

إعادة هندسة نظم المعلومات المحاسبية في ضوء تبني تقنية البلوك تشين: دراسة معيارية متكاملة لتطبيق معايير الجودة الآيزو 27032 والآيزو 31000 لتعزيز الأمن السيبراني وإدارة المخاطر المؤسسية.

Reengineering Accounting Information Systems in Light of Blockchain Technology Adoption: An Integrated Normative Study for Implementing ISO 27032 and ISO 31000 to Enhance Cybersecurity and Enterprise Risk Management.

ابراهيم صبيعات¹، عمر ميهوبي²

¹كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة البويرة، البويرة 10000، الجزائر، مخبر السياسات التنموية والدراسات الاستشرافية،

b.sebiat@univ-bouira.dz

²كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة البويرة، البويرة 10000، الجزائر، مخبر الإقليم، المقاولاتية والابتكار، o.mihoubi@univ-bouira.dz

univ-bouira.dz

تاريخ النشر: 2025/09/15

تاريخ القبول: 2025/09/13

تاريخ الاستلام: 2024/12/07

ملخص:

تهدف الدراسة إلى اقتراح نموذج معياري لإعادة هندسة نظم المعلومات المحاسبية باستخدام تقنية البلوك تشين، لمعالجة التحديات المرتبطة بالأمن السيبراني وإدارة المخاطر المؤسسية. انطلقت الدراسة من إشكالية ضعف التكامل بين نظم المعلومات المحاسبية الحديثة ومتطلبات الحماية السيبرانية وفق المعايير الدولية، مما يهدد موثوقية البيانات المحاسبية وسلامتها. استندت الدراسة إلى منهج وصفي تحليلي يعتمد على مراجعة الأدبيات السابقة وتحليل معايير *ISO 27032* و *ISO 31000* لتقديم استراتيجيات عملية لتحسين أمن البيانات وتقليل المخاطر التشغيلية. يركز النموذج المقترح على التكامل بين معايير الحماية وإدارة المخاطر لضمان الحماية السيبرانية وتعزيز الثقة في الأنظمة المحاسبية، مع الامتثال للمعايير الدولية. توصي الدراسة المؤسسات بتبني هذا النموذج لتعزيز فعالية نظمها المحاسبية واستثمار إمكانات تقنية البلوك تشين بطريقة آمنة ومستدامة.

الكلمات المفتاحية: إعادة هندسة نظم المعلومات المحاسبية، تقنية البلوك تشين، الأمن السيبراني، إدارة المخاطر، معيار *ISO 27032*، معيار *ISO 31000*.

التصنيف *JEL*: *M15, G32, O33, L86*.

Abstract:

The study aims to develop a normative model for the re-engineering of accounting information systems using blockchain technology to address challenges related to cybersecurity and enterprise risk management. It starts from the problem of insufficient integration between modern accounting information systems and cybersecurity requirements according to international standards, which threaten the reliability and integrity of accounting data. A descriptive-analytical method was adopted, where a comprehensive review of scientific literature

and analysis of ISO 27032 and ISO 31000 standards were proceeded to propose practical strategies that enhance data security and reduce operational risks. The proposed model focuses on integrating security and risk management standards to ensure cybersecurity and foster trust in accounting systems while maintaining compliance with international standards. The study recommends institutions to adopt this model for enhancing their accounting systems' efficiency and invest blockchain technology in a secure and sustainable manner.

Keywords: Re-engineering of accounting information systems, blockchain technology, cybersecurity, risk management, ISO 27032, ISO 31000.

JEL Classification Codes: M15, G32, O33, L86.

I. مقدمة

1- تمهيد

لقد أثر التطور السريع للتقنيات الرقمية بشكل عميق على الممارسات التنظيمية، لا سيما في مجالات المحاسبة والإدارة المالية. من بين هذه التقنيات، برزت تقنية البلوك تشين نظرًا لقدرتها على تعزيز الشفافية، والأمان، والكفاءة في إدارة البيانات (Nakamoto, 2008). تُعتبر البلوك تشين نظام دفتر أستاذ موزع حيث يتم الحفاظ على سلامة البيانات من خلال أساليب تشفيرية، مما يجعلها حلاً مثاليًا للتحديات التي تواجه نظم المعلومات الحاسوبية التقليدية (Tapscott & Tapscott, 2016). ومع ذلك، يتطلب تبني تقنية البلوك تشين تعديلات كبيرة على الأنظمة القائمة لتتوافق مع متطلبات الأمن السيبراني وإدارة المخاطر الناشئة.

يظل الأمن السيبراني هاجسًا رئيسيًا للمؤسسات التي تدمج التقنيات الرقمية ضمن نظم المعلومات المحاسبية، حيث تزيد الأنظمة المرتبطة بالمعلومات المحاسبية من احتمالية التعرض للهجمات السيبرانية (Stallings, 2018). يوفر معيار ISO 27032 إرشادات شاملة لتعزيز الأمن السيبراني في البيئات الشبكية، مع التركيز على ممارسات آمنة لتبادل البيانات وتخزينها (ISO/IEC 27032, 2023). وبالمثل، يُعد معيار ISO 31000 إطارًا عالميًا معترفًا به لإدارة المخاطر، حيث يتيح إطارًا منهجيًا لتحديد المخاطر المؤسسية وتقييمها وتخفيفها (ISO 31000, 2018). حيث يتيح دمج هذه المعايير ضمن نظم المعلومات المحاسبية القائمة على البلوك تشين إطارًا قويًا لمعالجة تحديات الأمان والمخاطر مع ضمان المرونة التشغيلية.

2- إشكالية الدراسة

تتمثل الإشكالية التي تتناولها هذه الدراسة في التفتت والهشاشة التي تعاني منها نظم المعلومات المحاسبية الحالية عند تعرضها للتهديدات السيبرانية الديناميكية والبيئات المعقدة لإدارة المخاطر. غالبًا ما تفتقر المؤسسات إلى استراتيجية متماسكة تجمع بين الابتكار التكنولوجي، مثل البلوك تشين، وأطر قوية مثل ISO 27032 و ISO 31000 لمعالجة هذه التحديات بشكل فعال. يؤدي غياب هذا النهج المتكامل إلى تهديد سلامة البيانات وكفاءة المؤسسة وجودة اتخاذ القرارات. من هنا، تبرز الإشكالية البحثية التالية: كيف يمكن لتبني تقنية البلوك تشين في نظم المعلومات المحاسبية أن يساهم في تحقيق الأمن السيبراني وإدارة المخاطر وفق معايير الأيزو 27032 والأيزو 31000؟

ويتفرع عن هذا التساؤل مجموعة من الأسئلة الفرعية:

- ✓ ما الخصائص والوظائف الرئيسة لتقنية البلوك تشين التي تجعلها مناسبة لتعزيز نظم المعلومات المحاسبية؟
- ✓ كيف يساهم تطبيق معيار ISO 27032 في رفع مستوى الأمن السيبراني داخل نظم المعلومات المحاسبية المبنية على البلوك تشين؟
- ✓ ما آليات ومعايير ISO 31000 التي يمكن تكييفها لإدارة المخاطر المرتبطة باستخدام تقنية البلوك تشين في المحاسبة؟
- ✓ ما الإطار المعياري المقترح الذي يدمج بين تقنية البلوك تشين ومعايير ISO 27032 و ISO 31000 لتحقيق التوازن بين الأمن السيبراني وإدارة المخاطر؟

3- فرضيات الدراسة

- ✓ **الفرضية الأولى:** يمتلك دمج تقنية البلوك تشين مع معيار ISO 27032 أثرًا إيجابيًا ملموسًا في تعزيز الأمن السيبراني لنظم المعلومات المحاسبية.
- ✓ **الفرضية الثانية:** يؤدي تطبيق معايير ISO 31000 في بيئة البلوك تشين إلى تحسين قدرة المؤسسات على تحديد المخاطر وتقييمها والتخفيف منها.
- ✓ **الفرضية الثالثة:** الدمج المعياري بين البلوك تشين ومعايير ISO 27032 و ISO 31000 يحقق تكاملًا فعالًا بين متطلبات الأمن السيبراني وإدارة المخاطر، مما يرفع من كفاءة وجودة نظم المعلومات المحاسبية.

4- أهداف الدراسة

تهدف هذه الدراسة إلى تطوير نموذج معياري لإعادة هندسة نظم المعلومات المحاسبية في ضوء تبني تقنية البلوك تشين، مع دمج معايير ISO 27032 و ISO 31000 كأطر توجيهية. من خلال استكشاف الأسس النظرية والتطبيقات العملية لهذه المعايير، تسعى الدراسة إلى اقتراح استراتيجيات قابلة للتنفيذ لتعزيز الأمن السيبراني وإدارة المخاطر المؤسسية. تقدم هذه الدراسة خارطة طريق للمؤسسات للاستفادة من الإمكانيات التحويلية لتقنية البلوك تشين مع ضمان الامتثال للمعايير الدولية وحماية أصولها الرقمية.

