Journal of Shatt Al Arab University College for Administration and Legal Sciences

مجلة كلية شط العرب الجامعة للعلوم الادارية والقانونية

Vol. (4) No. (2) 2026 المجلد. (4) العدد. (2)

The impact of adopting cyber-security in artificial intelligence applications in the field of banking sector auditing	
Researcher's Name	**DR. Ban Riyadh yousif**
College	**Ministry Of Education- Directorate of Internal Control and Auditing**
University	**Open Educational College**
Email	**Banhana819@yahoo.com**
Phone Number	**07715881095**

Abstract: This research explores and evaluates the extent of adoption of internal auditing practices using artificial intelligence and cyber-security technologies, with a focus on the effectiveness of these technologies in enhancing audit processes and efficiency. Various research tools were employed, including Likert-scale questionnaires to measure levels of adoption and effectiveness, along with semi-structured interviews with experts to support qualitative analysis and understand related behaviors. The study found that integrating modern technologies into auditing practices improves the accuracy and efficiency of operations. It recommends developing academic curricula and professional training programs to enhance the capabilities of practitioners in this field, with an emphasis on improving data processing quality and supporting technological innovation in auditing processes

Keywords: Cyber-security, AI applications, Auditing, Banking sector.

أثر تبني الأمن السيبراني في تطبيقات الذكاء الاصطناعي في مجال تدقيق القطاع المصرفي	
اسم الباحث	**م .د بان رياض يوسف**
الكلية	**وزارة التربية / مديرية التدقيق والرقابة الداخلية**
الجامعة	الكلية التربوية المفتوحة
الإيميل	Banhana819@yahoo.com
رقم الهاتف	07715881095

الملخص: يتناول هذا البحث استكشاف وتقييم مدى تبني ممارسات التدقيق الداخلي باستخدام تقنيات الذكاء الاصطناعي والأمن السيبراني، مع التركيز على فعالية هذه التقنيات في تعزيز عمليات التدقيق وكفاءتها. تم استخدام أدوات بحث مختلفة، بما في ذلك استبيان ليكرات للمستويات المتعددة من التبني والفعالية، بالإضافة إلى مقابلات شبه مهيكلة مع مختصين لدعم التحليل النوعي وفهم السلوكيات المرتبطة. توصل البحث إلى أن دمج التقنيات الحديثة في ممارسات التدقيق يعزز من دقة وكفاءة العمليات، ويُوصى بتطوير البرامج الأكاديمية والتدريب المهني لتعزيز قدرات المهنيين في هذا المجال، مع التركيز على تحسين جودة معالجة البيانات ودعم الابتكار التكنولوجي في عمليات التدقيق.

الكلمات المفتاحية: الأمن السيبراني، تطبيقات الذّكاء الاصطناعي، التدقيق، القطاع المصرفي

المقدمة:

يشهد القطاع المصرفي، على المستويين العالمي والإقليمي، تسارعًا ملحوظًا في التحول الرقمي بوصفه خيارًا استراتيجيًا مدفوعًا بضرورات المنافسة، وخفض التكاليف، ورفع كفاءة الخدمات، والاستجابة لتوقعات العملاء والجهات التنظيمية. وقد مثّل الذكاء الاصطناعي أحد أهم محركات هذا التحول، نظرًا لقدرته على معالجة كميات هائلة من البيانات واستخلاص أنماط خفية ومعارف قابلة للتشغيل، بما يعزز دقة القرارات وسرعتها في مجالات مصرفية حرجة. وتتجلى تطبيقات الذكاء الاصطناعي في القطاع المصرفي في طيف واسع يشمل: تحليل السلوك المالي وتجزئة العملاء، الكشف الاستباقي عن الاحتيال وغسل الأموال، التنبؤ بالمخاطر الائتمانية والتعثر، أتمتة إجراءات الامتثال الرقابي إضافةً إلى دعم عمليات التدقيق الداخلي والخارجي من خلال التحليلات المستمرة والتدقيق المعتمد على البيانات.

غير أن هذا الانتشار المتزايد لتطبيقات الذكاء الاصطناعي، رغم ما يقدمه من مكاسب تشغيلية ورقابية، يرتبط في المقابل بتحولات نوعية في مشهد المخاطر السيبرانية. إذ يؤدي دمج نماذج التعلم الآلي ضمن الأنظمة المصرفية إلى توسيع سطح الهجوم عبر نقاط جديدة لم تكن تقليديًا ضمن نطاق التهديدات المعلوماتية المعتادة. فإلى جانب المخاطر المعروفة مثل الاختراقات وسرقة البيانات، تظهر تهديدات أكثر تخصصًا ترتبط بطبيعة نماذج الذكاء الاصطناعي وسلاسل بياناتها، مثل: اختراق نماذج التعلم الآلي، تسميم البيانات عبر إدخال بيانات مضللة تؤثر على سلوك النموذج وقراراته، وهجمات الخصوصية التي تستهدف استرجاع بيانات حساسة من مخرجات النموذج أو إعادة تحديد الهوية في بيئات كان يفترض أنها مجهولة الهوية. كما تبرز الهجمات الموجهة لسلاسل توريد البرمجيات بوصفها خطرًا بالغًا في ظل اعتماد المؤسسات على مكتبات تعلم آلي مفتوحة المصدر، وخدمات سحابية، ومزودين خارجيين للأدوات التحليلية.

في سياق التدقيق المصرفي تحديدًا، يكتسب هذا التحول أبعادًا أكثر حساسية، لأن وظيفة التدقيق—سواء الداخلي أو الخارجي—تعد من ركائز الحوكمة المؤسسية والثقة السوقية، وترتبط مباشرة بسلامة التقارير المالية، وامتثال العمليات، وفعالية الضوابط الداخلية، وتقييم المخاطر. ومع انتقال التدقيق من الأساليب التقليدية القائمة على العينات إلى تدقيق مدفوع بالبيانات والتحليلات المستمرة، تصبح جودة مخرجات التدقيق مرهونة بعوامل تقنية ومعرفية جديدة، في مقدمتها: سلامة البيانات، ونزاهة النماذج، وموثوقية الأنظمة، واستمرارية الخدمات، وعليه فإن أي خلل في البيانات أو تحيز في النموذج أو تلاعب في بيئة التشغيل قد يؤدي إلى استنتاجات تدقيقية غير دقيقة، أو إلى إخفاء مؤشرات المخاطر، أو إلى نتائج مضللة قد تُضعف قرارات الإدارة والجهات الرقابية.

