عصر يحدده التحول الرقمي، ولن تحد هذه الاستراتيجيات القابلة للتنفيذ من المخاطر فحسب، بل ستمهد الطريق أيضا لعملية مراجعة تزدهر في العصر الرقمي.

١. استخدام تقنيات تشفير قوية لضمان أمان البيانات أثناء عمليات التحول الرقمي.
٢. الالتزام بمعايير الأمان والامتثال الصارمة للتخلص من أي تهديدات أمان محتملة.
٣. فحص التطبيقات الرقمية والأنظمة الجديدة لضمان فعالية وأمان التكنولوجيا.
٤. تقييم كيف يؤثر التحول الرقمي على ثقافة الشركة وضمان تكاملها مع أهداف الأمان والرقابة.
٥. توعية الموظفين حول مخاطر الأمان والتحول الرقمي.
٦. التواصل الفعال مع السلطات الرقابية للتأكد من الامتثال للمتطلبات القانونية.
٧. توفير نظام قوي لإدارة الهويات والوصول للتحكم في منح الصلاحيات.
٨. استخدام أنظمة مراقبة فعالة لتسجيل ومراقبة الأنشطة غير المصرح بها.
٩. تقييم التأثير المالي والأماني للتحول الرقمي على عمليات المؤسسة.

١٠- الدراسات المستقبلية

١. تأثير استخدام التحليل الضوئي للبيانات على إجراءات عملية المراجعة وانعكاساته علي جودة التقارير المالية.
٢. دور الذكاء الاصطناعي في تسريع عمليات المراجعة في العصر الرقمي.
٣. تكامل التحول الرقمي مع مفهوم المراجعة الداخلية الذكية: دراسة حالة في قطاع الخدمات المالية.
٤. تكنولوجيا سلسلة الكتل وتحسين النزاهة في عملية المراجعة الداخلية.
٥. تكامل تقنيات الذكاء الاصطناعي مع أنظمة إدارة المخاطر لتعزيز أداء المراجعة الداخلية.

١١-المراجع

Ageron, B., Bentahar, O., & Gunasekaran, A. (2020). Digital supply chain: challenges and future directions. *Supply Chain Forum: An International Journal*, *21*(3), 133–138. https://doi.org/10.1080/16258312.2020.1816361

Agu, E., EBERE, E., & Moses, T. (2019). *A HYBRID MODEL FOR REMOTE DYNAMIC DATA AUDITING (RDDA) ON CLOUD COMPUTING*. https://doi.org/10.13140/RG.2.2.15011.60967

Al-Ateeq, B., Sawan, N., Al-Hajaya, K., Altarawneh, M., & Al-Makhadmeh, A. (2022). Big data analytics in auditing and the consequences for audit quality: A study using the technology acceptance model (TAM). *Corporate Governance and Organizational Behavior Review*, *6*(1), 64–78. https://doi.org/10.22495/cgobrv6i1p5

Alonso, J., Orue-Echevarria, L., Casola, V., Torre, A. I., Huarte, M., Osaba, E., & Lobo, J. L. (2023). Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. *Journal of Cloud Computing*, *12*(1), 6. https://doi.org/10.1186/s13677-022-00367-6

Appelbaum, D. A., Kogan, A., & Vasarhelyi, M. A. (2018). Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics. *Journal of Accounting Literature*, *40*(1), 83–101. https://doi.org/10.1016/j.acclit.2018.01.001

Babayeva, A. (2022). *The Effects of Digitalization on Auditing A Study Investigating the Benefits and Challenges of Digitalization on the Audit Profession*. Lund School of Economics and Management, Lund University.

