الرقابة على نظم المعلومات والأمن السيبراني

بحث مقدم للمشاركة في مسابقة البحث العلمي الرابعة عشر لمنظمة الأرابوساي

إعداد الباحث

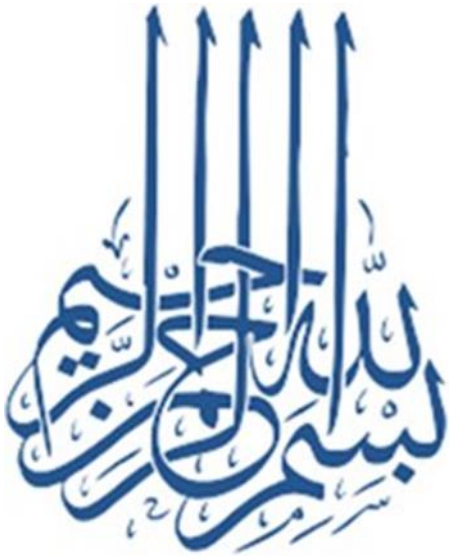
محاسب دكتور/ سامي علي محمد زغلول

مدير عام – الإدارة المركزية للرقابة المالية على البنوك

الجهاز المركزي للمحاسبات

جمهورية مصر العربية

٢٠٢٤


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله كما ينبغي لجلال وجهه ولعظيم سلطانه، والصلاة والسلام على سيدنا محمد صلى الله عليه وسلم، وعلى آله وصحبه أجمعين، وبعد.....

أتقدم بخالص الشكر والتقدير إلى كلٍ من السيد المستشار رئيس الجهاز المركزي للمحاسبات والسيد المستشار نائب رئيس الجهاز لتشجيعهما الدائم لأعضاء الجهاز على البحث العلمي والمشاركة في المسابقات العلمية والمساهمة في المحافل العلمية المحلية والدولية لما في ذلك من تعزيز كفاءات ومهارات وقدرات أعضاء الجهاز المركزي للمحاسبات، والشكر موصول لكل من عاونني في إتمام هذا العمل من قيادات وأعضاء الجهاز المركزي للمحاسبات.

كما أتقدم بخالص الامتنان إلى السادة القائمين على المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة (أرابوساي)، وأعضاء لجنة بناء القدرات المؤسسية لجهودهم المبذولة في تشجيعهم الدائم لمنسوبي أجهزة ودواوين المحاسبة في الوطن العربي على البحث العلمي لما لذلك من أثر في تعزيز تأهيلهم العلمي والمهني المستمر والذي يؤدي في النهاية إلى تحسين جودة أداء المهام الرقابية التي يؤدونها وبما يعود بالنفع على أوطانهم.

الباحث

دكتور/ سامي علي محمد زغلول

ملخص البحث

هدف هذا البحث إلى التعرف على دور تدقيق أمن المعلومات في الحد من مخاطر نظم المعلومات الإلكترونية في المنظمات الحكومية، وما يرتبط بذلك من تدقيق تكنولوجيا المعلومات ودور الأجهزة العليا للرقابة المالية، وقد تم تصميم استبانة لجمع البيانات وتوزيعها على عينة من منتسبي الجهاز الأعلى للرقابة في مصر، ومكاتب التدقيق وموظفي الإدارات المالية والمراجعة الداخلية وتكنولوجيا المعلومات في بعض البنوك المصرية، وقد اتبع الباحث المنهجين الوصفي والتحليلي لملاءمتهما طبيعة البحث.

وتوصل الباحث إلى عدة نتائج، أهمها:

- توجد علاقة ذات دلالة إحصائية بين لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية.
- إن تطبيق عمليات تدقيق نظم تكنولوجيا المعلومات بشكل منتظم يمكن أن يقلل بشكل كبير من مخاطر الأمن السيبراني وانتهاكات البيانات، مما يسهم في تعزيز أمان نظم المعلومات الإلكترونية.
- أهمية وجود إطار تنظيمي قوي ومستقل للرقابة على أنظمة المعلومات، حيث يمكن للأجهزة العليا للرقابة أن تلعب دوراً رئيسياً في تحديد المعايير والممارسات الأمنية، ومراقبة تنفيذها، وتوجيه المنظمات لتحسين أمان وموثوقية أنظمتهم. كما أن التعاون بين القطاعين العام والخاص يمكن أن يسهم في تعزيز فعالية جهود الرقابة وتحسين أمن المعلومات.
- يتعين على المنظمات التعامل مع تحديات متنوعة تتعلق بتدقيق تكنولوجيا المعلومات، مثل تطور التهديدات السيبرانية والتشريعات الجديدة المتعلقة بحماية البيانات. ومن الفرص المهمة الاستفادة من تطورات التكنولوجيا الحديثة لتعزيز قدرة الجهات المعنية على اكتشاف والتصدي للتهديدات الأمنية.
- يجب على الشركات والمؤسسات تطبيق استراتيجيات متعددة لتحسين عمليات تدقيق تكنولوجيا المعلومات، بما في ذلك توظيف الكوادر المؤهلة واعتماد تقنيات تحليل البيانات الضخمة والتعاون مع مزودي الخدمات الأمنية المتخصصين.

وخرج الباحث بعدة توصيات، منها:

- تعزيز توعية الموظفين وتدريبهم: يجب على المنظمات تعزيز توعية موظفيها بأهمية

أمان المعلومات وممارسات التكنولوجيا الآمنة، وتقديم تدريب مستمر لهم حول التهديدات السيبرانية وكيفية التعامل معها.

- تطبيق إجراءات تدقيق دورية: ينبغي على المنظمات تنفيذ عمليات تدقيق دورية لأنظمتها وتقنياتها للتأكد من مواكبتها لأحدث معايير الأمان والامتثال للتشريعات واللوائح.
- تعزيز التعاون مع الجهات العليا للرقابة: ضرورة قيام المنظمات بتعزيز التعاون مع الأجهزة العليا للرقابة والاستفادة من الإرشادات والتوجيهات التي تقدمها لتحسين أمن المعلومات.
- تبني أفضل الممارسات والتقنيات الحديثة: ينبغي على المنظمات استخدام أفضل الممارسات واعتماد التقنيات الحديثة في تطبيق عمليات التدقيق وتأمين الأنظمة الإلكترونية.

الكلمات المفتاحية: تدقيق، تدقيق تكنولوجيا المعلومات، مخاطر نظم المعلومات، الأجهزة العليا للرقابة المالية

Summary

The aim of this research was to identify the role of information security audit in mitigating the risks of electronic information systems in governmental banks, along with associated auditing of information technology and the role of the supreme audit institutions. A questionnaire was designed to collect data and distributed to a sample of members of the supreme audit institution in Egypt, audit firms, financial management employees, internal audit, and information technology departments in some Egyptian banks. The researcher followed both descriptive and analytical methodologies to suit the research nature.

The researcher reached several conclusions, including:

- There is a statistically significant relationship between information security audit policies and their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, code of conduct for information security auditing, external auditing) in mitigating the risks of electronic information systems in Egyptian banks.
- Regular application of information technology systems auditing processes can significantly reduce cybersecurity

risks and data breaches, thus enhancing the security of electronic information systems.

- The importance of having a strong and independent regulatory framework for information systems oversight, where SAIs can play a key role in setting security standards and practices, monitoring their implementation, and guiding organizations to improve the security and reliability of their systems. Collaboration between the public and private sectors can also enhance the effectiveness of oversight efforts and improve information security.
- Organizations must deal with various challenges related to information technology auditing, such as evolving cyber threats and new legislation related to data protection. Important opportunities include leveraging advancements in modern technology to enhance the ability of relevant entities to detect and combat security threats.
- Companies and institutions should adopt multiple strategies to improve information technology auditing processes, including employing qualified personnel, adopting big data analytics techniques, and collaborating with specialized security service providers.

The researcher made several recommendations, including:

- Enhancing employee awareness and training: Organizations should enhance their employees' awareness of the importance of information security and safe technology practices, and provide ongoing training on cyber threats and how to deal with them.
- Implementing regular auditing procedures: Organizations should conduct regular auditing of their systems and technologies to ensure compliance with the latest security standards and regulations.
- Strengthening cooperation with SAIs: Organizations need to enhance cooperation with higher oversight bodies and leverage the guidance and directives they provide to improve information security.
- Adopting best practices and modern technologies: Organizations should use best practices and adopt modern technologies in implementing auditing processes and securing electronic systems.

Key words: Audit, IT audit, Information systems risks, Supreme audit institutions

قائمة محتويات البحث

قائمة الجداول

قائمة الأشكال

الفصل التمهيدي

الإطار العام للبحث والدراسات السابقة

الفصل التمهيدي: الإطار العام للبحث

أولًا: المقدمة

في عصر التكنولوجيا الرقمية الحديثة، يسرت تكنولوجيا المعلومات ومازالت تيسر الحياة بصفة عامة وعالم المال والأعمال بصفة خاصة، وقد نشأت الحاجة للاستفادة من القدرات التي يمتاز بها نظم المعلومات وشبكات الاتصال؛ وأصبحت نظم المعلومات وتكنولوجيا المعلومات أساسية لنجاح أي منظمة أو مؤسسة.