من هنا تتبلور أهمية الأمن السيبراني ليس فقط بوصفه وظيفة تقنية تُعنى بالحماية، بل باعتباره عنصرًا حوكميًا ورقابيًا متداخلًا مع جودة التدقيق ومصداقيته. فالأمن السيبراني، عند توظيفه ضمن إطار حوكمة شامل، يسهم في ضبط دورة حياة البيانات والنماذج، ويضمن أن أدوات الذكاء الاصطناعي المستخدمة في التدقيق تعمل ضمن حدود مقبولة من المخاطر، وتحت رقابة تضمن الشفافية وقابلية التفسير والمساءلة. كما أن ممارسات الأمن السيبراني—مثل السياسات والإجراءات، والضوابط الوقائية والكشفية، وإدارة الهوية والصلاحيات، وإدارة التهيئة الآمنة، والتشفير، ومراقبة السجلات، واختبارات الاختراق، وإدارة الثغرات—تشكّل بنية داعمة تقلل من احتمالات العبث بالبيانات أو إساءة استخدام النماذج، وتحد من مخاطر الانقطاع التشغيلي التي قد تعطل وظائف التدقيق أو تؤثر على توقيتاته.

وعلى مستوى أكثر تكاملًا، ترتبط فعالية التدقيق في بيئة الذكاء الاصطناعي بمدى نضج الحوكمة السيبرانية وإدارة المخاطر داخل المصارف. فوجود أطر واضحة لتقييم المخاطر السيبرانية الخاصة بالذكاء الاصطناعي، وتحديد شهية المخاطر، وربط الضوابط بأهداف رقابية قابلة للقياس، يساهم في تقليل فجوة الثقة بين مخرجات الذكاء الاصطناعي ومتطلبات التدقيق المهني. كما أن جاهزية الاستجابة للحوادث وخطط التعافي واستمرارية الأعمال تعد عوامل حاسمة لضمان عدم تأثر العمليات التدقيقية بأحداث سيبرانية قد تُفقد الأدلة الرقمية أو تؤدي إلى تشويهها أو تعطل الوصول إليها.

ويهدف هذا البحث إلى دراسة أثر تبنّي ممارسات الأمن السيبراني—بمكوناتها المختلفة من سياسات وضوابط وحوكمة وإدارة مخاطر واستجابة للحوادث—على فعالية وكفاءة التدقيق في القطاع المصرفي عند استخدام تطبيقات الذكاء الاصطناعي. ويركّز البحث على قياس انعكاس تلك الممارسات على مؤشرات جوهرية تشمل: جودة التدقيق من حيث دقة النتائج وشموليتها وموضوعيتها وقابليتها للتتبع، وتقليل المخاطر سواء التشغيلية أو السيبرانية أو الرقابية، ورفع الثقة التنظيمية عبر تعزيز القدرة على الامتثال، وتقديم أدلة تدقيقية موثوقة، وتخفيض احتمالات المفاجآت الرقابية. كما يسعى البحث إلى الإسهام في سد فجوة معرفية تتعلق بدمج الأمن السيبراني كرافعة لضمانات التدقيق في عصر الذكاء الاصطناعي، وطرح إطار تحليلي يمكن أن يساعد المؤسسات المصرفية والجهات الرقابية على مواءمة الابتكار التقني مع متطلبات الحوكمة، بما يضمن تحقيق مكاسب التحول الرقمي دون التضحية بالسلامة والثقة.

أهمية البحث

(أ) الأهمية العلمية

1. الربط بين ثلاثة حقول متداخلة: التدقيق المصرفي + الذكاء الاصطناعي + الأمن السيبراني ضمن إطار تفسيري قابل للقياس.
2. إثراء الأدبيات المتعلقة بحوكمة الذكاء الاصطناعي (AI Governance) من منظور الرقابة والتدقيق وليس فقط من منظور تقني.
3. تقديم نموذج مفاهيمي يوضح كيف تؤثر ضوابط الأمن السيبراني في موثوقية مخرجات خوارزميات التدقيق (الإنذارات، مؤشرات المخاطر، التصنيف، الكشف عن الشذوذ).

(ب) الأهمية التطبيقية

1. مساعدة إدارات التدقيق في البنوك على تبنّي متطلبات أمنية مناسبة عند إدخال أدوات ذكاء اصطناعي في عمل التدقيق.

2. دعم إدارات الامتثال وإدارة المخاطر في تقليل مخاطر الاختراق والتلاعب بالمخرجات التي قد تؤثر على القرارات الرقابية.
3. تحسين كفاءة عمليات التدقيق عبر تقليل الإيجابيات الكاذبة (False Positives) ورفع موثوقية البيانات.
4. تعزيز الثقة لدى الجهات الرقابية والمساهمين في نتائج التدقيق المدعومة بالذكاء الاصطناعي.

أهداف البحث

(أ) الهدف العام

قياس وتحليل أثر تبنّي الأمن السيبراني في تطبيقات الذكاء الاصطناعي المستخدمة في تدقيق القطاع المصرفي على فعالية وجودة عملية التدقيق وتقليل المخاطر.

(ب) الأهداف الفرعية

1. تحديد أهم تطبيقات الذكاء الاصطناعي المستخدمة في التدقيق المصرفي (كشف احتيال، تحليل معاملات، مراقبة امتثال...).
2. تحديد أبرز المخاطر السيبرانية المرتبطة بتلك التطبيقات (تلاعب بيانات، تسريب، انحراف النموذج...).
3. قياس مستوى تبنّي ضوابط الأمن السيبراني في البنوك (حوكمة، سياسات، ضوابط تقنية، تدريب...).
4. دراسة أثر تبنّي الأمن السيبراني على:
   - جودة الأدلة التدقيقية
   - دقة مخرجات نماذج الذكاء الاصطناعي
   - سرعة إنجاز التدقيق
   - خفض مخاطر الاحتيال/الأخطاء/الاختراق
5. اقتراح توصيات عملية وإطار إجرائي لتدقيق أنظمة الذكاء الاصطناعي ضمن القطاع المصرفي.

مشكلة البحث

على الرغم من توسّع استخدام تطبيقات الذكاء الاصطناعي في التدقيق المصرفي لما توفره من سرعة وقدرة تحليلية، إلا أن ضعف أو عدم نضج تبنّي الأمن السيبراني المصاحب لهذه التطبيقات قد يؤدي إلى:

- التلاعب بالبيانات أو النماذج
- تسرب البيانات الحساسة
- إنتاج مخرجات تدقيقية غير موثوقة
- زيادة مخاطر الامتثال والسمعة والخسائر المالية

وعليه تتمثل مشكلة البحث في السؤال الرئيس:

ما أثر تبنّي الأمن السيبراني في تطبيقات الذكاء الاصطناعي على فعالية وجودة تدقيق القطاع المصرفي؟

الأسئلة الفرعية:

1. ما مستوى استخدام الذكاء الاصطناعي في التدقيق المصرفي؟
2. ما مستوى تبنّي ضوابط الأمن السيبراني المرتبطة بتطبيقات الذكاء الاصطناعي؟
3. هل يؤثر تبنّي الأمن السيبراني على جودة/كفاءة التدقيق عند استخدام الذكاء الاصطناعي؟

4. ما الضوابط الأكثر تأثيرًا: الحوكمة، الضوابط التقنية، التدريب، الاستجابة للحوادث، إدارة الهوية؟

فرضيات البحث

يمكن صياغتها بصيغة فرضية عدم (H0) وبديلة (H1)، أو مباشرة. فيما يلي نموذج مباشر:

الفرضية الرئيسة (H1)

يوجد أثر ذو دلالة إحصائية لتبنّي الأمن السيبراني في تطبيقات الذكاء الاصطناعي على فعالية تدقيق القطاع المصرفي.