5- منهجية الدراسة

اعتمدت الدراسة المنهج الوصفي التحليلي بهدف دراسة الظاهرة بعمق من خلال مراجعة الأدبيات الأكاديمية وتحليل العلاقة بين تقنية البلوك تشين ومعايير الأيزو 27032 والأيزو 31000. يتمثل النهج الوصفي في تحديد المفاهيم الأساسية وإطار العمل، بينما يركز النهج التحليلي على استكشاف العلاقة بين التقنية والمعايير ومدى تأثيرها على نظم المعلومات المحاسبية.

6- هيكل الدراسة

تتوزع هذه الدراسة على محورين رئيسيين؛ يتناول المحور الأول الإطار المفاهيمي للبحث، من خلال عرض المفاهيم الأساسية المرتبطة بتقنية البلوك تشين ونظم المعلومات الحاسوبية، إضافةً إلى استعراض الدراسات السابقة ذات الصلة، بما يتيح تأسيس خلفية علمية متينة للموضوع. أما المحور الثاني فيركز على تحليل مدى الامتثال لمتطلبات معايير ISO 27032 و ISO 31000 باعتبارهما إطارين دوليين لتعزيز الأمن السيبراني وإدارة المخاطر، وذلك كمدخل استراتيجي لتطوير نظم المعلومات الحاسوبية المدعومة بتقنية البلوك تشين وتحقيق التكامل بين الكفاءة التشغيلية وحماية البيانات.

II. المحور الأول: الإطار المفاهيمي والدراسة السابقة

1- تقنية البلوك تشين في نظم المعلومات الحاسوبية

تُعرف تقنية البلوك تشين بأنها نوع من تكنولوجيا دفتر السجلات الموزعة (DLT) أو تكنولوجيا مالية (FinTech)، حيث تعمل كقاعدة بيانات تسلسلية تتجاوز المفهوم التقليدي لدفتر السجلات المالي. هذه التقنية تسجل المعلومات المتعلقة بالمعاملات وتؤمنها باستخدام تقنيات التشفير، مع إدارة المعاملات عبر آلية توافق لضمان دقة وسلامة البيانات. تنوع التعريفات المختلفة للبلوك تشين يعكس تعدد التخصصات التي تدرسها، مما يشير إلى تعقيد إيجاد تعريف موحد لها بسبب اختلاف التفسيرات حسب المجال (Shiwakoti & et al, 2023, p. 3).

تمثل تقنية البلوك تشين حلاً مبتكراً للتحديات الراهنة في مجال المحاسبة، حيث تتيح وسائل جديدة تسهم في رفع الكفاءة وتقليل التكاليف الإدارية. يلخص الجدول رقم (02) الفوائد التي تقدمها المحاسبة المستندة إلى تقنية البلوك تشين، وذلك عبر استعراض التحديات المرتبطة بالمحاسبة التقليدية والميزات التي توفرها هذه التقنية. وبفضل هذه الفوائد، تتحقق زيادة في دقة البيانات وشفافيتها، مع الحد من الأخطاء، مما يعزز من موثوقية وكفاءة عمليات المحاسبة.

الجدول رقم (01): تطبيقات وفوائد تقنية البلوك تشين في مواجهة التحديات المحاسبية.

التحديات المحاسبية الحالية	محرك القيمة	فوائد تقنية البلوك تشين	أمثلة عملية على التطبيق
الوثائق اليدوية	تحسين الكفاءة وتبسيط العمليات	تحويل الوثائق إلى رقمية، مما يزيد الكفاءة ويقلل التكاليف والأخطاء البشرية، بالإضافة إلى أتمتة التسويات المالية.	استخدام نظام بلوك تشين لحفظ الفواتير والمستندات، مما يقلل من الحاجة للورق ويسرع الوصول إلى المعلومات.
العمليات التي تستغرق وقتاً طويلاً	تقليل وقت تسوية المعاملات	العقود الذكية تمكن من تنفيذ المعاملات تلقائياً عند استيفاء شروط معينة، مما يسرع إجراءات المحاسبة.	تطبيق العقود الذكية في دفع الفواتير تلقائياً بعد استلام السلع والتحقق من جودتها عبر الشبكة.
صعوبة تتبع المعاملات	تقليل مخاطر	توفر بيئة مشتركة وآمنة تتيح تسجيل المعاملات	استخدام بلوك تشين لتوثيق المعاملات بين الموردين

عبر دفاتر متعددة	الأطراف المقابلة	بشكل لا يقبل التغيير، مما يسهل عملية التدقيق.	والموزعين دون الحاجة لوسطاء.
مخاطر الاحتيال	الحد من الاحتيال	تتيح البلوك تشين سجلات غير قابلة للتعديل وتعزز الشفافية، مما يساعد في كشف التلاعب وتقليل الاحتيال.	اعتماد سجل بلوك تشين مركزي لمراجعة حركة المخزون، مما يسهل اكتشاف أي تلاعب في الكميات أو الأسعار.
التعقيدات التنظيمية والتكاليف العالية	تحسين الكفاءة التنظيمية	توفر تقارير دقيقة وسريعة من خلال أتمتة عمليات الامتثال التنظيمي باستخدام العقود الذكية.	استخدام بلوك تشين لأتمتة عمليات المراجعة والتدقيق لتلبية المتطلبات التنظيمية بشكل أسرع وأقل تكلفة.
تدخل الوسطاء في العمليات	تعزيز السيولة وزيادة الشفافية	يقلل البلوك تشين من الحاجة للوسطاء من خلال إتاحة الشفافية التامة بين جميع الأطراف في السوق.	توظيف تقنية بلوك تشين لتسجيل العقود مباشرة بين الشركات والموردين، مما يقلل من الحاجة لجهات ثالثة كوسطاء.

المصدر: من إعداد الباحثين، اعتماداً على: (Hongdan & et al, 2023)

يبين الجدول رقم (01) تطبيقات وفوائد تقنية البلوك تشين في مواجهة التحديات المحاسبية المختلفة. يتناول الجدول أبرز التحديات المحاسبية الحالية مثل الوثائق اليدوية، العمليات التي تستغرق وقتاً طويلاً، صعوبة تتبع المعاملات عبر دفاتر متعددة، مخاطر الاحتيال، التعقيدات التنظيمية والتكاليف العالية، وتدخل الوسطاء في العمليات. كما يعرض محركات القيمة المتعلقة بكل تحدٍ، وفوائد تقنية البلوك تشين في معالجة هذه التحديات، بالإضافة إلى أمثلة عملية على تطبيق هذه التقنية في مجال المحاسبة.

2- مبادئ تكنولوجيا البلوك تشين

في كتاب ثورة البلوك تشين: كيف تعمل التكنولوجيا وراء البيتكوين على تغيير المال والأعمال والعالم، يعرض المؤلفون "المبادئ السبعة لتقنية البلوك تشين" التي تشكل الأسس التي تقوم عليها هذه التكنولوجيا المبتكرة. يتمثل كل مبدأ في ميزة أساسية تساهم في تحقيق قوة البلوك تشين في تحقيق الثقة والشفافية واللامركزية في العديد من المجالات. فيما يلي جدول تفصيلي يبرز هذه المبادئ (Tapscott & Tapscott, 2016):

- ✓ **سلامة الشبكة** (النزاهة متأصلة وغير قابلة للتغيير في الشبكة): البيانات المسجلة في البلوك تشين لا يمكن تغييرها أو تعديلها بعد إدخالها، مما يضمن موثوقية وشفافية عالية.
- ✓ **الطاقة الموزعة** (لا توجد نقاط فشل واحدة): يتم توزيع البيانات على العديد من الأجهزة أو العقد في الشبكة، مما يعزز استقرارها ويقلل من احتمال الفشل المركزي.
- ✓ **القيمة كحافز** (مقارنة أسهل لقيمة المعاملة): يسمح النظام بتقييم المعاملات بسهولة أكبر من خلال استخدام الحوافز المالية، مثل مكافآت المعدنين في شبكة البيتكوين.
- ✓ **الأمن** (الأمن المتأصل): تكنولوجيا البلوك تشين توفر أماناً عالياً من خلال تشفير البيانات والتأكد المتعدد للمعاملات، مما يقلل من فرص الاحتيال والتلاعب.