ولقد نتج عن الاعتماد الكبير على تكنولوجيا المعلومات تغيرات كبيرة في مقومات نظم المعلومات؛ من حيث تغير تصميم هذه النظم وتركيباتها، إفرازها للعديد من المخاطر المستحدثة، افتقارها لمسار تدقيق مرئي، تغير طبيعة أدلة الإثبات واستحداث أخرى لم تتميز بها النظم التقليدية، كتغير هيكل الرقابة الداخلية الخاص بها وتعقده التقني الذي يتلاءم مع البيئة الالكترونية من رقابة عامة على بيئة النظم ورقابة خاصة على التطبيقات الالكترونية.

ولأن تدقيق الحسابات مهنة ترتكز أساسًا على إصدار رأي محايد مدعم بأدلة حول عدالة ومصداقية المعلومة المحاسبية التي هي مخرجات نظم معلومات إلكترونية أو هي إلكترونية في حد ذاتها؛ فلا شك أن ذلك سيتطلب الحصول على الفهم الوافي لطبيعة وخصائص هذه النظم المنتجة لتلك المعلومات، والتأكد من أن الرقابة على المدخلات وعملية المعالجة الالكترونية لها والمخرجات الناتجة عن ذلك تقوم على ضوابط رقابية سليمة، وأن النظام الالكتروني يسهم في حماية البيانات والمعلومات على حد سواء.

ولأن مدقق الحسابات يستدل ويسترشد في آدائه لعمله بمعايير مهنية، فلا شك أن ذلك يتطلب دراسة وتقييم مدى ملائمة معايير التدقيق مع البيئة الالكترونية الجديدة، ودراسة مدى إمكانية الاعتماد على معايير أخرى خارج معايير تدقيق الحسابات التي تهتم بالجانب الإلكتروني لنظم المعلومات، أو إمكانية اعتماد الحاسوب نفسه كأداة بعملية التدقيق (التدقيق الإلكتروني) في ظل استحداث برامج تطبيقية متخصصة في مجال تدقيق الحسابات.

ويعد تدقيق تقنية نظم المعلومات وتدقيق أمن المعلومات أدوات أساسية لضمان سلامة وأمان البيانات والمعلومات في العصر الرقمي. بالإضافة إلى ذلك، تعتبر الأجهزة العليا للرقابة شركاء أساسيين في تعزيز الثقة والشفافية وتحقيق أهداف المنظمة بنجاح.

ثانيًا: الدراسات السابقة

في حدود المسح الذي قام به الباحث للدراسات الأكاديمية المرتبطة، والتي لها علاقة بموضوع بحثه، يستعرض الباحث ملخص لهذه الدراسات وما انتهت إليه من نتائج فيما يلي:

الدراسات باللغة العربية

١. دراسة هاشم، هبة جمال، (٢٠٢٣)، بعنوان: "منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل ".

هدفت الدراسة إلى التوصل لمنهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل بالبيئة المصرية، وقد تناولت الدراسة انعكاسات مخاطر الأمن السيبراني على أعمال المدقق الخارجي وخطوات المنهج المقترح، واعتمدت منهجية الدراسة التطبيقية علي شركات المساهمة المقيدة في البورصة المصرية والعاملة في القطاعات والأنشطة المرتبطة بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا.

وقد توصلت الدراسة إلى أن تقييم مخاطر الأمن السيبراني يعتمد على عمليات المراجعة التي تدرس وتقيم مجموعة من الضوابط المحددة مسبقًا في الموضوعات المتعلقة بالأمن السيبراني، كما أوضحت النتائج وجود تأثير طردي معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المدقق الخارجي، ووجود ارتباط طردي معنوي بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المدقق الخارجي.

٢. دراسة العوامري، عبير عيسى، (٢٠٢٢) بعنوان: أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الالكترونية.

هدفت هذه الدراسة إلى استكشاف أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؛ وذلك بغرض زيادة الموثوقية، والمصداقية في نظم المعلومات المحاسبية الإلكترونية ومخرجاته.

وقد أظهرت نتائج الدراسة أن نظم المعلومات المحاسبية الإلكترونية تتعرض للعديد من المخاطر يتمثل أهمها في المخاطر الداخلية، كما يتمثل أهم أسباب حدوث تلك المخاطر في عدم كفاءة وفعالية الإجراءات والضوابط الرقابية لنظم المعلومات داخل الشركات محل الدراسة، وعدم تضمين عدد كبير من عينة الدراسة لأهداف ومبادئ كل من حوكمة أمن المعلومات وخدمات تأكيد الثقة داخل استراتيجيتها المستقبلية.

٣.دراسة العازمي، عبد الله فالح، (٢٠٢٢) بعنوان: دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات المحاسبية من المخاطر الالكترونية في ظل عصر الرقمنة.

هدفت الدراسة إلي التعرف على طبيعة المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في البنوك الكويتية ومعدلات تكرارها ومصادر حدوثها.

وقد أظهرت نتائج الدراسة أن نظم المعلومات المحاسبية الإلكترونية تتعرض للعديد من المخاطر، ووجود تأثير معنوي لتأثير تفعيل أبعاد حوكمة تكنولوجيا المعلومات على تأمين المعلومات المحاسبية من المخاطر الإلكترونية، وأن إتباع نظام معلومات محاسبية سليم يقلل من مخاطر نظم

المعلومات المحاسبية الإلكترونية، وأن الاستفادة من الخبرات العالمية في مجال أمن المعلومات يرفع من درجة الثقة في المعلومات المحاسبية الإلكترونية.

٤.دراسة حبيب، سمر، ٢٠٢٢ بعنوان " دور المحاسبة ومعايير التدقيق السحابي في تأكيد أمن البيانات والمعلومات: دراسة ميدانية من وجهة نظر مدققي الحسابات الخارجيين في سوريا "

هدفت الدراسة إلى استقصاء آراء مدققي الحسابات الخارجيين في سوريا حول دور فوائد ومخاطر المحاسبة والتدقيق السحابي عند تبني الحلول السحابية، وآرائهم حول دور معايير التدقيق السحابي (المعيار SAS70, SSAE16, ISO295) في تأكيد أمن البيانات والمعلومات، إضافة إلى استقصاء آرائهم حول مدى توافر ضوابط أمن البيانات والمعلومات الصادرة عن الهيئات والمنظمات المهنية الدولية في القواعد والتعليمات الصادرة عن المشرع السوري.

وتوصلت الدراسة إلى عدة نتائج منها وجود فروق ذات دلالة إحصائية في آراء مدققي الحسابات الخارجيين حول كل من دور فوائد ومخاطر المحاسبة والتدقيق السحابي عند تبني الحلول السحابية، دور معايير التدقيق السحابي في تأكيد أمن البيانات والمعلومات، وتوافر ضوابط أمن البيانات والمعلومات في القواعد الصادرة عن المشرع السوري.

الدراسات باللغة الإنجليزية

١.دراسة Mirwali Azizi & et al (2024) بعنوان:

The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges

تسعى الدراسة إلى تسليط الضوء على كيفية قيام المؤسسات بتسخير تدقيق تكنولوجيا المعلومات لتحسين مزايا التحول الرقمي مع تخفيف المخاطر المرتبطة به، وتفحص الفرص والتحديات التي تواجهها المنظمات على مستوى العالم، ومن خلال إجراء تدقيق شامل للأدبيات لعرض الدور المتطور وسبل التحسين والعقبات التي تمت مواجهتها تؤكد الدراسة على ضرورة تدقيق تكنولوجيا المعلومات للتكيف مع التطورات التكنولوجية مع التغلب على التحديات المعقدة للحفاظ على فعاليتها. وأن معالجة الأمن السيبراني وقيود الموارد تتطلب اتخاذ تدابير استباقية واستثمارات استراتيجية، كما يمكن للمؤسسات تحسين قيمة التحول الرقمي من خلال تعزيز تدقيق تكنولوجيا المعلومات من خلال المبادرات الاستباقية ورعاية تنمية المواهب.

٢.دراسة Yohannes Kurniawan & Archie Mulyawan, 2023 بعنوان:

The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting

هدفت الدراسة إلى استكشاف دور المدققين الخارجيين في تحسين الأمن السيبراني للشركات في التقارير المالية من خلال تطوير الضوابط الداخلية في العمليات القائمة على التكنولوجيا من خلال تحليل نتائج التدقيق.

أكدت الدراسة أن نمو التكنولوجيا المبتكرة يؤثر على قدرة المدقق على المساعدة في مراجعة نتائج وقياسات مخاطر التدقيق. ومع ذلك، فإن قدرة مدقق الحسابات على تطبيق التكنولوجيا لأداء التدقيق لها تأثير ضئيل.