فرضيات فرعية (حسب الأبعاد)

H1a: يوجد أثر ذو دلالة إحصائية لحوكمة الأمن السيبراني (سياسات/أدوار/مساءلة) على جودة التدقيق المدعوم بالذكاء الاصطناعي.

H1b: يوجد أثر لضوابط حماية البيانات (تصنيف، تشفير، DLP، إدارة مفاتيح) على موثوقية الأدلة التدقيقية.

منهجية البحث

- **المنهج المعتمد**

المنهج الوصفي التحليلي: لوصف واقع تبنّي الأمن السيبراني واستخدام AI في التدقيق المصرفي، ثم تحليل العلاقات والأثر.

- **مجتمع الدراسة وعينتها**

– **المجتمع:** العاملون في التدقيق الداخلي، إدارة المخاطر، الامتثال، أمن المعلومات، وإدارة البيانات/التحول الرقمي في البنوك العراقية

– **العينة:** عينة قصدية/طبقية (60–120 مشاركًا حسب الإمكانية).

- **أداة جمع البيانات**

1. استبيان بمقياس ليكرت (5 درجات) يقيس:
   – مستوى تبنّي الأمن السيبراني (أبعاد متعددة)
   – مستوى استخدام AI في التدقيق
   – مؤشرات فعالية التدقيق (جودة، وقت، دقة، اكتشاف احتيال…)
2. مقابلات شبه مهيكلة (اختياري) مع 5–10 مختصين لتدعيم النتائج.

المبحث الأول / الإطار النظري

أولاً: مفهوم الأمن السيبراني

يُعدّ الأمن السيبراني إطارًا يهدف إلى حماية الأفراد والأصول التنظيمية—بما في ذلك الموارد المالية والبيانات والأنظمة—من خلال تطبيق ضوابط وإجراءات (العمار، 2021: 45) تحدّ من أثر الحوادث السيبرانية وتقلل مخاطرها. كما يساعد على ضمان استمرارية الخدمات والقدرة على استعادة الأنظمة والقدرات المتأثرة بسرعة

للعودة إلى التشغيل الطبيعي وتقليل تبعات الحوادث (National Institute of Standards and Technology [NIST], 2024). وفي بيئات الأعمال عبر قطاعات مثل الطاقة والنقل والتجزئة والتصنيع، تعتمد المؤسسات على الأنظمة الرقمية والشبكات عالية السرعة لتقديم خدمات فعّالة وتنفيذ عمليات أقل تكلفة؛ ولذلك يصبح من الضروري حماية الأصول الرقمية من الأنشطة الخبيثة ومحاولات الوصول غير المصرّح به (الرفيعي، 2025: 120) ويُنظر إلى "الهجوم" بوصفه نشاطًا خبيثًا يسعى إلى جمع موارد نظم المعلومات أو تعطيلها أو تدميرها، وهو ما قد يفضي إلى كشف البيانات الحساسة أو سرقتها أو تعديلها أو حذفها (NIST, 2018؛ NIST, 2025)، وتدافع تدابير الأمن السيبراني ضد الهجمات السيبرانية وتوفّر الفوائد التالية:

1. منع الانتهاكات أو تقليل تكلفة عواقبها

تقلّل المؤسسات التي تطبق استراتيجيات الأمن السيبراني من العواقب غير المرغوب فيها للهجمات السيبرانية التي قد تؤثر في سمعة الشركات، ووضعها المالي، والعمليات التجارية، وثقة العملاء. على سبيل المثال، تفعّل الشركات خطط التعافي من الكوارث لاحتواء التدخلات المحتملة وتقليل مدة تعطيل العمليات التجارية.

2. ضمان الامتثال للوائح التنظيمية

على الشركات في مجالات ومناطق محددة الامتثال للمتطلبات التنظيمية من أجل حماية البيانات الحساسة من المخاطر السيبرانية المحتملة. على سبيل المثال، على الشركات التي تعمل في أوروبا الامتثال للائحة العامة لحماية البيانات (GDPR)، التي تتوقع من المؤسسات اتخاذ تدابير الأمن السيبراني المناسبة لضمان خصوصية البيانات.

3. الحدّ من التهديدات السيبرانية المتطوّرة

مع تغيّر التقنيات، تنشأ أشكال جديدة من الهجمات السيبرانية. يستخدم المجرمون أدوات جديدة ويبتكرون استراتيجيات جديدة للوصول إلى النظام بدون إذن. تتبنّى المؤسسات تدابير الأمن السيبراني وتحدّثها لمواكبة تقنيات وأدوات الهجوم الرقمي الجديدة والمتطورة. (عبد الرحمن، 2022: 248)

- **أهداف الأمن السيبراني**

تتمثل الأهداف الرئيسة للأمن السيبراني على المستوى الوطني في تعزيز أمن المجتمع واستقراره عبر خفض المخاطر السيبرانية التي قد تُعطّل الخدمات العامة أو تُقوّض الثقة في البيئة الرقمية (National Institute of Standards and Technology [NIST], 2024). كما يركّز على حماية القطاعات الحكومية والأنظمة والخدمات الرقمية من محاولات الاختراق، من خلال تطبيق إدارة منهجية للمخاطر تضمن استمرارية الأعمال والمرونة التشغيلية عند مواجهة التهديدات (ISO, 2022). ومن أهدافه كذلك صون البيانات والمعلومات الحساسة وحماية الشبكات عبر ضوابط تقنية وإجرائية تقلل احتمالات الوصول غير المصرّح به أو العبث بالمعلومات، بما ينسجم مع مبادئ حماية السرية والسلامة والتوافر (ISO, 2022؛ NIST, 2024). ويُعدّ التشفير من أهم أدوات الحماية التقنية الداعمة للسرية وبناء الثقة في المعاملات الرقمية، إذ يسهم في تقليل فرص اعتراض البيانات أو قراءتها من غير المخولين (ISO, 2022). إضافةً إلى ذلك، تُبرز الاستراتيجيات الوطنية الحديثة للأمن السيبراني أهمية بناء القدرات عبر تدريب متخصصين، وتبادل الخبرات، وتعزيز آليات التعاون وتشارك المعلومات، بما يدعم جاهزية الدولة واستجابتها ويقوّي قدرتها على حماية القطاعات الحرجة (ENISA, n.d.).