- ✓ الخصوصية (يتم التحكم في الخصوصية من قبل أصحاب البيانات وليس من قبل الأمناء المركزيين): تتيح البلوك تشين للمستخدمين التحكم الكامل في بياناتهم الخاصة دون الحاجة إلى وسطاء.
 - ✓ الحقوق محفوظة (لا يمكن انتزاع الحقوق): الضمانات المقدمة من البلوك تشين تضمن حقوق الأفراد ولا يمكن لأي جهة أو طرف ثالث انتزاع هذه الحقوق.
 - ✓ الإدماج يمكن للجميع المشاركة: تكنولوجيا البلوك تشين تتيح للجميع فرصة المشاركة في الشبكة، مما يعزز الوصول الشامل والفرص المتساوية لجميع المستخدمين.
- تساهم هذه المبادئ السبعة في تعزيز الوظائف الأساسية لتقنية البلوك تشين، والتي تشمل أمان المعاملات، والشفافية، واللامركزية. أولاً، من خلال ضمان "سلامة الشبكة" و"الأمن المتأصل"، يضمن البلوك تشين أن البيانات لا يمكن تعديلها بعد التوثيق، مما يقلل من المخاطر المتعلقة بالتلاعب أو الاحتيال. كما تسهم "الطاقة الموزعة" في تعزيز استقرار النظام، حيث تعمل الشبكة بشكل لامركزي ولا يوجد نقطة فشل واحدة. من جهة أخرى، يوفر "القيمة كحافز" آلية تحفيزية يمكن قياسها بسهولة من خلال المعاملات على الشبكة. تضمن "الخصوصية" للمستخدمين الحفاظ على سرية بياناتهم، وهو ما يعزز الثقة في النظام. أما "الحقوق محفوظة" فتعكس قدرة الأفراد على الحفاظ على ملكيتهم دون تعرضها للانتزاع. أخيراً، يوفر مبدأ "الإدماج" فرصة للمشاركة للجميع، مما يعزز ديمقراطية الوصول إلى الشبكة.

3- الأمن السيبراني والمخاطر المتعلقة بها

إن تبني المؤسسات لتقنيات التحول الرقيمة رغم المميزات والفوائد التي تجنيها من خلال تطبيق نظم المعلومات الإلكترونية إلا أنه ينبغي للمؤسسة أن تأخذ بعين الاعتبار أن البيانات والمعلومات التي يتم إيرادها على مستوى التطبيقات التكنولوجية، من المحتمل أن تتعرض للعديد من المخاطر التي من شأنها أن تساهم في سرقتها أو تحريفها وهو ما يعرف بالهجمات الإلكترونية، التي تتطلب من المؤسسة إتباع نهج من نظم المعلومات الإدارة التي تساهم في حد من هذه المخاطر، إذ تحتاج المنظمات العامة أو الخاصة إلى خطة استراتيجية ومدروسة للأمن السيبراني لحماية البنية التحتية الحيوية وأنظمة المعلومات للتعامل مع هذه القضايا والامتثال لإطارات الأمن السيبراني الوطنية. عند استخدامه بشكل صحيح، يسمح إطار العمل للأمن السيبراني لقادة أمن تكنولوجيا المعلومات بإدارة تهديدات الإنترنت في شركاتهم بشكل أكثر فعالية. يمكن للشركة استخدام إطار عمل للأمن السيبراني موجود أو إنشاء واحد من الصفر لتلبية متطلباتها الخاصة. (Basholli & et al, 2024, p. 97)

يتطلب الحفاظ على الأمن السيبراني في المنظمات الحديثة إطاراً متماسكاً لتقييم المخاطر يساعد في تصنيفها وفهمها لتحديد أولويات معالجتها. يتضمن هذا التقييم تحديد احتمالية حدوث المخاطر وتأثيرها على المنظمة في حال وقوعها. فيما يلي جدول يُبرز تصنيف المخاطر السيبرانية بناءً على درجة خطورتها، يليه تحليل يوضح أهمية هذه التصنيفات في دعم اتخاذ القرارات الاستراتيجية.

جدول رقم (02): تصنيف المخاطر السيبرانية حسب درجة الخطورة.

درجة المخاطر	الوصف	الإجراء المطلوب
--------------	-------	-----------------

عالية	تشير إلى وجود تهديدات عاجلة قد تؤثر بشكل كبير على العمليات أو الأصول الحيوية للمنظمة.	يتطلب هذا النوع من المخاطر استجابة فورية لتجنب الأضرار الجسيمة، بما في ذلك اتخاذ إجراءات تصحيحية سريعة، مثل تحديث البرمجيات وغيرها...
متوسطة	تهديدات قد تتفاقم مع مرور الوقت إذا لم يتم معالجتها، لكنها لا تشكل تهديدًا مباشرًا.	يجب تنفيذ خطط لتقليل المخاطر ضمن إطار زمني معقول، مثل تحسين التحكم في الوصول أو تحديث البروتوكولات الأمنية، مع تحديد مواعيد نهائية واضحة لهذه الإجراءات.
منخفضة	تهديدات طبيعية أو بسيطة تمثل خطرًا قليلًا ومن غير المحتمل أن تؤثر بشكل كبير على النظام.	في هذه الحالة، يمكن متابعة الوضع عبر مراقبة دورية وتحديثات أمنية بسيطة دون الحاجة إلى تدخل فوري.

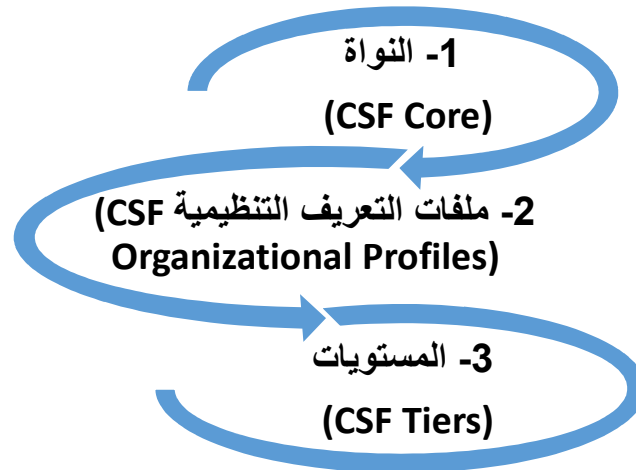
الجدول: من إعداد الباحثين، اعتماداً (Wahhab & et al, 2022, p. 19)

يبيّن الجدول أعلاه أن تصنيف المخاطر السيبرانية يعتمد على شدة التهديد واحتمالية حدوثه. فالمخاطر العالية تشير إلى تهديدات عاجلة قد تؤثر بشكل كبير على الأصول الحيوية للمنظمة، مما يستدعي استجابة فورية واتخاذ إجراءات تصحيحية سريعة. بالمقابل، المخاطر المتوسطة تشير إلى تهديدات قد تتفاقم بمرور الوقت إذا لم يتم معالجتها، لذا يجب وضع خطط لتقليلها ضمن إطار زمني معقول. أما المخاطر المنخفضة، فهي تهديدات غير ملحة تمثل خطرًا بسيطًا، وعليه يتم معالجتها من خلال المتابعة والمراقبة الدورية دون الحاجة إلى تدخلات طارئة.

4- إطار عمل الأمن السيبراني 2.0 (CSF)

إطار عمل الأمن السيبراني (Cybersecurity Framework) هو أداة إرشادية طورها المعهد الوطني للمعايير والتكنولوجيا (NIST) بهدف مساعدة المنظمات على إدارة مخاطر الأمن السيبراني بشكل فعال، ويشمل المكونات التالية:

الشكل رقم (01): مكونات إطار عمل الأمن السيبراني.



المصدر: من إعداد الباحثين، اعتماداً على: (NIST CSWP 29, 2024, p. 1)

يبين الشكل أعلاه الإصدار 2.0 من إطار عمل الأمن السيبراني (CSF) حيث يمثل أداة شاملة لمساعدة المنظمات في إدارة مخاطر الأمن السيبراني. إذ يبرز الشكل أن الإطار يتضمن عدة مكونات أساسية، أبرزها النواة (CSF Core)، التي تقدم تصنيفاً هرمياً للنتائج الرئيسية للأمن السيبراني (NIST CSWP 29, 2024, p. 1)، بدءاً من الوظائف والفئات إلى الفئات الفرعية، مما يوضح كل نتيجة بشكل متكامل. تم تصميم هذه النتائج لتكون سهلة الفهم بالنسبة لمجموعة واسعة من المستخدمين، بما في ذلك التنفيذيين والإداريين والممارسين، بغض النظر عن مستوى خبرتهم. كما يتميز الإطار بالحيادية تجاه القطاعات والدول والتكنولوجيا، مما يتيح مرونة كبيرة للمنظمات لمعالجة التحديات المرتبطة بمخاطرها واحتياجاتها الفريدة.

يشمل الإطار أيضاً ملفات التعريف التنظيمية (Organizational Profiles)، التي توفر آلية لتحديد الوضع الحالي والمستهدف للأمن السيبراني للمنظمة، بالإضافة إلى المستويات (CSF Tiers) التي تقدم أداة لتقييم مدى صرامة ممارسات الحوكمة وإدارة المخاطر (NIST CSWP 29, 2024, p. 1). يهدف إطار العمل إلى وصف النتائج المرغوبة دون فرض أساليب محددة لتحقيقها، مع توفير موارد إضافية عبر الإنترنت لمساعدة المنظمات في تبني وتنفيذ الممارسات والضوابط اللازمة لتحقيق هذه النتائج. بفضل هذه المكونات، يصبح الإطار أداة مرنة تناسب احتياجات المنظمات على اختلاف أحجامها ومستوياتها التقنية.