Bansal, H., Gupta, D., & Anand, D. (2022). Analysis of Consensus Algorithms in context of the Blockchain based Applications. *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–7. https://doi.org/10.1109/ICRITO56286.2022.9964653

Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, *56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021

Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral Implications of Big Data's Impact on Audit Judgment and Decision Making and Future Research Directions. *Accounting Horizons*, *29*(2), 451–468. https://doi.org/10.2308/acch-51023

Brunsdon, C., & Comber, A. (2020). Big issues for big data: challenges for critical spatial data analytics. *Journal of Spatial Information Science*, *21*. https://doi.org/10.5311/JOSIS.2020.21.625

Chen, Z., Ji, X., Li, M., & Li, J. (2023). How corporate social responsibility auditing interacts with supply chain information transparency. *Annals of Operations Research*, *329*(1–2), 1221–1240. https://doi.org/10.1007/s10479-022-04601-x

Cheng, L., Varshney, K. R., & Liu, H. (2021). Socially Responsible AI Algorithms: Issues, Purposes, and Challenges. *Journal of Artificial Intelligence Research*, *71*, 1137–1181. https://doi.org/10.1613/jair.1.12814

Contag, M., Li, G., Pawlowski, A., Domke, F., Levchenko, K., Holz, T., & Savage, S. (2017). How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles. *2017 IEEE Symposium on Security and Privacy (SP)*, 231–250. https://doi.org/10.1109/SP.2017.66

CPA, C. (2020). *The Data-Driven Audit: How Automation and AI are Changing the Audit and the Role of the Auditor*.

CSA. (2019). *Top Threats to Cloud Computing: Egregious Eleven*. Cloud Security Alliance (CSA). https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/

Dasaklis, T. K., Voutsinas, T. G., Tsoulfas, G. T., & Casino, F. (2022). A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations. *Sustainability*, *14*(4), 2439. https://doi.org/10.3390/su14042439

Deloitte. (2017). *Blockchain risk management*. https://www2.deloitte.com/us/en/pages/risk/articles/blockchain-security-risks.html

Deloitte. (2018). *Blockchain and its potential impact on the audit profession*.

Deloitte. (2023). *AI regulation | Deloitte Insights*. https://www2.deloitte.com/us/en/insights/industry/public-sector/ai-regulations-around-the-world.html

Dhirani, L. L., Newe, T., & Nizamani, S. (2019). *Federated Hybrid Clouds Service Level Agreements and Legal Issues* (pp. 471–486). https://doi.org/10.1007/978-981-13-1165-9_44

Diego, V., & Francisco, F. M. (2021). Internet of things: Emerging impacts on digital reporting. *Journal of Business Research*, *131*, 549–562. https://doi.org/10.1016/j.jbusres.2021.01.056

Dimitris, B., Panagiotis, K., Nikolaos, E., & Dimitrios, V. (2020). Big Data, Data Analytics and External Auditing. *Journal of Modern Accounting and Auditing*, *16*(5). https://doi.org/10.17265/1548-6583/2020.05.002

Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, *142*, 102067. https://doi.org/10.1016/j.tre.2020.102067

ENISA. (2018). *Good Practices for Security of Internet of Things in the context of Smart Manufacturing — ENISA*. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/

Eprs. (2023). *BRIEFING EU Legislation in Progress*.

Fadlallah, H., Kilany, R., Dhayne, H., El Haddad, R., Haque, R., Taher, Y., & Jaber, A. (2023). Context-aware Big Data Quality Assessment: A Scoping Review. *Journal of Data and Information Quality*, *15*(3), 1–33. https://doi.org/10.1145/3603707

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*, *27*(3), 938–985. https://doi.org/10.1007/s11142-022-09697-x

Flexera. (2023). *Cloud computing Stats: Flexera 2023 State of the Cloud Report*. https://www.flexera.com/blog/cloud/cloud-computing-trends-flexera-2023-state-of-the-cloud-report/

Forcepoint. (2019). *The Practical Executive's Guide to Data Loss Prevention*.