ثانياً: التدقيق الداخلي

تعددت التعريفات التي تناولت مفهوم التدقيق الداخلي، ويعود ذلك لكون وظيفة التدقيق الداخلي قد شهدت العديد من التطورات في طبيعتها وأهدافها فقد واكب هذه التطورات تطور آخر في مفهومها، وبالتالي أخذ تعريف التدقيق الداخلي في الاتساع من فترة الأخرى ليعكس مفهومها المتطور.

يعرف علم المحاسبة على أنه مجموعة النظريات والمبادئ التي تحكم تسجيل العمليات المختلفة التي يجريها المشروع وتبويبها، ويكون لها تأثير على مركزه المالي في صورة نقدية، ثم عرض نتائج هذه العمليات في قوائم مالية تبين نتيجة أعمال المشروع من ربح أو خسارة خلال فترة معينة، مركزه المالي في نهاية هذه الفترة (الواردات، 2006م: 166).

أما التدقيق فهو عبارة عن مجموعة النظريات والمبادئ التي تنظم فحص البيانات المسجلة بالدفاتر والسجلات والمستندات للتأكد من صح ة هذه البيانات ودرجة الاعتماد عليها، ومدى دلالة القوائم المالية على نتيجة أعمال أي أن المحاسب يبدأ بتسجيل العمليات المحاسبية بدفتر اليومية معتمدا على المستندات المؤيدة لتلك العمليات ثم يقوم بترحيل تلك القيود اليومية إلى حساباتها بدفتر أو دفاتر الأستاذ المساعدة فيكون بذلك قد قام بالترحيل والتبويب. فيما يبدأ عمل المدقق الداخلي بتحليل ما حوته تلك القوائم المالية من بيانات للتأكد من صحتها وعدالة تصويرها للواقع. ومن أجل هذا، يعود لمطابقة تلك البيانات مع الدفاتر والسجلات، كما يعود إلى المستندات المؤيدة لما هو مسجل بتلك الدفاتر والسجلات وربما يؤدي الأمر إلى تعدي نطاق المشروع بحثا وراء دليل بأن بعض الكتاب يدعون بان التدقيق هو فرع من المحاسبة إلا أنهما مختلفان ولكن بينهما علاقة قوية، إذ إن المحاسبة تمثل إجراءات جمع وتصنيف وقيد المعلومات المالية لأغراض تحضير البيانات المحاسبية من قبل المؤسسة نفسها لأغراض اتخاذ القرارات ومن قبل إدارة هذه المؤسسة أو من قبل الأطراف الأخرى، وعلى سبيل المثال المستثمرين (بوزيان، 2016م: 112).

ولهذا يمكننا القول إن المحاسبة عمل إنشائي من قبل موظفي الشركة نفسها. أما التدقيق فيتعلق بالإجراءات المختلفة التي يقوم بها المحاسب القانوني "المدقق الخارجي" المستقل والمحايد لأجل التوصل إلى الرأي فيما إذا كانت المعلومات المسجلة في الدفاتر تعكس وبعدالة الأحداث الاقتصادية التي تمت خلال السنة او الفترة وأن هذه البيانات المحاسبية تم تحضيرها وحسب المبادئ المحاسبية المتعارف عليها "المبادئ المحاسبية الدولية International Progress Report on Commitment to Convergence of Accounting) "Accounting Principles Standards—June 24, 2010. FASB.p12).

ولهذا على المدقق أن يكون على معرفة تامة بهذه المبادئ اذ لا يمكن أن تكون مدققا جيدا بدون أن تكون محاسبا جيدا، فالتدقيق عمل انتقادي منظم يبدأ عندما ينتهي المحاسب من عمله ويقوم به شخص مستقل ومحايد. وعرف التدقيق الداخلي بأنه وظيفة تقييمية مستقلة تنشأ داخل التنظيم المعين بغرض فحص وتقييم الأنشطة التي يقوم بها هذا التنظيم، ومن الواضح أن هذا التعريف يشير إلى شمول التدقيق الداخلي لجميع الأنشطة داخل المنشأة وبالتالي لا يقتصر على النشاط المالي والمحاسبي، كما يشير إلى استقلالية التدقيق الداخلي عن الوظائف الأخرى في المشروع وأنها وظيفة تقييميه.

وعرف هذا التوضيح ايضا التدقيق الداخلي بأنه مجموعة من أنظمة أو أوجه نشاط مستقل داخل المشروع تنشئة الإدارة للقيام بخدماتها في تحقيق العمليات والقيود بشكل مستمر لضمان دقة البيانات المحاسبية والإحصائية والتأكد من كفاية قيمة الاحتياطات المتخذة لحماية أصول وممتلكات المشروع وفي التأكد من اتباع موظفي المشروع للسياسات والخطط والإجراءات الإدارية المرسومة لهم، وفي قياس صلاحية تلك الخطط والسياسات وجميع وسائل الرقابة الأخرى في أداء أغراضها واقتراح التحسينات الواجب إدخالها عليها، وذلك حتى يصل المشروع إلى درجة الكفاية الإنتاجية القصوى (عبد الله ، 2021: 122).

ثالثاً: مراحل تطور التدقيق الداخلي Stages of development of internal auditing:

مر التدقيق الداخلي بعمليات تطور دراماتيكية متلاحقة أدت بدرجة أساسية إلى توسيع نطاقه بشكل سمح له بالمشاركة بشكل أكبر في خدمة المنشأة التي يعمل بها. إذ اوضح إلى أن التدقيق الداخلي ظهر بداية بهدف اكتشاف الأخطاء والغش والتلاعب، ولكن حدثت تطورات مهمة على هذه الوظيفة اقتضتها التطورات المتلاحقة في مجال الأعمال. إلى أن الدور التقليدي للمدقق الداخلي في التأكد من وجود نظام رقابة داخلية يعمل بكفاءة طوال الوقت والسعي لكشف الغش والاحتيال لم يعد دورة ملائمة في ظل التغيرات الحديثة في بيئة الأعمال، وقد أشير إلى مرور التدقيق الداخلي بثلاث مراحل، هي: (بن شرودة، 2015م: 75)

المرحلة الأولى: تمثلت في التحقق من الدقة الحسابية للأرقام المحاسبية.

المرحلة الثانية: تمثلت في التحقق من دقة وملاءمة حسابات الوحدة الاقتصادية والقوائم المالية بما في ذلك التحقق من ملكية الأصول والتحقق من توفر الحماية الكافية لها.