لتحقيق النجاح في إنشاء إطار عمل فعال للأمن السيبراني، من الضروري اتباع الخطوات التي تم الإشارة إليها في التقرير السابق، والمتضمنة ما يلي (NIST CSWP 29, 2024, pp. 6-7):

✓ **تحديد نطاق الملف التعريفي التنظيمي:** يجب البدء بتوثيق الحقائق والافتراضات الرئيسية التي يستند إليها الملف التعريفي بهدف تحديد نطاقه. يمكن للمنظمة أن تنشئ ملفات تعريفية متعددة، لكل منها نطاق مختلف، مثل التركيز على أمن المنظمة ككل أو على أنظمة مالية محددة، أو حتى مواجهة تهديدات برامج الفدية والتعامل مع الحوادث المتعلقة بها.

✓ **جمع المعلومات الضرورية لإعداد الملف التعريفي التنظيمي:** من بين المعلومات التي يجب جمعها، يمكن أن تشمل السياسات التنظيمية، أولويات إدارة المخاطر والموارد، ملفات تعريف المخاطر المؤسسية، سجلات تحليل الأثر التجاري (BIA)، المتطلبات والمعايير السيبرانية المعتمدة، بالإضافة إلى الممارسات والأدوات المستخدمة مثل الإجراءات الوقائية، وتحديد الأدوار الوظيفية داخل المنظمة.

✓ **إنشاء الملف التعريفي التنظيمي:** يتم تحديد نوع المعلومات اللازمة لتوثيقها في الملف التعريفي لتحقيق الأهداف المستهدفة من مؤشرات النجاح الأساسية (CSF). في هذه المرحلة، ينبغي أخذ تداعيات المخاطر الخاصة بالملف الحالي بعين الاعتبار أثناء التخطيط للملف المستهدف وترتيب أولويات التعديلات المطلوبة. كما يمكن الاستفادة من الملف التعريفي المجتمعي كأساس لتطوير الملف المستهدف.

✓ **تحليل الفجوات بين الملف التعريفي الحالي والمستهدف وإعداد خطة العمل:** من خلال إجراء تحليل دقيق للفجوات بين الملفين الحالي والمستهدف، يتم تحديد الاختلافات وتطوير خطة عمل ذات أولويات لمعالجة تلك الفجوات، مثل إنشاء سجل المخاطر، تقرير تحليل المخاطر، وخطة العمل والمعالج (POA&M).

✓ تنفيذ خطة العمل وتحديث الملف التعريفي التنظيمي: بعد إعداد خطة العمل، يتم تنفيذها لمعالجة الفجوات وتحقيق التقدم نحو الملف التعريفي المستهدف. قد تكون هذه الخطة محددة بموعد نهائي أو قد تكون عملية مستمرة.

ونظراً لأهمية التحسين المستمر، يمكن للمنظمة تكرار هذه الخطوات وفقاً لاحتياجاتها. وتجدر الإشارة إلى أن هناك استخدامات إضافية للملفات التعريفية التنظيمية، مثل استخدامها في التواصل مع الأطراف الخارجية (الشركاء التجاريين أو العملاء المحتملين) لإظهار القدرات السيبرانية للمنظمة وفرص التحسين المتاحة.

5- الدراسات السابقة

من بين أهم الدراسات التي تناول إحدى متغيرات الدراسة ما يلي:

✓ تناولت دراسة "مماريات البرمجيات للبيانات الضخمة: مراجعة منهجية للدراسات السابقة" أهمية تصميم مماريات برمجية مناسبة لأنظمة البيانات الضخمة لتحقيق المتطلبات الوظيفية والجودة المطلوبة. أشارت الدراسة إلى أن أنظمة البيانات الضخمة تتكون عادةً من مكونات رئيسية مثل استخراج المعلومات، المعالجة الأولية، معالجة البيانات، التكامل، التحليل، والتصور. ومع اختلاف احتياجات الأنظمة، تختلف التكوينات التصميمية لمماريات البرمجيات. وبالرغم من أن العديد من القضايا المتعلقة بأنظمة البيانات الضخمة تم تناولها في الأبحاث السابقة، إلا أن مفهوم المماريات البرمجية لهذه الأنظمة لم يتم بحثه بشكل كافٍ. اعتمدت الدراسة منهجية مراجعة منهجية للأدبيات من خلال عملية اختيار متعددة المراحل للمصادر العلمية، مما يوفر إطاراً تحليلياً لفهم اهتمامات الأطراف المعنية وجودة الأنظمة في مجال البيانات الضخمة (Avci & et al, 2020).

✓ في دراستهم بعنوان "تدقيق مخاطر الأمن السيبراني في ضوء عصر المعلومات وتأثيره على استمرارية الشركات"، تناول أسعد محمد علي وهاب وآخرون دور المدقق الخارجي في تدقيق مخاطر الأمن السيبراني وحجم المخاطر التي تتعرض لها الشركات العراقية. وقد هدفت الدراسة إلى تحديد إجراءات المدققين الخارجيين والمكاتب التدقيقية العراقية في تدقيق هذه المخاطر وملاءمتها، بالإضافة إلى دراسة تأثير هذه المخاطر على استمرارية الشركات العراقية. تم توزيع 85 استبياناً على عينة من المدققين الخارجيين ذوي الخبرة في تدقيق الأنظمة الحاسوبية الإلكترونية في العراق، وتم استرداد 77 استبياناً صالحاً للتحليل باستخدام برنامج SPSS الإحصائي. أظهرت النتائج أن هناك تطوراً نسبياً في استخدام الأنظمة الحاسوبية والإدارية الإلكترونية من قبل الشركات العراقية المساهمة، وأن هناك تأثيراً واضحاً على استمرارية الشركات نتيجة لمخاطر الأمن السيبراني التي يصعب تجنبها، بالإضافة إلى نقص الخبرة الكافية لدى العديد من فرق العمل في مكاتب التدقيق لتدقيق هذه المخاطر (Wahhab & et al, 2022).

✓ في دراستهم المنشورة بعنوان "الذكاء الاصطناعي للأمن السيبراني في الأنظمة والحواسيب الشبكية"، استعرض محمد حسن حديا وأسماء علي جاسم مجموعة شاملة من التقنيات المستخدمة في الذكاء الاصطناعي لمواجهة تحديات الأمن السيبراني، بما في ذلك التعلم الآلي والتعلم العميق. تتناول الدراسة الطريقة التي يمكن للذكاء الاصطناعي تحسين الأنظمة الأمنية من خلال جعلها أكثر استباقية وذكاءً في تحديد التهديدات ومعالجتها، فضلاً عن تبسيط عمليات الأمان من خلال أتمتة العمليات المتكررة لتوفير الوقت. أجريت مقابلات مع موظفي شركة تأمين متخصصة في مراقبة الشبكات وأمنها لتحديد التحديات المحددة التي تواجههم

في أداء مهامهم. أظهرت الدراسة مدى فعالية الذكاء الاصطناعي في تحسين الأمن السيبراني وقدرته على تعزيز استراتيجيات الكشف والتصدي للتهديدات بطريقة أكثر فعالية (Hadia & Jasimb, 2024).

✓ في دراسة أجراها غورجي وآخرون (2024) تحت عنوان "التحول الرقمي المدعوم بالبلوك تشين: مراجعة منهجية للأدبيات"، أشار الباحثون إلى أن التحول الرقمي أصبح توجهاً حتمياً يؤثر على كافة القطاعات، وأن البلوك تشين يعد من التقنيات الأساسية الداعمة لهذا التحول إلى جانب التقنيات الناشئة الأخرى. هدفت الدراسة إلى تقديم مراجعة منهجية للأدبيات لاستكشاف كيفية تمكين البلوك تشين للتحول الرقمي، حيث قام الباحثون بتحليل 41 مقالاً لتقييم الوضع الحالي للتكنولوجيا، وتحديد الفجوات البحثية، وتوضيح أجندات البحث المستقبلية. خلصت الدراسة إلى أن البلوك تشين يمتلك إمكانيات واعدة توفر فرصاً واسعة للشركات، إلا أن المقالات التي تم تحليلها كشفت عن وجود تحديات وعوائق، بالإضافة إلى الفوائد المحتملة للتقنية في سياق التحول الرقمي. كما تم تطوير إطار نظري يساعد في توضيح دور البلوك تشين في تمكين التحول الرقمي، مع إبراز القضايا المفتوحة التي تحتاج إلى معالجة في الأبحاث المستقبلية لتجاوز التحديات المتعلقة بتبني هذه التقنية (Gurzhii & et al, 2024).