٣.دراسة Mohammad Aljanabi & et al, 2023 بعنوان:

The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment

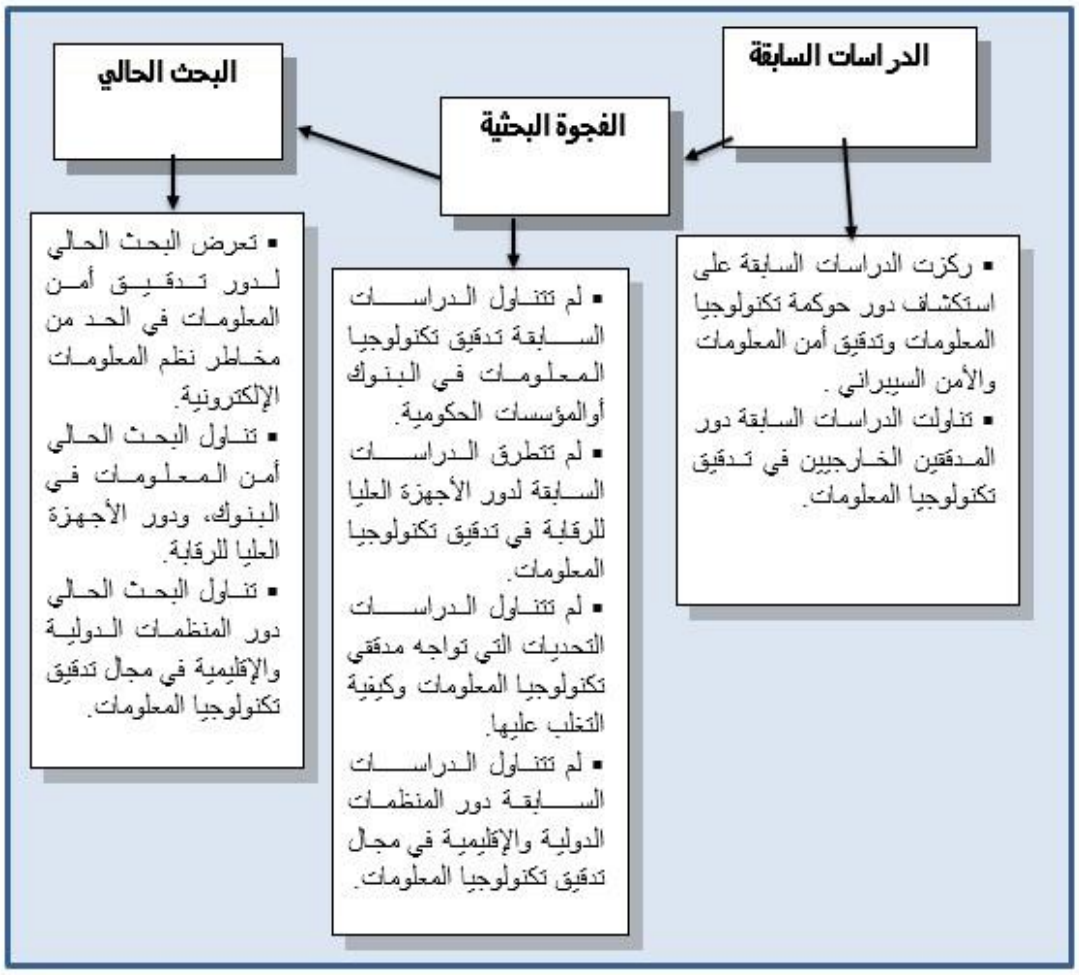
هدفت الدراسة إلى إجراء مسح حول حوكمة الأمن السيبراني والتحول الرقمي وأهميتهما في خلق بيئة رقمية خالية من الاختراقات وسرقة البيانات وخدمة جميع المواطنين في تنظيم حياتهم بشكل أفضل بالاعتماد على تقنيات الذكاء الاصطناعي.

أكدت الدراسة أن الأمن السيبراني أحد التحديات التي تواجهها العديد من الحكومات أثناء تطور عمليات القرصنة والبرمجيات الضارة والتقنيات التي تساهم في إحداث ثغرات في شبكات الكمبيوتر، وأن الاعتماد بشكل كبير على تقنيات الذكاء الاصطناعي يسهم في تطوير البيئة الرقمية والحفاظ على البيانات لما لهذه التقنيات من قدرة على دراسة سلوك الأشخاص غير المصرح لهم والبرامج الخبيثة.

ثالثًا: التعليق على الدراسات السابقة والفجوة البحثية

بمراجعة الدراسات السابقة والتي أمكن للباحث تناولها بالدراسة، يستخلص الباحث النتائج الموضحة بالشكل التالي:

شكل رقم (1): التعليق على الدراسات السابقة والفجوة البحثية



المصدر: من إعداد الباحث

يتضح من الشكل السابق أن الباحث حاول في البحث الحالي تغطية الفجوة البحثية في الدراسات السابقة وتناول التحديات التي تواجه مدققي تكنولوجيا المعلومات وكيفية التغلب عليها، ودور المنظمات المهنية في هذا الشأن.

رابعًا: المشكلة البحثية

في ظل التطور المستمر لتكنولوجيا المعلومات والانتقال إلى البيئة الرقمية، تواجه المنظمات الحكومية تحديات متزايدة فيما يتعلق بأمان وسلامة البيانات والمعلومات، ويعتبر تدقيق نظم المعلومات الإلكترونية وتدقيق أمن المعلومات أدوات أساسية لتقييم وتحسين أمان البيانات في هذه المنظمات. إلا أنه، على الرغم من أهمية تلك الأدوات، يظل هناك تحديات محددة تتعلق بتطبيقها في البيئة الحكومية.

بالنظر إلى هذا السياق، تهدف هذه الدراسة إلى تحليل تأثير تدقيق أمن المعلومات على تقليل مخاطر نظم المعلومات الإلكترونية في البنوك المصرية، وتقديم التوصيات اللازمة لتعزيز أمان المعلومات والبيانات في هذه البنوك.

ومن خلال ما سبق تمحورت إشكالية هذا البحث من خلال التساؤل التالي:

ما دور تدقيق أمن المعلومات في الحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية؟"

خامسًا: متغيرات البحث

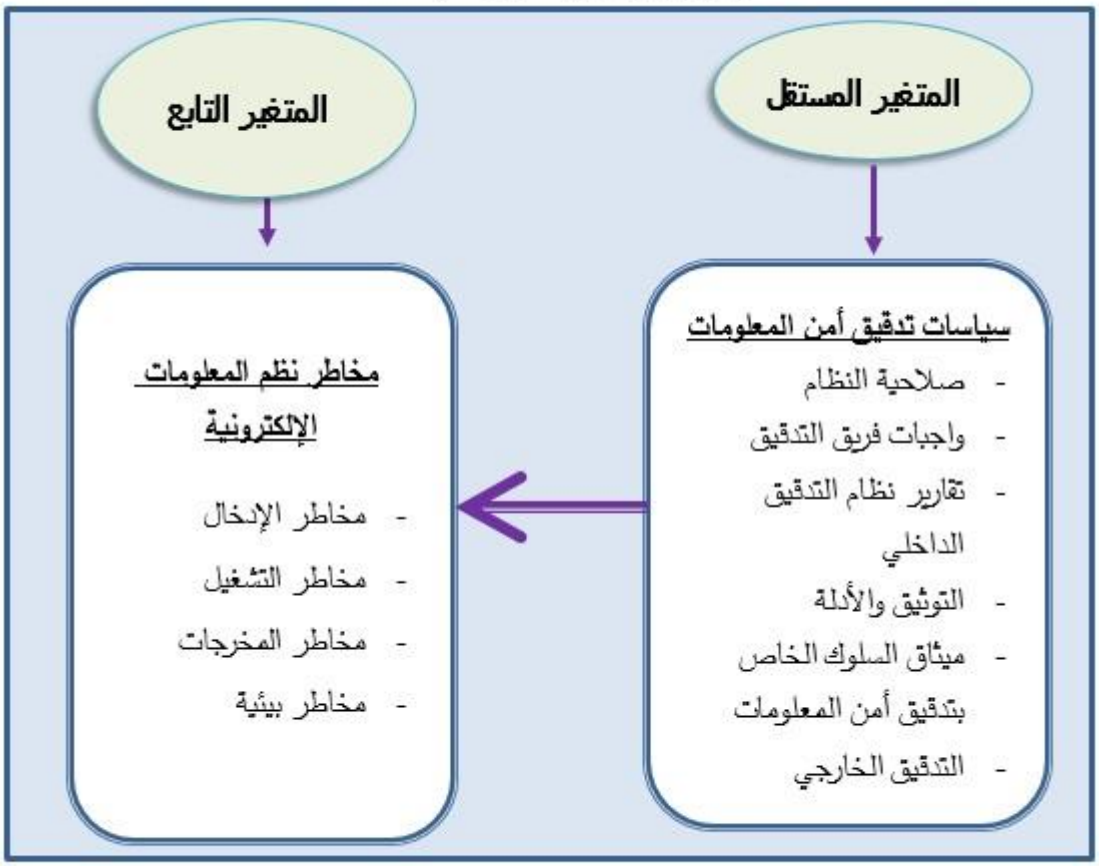
تتمثل متغيرات الدراسة فيما يلي:

المتغير المستقل: سياسات تدقيق أمن المعلومات.

المتغير التابع: مخاطر نظم المعلومات الإلكترونية.

سادسًا: هيكل متغيرات البحث

شكل رقم (2): هيكل متغيرات البحث



المصدر: من إعداد الباحث

سابعًا: فرضيات البحث

بناء على مشكلة الدراسة وأهدافها يمكن صياغة الفرضية الرئيسية على النحو التالي:

يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية.

وتحقيقًا لهدف البحث يمكن وضع الفرضيات التالية:

الفرضية الأولى:

يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر الإدخال في البنوك.

الفرضية الثانية:

يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات) في الحد من مخاطر التشغيل في البنوك.

الفرضية الثالثة:

يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر المخرجات في البنوك.

الفرضية الرابعة:

يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من المخاطر البيئية في البنوك.