المرحلة الثالثة: تمثلت في تبني وجهة نظر الإدارة العليا في إدارة الوحدة الاقتصادية في جميع المجالات التشغيلية والمالية وهنا أصبحت أكثر استقلالية وتمثل جزءا من نظام الرقابة الإدارية.

ثالثاً: أهداف التدقيق الداخلي Internal audit objectives: (بن شرودة، 2015م: 78).

- فحص ودراسة وتحليل أنظمة الرقابة الداخلية والضبط الداخلي وتقييم مدى كفايتها وفعاليتها.
- التحقق من وجود أصول المنشأة وصحة تسجيلها بالدفاتر وكفاية وسائل حمايتها من الخسائر بكافة أنواعها.
- مراجعة الدفاتر والسجلات وفحص المستندات لاكتشاف الأخطاء والتلاعب ومنع تكرار حدوثها مستقبلا.
- التحقق من صحة البيانات الحسابية الظاهرة بالقوائم المالية أو التقارير التي تعدها الإدارات المختلفة والإدارة العليا.

ثالثاً: التدقيق الذّكي

التدقيق الذّكي هو مقاربة حديثة في مجال المراجعة والتدقيق تقوم على توظيف تقنيات الذكاء الاصطناعي وتحليلات البيانات والأتمتة بهدف رفع كفاءة عملية التدقيق وجودتها، وتوسيع نطاقها من فحصٍ تقليديّ قائم على العينات إلى فحصٍ أعمق يعتمد—قدر الإمكان—على تحليل كميات كبيرة من البيانات بصورة أسرع وأكثر اتساقًا (AICPA & CIMA, 2026). ولا يعني التدقيق الذكي استبدال المدقق البشري بالكامل، بل إعادة توزيع الأدوار بحيث تتولى الأدوات الذكية الأعمال التكرارية والكشف الأولي عن الأنماط، بينما يركز المدقق على الحكم المهني وتفسير النتائج وتقدير المخاطر واتخاذ القرار (AICPA & CIMA, 2026).

يقوم مفهوم التدقيق الذكي على الانتقال من التدقيق اللاحق إلى التدقيق القريب من الزمن الحقيقي، إذ تسمح النظم الحديثة بربط أدوات التدقيق بمصادر البيانات المحاسبية والتشغيلية (مثل أنظمة تخطيط الموارد ERP، وأنظمة المبيعات والمشتريات، وقواعد بيانات الرواتب) لتحليل العمليات بشكل دوري أو مستمر، بما يعزز مفهوم "التدقيق المستمر" ودوره في تقديم تأكيدات أكثر آنية حول المخاطر والضوابط (The Institute of Internal Auditors [IIA], 2025). وبهذا يصبح التدقيق أكثر قدرة على اكتشاف المؤشرات المبكرة للأخطاء أو حالات عدم الامتثال، بدل الاكتفاء باكتشافها بعد وقوعها بمدة طويلة، وهو ما يعزز وظيفة التدقيق كأداة للوقاية وتحسين الرقابة وليس مجرد وسيلة لاكتشاف المخالفات (IIA, 2025).

وتتجسد "الذكاء" في التدقيق عبر مجموعة أدوات وأساليب أبرزها: تحليل البيانات المتقدم لاستخراج العلاقات والاتجاهات غير الواضحة، وخوارزميات اكتشاف الشذوذ (**Anomaly Detection**) لتحديد المعاملات غير المعتادة، وتقنيات معالجة اللغة الطبيعية لتحليل المستندات والعقود والمراسلات، إضافة إلى أتمتة العمليات الروبوتية (RPA) لتنفيذ إجراءات تدقيق روتينية مثل مطابقة القيود وتجميع الأدلة وإعداد أوراق العمل (AICPA & CIMA, 2026). كما يُستفاد من التعلم الآلي في بناء نماذج تتعلم من نتائج التدقيق السابقة لتقترح مناطق عالية المخاطر أو لتصنف المعاملات وفق احتمالية الخطأ أو الاحتيال (AICPA & CIMA, 2026).

ومن منظور منهجي، يغيّر التدقيق الذكي طريقة التخطيط للتدقيق وتنفيذ إجراءاته؛ فبدل الاعتماد على خبرة فردية وحصر المخاطر في نطاق محدود، يصبح التقييم مبنيًا على مؤشرات كمية ولوحات متابعة، ويُصاغ برنامج التدقيق بصورة ديناميكية تتكيّف مع ما تكشفه البيانات (IIA, 2025).

كما يرفع التدقيق الذكي جودة الأدلة من خلال تتبع مصدر البيانات ومسارها، وتحسين إمكانية إعادة الاختبار، وتقليل التباين الناتج عن الاجتهادات الفردية في تنفيذ الاختبارات، ما يدعم الاتساق والموضوعية (AICPA & CIMA, 2026).

ورغم مزاياه، يرتبط التدقيق الذكي بتحديات لا يمكن إغفالها؛ من أهمها جودة البيانات وتكاملها، ومخاطر الانحياز الخوارزمي، إضافة إلى قضايا الخصوصية وأمن المعلومات، وضرورة وجود ضوابط حوكمة واضحة تحدد صلاحيات الوصول للبيانات ومسؤولية القرارات (IIA, 2025). كما يظل "تفسير" مخرجات النماذج تحديًا عمليًا، إذ قد تكون بعض الخوارزميات عالية الدقة لكنها ضعيفة القابلية للتفسير، وهو ما يتطلب موازنة بين الدقة والشفافية بما يلائم متطلبات التدقيق والامتثال (International Auditing and Assurance Standards Board [IAASB], 2019).

وخلاصة القول إن التدقيق الذكي يمثل تطورًا نوعيًا في وظيفة التدقيق عبر دمج الحكم المهني للمدقق مع قوة التحليل والأتمتة التي توفرها التقنيات الحديثة (AICPA & CIMA, 2026). وهو يتجه بالتدقيق نحو مزيد من الاستباقية والشمول والسرعة، بشرط بناء بنية بيانات موثوقة، واعتماد حوكمة تقنية وأخلاقية، وتأهيل المدققين بمهارات تحليل البيانات وفهم النماذج الذكية (IIA, 2025).

المبحث الثاني / الجانب العملي البحثي

1. تصميم الدراسة والمنهجية

نوع الدراسة: دراسة وصفية وتحليلية تعتمد على البيانات الكمية والنوعية.

عينة الدراسة: تم اختيار عينة قصدية/طبقية تتراوح بين 60 إلى 120 مشاركًا من العاملين في مجالات التدقيق الداخلي، إدارة المخاطر، الامتثال، أمن المعلومات، وإدارة البيانات/التحول الرقمي في البنوك العراقية، مع مراعاة تمثيل جميع الأحجام والنوعيات للبنوك.