6- مميزات الدراسة الحالية عن الدراسات السابقة

شهدت الأبحاث السابقة تطوراً ملحوظاً في دراسة الجوانب المتعلقة بنظم المعلومات الحاسوبية، الأمن السيبراني، وتقنيات التحول الرقمي مثل البلوك تشين. وعلى الرغم من ذلك، فإن معظم هذه الدراسات ركزت على جوانب منفصلة دون تقديم حلول متكاملة تربط بين الأمن السيبراني، إدارة المخاطر، وتقنيات المعلومات الحاسوبية وفق معايير دولية معترف بها. من هنا، تأتي أهمية الدراسة الحالية التي تسعى إلى سد هذه الفجوة البحثية من خلال تقديم نموذج معياري شامل يجمع بين معايير ISO 27032 و ISO 31000 في إطار تبني تقنية البلوك تشين، فيما يلي مميزات الدراسة الحالية مقارنة بالدراسات السابقة:

✓ بينما ركزت الدراسات السابقة على جوانب منفصلة مثل معمارية البرمجيات (Avci et al., 2020) أو تدقيق مخاطر الأمن السيبراني (Wahhab et al., 2022)، تجمع الدراسة الحالية بين إعادة هندسة نظم المعلومات الحاسوبية وتطبيق معايير ISO 27032 (لحماية الأمن السيبراني) و ISO 31000 (لإدارة المخاطر)، مما يحقق نموذجاً متكاملاً وشاملاً لتطبيق التقنية.

✓ بخلاف الدراسات مثل دراسة (Hadia & Jasimb, 2024) التي تناولت الذكاء الاصطناعي للأمن السيبراني، تتفرد الدراسة الحالية بتركيزها على استخدام تقنية البلوك تشين لتحسين الأمن السيبراني وإدارة المخاطر في نظم المعلومات الحاسوبية، مما يضيف بُعداً عملياً غير مسبق في الأبحاث السابقة.

✓ الدراسات السابقة مثل (Wahhab et al., 2022) ركزت على الأمن السيبراني وتأثيره على استمرارية الشركات بشكل عام، بينما تضيف الدراسة الحالية قيمة من خلال تحليل تأثير الأمن السيبراني في السياق المحاسبي، مما يساعد المؤسسات على تحسين موثوقية بياناتها المحاسبية.

✓ على عكس دراسة (Gurzhii et al., 2024) التي ركزت على مراجعة الأدبيات لتوضيح دور البلوك تشين في التحول الرقمي، تقدم الدراسة الحالية نموذجاً معيارياً تطبيقياً يمكن للمؤسسات استخدامه بشكل عملي لتلبية معايير الأمن السيبراني وإدارة المخاطر.

✓ الدراسة الحالية لا تقتصر على مراجعة الأدبيات فقط كما في دراسة (Avci et al., 2020) ، بل تتبنى نهجًا معياريًا تحليليًا يربط بين الحلول التقنية (البلوك تشين) والمعايير الدولية (ISO) لتقديم توصيات عملية تخدم المؤسسات. الدراسة الحالية تتفوق من حيث التكامل والمنهجية المعيارية، مما يجعلها مرجعًا هامًا في معالجة الأمن السيبراني وإدارة المخاطر ضمن نظم المعلومات الحاسوبية باستخدام تقنية البلوك تشين.

III. المحور الثاني: الامتثال لمتطلبات معايير ISO 27032 و ISO 31000 كطريق نحو تعزيز نظم المعلومات الحاسوبية المدعومة بتقنيات بلوك تشين

1- إطار تطبيق نظام إدارة الأمن السيبراني وفقًا لمتطلبات معيار الآيزو 27032

ISO 27032 هو مواصفة تقدم إرشادات لتحسين الأمن السيبراني في المنظمات من خلال إطار عمل يعتمد على إدارة المخاطر. تغطي هذه المواصفة عدة مجالات مهمة، أبرزها أمان المعلومات، أمان الشبكة، أمان الإنترنت، حماية البنى التحتية للمعلومات، وإدارة الأمن السيبراني. تم تطوير ISO 27032 لأول مرة في يوليو 2012، وذلك في ظل تزايد الجرائم السيبرانية بين عامي 2000 و2012. فيما يخص الأمن السيبراني والفضاء السيبراني، فإن الفضاء السيبراني يشير إلى البيئة المعقدة الناتجة عن تفاعل الأفراد والخدمات عبر الإنترنت، بينما يشمل الأمن السيبراني كافة الإجراءات الأمنية التي تهدف إلى حماية هذا الفضاء. (ISO/IEC 27032، 2023)

إن إطار نظام إدارة الأمن السيبراني يتكون من أربعة مجالات رئيسية وفق ما نص عليه المعيار حيث تهدف إلى تعزيز حماية الأنظمة والمعلومات. يشمل المجال الأول "المنع"، الذي يركز على تقليل آثار أحداث الأمن السيبراني. يليه "الحماية والكشف"، الذي يتضمن تطبيق الضوابط لمراقبة الأحداث الأمنية. أما "الاستجابة والتواصل"، فيتعلق بإجراءات تخفيف الاختراقات حال حدوثها، بينما يعني "التعافي والتعلم" باستعادة الأنظمة والخدمات بعد أي تهديد. (ISO/IEC 27032، 2023)

يعد بناء نظام إدارة الأمن السيبراني عملية متكاملة تهدف إلى حماية المنظمة من التهديدات الرقمية المتزايدة التي قد تؤثر على بنيتها التحتية وبياناتها. تعتمد هذه العملية على منهجية منهجية تتضمن مجموعة من الخطوات التي تضمن تحليل المخاطر، وضع الاستراتيجيات، وتنفيذ التدابير الوقائية لضمان استمرارية العمل وحماية الأنظمة. في هذا السياق، يوضح الجدول أدناه المراحل الأربع الرئيسية لهذه المنهجية وما يتضمنه كل منها.

عنوان الجدول (03): المراحل الرئيسية لبناء نظام إدارة الأمن السيبراني

المرحلة	الوصف	الأنشطة الرئيسية
فهم المنظمة	تهدف هذه المرحلة إلى فهم شامل لبيئة العمل والعمليات التنظيمية، بما في ذلك البنية التحتية، السياسات، والبرمجيات، من أجل تأسيس قاعدة بيانات شاملة حول الحالة الراهنة للأمن السيبراني.	✓ مراجعة العمليات والوظائف (الهياكل التنظيمية، الأوصاف الوظيفية). ✓ فحص مراكز البيانات وغرف الحاسوب والأجهزة. ✓ مراجعة السياسات والإجراءات الأمنية. ✓ التحقق من الامتثال للمعايير الدولية (ISO 27001). ✓ جمع الوثائق المرتبطة بالأمن السيبراني.

✓ تحديد التهديدات (طبيعية، تقنية، بشرية). ✓ تقييم نقاط الضعف الداخلية والخارجية. ✓ تقدير احتمالية وتأثير التهديدات. ✓ تطوير استراتيجيات للحد من المخاطر (التجنب، القبول، السيطرة). ✓ وضع أولوية للأنشطة ذات الأهمية العالية.	تقييم المخاطر التي قد تواجه المنظمة، بما في ذلك التهديدات الطبيعية، التقنية، والبشرية، مع التركيز على تحديد نقاط الضعف وتأثيرها المحتمل لتطوير خطة للتعامل مع المخاطر.	تحليل المخاطر
✓ صياغة سياسات الأمن السيبراني. ✓ تحديد الضوابط التقنية والإدارية. ✓ تحسين البنية التحتية للأمن السيبراني (UPS، التبريد، الأنظمة). ✓ تطوير حلول لضمان استمرارية الأعمال والتعافي من الكوارث. ✓ تقديم توصيات لتحسين التقنيات والعمليات.	وضع خطة استراتيجية شاملة لتعزيز الأمن السيبراني بناءً على تحليل المخاطر، مع تحديد الأدوار والمسؤوليات والإجراءات التقنية الواجب اتخاذها لتحقيق أهداف الأمان.	تخطيط الأمن السيبراني
✓ تنفيذ السياسات الأمنية المقررة. ✓ إعداد أنظمة كشف التهديدات ومراقبة الشبكات. ✓ تحديث البرمجيات ونظم الحماية بشكل دوري. ✓ تدريب الموظفين على إجراءات الأمن السيبراني. ✓ إجراء مراجعات دورية للتأكد من فعالية النظام. ✓ تطبيق أدوات منع التصيد والهجمات الإلكترونية وتقييم آليات الوقاية.	تطبيق الخطة الأمنية عبر تنفيذ التدابير التقنية والتنظيمية مع التركيز على الوقاية والتوعية والمراقبة المستمرة، لضمان الامتثال وتحقيق الأمان.	التنفيذ