ثامنًا: أهداف البحث

يمكن بلورة الأهداف التي يسعى البحث إلى تحقيقها فيما يلي:

- التعرف على الإطار المفاهيمى لتدقيق تكنولوجيا المعلومات.
- تحديد مخاطر نظم المعلومات الإلكترونية في المنظمات الحكومية.
- تحليل تأثير تدقيق أمن المعلومات على تقليل مخاطر نظم المعلومات الإلكترونية.
- تقديم توصيات لتعزيز أمن المعلومات في المنظمات الحكومية.

من خلال تحقيق هذه الأهداف، يمكن للدراسة أن تسهم في تعزيز أمان المعلومات والبيانات في المنظمات الحكومية وتقديم توجيهات عملية لتطبيق أفضل الممارسات في مجال تدقيق نظم المعلومات وأمن المعلومات.

تاسعًا: أهمية البحث

تتمثل أهمية البحث – من وجهة نظر **الباحث** – فيما يلي:

<u>من الناحية العلمية</u>

يسهم هذا البحث في توسيع المعرفة العلمية في مجال تدقيق نظم المعلومات الإلكترونية وأمن المعلومات، ويساعد في فهم العلاقة بين تدقيق تكنولوجيا المعلومات وتقليل مخاطر نظم المعلومات في المنظمات الحكومية.

كما يكتسب هذا البحث أهميته العلمية من كونه يساير التطورات الحديثة فى مجال البحوث المحاسبية التى تركز على أثر تكنولوجيا المعلومات في التدقيق ودور الأجهزة العليا للرقابة.

من الناحية التطبيقية

١. **توفير التوجيهات العملية:** يوفر هذا البحث توجيهات عملية ومنهجيات لتطبيق أفضل الممارسات في تدقيق نظم المعلومات وأمن المعلومات في المنظمات الحكومية.
٢. **تعزيز الأمان والثقة:** يسهم هذا البحث في تعزيز أمان المعلومات والبيانات في المنظمات الحكومية، وبالتالي زيادة الثقة في العمليات والتقارير المالية والإدارية.
٣. **تقديم التوصيات العملية:** يساعد هذا البحث في تقديم توصيات عملية للمنظمات الحكومية لتحسين إدارة أمن المعلومات وتطبيق تدقيق أمن المعلومات بطريقة فعالة.

بشكل عام، يعتبر هذا البحث مهماً على الصعيدين العلمي والتطبيقي، حيث يسهم في تطوير المعرفة العلمية وتقديم الحلول العملية لزيادة أمان وموثوقية نظم المعلومات الإلكترونية في المنظمات الحكومية.

عاشرًا: أسلوب البحث

لتحقيق أهداف البحث استخدم الباحث المنهج الوصفى والتحليلى الذى يعتمدا على دراسة الواقع أو الظاهرة ويهتم بوصفها وصفًا دقيقًا وكميًا، ومن خلال استخدام الأسلوب التطبيقى، وقد تم جمع البيانات والمعلومات، وتم الاستعانة بما توفر من تدقيق ودوريات وشبكة الانترنت فى تغطية الجانب النظرى فيما اعتمدت استمارة الاستبيان فى الجانب التطبيقى التى تعد الوسيلة الرئيسة إذ تمت صياغة فقراتها بما يتلاءم مع متغيرات البحث بالاستفادة من الدراسات المذكورة فى الجانب النظرى التى تناولت تلك المتغيرات وقد روعى فى صياغة فقرات الاستبان البساطة والوضوح.

وبعد جمع البيانات اللازمة من مصادرها المختلفة سواء كانت بيانات أولية أو بيانات ثانوية، تم إخضاع هذه البيانات للتحليل الإحصائي من أجل استخراج مجموعة من المؤشرات ذات دلالات معينة تفيد في اختبار الفرضيات، والكشف عن الغموض في مشكلة البحث وتحقيق أهدافه.

إحدى عشر: مجتمع وعينة البحث

تألف مجتمع الدراسة من أعضاء الجهاز الأعلى للرقابة في مصر، وموظفي القطاع المالي وقطاع تكنولوجيا المعلومات وقطاع التدقيق الداخلي في البنوك المصرية التي تنتمي للقطاع العام، وتم أخذ عينة عشوائية عددها ٥٠ فرد من مجتمع الدراسة تمثلوا في المدراء، المدققين الخارجيين، والمحاسبين، ورؤساء الأقسام والمدققين الداخلين ومساعديهم، موظفي تكنولوجيا المعلومات في البنوك محل الدراسة.

ثاني عشر: محتويات البحث

لتحقيق هدف البحث ومعالجة مشكلته بصورة علمية، اشتمل البحث بشقيه النظري والتطبيقي على الفصول التالية:

الفصل التمهيدي: الإطار العام للبحث والدراسات السابقة

الفصل الأول: الإطار المفاهيمي لتدقيق نظم المعلومات الإلكترونية

المبحث الأول: تدقيق تكنولوجيا المعلومات والاتصال.

المبحث الثاني: مخاطر نظم المعلومات الإلكترونية.

الفصل الثاني: الدراسة التطبيقية.

الفصل الثالث: النتائج والتوصيات

المراجع

الملاحق

الفصل الأول
الإطار المفاهيمي لتدقيق نظم المعلومات الإلكترونية

الفصل الأول
الإطار المفاهيمي لتدقيق نظم المعلومات الإلكترونية

أحدثت التطورات المتلاحقة في مجال تكنولوجيا المعلومات نقلة نوعية كبيرة نجم عنها تقدمًا ملحوظًا في أنماط العمل لدى منظمات الأعمال ومنظمات وهيئات القطاع العام والحكومي وشتى نواحي الحياة، حيث ساهم هذا التقدم في إحداث تغييرات جذرية على البيئة المعلوماتية في المنظمات المختلفة، وقد أدى ذلك إلى ظهور نظم المعلومات الإلكترونية المختلفة، والتي سهلت العمليات وساهمت في الحصول على نتائج عمل أكثر دقة بأقل وقت وجهد ممكن، إلا أنه رافق ذلك عوائق أدت إلى إحداث ثغرات في عمل تلك الأنظمة حيث ظهرت العديد من المخاطر المرتبطة بنظم المعلومات الإلكترونية والتي تتمثل في مخاطر إدخال البيانات ومخاطر التشغيل ومخاطر المخرجات والمخاطر البيئية وغيرها من المخاطر والتي من شأنها أن تؤثر سلبًا على فعالية أداء النظام والأهداف المرجوة من وجوده، والتي قد تكون بفعل مقصود أو غير مقصود، وقد يعود ذلك إلى أسباب تتعلق بقلة الوعي والتدريب لدى موظفي المنظمات وضعف الأدوات والإجراءات الرقابية المطبقة. (أنور، ٢٠١٧، ١٥:١٦)

ونظرًا للأهمية المتزايدة لتكنولوجيا المعلومات في المنظمات الحكومية والقطاع العام، يجب على العديد من عمليات التدقيق التي يقوم بها المدققون في الجهات العليا للرقابة النظر في قضايا تكنولوجيا المعلومات وتضمين مكونات ذات علاقة بها.

ونظرًا لذلك ظهر مجال تدقيق نظم المعلومات الإلكترونية أو ما يعرف بتدقيق تكنولوجيا المعلومات وتدقيق أمن المعلومات لمواجهة التحديات التي تواجهها المنظمات مع التطورات اللامتناهية في تكنولوجيا المعلومات، وذلك لتفادي وإزالة أي مخاطر من الممكن أن تتعرض لها نظم المعلومات والتأكد من أن احتمالية تعرض نظمها إلى أي من التهديدات الداخلية أو الخارجية أصبح من الممكن اكتشافه.

لذلك تناول الباحث موضوع الإطار المفاهيمي لتدقيق نظم المعلومات الإلكترونية على النحو التالي:

المبحث الأول: تدقيق تكنولوجيا المعلومات والاتصال

المبحث الثاني: مخاطر نظم المعلومات الإلكترونية

المبحث الأول
تدقيق تكنولوجيا المعلومات والاتصال

١/١/١ تمهيد

لقد غيرت الطبيعة العالمية لتكنولوجيا المعلومات الطريقة التي نعمل بها جميعًا بطرق عديدة، ومهنة التدقيق ليست استثناءً، فمع تقدم التكنولوجيا، اعتمدت منظمات الأعمال والحكومات ومنظمات القطاع العام تكنولوجيا المعلومات في أنظمة المعلومات الخاصة بها بهدف زيادة الكفاءة وتعزيز تقديم منتجاتها وخدماتها المختلفة. كما تحول نمط تقديم الخدمات العامة بسرعة من المادية إلى الإلكترونية. وقد أدى هذا التحول إلى اضطرار المنظمات الحكومية إلى العمل كمنصات رقمية لتقديم الخدمات للجمهور، فضلًا عن مقدمي البنية التحتية لأنظمة تكنولوجيا المعلومات الداعمة لهم. كما أن التحول الرقمي المستمر للمعلومات، أدى أيضًا إلى زيادة الاعتماد العام على أنظمة تكنولوجيا المعلومات. (Rabii, 2023, 539: 551)

ومع زيادة الاستثمار والاعتماد على أنظمة تكنولوجيا المعلومات من قبل المنظمات الخاضعة للتدقيق، فمن الضروري لمدقق تكنولوجيا المعلومات أن يتبنى منهجية ونهج مناسبين. يمكن أن يساعد ذلك في ضمان قدرة التدقيق على تحديد المخاطر التي تهدد سلامة البيانات وتوافرها وصلاحيتها وإساءة استخدامها وخصوصيتها، وكيفية التعامل مع تلك المخاطر ونقاط الضعف. (حسين، ٢٠٢٠، ٢٥: ٥٠)

١/١/٢ مفهوم تدقيق أنظمة تكنولوجيا المعلومات والاتصال.