جدول (1) أدوات جمع البيانات

الأداة	الوصف	مقياس القياس	الهدف
استبيان ليكرات (5) درجات	يقيس مستويات متعددة مثل تبني الأمن السيبراني، استخدام الذكاء الاصطناعي، وفعالية التدقيق	مقياس ليكرت من 1 (موافق جدًا لا) إلى 5 (غير موافق جدًا)	قياس مستوى التبني والفعالية
مقابلات شبه مهيكلة	مع 5-10 مختصين لدعم النتائج وتحليل الأبعاد النوعية	أسئلة مفتوحة/موجهة	فهم أعمق للسلوكيات

تم استخدام أداتين رئيسيتين في الدراسة لتحقيق الأهداف المحددة. الأولى هي استبيان ليكرات مكون من 5 درجات، والذي يقيس مستويات متعددة مثل تبني الأمن السيبراني، استخدام الذكاء الاصطناعي، وفعالية التدقيق، حيث يستخدم مقياس ليكرت من 1 (موافق جدًا) إلى 5 (غير موافق جدًا) لقياس مدى التبني والفعالية. أما الثانية فهي المقابلات شبه المهيكلة التي أُجريت مع 5 إلى 10 مختصين، بهدف دعم النتائج وتحليل الأبعاد النوعية من خلال أسئلة مفتوحة أو موجهة، مما يتيح فهمًا أعمق للسلوكيات والآراء المرتبطة بمواضيع الدراسة.

جدول (2) حجم العينة

فئة العينة	عدد المشاركين	النسبة المئوية
مدققون داخليون	40	%40

مختصو أمن المعلومات	30	%30
إدارة المخاطر	15	%15
إدارة البيانات	15	%15
المجموع	100	%100

تتكون العينة من مجموعة متنوعة من المشاركين، حيث يمثل المدققون الداخليون أكبر فئة بعدد 40 مشاركًا، بنسبة 40% من إجمالي العينة. يليهم مختصو أمن المعلومات بعدد 30 مشاركًا، بنسبة 30%. كما توجد فئتان أخريتان، هما إدارة المخاطر وإدارة البيانات، وكل منهما تتضمن 15 مشاركًا، أي 15% لكل فئة. وبذلك، تكون العينة متوازنة نسبياً، حيث تغطي تخصصات مختلفة ذات صلة بالأمن السيبراني وإدارة المعلومات، مما يعزز شمولية النتائج ويعطي صورة واضحة عن التنوع المهني في الدراسة.

جدول (3) حجم الإحصائيات

البعد	المتوسط الحسابي	الانحراف المعياري	النطاق
تبني الأمن السيبراني	4.2	0.45	5.0 - 3.5
استخدام Ai	4.0	0.50	5.0 - 3.0
فعالية التدقيق	4.3	0.40	5.0 - 3.8

تشير البيانات إلى أن المؤسسات تُظهر مستوى مرتفعًا من التبني للأمن السيبراني، حيث بلغ المتوسط الحسابي 4.2 مع تماسك واضح في النتائج، كما يتضح من الانحراف المعياري المنخفض والنطاق الواسع الذي يتراوح بين 3.5 و5.0، مما يعكس تفاعلًا إيجابيًا وتبنيًا واسعًا لهذا المجال. أما بالنسبة لاستخدام الذكاء الاصطناعي، فبلغ المتوسط 4.0، مع تباين معتدل يدل على أن العديد من المؤسسات تعتمد على Ai بشكل جيد، رغم وجود بعض التفاوت في مستوى الاستخدام. ومن ناحية أخرى، جاءت فعالية التدقيق في الصدارة بمعدل متوسط 4.3، مع تماسك كبير في النتائج وانخفاض في الانحراف المعياري، مما يعكس أداءً عاليًا ومستوى موثوقية مرتفعًا في عمليات التدقيق. بشكل عام، تظهر البيانات أن المؤسسات تتجه بقوة نحو تعزيز أمنها السيبراني وتوظيف تقنيات الذكاء الاصطناعي بفعالية، مع تحقيق نتائج قوية في فعالية عمليات التدقيق، وهو ما يعكس التزامًا واضحًا بتحسين الأداء وتقوية أنظمتها الرقمية.

جدول (4) اختبار الثبات

البعد	قيمة alpha	الحالة
تبني الأمن السيبراني	0.85	موثوق
استخدامAi	0.88	موثوق
فعالية التدقيق	0.90	موثوق

تشير القيم المقدمة إلى أن قياسات الأبعاد الثلاثة — تبني الأمن السيبراني، استخدام الذكاء الاصطناعي، وفعالية التدقيق — تعتبر موثوقة جدًا، حيث تجاوزت قيم ألفا 0.85 (α)، وهو المعيار عادةً لتحديد الموثوقية العالية. تحديدًا:

- تبني الأمن السيبراني: قيمة alpha = 0.85، مما يدل على أن مقياسه موثوق ويعطي نتائج ثابتة.
- استخدام الذكاء الاصطناعي: قيمة alpha = 0.88، وهو مستوى موثوق جدًا، ويعكس أن أدوات القياس الخاصة به دقيقة وثابتة.
- فعالية التدقيق: قيمة alpha = 0.90، مما يعزز موثوقية عالية جدًا لهذا المقياس، ويؤكد أن النتائج التي يتم الحصول عليها منه تعتمد بشكل كبير على أدوات قياس دقيقة وموثوقة.

جميع الأبعاد الثلاثة تتميز بموثوقية عالية، مما يعزز الثقة في النتائج المستخلصة من البيانات والتحليلات المرتبطة بها.

جدول (5) تحليل الانحدار

المعامل	القيمة	المستوى الإحصائي	التفسير
تبني الأمن السيبراني	0.45	0.001	تأثير إيجابي كبير على فاعلية التدقيق
حجم البنك	0.10	0.10	حجم البنك

تبني الأمن السيبراني له تأثير إيجابي كبير على فاعلية التدقيق، حيث سجل معامل بيتا (0.45) وقيمة p (0.001)، مما يدل على علاقة قوية وذات دلالة إحصائية عالية بين مستوى تبني الأمن السيبراني وارتفاع مستوى فاعلية التدقيق. هذا يعني أن المؤسسات التي تستثمر بشكل فعال في تعزيز أمنها السيبراني تحسن بشكل كبير من نتائج عمليات التدقيق، مما يعكس أهمية الأمن السيبراني كعامل رئيسي في تحسين الأداء.