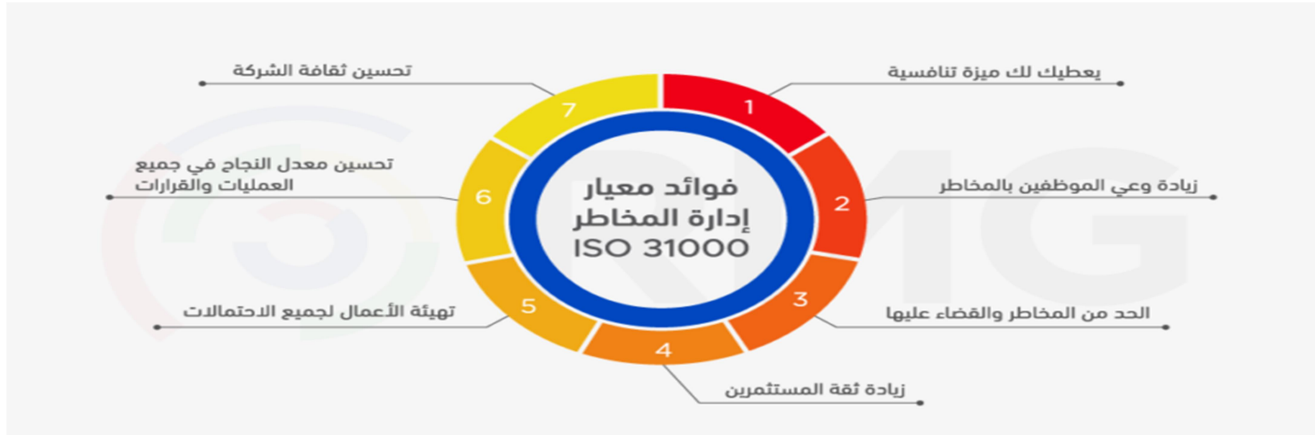
المصدر: من إعداد الباحثين، اعتماداً على: (ISO/IEC 27032, 2023)

يتضح من الجدول أن المراحل الأربع تمثل الركائز الأساسية لنظام إدارة الأمن السيبراني الفعال، حيث تُسهم في تحقيق توازن بين تقييم الوضع الحالي وتنفيذ الحلول المناسبة. تبدأ العملية بفهم المنظمة من خلال تحليل البنية التحتية والإجراءات التنظيمية، مما يضع الأساس لوضع استراتيجية أمنية ملائمة. يلي ذلك تحليل المخاطر لتحديد التهديدات ونقاط الضعف التي يمكن أن تؤثر على عمليات المنظمة، مما يمكن من ترتيب أولويات الحماية. تُترجم هذه النتائج إلى خطة استراتيجية شاملة في مرحلة التخطيط، تتضمن تطوير سياسات وتعزيز البنية الأمنية. وأخيراً، يتم تنفيذ التدابير الأمنية مع التركيز على المراقبة المستمرة وتحسين آليات الوقاية، مما يوفر للمنظمات نهجاً مرناً لتعزيز أمنها السيبراني وضمان استدامة أنشطتها.

2- إطار إدارة نظم المخاطر وفقاً لمتطلبات معيار الآيزو 31000.

ISO 31000 هو معيار دولي لإدارة المخاطر تم تطويره من قبل منظمة المعايير الدولية للجودة (ISO) في عام 2009، حيث تم إصدار أحدث نسخة منه في 2018 تحت مسمى (ISO 31000:2018). يحدد هذا المعيار مجموعة من المبادئ التوجيهية والعمليات التي يجب على المنظمات والشركات اتباعها لتحديد المخاطر، إدارتها، ومعالجتها. كما يشمل تقييم المخاطر من حيث حجم تأثيرها وتحديد الاستراتيجيات اللازمة لإدارتها ومراقبة المخاطر المحتملة. يهدف هذا المعيار إلى تحقيق أهداف المؤسسة والإدارة العليا، مع ضمان استمرارية العمل وتجنب الأحداث المفاجئة التي قد تعطل العمليات (ISO 31000, 2018). كما أن تطبيق متطلبات المعيار تسهم في توفير مجموعة من المميزات، يمكنك إظهارها من خلال الشكل التالي:

الشكل (02): فوائد معيار إدارة المخاطر ISO31000



المصدر: (RMG, 2024)

من خلال الشكل أعلاه يتبين أن تطبيق معيار ISO 31000 لإدارة المخاطر يوفر العديد من الفوائد التي تساهم في تحسين الأداء العام للمنشآت. فهو يعزز من قدرتك التنافسية في السوق بفضل اعترافه الدولي الذي يزيد من ثقة العملاء، كما يساهم في زيادة وعي الموظفين وتثقيفهم حول المخاطر المحتملة، مما يساعد في الحد من هذه المخاطر أو القضاء عليها. كذلك، يعزز النظام من شفافية تقارير المخاطر، مما يزيد من ثقة المستثمرين ويساهم في تحسين ثقافة التعاون بين الإدارات المختلفة داخل المؤسسة. كما يُحسن معدل نجاح العمليات والقرارات عبر اتباع نهج استباقي في التفكير، ويُعد المنشأة لتوقع أسوأ السيناريوهات والتعامل معها بفعالية، مما يؤدي إلى الاستفادة القصوى من الموارد والفرص المتاحة.

حدد معيار ISO 31000 مجموعة من المبادئ والمراحل التي تمكن المنشآت من تحديد المخاطر وتحليلها والتعامل معها بشكل يضمن تحقيق أهدافها وتقليل الآثار السلبية لتلك المخاطر. في الجدول التالي، سيتم توضيح المراحل الرئيسية لإطار إدارة المخاطر وفقاً للمعيار ISO 31000 مع أهداف كل مرحلة من مراحل تطبيقه في المؤسسات.

الجدول رقم (05): مراحل وأهداف إطار إدارة المخاطر وفقاً للمعيار ISO 31000

الهدف/الشرح	الجال
- مواءمة إدارة المخاطر مع أهداف المنشأة وثقافتها. - إصدار سياسات واضحة بشأن نهج إدارة المخاطر.	القيادة والالتزام

التكامل (الإنسجام)	- تحديد أدوار ومسؤوليات الإدارة التنظيمية. - التأكد من أن إدارة المخاطر جزء متكامل من جميع أقسام المنشأة. - فهم المنشأة وسياقها (الداخلي والخارجي). - تخصيص الموارد اللازمة لإدارة المخاطر. - وضع بروتوكولات وآلية تواصل بين الجهات المعنية.
التنفيذ	- تحديد الأهداف والمواعيد النهائية. - تحديد عملية صنع القرار بوضوح. - تقييم عملية صنع القرار وإجراء التعديلات حسب الحاجة.
التقييم	- مراجعة الأعمال المنجزة ضمن نظام إدارة المخاطر. - تقييم الأداء مقارنة بالأهداف المطلوبة. - إجراء تحليل الفجوات لتحديد أي تحسينات ضرورية.
التحسين المستمر	- الرصد المستمر لجميع جوانب إطار إدارة المخاطر. - معالجة التغيرات الداخلية والخارجية. - التخطيط واتخاذ الإجراءات لتحسين النظام بشكل دوري.

المصدر: من إعداد الباحثين، اعتماداً على: (ISO 31000, 2018)

من خلال الجدول يتبين أن إطار إدارة المخاطر ISO 31000 يقدم نهجاً شاملاً ومرناً يساعد المؤسسات على تحديد المخاطر، وتقييمها، وإدارتها بشكل استباقي. من خلال الالتزام بالقيم القيادية وتطبيق الأنظمة المتكاملة عبر كافة أقسام المنشأة، يعزز هذا المعيار التوافق بين الأهداف الاستراتيجية والعمليات اليومية. كما أن تخصيص الموارد بشكل فعال ووضع سياسات واضحة يساهم في تعزيز قدرات المؤسسة على التكيف مع المخاطر. يعد التخطيط والتنفيذ المستمرين في إطار النظام أساسياً لتحقيق استدامة الأعمال في بيئة ديناميكية. من خلال المراجعة المستمرة والتحسين، يمكن للمؤسسات تطوير أدائها بما يتماشى مع التغيرات الداخلية والخارجية، مما يعزز قدرتها على مواجهة التحديات المستقبلية.

3- التكامل بين المعايير الدولية ISO 31000 و ISO/IEC 27032 لتعزيز تطبيقات البلوكشين في الحاسبة

تعتبر تقنية البلوكشين من بين أهم الابتكارات الحديثة التي أثرت في مجال الحاسبة، حيث ساعدت في تحسين أمان وسلامة البيانات المالية وتقليل مخاطر التلاعب. ومع ذلك، فإن تطبيق البلوكشين في الحاسبة يواجه مجموعة من التحديات، بما في ذلك المخاطر المالية، التقنية، والتنظيمية. يهدف الجدول أدناه إلى توضيح كيفية توظيف المعيارين الدوليين ISO 31000 (إدارة المخاطر) و ISO/IEC 27032 (الأمن السيبراني) في معالجة هذه التحديات، من خلال توفير إطار عمل متكامل لإدارة المخاطر وتعزيز الأمن السيبراني لأنظمة الحاسبة المعتمدة على البلوكشين.

الجدول رقم (06): دور المعيارين ISO 31000 و ISO/IEC 27032 في تعزيز كفاءة وأمان تطبيقات البلوكشين الحاسوبية.