يمكن تعريف تدقيق أنظمة تكنولوجيا المعلومات والاتصال بشكل عام بأنه فحص لجوانب استخدام المنظمة لتكنولوجيا المعلومات، بما في ذلك البنية التحتية لتكنولوجيا المعلومات والضوابط والسياسات والإجراءات والتطبيقات واستخدام البيانات، فهو عملية جمع وتقييم الأدلة لتحديد ما إذا كان استخدام الحاسب الآلي يسهم في حماية أصول المنظمة ويؤكد سلامة بياناتها ويحقق أهدافها بفعالية ويستخدم مواردها بكفاءة" (يونس، ومصطفى، ٢٠١٥، ١٠٤)

كما يُعرف بأنه التدقيق الذي موضوعه أنظمة تكنولوجيا المعلومات والاتصال للمؤسسة، وتسييرها وعملياتها وكافة الإجراءات والعمليات ذات العلاقة أو بأنه التدقيق الذي يعنى بفحص أنظمة تكنولوجيا المعلومات والاتصال للتأكد من أنها تلبي احتياجات المنظمة دون المساس بالخصائص الهامة للمؤسسة كالأمن والخصوصية والتكلفة.(INTOSAI, 2023, 9)

قد يكون مثل هذا التدقيق مكرسًا بالكامل لقضايا تكنولوجيا المعلومات، أو يمكن أن يكون جزءًا من تدقيق مستهدف نحو موضوع محدد. في كلتا الحالتين، يكون هدف التدقيق التكنولوجي تحديد حالات الانحراف عن معايير محددة تم التعرف عليها استنادًا إلى نوع عملية التدقيق، مثل التدقيق المالي أو التدقيق في الالتزام أو التدقيق في الأداء.

١/١/٣ متطلبات إجراء عمليات تدقيق تكنولوجيا المعلومات

يرد تفويض الجهاز الأعلى للرقابة المالية (SAI) لإجراء مراجعة أنظمة تكنولوجيا المعلومات في إعلان ليما (انتوساي، ١٩٧٧). وكذلك، فإن تفويض الجهاز الأعلى للرقابة المالية لمراجعة أنظمة تكنولوجيا المعلومات مستمد من التفويض العام للأجهزة العليا للرقابة بإجراء تدقيق الأداء، وعمليات التدقيق المالي والالتزام أو مزيج منها، وذلك وفقًا للمبادئ الأساسية للتدقيق في القطاع العام (انتوساي، ٢٠١٩:١٠٠)، ومبادئ التدقيق المالي (انتوساي ٢٠٢٠:٢٠٠)، ومبادئ التدقيق الأداء (انتوساي، ٢٠١٩:٣٠٠)، ومبادئ تدقيق الالتزام (انتوساي، ٢٠١٩:٤٠٠).

١/١/٤ نطاق تدقيق أنظمة تكنولوجيا المعلومات والاتصال

يعمل تدقيق تكنولوجيا المعلومات والاتصال بالترابط مع الأنواع المختلفة للتدقيق، حيث أن نشاط مدقق تكنولوجيا المعلومات والاتصال قد يتخلل عمل المدقق المالي من خلال قيامه بفحص القوائم المالية، وتدقيق العمليات من خلال تقييم الرقابة في مختلف أنشطة المؤسسة، ويتقاطع مع تدقيق الأداء في تقييم الجوانب المتعلقة بتكنولوجيا المعلومات والاتصال، كما يتفق مع التدقيق لأغراض خاصة عندما يتعلق الأمر بتقييم الخدمات المقدمة من طرف ثالث، وكذا يمكن أن يتخلل التدقيق القضائي وتدقيق الامتثال (INTOSAI, IDI, 2022, 10) ، فعلى سبيل المثال:

- **في سياق التدقيق المالي**، يمكن أن يكون أحد أمثلة تدقيق تكنولوجيا المعلومات هو فحص الضوابط العامة التي تضمن تشغيل أنظمة المعلومات التي تكمن وراء العمليات المالية للمنظمة، كما هو موضح من خلال بياناتها المالية. (انتوساي، ٢٠٠، ٢٠٢٠)
- **في سياق تدقيق الأداء**، يمكن أن يكون أحد أمثلة تدقيق تكنولوجيا المعلومات هو تحديد المدى الذي أدى فيه اعتماد المنظمة للتكنولوجيا الجديدة إلى تحقيق فوائد قابلة للقياس على مستوى الحكومة وتوفير في التكاليف. (انتوساي، ٣٠٠، ٢٠٢٠)
- **في سياق تدقيق الامتثال**، يمكن أن يكون أحد أمثلة تدقيق تكنولوجيا المعلومات هو فحص كفاءة أنظمة المعلومات التي تنتج تقارير الامتثال، مما يمكّن الموظفين من إدارة عمليات المنظمة والتحكم فيها. قد يتضمن ذلك، بين أمور أخرى، تحليل التزام الجهة الخاضعة للرقابة بمتطلبات اللائحة العامة لحماية البيانات أو الأعمال القانونية المتعلقة بتكنولوجيا المعلومات. (انتوساي، ٤٠٠، ٢٠٢٠)
- ويمكن ألا يكون إجراء تدقيق تكنولوجيا المعلومات جزءًا من تدقيق الأداء أو التدقيق المالي أو تدقيق الالتزام؛ ومع ذلك، فإن المبادئ العامة والإجراءات والمعايير والتوقعات المطبقة على عمليات التدقيق المالي وتدقيق الأداء والامتثال تنطبق أيضًا على عمليات تدقيق تكنولوجيا المعلومات.

وقد تتعامل عمليات تدقيق تكنولوجيا المعلومات مع مجموعة متنوعة من المجالات المتنوعة، مثل حوكمة تكنولوجيا المعلومات، واستثمارات تكنولوجيا المعلومات، وما إذا كانت هناك ضوابط كافية لحماية البيانات لكيانات مثل الحكومات المحلية، وتحليل تطبيق التقنيات الجديدة مثل الذكاء الاصطناعي، أو تطوير واقتناء وتشغيل أنظمة تكنولوجيا المعلومات، كما تتعامل أيضًا مع جوانب أمن المعلومات والأمن السيبراني، والتي ترتبط بها ارتباطًا وثيقًا. (ISACA, 2019, 23: 45)

وبما أن تدقيق تكنولوجيا المعلومات هو فحص للضوابط. فإن هذه الضوابط تتمثل في أي إجراءات لتقليل خطر الأحداث الضارة. وقد تكون إجراءات يدوية أو آلية، وسياسة، وسيلة، وممارسة، وعملية، وغير ذلك. يمكن تصنيف الضوابط على أنها ضوابط عامة وضوابط خاصة بالتطبيق (انتوساي، ٢٠١٩، معيار ٥١٠٠).

أ- **الضوابط العامة:** وهي تهدف إلى تحقيق الخصائص المرغوبة للمعلومات (على سبيل المثال، السرية والنزاهة والتوافر) في البيئات البشرية والتقنية والمالية والمادية وغيرها التي يتم تطوير أنظمة المعلومات وصيانتها وتشغيلها ضمنها.

ب-**الضوابط الخاصة بالتطبيق:** وهي إجراءات يدوية أو آلية تعتمد على تكنولوجيا المعلومات ضمن نظام معلوماتي تؤثر على معالجة المعلومات. يمكن أن تتعامل الضوابط الخاصة بالتطبيق مع التحقق من البيانات ومعالجتها وتوصيلها وتأمينها ومسائل ذات صلة.

وتم تناول هذه الضوابط بالتفصيل في المبحث الثاني من هذا الفصل.

١/١/٥ أنواع تدقيق أنظمة تكنولوجيا المعلومات والاتصال

يمكن تحديد أنواع تدقيق تكنولوجيا المعلومات والاتصال كما يلي (Richard, 2015, 9:15):

١- تدقيق استراتيجية الإعلام والاتصال

وهو التدقيق الذي يهدف إلى ضمان توافق نظام المعلومات مع الاستراتيجية العامة للمؤسسة، والتحديات والمخاطر المحددة. حيث لا يكفي أن يكون نظام المعلومات متوافقًا مع القوانين ومتحكمًا فيه، بل يجب أن يتوافق مع تنظيم المنظمة وثقافتها؛ وأن تكون الاستثمارات الموجهة لتكنولوجيا المعلومات تخدم الاحتياجات الحالية والمستقبلية للمؤسسة.

٢- تدقيق وظيفة الإعلام والاتصال

وهو التدقيق الذي يهدف إلى ضمان أن الهيكل التنظيمي والعمليات ملائمين ومتوافقين مع القواعد، سواء كانت العمليات متعلقة بالتخطيط، التوجيه، وتطوير التطبيقات وتقديم الخدمات والدعم.

ويذكر أن المرجع الأساسي لهذا النوع من التدقيق هو إصدارات أهداف الرقابة على المعلومات والتكنولوجيا المرتبطة بها (COBIT).