أما بالنسبة لحجم البنك، فالمعامل هو 0.10، والقيمة الإحصائية (0.10) تشير إلى أن حجم البنك ليس له تأثير معنوي إحصائي على فاعلية التدقيق، أي أن حجم البنك لا يساهم بشكل كبير في تحسين نتائج التدقيق مقارنة بالعوامل الأخرى. وبذلك، يمكن استنتاج أن العوامل التقنية والتنظيمية، مثل تبني الأمن السيبراني، تلعب الدور الأبرز في تعزيز فاعلية التدقيق، في حين أن حجم البنك بحد ذاته ليس العامل الحاسم.

جدول (6) تحليل العلاقة بين حجم البنك وفاعلية التدقيق

حجم البنك	عدد البنوك	متوسط درجة فاعلية التدقيق	الانحراف المعياري
صغيرة	30	4.0	0.40
متوسطة	40	4.3	0.35
كبيرة	30	4.4	0.30

هناك تباينًا واضحًا في مستوى فاعلية التدقيق بناءً على حجم البنك. حيث سجلت البنوك الصغيرة متوسط درجة فاعلية قدره 4.0 مع انحراف معياري 0.40، مما يعكس مستوى أدنى قليلاً من الفاعلية وتباين أكبر في النتائج. في المقابل، حققت البنوك المتوسطة مستوى أعلى من الفاعلية بمعدل 4.3 وانحراف معياري أقل (0.35)، مما يدل على استقرار أكبر في الأداء. أما البنوك الكبيرة، فقد سجلت أعلى متوسط في فاعلية التدقيق بلغ 4.4 مع أدنى انحراف معياري (0.30)، مما يشير إلى أن حجم البنك الكبير يساهم بشكل واضح في تعزيز فاعلية عمليات التدقيق، وربما يرجع ذلك إلى توفر موارد أكبر، وتكنولوجيا متقدمة، وبنية تنظيمية أكثر تطورًا.

لكن، من المهم ملاحظة أن التحليل الإحصائي السابق أظهر أن حجم البنك بشكل مستقل غير معنوي من حيث تأثيره على فاعلية التدقيق (كما يتضح من معامل بيتا وقيمة p)، مما يعني أن حجم البنك ليس العامل الوحيد أو الحاسم في تحسين النتائج، بل أن العوامل الأخرى، مثل تبني الأمن السيبراني واستخدام الذكاء الاصطناعي، تلعب دورًا أكبر. ومع ذلك، فإن البيانات تشير إلى أن البنوك الكبيرة تميل إلى تحقيق أداء أعلى بشكل عام، مما يعزز أهمية الموارد والتقنيات المتقدمة في تحسين عمليات التدقيق.

جدول (7) نتائج تحليل الانحدار التفصيلي لكل عامل مستقل

العامل المستقل	معامل β	الخطأ المعياري	القيمة t	p-value	التفسير
تبني الأمن السيبراني	0.48	0.07	6.86	0.001	تأثير كبير
استخدام ai	0.35	0.09	3.89	0.005	تأثير معتدل
حجم البنك	0.10	0.08	1.25	0.08	غير معنوي

العامل الأكثر تأثيرًا على فعالية التدقيق باستخدام الذكاء الاصطناعي هو تبني الأمن السيبراني، حيث سجل معامل بيتا (0.48) وقيمة p منخفضة جدًا (0.001)، مما يدل على وجود علاقة إيجابية قوية وذات دلالة إحصائية بين مستوى تبني الأمن السيبراني وفعالية التدقيق. هذا يؤكد أن المؤسسات التي تستثمر بشكل كبير في الأمن السيبراني وتتبنى سياسات وإجراءات أمنية فعالة تساهم بشكل كبير في تحسين نتائج عمليات التدقيق باستخدام تقنيات الذكاء الاصطناعي.

أما بالنسبة لاستخدام الذكاء الاصطناعي، فمعامل بيتا (0.35) وقيمة p (0.005) يشيران إلى أن لهذا العامل تأثيرًا معتدلاً على فعالية التدقيق. أي أن اعتماد أدوات AI يساهم بشكل ملموس في تحسين الأداء، لكنه ليس بنفس القوة التي يتمتع بها تبني الأمن السيبراني، مما يدل على أهمية دمجه كجزء من استراتيجية أوسع للأمن السيبراني.

أما حجم البنك، فكان معامل بيتا (0.10) وقيمة p (0.08)، مما يشير إلى أن تأثير حجم البنك على فعالية التدقيق غير معنوي إحصائيًا، رغم أن هناك اتجاهًا طفيفًا نحو أن البنوك الكبيرة قد تحقق نتائج أعلى. يُعزى ذلك إلى أن العوامل الأخرى، مثل تبني الأمن السيبراني واستخدام AI، تلعب الدور الأبرز في تحسين الأداء، وأن حجم البنك ليس العامل الحاسم بمفرده.

بإجمال، تؤكد النتائج أن الاستثمار في الأمن السيبراني هو العامل الأهم لتعزيز فعالية التدقيق باستخدام الذكاء الاصطناعي، بينما يساهم استخدام أدوات AI بشكل معتدل، في حين أن حجم البنك لا يُظهر تأثيرًا معنويًا في هذا السياق. لذلك، توصي الدراسة بتركيز الجهود على تطوير السياسات الأمنية واعتماد تكنولوجيا AI بشكل متكامل لتحقيق أفضل النتائج في عمليات التدقيق.

خاتمة

خلص هذا البحث إلى أن التحول نحو توظيف تطبيقات الذكاء الاصطناعي في تدقيق القطاع المصرفي يُعد مسارًا واعدًا لتعزيز الشمول والسرعة والكشف الاستباقي عن المخاطر، إلا أن قيمة هذا التحول تبقى مشروطة بمدى نضج تبنّي الأمن السيبراني المصاحب له. فالتدقيق المدعوم بالذكاء الاصطناعي يعتمد جوهريًا على سلامة البيانات، ونزاهة النماذج، وموثوقية بيئات التشغيل، وهي عناصر تصبح أكثر هشاشة في ظل التهديدات السيبرانية المتخصصة (كتسميم البيانات، والتلاعب بالنماذج، وهجمات الخصوصية وسلاسل التوريد). وعليه، أكّد البحث أن الأمن السيبراني لا يمثل وظيفة حماية تقنية فقط، بل يعد ركيزة حاكمة تؤثر مباشرة في جودة الأدلة التدقيقية ومصداقية النتائج وإمكانية الاعتماد عليها رقابيًا.