المعيار الدولي	المفاهيم الأساسية	تطبيق البلوكشين في المحاسبة
ISO 31000 (إدارة المخاطر)	تحديد المخاطر: تحديد المخاطر مثل الاحتيال المالي، القضايا التنظيمية، وعدم الكفاءة التشغيلية في تبني تقنية البلوكشين في المحاسبة.	يجب مراقبة أنظمة البلوكشين في المحاسبة لاكتشاف مخاطر مثل المعاملات الاحتيالية، العقود الذكية التي تحتوي على أخطاء، والتناقضات في التقارير المالية.
	تقييم المخاطر: تقييم احتمالية وتأثير المخاطر على أنظمة المحاسبة المعتمدة على البلوكشين.	تحتاج معاملات البلوكشين في المحاسبة إلى تحليل المخاطر مثل التقارير المالية غير الدقيقة وانتهاكات الامتثال نتيجة ثغرات النظام.
	معالجة المخاطر: الحد من المخاطر من خلال تنفيذ ضوابط مثل سجلات التدقيق، التحكم في الوصول، والتحقق من المعاملات.	معالجة المخاطر في تطبيقات البلوكشين المحاسبية من خلال تدقيق العقود الذكية، استخدام محافظ متعددة التوقيع، وأنظمة زائدة لضمان سلامة البيانات المالية.
	المراقبة والمراجعة: مراجعة مستمرة لأنظمة المحاسبة المعتمدة على البلوكشين لتحديد مخاطر جديدة أو التخفيف من الثغرات القائمة.	تحتاج أنظمة البلوكشين إلى مراقبة دائمة لضمان موثوقية المعاملات المالية والكشف المبكر عن الاختراقات السيبرانية التي تؤثر على البيانات المالية.
ISO/IEC 27032 (الأمن السيبراني)	أمن الاتصال: حماية سرية وسلامة البيانات المتبادلة داخل شبكة البلوكشين.	يجب على شبكات البلوكشين التي تتعامل مع المعاملات المحاسبية استخدام تشفير البيانات لحماية خصوصية ودقة البيانات المالية.
	تهديدات الأمن السيبراني: تحديد الهجمات السيبرانية المحتملة، مثل التصيد، والتلاعب بالبيانات، أو ثغرات العقود الذكية.	أنظمة المحاسبة القائمة على البلوكشين معرضة لتهديدات مثل التلاعب بالمعاملات والهجمات السيبرانية التي تهدد سلامة البيانات المالية.
	التحكم في الوصول: ضمان أن الوصول إلى البيانات المالية الحساسة يقتصر فقط على المستخدمين المصرح لهم.	استخدام التحقق متعدد العوامل (MFA) والتحكم في الوصول المستند إلى الأدوار (RBAC) لتقييد الوصول غير المصرح به إلى سجلات المعاملات المالية على أنظمة البلوكشين.
	الاستجابة للحوادث: تطوير استراتيجيات لمعالجة الحوادث الأمنية والانتهاكات التي تؤثر على بيانات المحاسبة في البلوكشين.	في حالة وقوع حوادث سيبرانية، يجب أن تكون لدى أنظمة البلوكشين المستخدمة في المحاسبة إجراءات واضحة لاسترداد المفاتيح واستعادة النظام.

المصدر: من إعداد الباحثين، اعتماداً على (ISO 31000, 2018) و (ISO/IEC 27032, 2023)

يبين الجدول أعلاه كيف تساهم المعايير الدولية ISO 31000 و ISO/IEC 27032 في تعزيز استخدام تقنية البلوكشين في المحاسبة من خلال تقديم إطار متكامل لإدارة المخاطر والأمن السيبراني. يوضح المعيار ISO 31000 آليات تحديد وتقييم ومعالجة المخاطر المرتبطة باستخدام البلوكشين، مثل المخاطر التشغيلية والاحتيال المالي، مع التركيز على المراقبة المستمرة لضمان سلامة البيانات المالية. من ناحية أخرى، يقدم المعيار ISO/IEC 27032 حلولاً عملية لتعزيز أمان الاتصال والتحكم في الوصول والتصدي

للهجمات السيبرانية، مما يضمن حماية البيانات المالية الحساسة على شبكات البلوكشين. من خلال الدمج بين المعيارين، يمكن بناء أنظمة محاسبية قائمة على البلوكشين تتسم بالشفافية، الموثوقية، والأمان، مما يعزز الامتثال التنظيمي ويقلل من المخاطر المالية والتشغيلية.

4- إطار تكاملي لإدارة المخاطر والأمن السيبراني في المحاسبة المعتمدة على تقنية البلوكشين

تمثل تقنية البلوكشين نقلة نوعية في مجال المحاسبة من خلال تعزيز الشفافية وتوفير سجلات غير قابلة للتغيير للمعاملات المالية. ومع ذلك، فإن اعتمادها يترافق مع تحديات كبيرة تتعلق بإدارة المخاطر وضمان الأمن السيبراني. يتيح المعياران ISO 31000 و ISO/IEC 27032 إطاراً متكاملًا للتعامل مع هذه التحديات، حيث يركز الأول على تحليل المخاطر وإدارتها، بينما يعالج الثاني الجوانب المتعلقة بالأمن السيبراني. يهدف الجدول أدناه إلى توضيح كيفية تطبيق هذين المعيارين بشكل تكاملي لتعزيز كفاءة وأمان أنظمة المحاسبة المبنية على البلوكشين.

الجدول رقم (07): التكامل بين ISO 31000 و ISO/IEC 27032 في إدارة مخاطر وأمن أنظمة المحاسبة القائمة على البلوكشين

مجال العمل	إطار ISO 31000	ممارسات الأمن السيبراني وفق ISO/IEC 27032	التطبيق المشترك في محاسبة البلوكشين
تحديد المخاطر	تحديد مخاطر المحاسبة المتعلقة بالبلوكشين مثل أخطاء التقارير المالية، الاحتيال، أو عدم الامتثال التنظيمي.	تحديد مخاطر الأمن السيبراني مثل الوصول غير المصرح به، فقدان المفاتيح الخاصة، أو التلاعب بسجلات المعاملات.	يشمل تحديد المخاطر فهم كيفية تعرض تقنية البلوكشين في المحاسبة للهجمات السيبرانية التي تتلاعب بالبيانات المالية أو فشل أنظمة إدارة المفاتيح التي تؤثر على أمان المعاملات.
تقييم المخاطر	تقييم الخسائر المالية المحتملة، والغرامات التنظيمية، والاضطرابات التشغيلية الناتجة عن مخاطر البلوكشين.	تقييم تأثير الانتهاكات السيبرانية مثل الاختراقات أو الثغرات في العقود الذكية التي قد تؤثر على سلامة البيانات المالية.	يساعد التكامل بين المعيارين ISO 31000 و ISO/IEC 27032 في تقييم احتمالية حدوث خسائر مالية أو انتهاكات تنظيمية نتيجة ثغرات البلوكشين وضعف الأمن السيبراني.
معالجة المخاطر	تنفيذ تدابير مضادة مثل سجلات التدقيق، أنظمة التحقق المزدوجة، وتحديث العقود الذكية.	استخدام أدوات الأمن السيبراني مثل تشفير البيانات، التحقق متعدد التوقيع، وبروتوكولات المعاملات الآمنة لتقليل المخاطر.	تستفيد تطبيقات المحاسبة القائمة على البلوكشين من منهجية ISO 31000 العامة للتخفيف من المخاطر (مثل الأنظمة الزائدة) واعتماد تدابير ISO/IEC 27032 المحددة لضمان سلامة البيانات والمعاملات.
إدارة الحوادث	تطوير إجراءات لإدارة إخفاقات البلوكشين الحاسوبية مثل أخطاء المعاملات أو تناقضات التدقيق.	تنفيذ بروتوكولات الاستجابة للحوادث للتعامل مع الهجمات السيبرانية، تعطيل الشبكات، أو إخفاقات استرداد المفاتيح في أنظمة البلوكشين.	يجمع إدارة الحوادث بين التركيز على الاسترداد المالي وفق ISO 31000 واستعادة النظام بعد الانتهاكات السيبرانية وفق ISO/IEC 27032 للحفاظ على استمرارية الأعمال في الأنظمة المحاسبية.

المصدر: من إعداد الباحثين، اعتماد على (ISO 31000, 2018) و (ISO/IEC 27032, 2023) و (Tapscott &

Tapscott, 2016)

يبين الجدول أعلاه كيفية التكامل بين المعيارين ISO 31000 و ISO/IEC 27032 لتوفير إطار شامل يعالج التحديات المتعلقة بالمخاطر والأمن السيبراني في أنظمة المحاسبة المعتمدة على البلوكشين. يعمل المعيار ISO 31000 على تحديد وتقييم ومعالجة المخاطر المحاسبية مثل الاحتيال والأخطاء التنظيمية، بينما يركز ISO/IEC 27032 على حماية أنظمة البلوكشين من التهديدات السيبرانية مثل الاختراقات والتلاعب بالبيانات. يعزز الجمع بين المعيارين فعالية إدارة المخاطر من خلال تطبيق تدابير وقائية مثل التشفير، وسجلات التدقيق، وإجراءات الاستجابة للحوادث، مما يضمن استمرارية العمليات المحاسبية وسلامة البيانات المالية. هذا التكامل يسهم بشكل كبير في تعزيز الثقة في أنظمة المحاسبة الحديثة و يتيح لها مواجهة التحديات الرقمية بكفاءة.