٣- تدقيق العمليات المحوسبة للمؤسسة

يهدف هذا النوع من التدقيق إلى ضمان أن نظام تكنولوجيا المعلومات مؤكد، وأن تشغيل النظام يكون بشكل مؤكد ومستمر وأمن، لكون هذه الخصائص تعتبر من شروط استمرارية العمل في المؤسسة، ويجب الاعتناء بها نظراً لكون الأعطال وفقدان البيانات والتهديدات الناتجة عن الشبكات المفتوحة تزيد من المخاطر الممكنة في المؤسسة، وفي هذا الإطار يهتم التدقيق بكل ما يتعلق بكون النظام مؤكدًا – توفر النظام، استمرارية الخدمة، الموثوقية، الأمن والصيانة– وبتوفر هذه الخصائص حالياً ومستقبلياً في المنظمة .

كما يمكن التفريق بين الأنواع التالية: (أبو الهيجاء، ٢٠١٧، ٥٠: ٥٥) (أبو شيبة، ٢٠١٧، ٨٠: ٩٨)

١- التدقيق حول الحاسوب

يقوم المدقق في هذا النوع من التدقيق بتجاهل الحاسب كليًا، ويقوم بتشغيل عملية مجموعة عمليات من بدايتها إلى نهايتها يدوياً من خلال الحصول على المستندات الأصلية لها، ثم يقوم بمقارنة مخرجاته بمخرجات التشغيل الإلكتروني للمؤسسة؛

٢- التدقيق باستخدام الحاسوب

ويتضمن هذا النوع من التدقيق فحص واختبار إجراءات الرقابة الآلية والوضعية للنظام الآلي للتحقق من مدى كفايتها وسلامتها، وتوجد عدة أساليب لهذا النوع من التدقيق:

- يمكن للمدقق إعداد مجموعة من العمليات الصورية المشابهة لعمليات المنظمة الفعلية، ويقوم بتشغيلها بواسطة أجهزة وبرامج المؤسسة، وذلك بهدف تقييم إجراءات الرقابة الوضعية التي تدخل في تصميم برامج المؤسسة؛
- طريقة برامج الرقابة: والتي تتطلب من المدقق أن يقوم بإعداد برامج مشابهة لبرامج المؤسسة، ويقوم بتشغيل العمليات الفعلية للمؤسسة ومقارنة النتائج، وذلك بهدف اختبار قدرة برامج المنظمة على إنتاج بيانات دقيقة وكذلك لضمان عدم إمكانية تعديل بيانات المؤسسة؛
- طريقة برامج التدقيق العامة: تعد برامج التدقيق العامة برامج قادرة على أداء بعض إجراءات التدقيق، ومن أهم عمليات هذه البرامج المحاكاة المتوازية والتي تتمثل في استخدام نفس الملفات الرئيسية ونفس ملفات العمليات وإنتاج نفس المخرجات، ومقارنة مخرجات عملية المحاكاة بالمخرجات الفعلية؛

٣- التدقيق خلال الحاسوب

وتتضمن إجراءاته التدقيق على عملية تشغيل البيانات داخل الحاسب وتدقيق المدخلات والمخرجات، حيث يقوم المدقق بالتأكد من صحة المدخلات وعملية التشغيل وصحة المخرجات.

١/١/٦ خصائص بيئة تدقيق أنظمة تكنولوجيا المعلومات والاتصال

تتميز بيئة تدقيق أنظمة تكنولوجيا المعلومات والاتصال بمجموعة من الخصائص يمكن تلخيصها في الآتي:

أولًا: الرقابة الداخلية وتقييم المخاطر

١- الرقابة الداخلية في بيئة تكنولوجيا المعلومات والاتصال

تتميز الرقابة الداخلية في بيئة تكنولوجيا المعلومات والاتصال بأنها تشمل مجموعة من الإجراءات اليدوية وأخرى مصممة في برامج الحاسوب، وتتزايد أهمية الرقابة الداخلية لأنظمة تكنولوجيا المعلومات والاتصال نظرًا لتعدد المخاطر ما بين اختفاء السجلات المادية واختفاء سند التدقيق، وكذا مخاطر الغش والتلف الناتج عن الفيروسات، إضافة للمخاطر الناتجة عن عدم كفاءة العاملين وإهمالهم (الطيب، والصديق، ٢٠١٤، ١٤٤) (السعداوي، ٢٠١٧، ٣٢: ٣٨)

وتتميز الرقابة الداخلية في إطار أنظمة تكنولوجيا المعلومات والاتصال بما يلي:

(IFAC, ISA 315, 2013) (Alsaleem & Husin, 2023, 1: 24)

أ. يحتوي نظام الرقابة الداخلية على عناصر يدوية وأخرى آلية، وتؤثر خصائص العناصر اليدوية والآلية على تقييم المخاطر ونوعية الإجراءات المتبعة؛

ب. يمكن للمؤسسة أن تستخدم إجراءات آلية في مباشرة وتسجيل ومعالجة وإعداد التقارير حول المعاملات، وتحل السجلات الإلكترونية في هذه الحالة محل السجلات الورقية؛

د. إن استخدام المنظمة لإجراءات رقابية يدوية وأخرى آلية، يختلف حسب نوع المنظمة ودرجة اعتمادها على تكنولوجيا المعلومات، ولكل من هذين النوعين مخاطر خاصة، حيث تنتج عن الإجراءات الآلية مخاطر الوصول غير المصرح به، وكذا التغيير غير المصرح في البرامج والأنظمة، وتلف البيانات والأنظمة، بينما تتميز بضمان اتساق الإجراءات والقواعد المحددة سلفًا، وضمان تدفق المعلومات وزيادة القدرة على تطبيق فصل المهام من خلال عناصر الأمن والرقابة في التطبيقات وقواعد البيانات والأنظمة التشغيلية؛

ذ. تتمثل برامج الرقابة العامة على تكنولوجيا المعلومات في السياسات والإجراءات التي تتعلق بالتطبيقات وتدعم العمل الفعال لعناصر الرقابة عليها، وتحافظ على نزاهة المعلومات وأمن البيانات، ويمكن أن تكون هذه البرامج وقائية تحتاط من الأخطاء أو استكشافية لمعرفة المخاطر التي وقعت؛

ر. يؤدي الاعتماد على الأنظمة الآلية لتشغيل البيانات إلى دمج الكثير من العمليات اليدوية في خطوة واحدة، مما يؤدي لضعف الرقابة الناتجة عن فصل المهام، وتفرض زيادة وإحكام الإجراءات الرقابية للتحكم الجيد في المخاطر. (الوردات، ٢٠١٩، ٢٦٠)

٢- المخاطر في بيئة تكنولوجيا المعلومات والاتصال

إن أنظمة تكنولوجيا المعلومات والاتصال تنتج المزيد من المخاطر التي تتمثل في: (الوردات، ٢٠١٩، ٢٦٢) (دلال، والفتال، ٢٠١٩، ٢٣ :٣٠)

أ. **مخاطر تطبيقات الأعمال:** والتي تنتج عن صحة وتكامل البيانات التي يتم تبادلها بين الأطراف المختلفة، خاصة وأن هذه الأطراف لا تكون بينها معرفة في الغالب؛

ب.**مخاطر تكامل العمليات:** وتشير إلى تعرض المستخدم لمخاطر تغير أو فقدان البيانات أو ازدواجها عند التنفيذ، أو التشغيل غير الصحيح للبيانات نتيجة لضعف الإجراءات الرقابية؛ أي المخاطر الناتجة عن تغير بيانات عند تغيير أو تعديل ملفات أخرى نتيجة لضعف الرقابة؛

ج. **مخاطر حماية المعلومات:** وتنتج هذه المخاطر عن انتهاك سرية البيانات المتبادلة باستخدام شبكة الإنترنت.

وقد تناول الباحث هذه المخاطر بالتفصيل في المبحث الثاني المتعلق بمخاطر نظم المعلومات الإلكترونية.

٣- مراحل تقييم المخاطر في بيئة أنظمة تكنولوجيا المعلومات والاتصال

يمكن اعتبار مراحل وأساليب تقييم المخاطر في أنظمة تكنولوجيا المعلومات والاتصال حلقات تتضمن مستويات مختلفة للرقابة، حيث إذا ما أخفق المستوى الحالي في درء الخطأ انتقل للمستوى الموالي، وتتمثل هذه المستويات فيمايلي: (حسين، ٢٠٢٠، ١: ٧٢)

أ. **مرحلة منع وقوع الخطر:** ويعد الهدف الرئيسي للرقابة في هذا المستوى هو تجنب حدوث الخطأ؛

ب.**مرحلة اكتشاف الخطر:** في هذه المرحلة يكون الهدف هو تصميم الطرق الخاصة بمراقبة المخاطر المحتملة والتقرير عنها للمسؤولين؛

ج. **مرحلة الحد من الآثار الناتجة عن الخطر:** عند وقوع الخطر يكون الهدف هو تقليل الخسائر الناتجة عنه لأقصى قدر ممكن، ومثال ذلك قيام المنظمة بحفظ ملفات احتياطية عن الملفات الرئيسية لتخفيض الخسائر الناتجة عن وقوع خطر تلف الملفات الأصلية؛

د. **مرحلة التحري والتحقق:** في هذه المرحلة يتم القيام بتحقيقات لمعرفة سبب وقوع الخطر بهدف الإفادة بمعلومات مفيدة في وضع سياسة الأمن المتعلقة بالأنظمة.