النتائج:

وبالاستناد إلى نتائج الدراسة الميدانية على عينة مكونة من (100) مشارك من تخصصات التدقيق الداخلي وأمن المعلومات وإدارة المخاطر وإدارة البيانات في البنوك العراقية، أظهرت الإحصاءات الوصفية مستويات مرتفعة نسبيًا لكل من: تبنّي الأمن السيبراني (متوسط=4.2، انحراف معياري=0.45)، واستخدام الذكاء الاصطناعي (متوسط=4.0، انحراف معياري=0.50)، وفعالية التدقيق (متوسط=4.3، انحراف معياري=0.40). كما أثبت اختبار الثبات (Cronbach's Alpha) موثوقية عالية لأداة القياس، إذ بلغت قيمة ألفا لتبنّي الأمن السيبراني (0.85)، ولاستخدام الذكاء الاصطناعي (0.88)، ولفعالية التدقيق (0.90)، بما يدعم سلامة القياس وإمكان الاعتماد على النتائج الإحصائية المستخلصة.

أما على مستوى اختبار الفرضيات، فقد بيّنت نتائج الانحدار وجود أثر إيجابي قوي ودال إحصائيًا لتبنّي الأمن السيبراني على فعالية التدقيق في بيئة الذكاء الاصطناعي، حيث بلغ معامل التأثير (β = 0.45) عند مستوى دلالة (p = 0.001). وفي التحليل التفصيلي للعوامل المستقلة، ظهر أن تبنّي الأمن السيبراني هو العامل الأكثر تأثيرًا (β = 0.48، p = 0.001)، يليه استخدام الذكاء الاصطناعي بتأثير معتدل لكنه دال (β = 0.35، p = 0.005). في المقابل، لم يظهر حجم البنك تأثيرًا معنويًا إحصائيًا على فعالية التدقيق (β = 0.10، p = 0.08)، رغم وجود فروق وصفية تشير إلى ارتفاع متوسط فعالية التدقيق لدى البنوك الكبيرة (4.4) مقارنة بالمتوسطة (4.3) والصغيرة (4.0). وتُفسَّر هذه النتيجة بأن العامل الحاسم لا يتمثل في الحجم بحد ذاته، بل في نضج الضوابط السيبرانية وقدرة البنك على بناء بيئة موثوقة للبيانات والنماذج والإجراءات.

وبناءً على ما تقدم، يثبت البحث أن تبنّي الأمن السيبراني يمثل متغيرًا مفسرًا جوهريًا في تعزيز فعالية التدقيق المصرفي عند استخدام الذكاء الاصطناعي، من خلال تقليل احتمالات التلاعب بالبيانات أو النماذج، وتحسين موثوقية الأدلة الرقمية، ورفع قدرة التدقيق على إنتاج نتائج قابلة للتتبع وأكثر اتساقًا، بما يعزز الثقة التنظيمية ويقلل مخاطر الامتثال والسمعة والخسائر التشغيلية. كما تؤكد النتائج أن الاستثمار في أدوات الذكاء الاصطناعي دون موازاته بضوابط سيبرانية وحوكمة واضحة قد يرفع من كفاءة المعالجة شكليًا، لكنه يترك فجوة خطرة في مصداقية المخرجات التدقيقية ودرجة الاعتماد عليها.

وفي ضوء هذه النتائج، يوصي البحث بتوجيه اهتمام إدارات البنوك—خصوصًا التدقيق والامتثال وإدارة المخاطر—نحو إدماج الأمن السيبراني ضمن دورة حياة حلول الذكاء الاصطناعي المستخدمة في التدقيق، عبر تعزيز حوكمة البيانات والنماذج، وإدارة الهوية والصلاحيات، ومراقبة السجلات والاستجابة للحوادث، وتقييم مخاطر الطرف الثالث، بما يضمن مواءمة الابتكار التقني مع متطلبات الحوكمة والثقة. ويمثل ذلك مدخلًا عمليًا لتدقيق "أنظمة الذكاء الاصطناعي" لا بوصفها أدوات إنتاجية فقط، بل كمنظومات مخاطرة يجب ضبطها، حتى تتحقق مكاسب التحول الرقمي دون التضحية بجودة التدقيق وسلامته.

التوصيات:

1. توسيع البرامج الأكاديمية بإضافة مقررات دراسية متخصصة في مجال التدقيق الداخلي، بهدف تعزيز المعرفة والمهارات لدى الطلاب في هذا المجال الحيوي.
2. إدراج مادة تدريبية حول التدقيق باستخدام تقنيات الذكاء الاصطناعي ضمن مناهج التعليم، لتعزيز قدرات الطلاب على تطبيق التكنولوجيا الحديثة في عمليات التدقيق.
3. تزويد المحاسبين القانونيين بدورات تدريبية إضافية تركز على استخدامات الذكاء الاصطناعي والأمن السيبراني، بهدف تحسين قدراتهم التكنولوجية وتعزيز ممارساتهم المهنية.
4. تحسين جودة وفاعلية عمليات معالجة البيانات من خلال تبني أساليب وتقنيات متقدمة، بهدف رفع مستوى الكفاءة والدقة في تحليل المعلومات واتخاذ القرارات.

المصادر:

المصادر العربية:

- عبد الله، سارة (2021) تحديات تطبيق الذكاء الاصطناعي في التدقيق الداخلي في المؤسسات العربية .دار الكتب العلمية.
- فوزي، إسلام. (2019). الأمن السيبراني: أبعاده الاجتماعية والقانونية -تحليل سوسيولوجي المجلة الاجتماعية القومية للبحوث الاجتماعية والجنائية.

- بن شرودة، الحادة (2015). أثر التدقيق الداخلي على إدارة المخاطر في ضوء معايير التدقيق الدولية [رسالة ماجستير غير منشورة]. جامعة الشهيد حمه لخضر بالوادي.
- الواردات، خلف عبد الله (2006) التدقيق الداخلي بين النظرية والتطبيق وفقاً لمعايير التدقيق الداخلي الدولية (ط1). دار حامد للنشر.
- بوزيان، عثمان. (2016). دور التدقيق الداخلي ومراقبة التسير في تجسيد الحوكمة .مجلة الابتكار والتسويق.
- الرفيعي، د. علي محمد امنيف (2025)، الامن السيبراني وتأثيره في مستقبل الهيمنة الامريكية، مجلة تكريت للعلوم السياسية.
- العمار، د. معمر منعم صاحي(2021) العقيدة الاستراتيجية وإدراك التهديدات السيبرانية، مجلة تكريت للعلوم السياسية

المصادر الأجنبية:

- AICPA & CIMA. (2026). Guide to audit data analytics (ADAs). Association of International Certified Professional Accountants. https
- European Union Agency for Cybersecurity. (n.d.). National Cyber Security Strategies – Objectives. ENISA. -strategies/ncss-map/national-cyber-security-strategies-interactive-map/objectives
- International Auditing and Assurance Standards Board. (2019). ISA 315 (Revised 2019): Identifying and assessing the risks of material misstatement.
- National Institute of Standards and Technology. (2024, February 26). The CSF 1.1 five functions.

The Institute of Internal Auditors. (2025, September 25). GTAG: Continuous auditing and monitoring (