IV. خاتمة

تُمثل إعادة هندسة نظم المعلومات المحاسبية بالاعتماد على تقنية البلوك تشين إطارًا مبتكرًا لمواجهة التحديات المرتبطة بالأمن السيبراني وإدارة المخاطر المؤسسية، في ظل التسارع الملحوظ للتطورات التكنولوجية الرقمية. وقد سعت هذه الدراسة إلى بلورة نموذج معياري متكامل يجمع بين معيار ISO 27032 الخاص بالأمن السيبراني ومعيار ISO 31000 المتعلق بإدارة المخاطر، بما يتيح رؤية شاملة لضمان أمان وكفاءة نظم المعلومات المحاسبية. في هذا السياق، تناول المحور الأول الإطارين المفاهيمي والتطبيقي للدراسة، حيث تم تقديم تعريف دقيق لتقنية البلوك تشين وخصائصها الجوهرية، وبيان دورها في دعم نظم المعلومات المحاسبية من خلال تعزيز الشفافية والمصادقية وحماية البيانات من أي تلاعب محتمل. كما تم استعراض أهم الدراسات السابقة التي كشفت عن مواطن القوة والقصور في النظم التقليدية، مع تسليط الضوء على التحديات الأمنية والمخاطر التي تواجه المؤسسات في بيئة التحول الرقمي.

أما المحور الثاني، فقد ركّز على دراسة متطلبات ومعيار ISO 27032 الخاصة بالأمن السيبراني، ومعيار ISO 31000 المتعلق بإدارة المخاطر، مع تحليل سبل دمجهما في بيئة البلوك تشين لبناء نظم معلومات محاسبية أكثر أمانًا ومرونة. كما تم إبراز أوجه التكامل بين هذين المعيارين، والتأكيد على أهمية الامتثال لهما لتحقيق الكفاءة التشغيلية وتقليل المخاطر المؤسسية.

استنادًا إلى ما توصلت إليه الدراسة، يمكن القول إن النتائج قد أكدت صحة فرضيات البحث الثلاث؛ إذ بينت أن دمج تقنية البلوك تشين مع معيار ISO 27032 يسهم بشكل فعال في تعزيز مستوى الأمن السيبراني، من خلال رفع قدرة النظم المحاسبية على حماية البيانات وضمان سلامة المعاملات المالية. كما أظهر التحليل أن تطبيق معايير ISO 31000 ضمن بيئة البلوك تشين يوفر إطارًا منهجيًا واضحًا لتحديد المخاطر وتقييمها والحد من آثارها، الأمر الذي يعزز قدرة المؤسسات على مواجهة التحديات الرقمية المتزايدة. وأخيرًا، أوضحت النتائج أن الدمج المعياري بين البلوك تشين ومعيار ISO 27032 و ISO 31000 يحقق تكاملًا فعالًا بين متطلبات الأمن السيبراني وآليات إدارة المخاطر، بما يعكس إيجابًا على جودة نظم المعلومات المحاسبية وكفاءتها التشغيلية. بناءً على ما سبق يمكن حصر نتائج الدراسة فيما يلي:

✓ إن توظيف ممارسات الأمن السيبراني وفق معيار ISO 27032 يساهم بشكل فعال في حماية البيانات المالية الحساسة ضمن أنظمة البلوكشين، من خلال تأمين الاتصال بين الأطراف، وضبط الوصول إلى المعلومات عبر آليات تحقق متعددة العوامل، إضافة إلى وضع استراتيجيات استجابة سريعة للحوادث الأمنية. هذا التطبيق يقلل من احتمالية التلاعب بالمعاملات أو سرقة البيانات، ويعزز من ثقة المستخدمين والمستثمرين في هذه النظم.

✓ تطبيق المعيار الدولي ISO 31000 في بيئة البلوكشين الحاسوبية يوفر آلية منهجية لتحديد المخاطر المحتملة، مثل الاحتيال المالي أو الإخفاقات التشغيلية أو التعارض مع المتطلبات التنظيمية، ثم تقييم احتمالية حدوثها وتأثيرها، وأخيراً وضع إجراءات وقائية وعلاجية مثل التدقيق المستمر، وأنظمة التحقق المزدوج، وتحديث العقود الذكية. هذا الإطار يرفع من قدرة المؤسسات على التنبؤ بالمخاطر والحد منها قبل أن تؤثر على سلامة التقارير المالية.

✓ الدمج بين المعيارين ISO 31000 و ISO/IEC 27032 يشكل إطاراً تكاملياً لمعالجة التحديات المعقدة التي تواجه أنظمة الحاسبة المعتمدة على البلوكشين، إذ يسمح هذا التكامل بمواجهة المخاطر من منظور مزدوج؛ الأول يركز على الجانب الاستراتيجي لإدارة المخاطر، والثاني يركز على التدابير التقنية لحماية البيانات من التهديدات السيبرانية. وقد أثبتت النتائج أن هذا التكامل يساهم في استمرارية العمليات، ويحسن من جودة البيانات المالية، ويعزز الامتثال التنظيمي.

✓ إن الجمع بين تقنيات البلوكشين والمعايير الدولية المدروسة يعزز من شفافية العمليات الحاسوبية عبر توفير سجلات غير قابلة للتعديل للمعاملات، مما يحد من فرص الاحتيال ويوفر مرجعية دقيقة وموثوقة لمراجعي الحسابات والهيئات الرقابية، وهو ما يرفع من مصداقية التقارير المالية ويقوي سمعة المؤسسة أمام الأطراف المعنية.

بناءً على النتائج المتوصل إليها، تقترح الدراسة جملة من التوصيات على النحو الآتي:

✓ ضرورة إدماج معايير ISO 27032 و ISO 31000 ضمن التخطيط الاستراتيجي للمؤسسات، لضمان استدامة نظم المعلومات الحاسوبية.

✓ الاستثمار في برامج تدريبية وتوعوية لرفع كفاءة الموارد البشرية في التعامل مع النظم المدججة بين البلوك تشين ومعايير الأيزو.

✓ إجراء تقييمات دورية لمستوى الأمان وإدارة المخاطر في النظم الحاسوبية للتأكد من مواكبتها للتطورات التقنية.

✓ تشجيع البحوث التطبيقية حول دمج الابتكارات التكنولوجية مع الأطر المعيارية لتعزيز حوكمة النظم المالية والحاسوبية.

في الختام، تقدم هذه الدراسة خارطة طريق للمؤسسات الساعية لتحقيق التكامل بين أمن المعلومات وإدارة المخاطر، مع توظيف إمكانيات تقنية البلوك تشين. يمثل هذا النموذج المعياري محاولة لتحقيق استدامة نظم المعلومات الحاسوبية ودعم دورها الفعال في دعم الأهداف المؤسسية على المدى الطويل.

٧. قائمة المراجع

1. Avci, C., & et al. (2020). Software architectures for big data: a systematic literature review. *Avci et al. Big Data Analytics* 5(5), 1-53.
2. ISO/IEC 27032. (2023). *Guidelines for cybersecurity*. Published in Switzerland: International Organization for Standardization.
3. Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. United States: Addison-Wesley Professional.

4. Basholli, F., & et al. (2024). Framework, tools and challenges in cyber security. *Karshi Multidisciplinary International Scientific Journal Vol. 1(1)*, 96-106.
5. Gurzhii, A., & et al. (2024). Blockchain Enabled Digital Transformation: A Systematic Literature Review. *Software Engineering, LENS, LUT University, 53850, Lappeenranta, Finland*.
6. Hadia, m., & Jasimb, A. (2024). Artificial Intelligence for Cybersecurity in Computer Systems and Networks. *Journal of Iraqi Al-Khwarizmi (JIKh)*, 8(2), 86-98.
7. Hongdan, H., & et al. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems*, 48.
8. ISO 31000. (2018). : *Risk management — Guidelines*. ISO. Published in Switzerland: International Organization for Standardization.
9. Mathur, R. K. (2021). Introduction to Blockchain Technology. *National Telecommunications Institute for Policy Research, Innovation & Training (NTIPRIT)*, 1-32.
10. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *A white paper published through the Metzdowd forum, specialized in cryptography (Cryptography Mailing List)*.
11. NIST CSWP 29. (2024). Cybersecurity Framework Version 2.0. U.S. Department of Commerce. *National Institute of Standards and Technology*, 1- 27.
12. RMG. (2024, 11 26). *ISO 31000 Consultancy for Risk Management System Implementation*. Retrieved from Renad Al-Majd Information Technology Group: <https://www.rmg-sa.com/>
13. Rossi, M., Christoph , M.-B., Jason , B., & Roman , B. (2019). Blockchain Research in Information Systems. *Current Trends and an Inclusive Future*.
14. Shiwakoti , R., & et al. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems*,.
15. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. New York, USA:: Penguin Random House.
16. Wahhab, A. M., & et al. (2022). Auditing cybersecurity risks considering the information renaissance and its impact on the continuity of companies. *technium social sciences journal vol 35*, 18-35.