ثانيًا: التوثيق

يتمثل التوثيق في تسجيل إجراءات عملية التدقيق المنفذة والأدلة المناسبة التي تم الحصول عليها، والاستنتاجات التي تم الوصول إليها، وتنص المعايير الدولية للتدقيق أنه على المدقق توثيق عمله من خلال توثيق مخطط مهمته وبرنامج التدقيق، طبيعة ومدى وتوقيت القيام بمهامه، الخصائص التي على أساسها ثم اختيار العناصر التي سيقوم بفحصها، تحديد نتائج إجراءات فحص هذه العناصر، ومختلف

المشكلات والقضايا ذات الأهمية المتعلقة بالعناصر التي تم فحصها والنتائج التي تم الوصول إليها أثناء عملية التدقيق. (IFAC, ISA 230, ٢٠٠٩)

وتظهر ميزة التوثيق في بيئة تكنولوجيا المعلومات والاتصال بسبب اختفاء أو قلة المستندات والأدلة الورقية مما يؤدي لاختفاء مسار التدقيق، وعدم وجود أدلة توضح مراحل سير العمليات، حيث يصبح مسار معالجة العمليات داخل النظام وبالتالي فهو غير ملموس، وخاصة في حال وجود المستندات والقيام بالإدخال في مكان، ومعالجة المدخلات والحصول على المخرجات في مكان آخر. (الذيبة، وآخرون ٢٠١٤، ٣٤)

ومن جهة أخرى فإن الوثائق في أنظمة تكنولوجيا المعلومات والاتصال تنقسم إلى: (سليمان،٢٠١٧، ٧٠: ٧٥) (مانيش، وأخرون، ٢٠١٨، ٢٠ :٢٥)

١) **ملف الوثائق الرئيسية الكاملة:** وتمثل الأوراق التي لها علاقة بالنظام من أوامر تكوين فرق العمل، البرامج المكتوبة، والمخططات المنطقية لها، وانتهاء بالأمور المتعلقة بالتطبيق وأهمها رسالة تطبيق النظام؛

٢) **ملف تعليمات التشغيل:** وهو ملف يقوم بإعداده المبرمجون الذين قاموا بكتابة برامج النظام كل حسب البرامج التي ساهم فيها، ويسلم إلى مسؤول قسم التشغيل لأجل اتباعه؛

٣) **ملف تعليمات التثقيب:** وهو ملف يعده مصمم الأنظمة والمبرمجون ويتكون من تعليمات التثقيب والمراجعة لكافة المدخلات وبرامج التثقيب والمراجعة لكل نوع من أنواع المدخلات؛

٤) **ملف الرقابة:** ويقوم بإعداد هذا الملف مصمم الأنظمة والمبرمجون، ويتضمن التعليمات التي يجب أن يتبعها قسم الرقابة أثناء الدورة التشغيلية بداية من استلام المدخلات وحصرها وإعادة المرفوضات وتعقب ورودها مصححة إلى تسليم المخرجات للأشخاص الملائمين في الوقت المناسب؛

٥) **ملف المستفيدين:** يقوم بإعداده مصمم الأنظمة ويتضمن أساسًا كيفية ملء استمارات الإدخال والحالات والأوقات التي تُرفع بها إلى قسم الحاسب، إضافة إلى مختلف الإجراءات الرقابية كتدقيق نماذج من المخرجات وغيرها من الإجراءات ذات الأهمية في حسن سير النظام وفاعلية تشغيله.

١/١/٧ أهداف تدقيق أنظمة تكنولوجيا المعلومات والاتصال

لا تختلف أهداف تدقيق أنظمة تكنولوجيا المعلومات والاتصال عن الأهداف العامة للتدقيق، ولكن هذا النوع من التدقيق يتميز بمساهمته في تحقيق مجموعة من الأهداف والغايات الخاصة التي تتمحور أساسًا حول تقييم مدى مساهمة تكنولوجيا المعلومات والاتصال في خدمة أهداف المؤسسة.

إن الهدف الأساسي لتدقيق أنظمة تكنولوجيا المعلومات والاتصال هو توفير الحماية الكافية لأصول المؤسسة، وتختلف هذه الأصول بين: (Chris ,2015, 32: 35)

- البيانات بمختلف أنواعها بمفهومها الواسع وما يتعلق بها من أنظمة التوثيق وغيرها؛
- انظمة التشغيل اليدوية والإلكترونية؛

- التكنولوجيا المستعملة فى المنظمة بما تتضمنه من معدات، وأنظمة العمليات، وأنظمة تسيير قواعد البيانات، وأنظمة الاتصال، والوسائط المتعددة المستعملة فى إنجاز العمليات وفى الاتصال؛
- الأفراد وما يمتلكونه من مهارات ووعي وإنتاجية تمكنهم من تخطيط، وبرمجة، اكتساب ونقل ودعم ومراقبة أنظمة المعلومات والخدمات المتعلقة بها.

بصفة عامة يهدف تدقيق أنظمة تكنولوجيا المعلومات والاتصال إلى تحقيق مجموعة من الأهداف هى: (Bradford, M., et al,2020, 521: 547)

أ. **الاقتصاد:** ويتمثل هذا الهدف في سعى المدقق لفحص استخدام الحاسب وذلك للتأكد من أن التكنولوجيا تستخدم بأقصى طاقة ممكنة لخدمة المنظمة وبأقل التكاليف الممكنة، وتوفر المعلومات والبيانات المطلوبة في الوقت المناسب مما يعود بالمنفعة على المؤسسة؛

ب. **الفعالية:** ويكون هدف المدقق فحص فعالية الأدوات الرقابية للتأكد من كفاءة نظام الرقابة الداخلية في جميع الأنشطة والوظائف الإدارية والمالية والتشغيلية؛

ج. **الكفاية:** أي أنه يجب على المدقق أن يتحقق من استخدام التكنولوجيا لتلبية المتطلبات الأكثر أهمية بالنسبة للمؤسسة، وذلك حسب مبدأ الأهمية النسبية؛

د. **الحماية:** ويعني هذا الهدف أن يتأكد المدقق من حماية نظام تكنولوجيا المعلومات والاتصال من مختلف المخاطر المرافقة لاستخدامه، كانهيار النظام وفقدان البيانات المخزنة على الأقراص ومشكلات الفيروسات وتلف وسرقة البيانات، أو التخريب المتعمد الذي قد تتعرض له النظم لتغطية المخالفات التي قد يرتكبها بعض العاملين.

كما يمكن تحديد أهداف تدقيق أنظمة تكنولوجيا المعلومات والاتصال من خلال مجال اهتمام المدقق كما يلي: (كراسنة، ٢٠١٧، ٢٠: ٢٥) (الظاظا، ٢٠١٦، ١٥: ١٧)

أ. **التطبيق:** ويعني هذا الهدف أن يتأكد المدقق من وجود الضوابط الرقابية لتقديم تأكيد معقول بأن عمليات المنظمة تامة وصحيحة ومسجلة بشكل ووقت ملائمين؛

ب. **التطوير:** حيث يهدف تدقيق أنظمة تكنولوجيا المعلومات والاتصال إلى المساهمة في تطوير الأنظمة قبل وبعد تنفيذها، لضمان احتوائها على ضوابط رقابية ملائمة، وضمان تلبية اهتمامات المنظمة وإدماجها في النظام؛

ج. **العمليات التشغيلية:** ويتضمن هذا الهدف الاهتمام بالبيئة الرقابية، واستدراك أي نقص أو ضعف في أنظمة الرقابة العامة لتفادي التأثيرات السلبية على مختلف أنشطة ووظائف المؤسسة؛

د. **الإدارة:** يركز هذا الهدف على الاهتمام بتقييم البيئة الرقابية الشاملة وتنظيم نظم المعلومات، وتقييم نقاط الضعف التى يمكن أن تؤثر على مختلف التطبيقات خاصة في الجانب الإدارى؛

هـ. **التكنولوجيا:** حيث يهدف تدقيق أنظمة تكنولوجيا المعلومات والاتصال إلى تدقيق تكنولوجيا معينة تستخدم في النظام، وذلك بغرض التقييم العام لبيئة الرقابة.

١/١/٨ أهمية تدقيق أنظمة تكنولوجيا المعلومات والاتصال

تظهر أهمية تدقيق أنظمة تكنولوجيا المعلومات والاتصال من خلال تزايد دور المدقق في المنظمة نتيجة لإدماج التكنولوجيا في مختلف أنشطة وإدارات المؤسسة، مما أضاف للمدقق دورًا جديدًا نتيجة للتشغيل الإلكتروني لأغلب البيانات والمعاملات التي سيتم تشغيلها، حيث أصبح من الضروري على المدقق أن يكون ملمًا بالأنظمة الموضوعة وأن يشترك في تصميمه لتقييم النظام ومعرفة نقاط القوة والضعف فيه، والإلمام بأنواع المخاطر التي تنتج عن التكنولوجيا.

كما تتضح أهمية تدقيق أنظمة تكنولوجيا المعلومات والاتصال من خلال كونه ضروريًا لفهم عناصر ومكونات تكنولوجيا المعلومات والاتصال، وآلية مهمة تعمل على إيجاد قيمة للتكنولوجيا في المؤسسة، وتقليل المخاطر الناتجة عنها، والإلمام بمختلف الجوانب المتعلقة بالتكنولوجيا في المؤسسة، وقياس مدى نضج التقنية في المنظمة والسماح للإدارة بمعرفة مدى توافق الممارسات المتعلقة بتكنولوجيا المعلومات والاتصال في المنظمة مع المعايير والأطر المتعارف عليها دوليًا. (أبوشيبة، والفطيمي، ٢٠١٧، ١: ٢٠).