FTC. (2022). *Federal Register : Trade Regulation Rule on Commercial Surveillance and Data Security*. Federal Trade Commission. https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

Gartner. (2016). *Definition of Digitalization - IT Glossary | Gartner*. https://www.gartner.com/en/information-technology/glossary/digitalization

Graham, D. (2023). Blockchain and Digital Currency. In *Integrated Electronic Payment Technologies for Smart Cities* (pp. 123–130). Springer International Publishing. https://doi.org/10.1007/978-3-031-38222-2_9

Gürcan, B. (2020). *JURISDICTION ON THE BLOCKCHAIN*.

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*, 100598. https://doi.org/10.1016/j.accinf.2022.100598

Hasan, A., Brown, S., Davidovic, J., Lange, B., & Regan, M. (2022). Algorithmic Bias and Risk Assessments: Lessons from Practice. *Digital Society*, *1*(2), 14. https://doi.org/10.1007/s44206-022-00017-z

Hasan, A. R. (2022). Artificial Intelligence (AI) in Accounting & Auditing: A Literature Review. *Open Journal of Business and Management*, *10*(01), 440–465. https://doi.org/10.4236/ojbm.2022.101026

Hezam, Y. A. A., Anthonysamy, L., & Suppiah, S. D. K. (2023). Big Data Analytics and Auditing: A Review and Synthesis of Literature. *Emerging Science Journal*. https://api.semanticscholar.org/CorpusID:257210594

ICAEW. (2017). *UNDERSTANDING THE IMPACT OF TECHNOLOGY IN AUDIT AND FINANCE*.

IIA. (2022). *An Integrated Approach to Supply Chain Risk Management* .

Ismail, G., & Taliep, N. (2023). The Delphi Method. In *Handbook of Social Sciences and Global Public Health* (pp. 1–19). Springer International Publishing. https://doi.org/10.1007/978-3-030-96778-9_66-1

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation. *Journal of Emerging Technologies in Accounting*, *13*(2), 1–20. https://doi.org/10.2308/jeta-10511

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, *32*(9), 775–788. https://doi.org/10.1080/09537287.2020.1768450

Joshi, P. L. (2021). *Will Artificial Intelligence (AI) Replace Accountants and Auditors in Future?* (pp. 27–48).

Kalia, P., Bansal, D., & Sofat, S. (2021). Privacy Preservation in Cloud Computing Using Randomized Encoding. *Wireless Personal Communications*, *120*(4), 2847–2859. https://doi.org/10.1007/s11277-021-08588-9

Kallinikos, J., Aaltonen, A., & Marton, A. (2013). The Ambivalent Ontology of Digital Artifacts. *MIS Quarterly*, *37*(2), 357–370. https://doi.org/10.25300/MISQ/2013/37.2.02

Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. *European Journal of Information Systems*, *31*(3), 388–409. https://doi.org/10.1080/0960085X.2021.1927212

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Larson, P. D. (2001). Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies, David Simchi-Levi Philip Kaminsky Edith Simchi-Levi. *Journal of Business Logistics*, *22*(1), 259–261. https://doi.org/10.1002/j.2158-1592.2001.tb00165.x

Lombardi, R., de Villiers, C., Moscariello, N., & Pizzo, M. (2022). The disruption of blockchain in auditing – a systematic literature review and an agenda for future research. *Accounting, Auditing & Accountability Journal*, *35*(7), 1534–1565. https://doi.org/10.1108/AAAJ-10-2020-4992

MacCarthy, B. L., & Ivanov, D. (2022). The Digital Supply Chain—emergence, concepts, definitions, and technologies. In *The Digital Supply Chain* (pp. 3–24). Elsevier. https://doi.org/10.1016/B978-0-323-91614-1.00001-0

McAllum, M. (2016). No Ordinary Disruption: The Four Global Forces Breaking All the Trends, by RichardDobbs, JamesManyika and Jonathan R.Woetzel (PublicAffairs, New York, 2015), pp. vi + 279. *Economic Record*, *92*(297), 323–325. https://doi.org/10.1111/1475-4932.12272

Mökander, J., Morley, J., Taddeo, M., & Floridi, · Luciano. (2021). Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations. *Science and Engineering Ethics*, *27*(4), 44. https://doi.org/10.1007/s11948-021-00319-4

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The Ethical Implications of Using Artificial Intelligence in Auditing. *Journal of Business Ethics*, *167*(2), 209–234. https://doi.org/10.1007/s10551-019-04407-1

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

NIST SP 800-37. (2018). *Risk management framework for information systems and organizations:* https://doi.org/10.6028/NIST.SP.800-37r2

Nurhajati, Y. (2016). The Impact Of Cloud Computing Technology On The Audit Process And The Audit Profession. *International Journal of Scientific & Technology Research*, *5*, 185–193. https://api.semanticscholar.org/CorpusID:115415910

Pasula, M., Nerandzic, B., & Radosevic, M. (2013). Internal audit of the supply chain management in function of cost reduction of the company. *Journal of Engineering Management and Competitiveness*, *3*(1), 32–36. https://doi.org/10.5937/jemc1301032P

PCAOB. (2010). *AS 1105: Audit Evidence | PCAOB.* https://pcaobus.org/oversight/standards/auditing-standards/details/AS1105

Peng, F., Tian, H., Quan, H., & Lu, J. (2020). *Data Auditing for the Internet of Things Environments Leveraging Smart Contract* (pp. 133–149). https://doi.org/10.1007/978-981-15-9739-8_12

Pettit, T. J., Croxton, K. L., & Fiksel, J. (2019). The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience. *Journal of Business Logistics*, *40*(1), 56–65. https://doi.org/10.1111/jbl.12202

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2021). Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1972–1986. https://doi.org/10.1109/TETC.2019.2949510

Powell, W. (2022). Blockchain With Chinese Characteristics – Healthy China 2030, Supply Chains and Data Integrity. In *China, Trust and Digital Supply Chains* (pp. 52–88). Routledge. https://doi.org/10.4324/9781003184614-3

Praveena, D., Thanga Ramya, S., Gladis Pushparathi, V. P., Bethi, P., & Poopandian, S. (2021). *Hybrid Cloud Data Protection Using Machine Learning Approach* (pp. 151–166). https://doi.org/10.1007/978-3-030-75657-4_7

PwC. (2017). *Robotic process automation: A primer for internal audit professionals*.

Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud Computing*. CRC Press. https://doi.org/10.1201/9781439806814

Robson, S., & Sowel, T. (2022). *Four Pillars of a Trusted Information Infrastructure*. AVEVA. https://resources.osisoft.com/presentations/four-pillars-of-a-trusted-information-infrastructure/

Sabri, E. (2019). Technology Optimization and Change Management for Successful Digital Supply Chains. *Advances in Logistics, Operations, and Management Science*. https://api.semanticscholar.org/CorpusID:219403265

Small, M., & Whitepaper, K. (2019). *KuppingerCole Whitepaper Big Data Analytics-Security and Compliance Challenges in 2019*. https://ico.org.uk/action-weve-taken/enforcement/the-carphone-warehouse-ltd/

Stancheva, E. (2018). *HOW ARTIFICIAL INTELLIGENCE IS CHALLENGING ACCOUNTING PROFESSION*. *12*, 126–141.

Torkura, K. A., Sukmana, M. I. H., Cheng, F., & Meinel, C. (2021). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security*, *102*, 102124. https://doi.org/10.1016/j.cose.2020.102124

Vehent, J. (2018). *Securing DevOps: Security in the Cloud* (1st ed.). Manning Publications Co.

Walshe, R. (2021). The Road to Big Data Standardisation. In *The Elements of Big Data Value* (pp. 333–354). Springer International Publishing. https://doi.org/10.1007/978-3-030-68176-0_14

WEF. (2020). *Global Risk Report 2020 | World Economic Forum | World Economic Forum*. https://www.weforum.org/publications/the-global-risks-report-2020/