وتتزايد أهمية تدقيق أنظمة تكنولوجيا المعلومات والاتصال بسبب الإنفاق الكبير للمؤسسات على الجوانب التقنية، مما يزيد من حاجتها لضمان اتساق الأنظمة وأمنها ضد التهديدات والهجمات المختلفة. (الذيبه وآخرون، ٢٢٣؛ ٢٢٥) (كرسوع، ٢٠٢٣، ٣٠: ٤٩) (Slapnicar,2022, 1: 21)

١/١/٩ مهام مدقق أنظمة تكنولوجيا المعلومات والاتصال

يقوم مدقق أنظمة تكنولوجيا المعلومات بجملة من المهام أهمها: (Alan &Taljanovic,٢٠١٣, ٢٨٩)

أ. تقويم نظم الرقابة الداخلية على المدخلات من ناحية تجهيزها وإدخالها في النظام، والبرامج التي تستعمل في التشغيل والمعالجة؛

ب. التأكد من سلامة وصلاحية البرامج المستعملة في معالجة المدخلات، وملاءمتها لتحقيق أهداف النظام، ويمكن له الاستعانة بأهل الخبرة والاختصاص في ذلك؛

ج. التأكد من صلاحية التجهيزات الخاصة بالتشغيل الإلكتروني بالبيانات من حيث سلامة التشغيل؛

د. التأكد من سلامة سبل وأساليب تحليل البيانات بواسطة الحاسب الآلي، وأنها تفي بالغرض المنشود؛

هـ. التأكد من سلامة نظم الحماية الخاصة بالبرامج والأجهزة المستعملة في تشغيل النظام، وانتظام عمليات الصيانة بشكل دوري، وكذا انتظام واستمرارية عمليات التحديث والتطوير لضمان كفاءة وفعالية مخرجات النظام؛

و. التأكد من سلامة ودقة نظام توزيع المعلومات وحمايتها وإمكانية استرجاعها، والتأكد من فعالية نظام التغذية العكسية؛

ز. التأكد من سلامة حفظ الملفات لحمايتها من أي تلاعب ممكن؛

ح. التأكد من أن التعديلات التي تتم على برامج التشغيل الإلكتروني للبيانات معتمدة من طرف له السلطة والتفويض الملائم، وأن هذه التعديلات موضوعية، ومتوافقة مع التطورات المستجدة في البيئة الداخلية والخارجية.

١/١/١٠ الأطر القانونية ومعايير وأدلة تدقيق انظمة تكنولوجيا المعلومات والاتصال

يوفر إعلان ليما (INTOSAI 1977) الأساس العام للإطار القانوني الذي يحكم تدقيق تكنولوجيا المعلومات الذي تقوم به الأجهزة العليا للرقابة. وينص على أنه يجب تحديد إنشاء الأجهزة العليا للرقابة في الدستور ويمكن تحديد التفاصيل في التشريع، وفي الفقرة ٢٢ من إعلان ليما، يتم تقديم ولاية التدقيقات في مرافق معالجة البيانات الإلكترونية مع الجوانب الرئيسية لهذه التدقيقات. كما يمكن أن تكون هناك ولايات خاصة للأجهزة العليا لإجراء تدقيقات تكنولوجيا المعلومات. كما تتضمن هذه الأطر القوانين الوطنية المتعلقة بأمن المعلومات أو الخصوصية، واستراتيجيات أمن المعلومات، وغيرها.

يخضع تدقيق أنظمة تكنولوجيا المعلومات والاتصال للمعايير المتعارف عليها بشكل عام في كافة أنواع التدقيق، ولكن الخصائص التي تتميز بها البيئة الرقابية لهذا النوع من التدقيق، وتميز أدلة الإثبات والجانب الإجرائي له، ألزم المنظمات الدولية المهتمة بالتدقيق بشكل عام بوضع إطار عام خاص بالمهنة من خلال إصدار مجموعة من المعايير والأدلة الإرشادية الخاصة بطبيعة هذا المجال . (Taherdoost, 2022, 1:20)

تلعب معايير وأدلة تدقيق تكنولوجيا المعلومات تلعب دورًا حاسمًا في توجيه المدققين وتوجيه جهودهم. فهي تقدم إطارًا موحدًا ومعايير مقبولة دوليًا لإجراء عمليات التدقيق بشكل كفء وفعّال.

بصفتها مرجعًا موثوقًا به، تسهم المعايير والأدلة أيضًا في توحيد الممارسات وتعزيز التواصل بين المدققين والجهات المعنية، وهذا يعزز الشفافية والثقة في نتائج التدقيق والتوصيات الناتجة عنه.

تشمل المعايير والأطر الدولية ذات الصلة بتدقيقات تكنولوجيا المعلومات التوجيهات الصادرة عن المنظمة الدولية للأجهزة العليا للرقابة (انتوساي)، مثل التوجيه ٥١٠٠ حول تدقيق نظم المعلومات (INTOSAI 5100:2019)، بالإضافة إلى كتيب WGITA IDI حول تدقيق تكنولوجيا المعلومات للأجهزة العليا للرقابة.(WGITA – IDI 2022)

يغطي كتيب WGITA IDI مواضيع تدقيق تكنولوجيا المعلومات وحوكمة تكنولوجيا المعلومات والتطوير والاستحواذ والعمليات والاستعانة بالخبرات الخارجية وخطة استمرارية الأعمال وخطة استعادة الكوارث وأمن المعلومات وضوابط التطبيق ومواضيع إضافية مهمة.

كما تتضمن الأطر كتيب تقييم أداء نظم المعلومات التي أصدرتها مجموعة تكنولوجيا المعلومات بمنظمة اليوروساي عام ٢٠٢٤.

قدمت ISACA أطر وأدلة مهمة حول تدقيقات تكنولوجيا المعلومات. يقدم إطار التدقيق التكنولوجي، ITAF الطبعة الرابعة (ISACA 2019) معايير تدقيق نظام المعلومات وضمن طبعاته السابقة – كذلك أدلةعلى تدقيق نظام المعلومات وأدوات وتقنيات التدقيق نظام المعلومات والضمان. نشرت ISACA عدة طبعات من إطار COBIT لحوكمة وإدارة المعلومات والتكنولوجيا.

يجب مراعاة هذه الأطر مع دلائل أخرى حول الأجهزة العليا للرقابة ومستويات التدقيق في فيها، مثل المبادئ الأساسية لتدقيق القطاع العام (ISSAI 100). كما تساعد التشريعات المتعلقة بالتدقيق المالي والأداء على فهم الشمول التكنولوجي والحاجة إلى مهارات التدقيق في تكنولوجيا المعلومات. على سبيل المثال، تكمل المبادئ الأساسية للتدقيق المالي (ISSAI 200)، ومبادئ تدقيق الأداء (ISSAI 300)، ومبادئ تدقيق الالتزام (ISSAI 400).

وتتمثل أهم المعايير والأدلة الأخرى فيمايلي:

أ. <u>إصدارات الإتحاد الدولي للمحاسبين</u>

قام الاتحاد من خلال مجلسه الفرعي (IAASB) "مجلس معايير التدقيق والتأكيد الدولي" بإصدار مجموعة من المعايير والبيانات كما يلي:

- المعيار الدولي للتدقيق (ISA ٤٠١) "التدقيق في بيئة أنظمة معلومات تستعمل الحاسوب"
- المعيار الدولي(ISA ٣١٥) (المنقح) الموسوم بـ: "تحديد وتقييم مخاطر الأخطاء الجوهرية من خلال فهم المنظمة وبيئتها "
- المعيار الدولي (ISA ٤٠٠) تقييم المخاطر والرقابة الداخلية
- المعيار (ISA ٣٣٠) "استجابة المدقق للمخاطر التي تم تقييمها "

ب. <u>بيانات اللجنة الدولية لمهنة التدقيق</u>:

قامت هذه اللجنة بإصدار أربعة معايير أساسية هي:

- البيان ١٠٠١: بيئة أنظمة المعلومات المحوسبة– الحواسيب الشخصية المستقلة
- البيان ١٠٠٢: بيئة أنظمة المعلومات المحوسبة – أنظمة الحواسيب المباشرة
- البيان ١٠٠٣: بيئة أنظمة المعلومات المحوسبة– أنظمة قاعدة البيانات
- البيان ١٠٠٨: تقدير المخاطر والضبط الداخلي خواص واعتبارات لأنظمة معلومات تستخدم الحاسوب
- البيان ١٠٠٩: طرق التدقيق بواسطة الحاسوب

ج. <u>إصدارات المنظمة الدولية للتقييس (ISO)</u>

تعد المنظمة الدولية للتقييس (Intrenational Organisation for Standardization) منظمة دولية وتقوم بإصدار معايير تمنح المواصفات العالمية للمنتجات والخدمات والأنظمة لضمان الجودة والسلامة والكفاء (الصرن، ٢٠٢١، ٢٥١: ٢٦٠)

(Alan & Steve, 2013, 65: 75) ، وقامت هذه المنظمة بتطوير العديد من المعايير ذات الصلة بتدقيق تكنولوجيا المعلومات ومنها:

- ISO9000: أنظمة الجودة
- ISO31000: إدارة المخاطر
- ISO38500: لحوكمة تكنولوجيا المعلومات
- ISO27002 / ISO 27001 / ISO 27000 لأمن المعلومات
- ISO 27006 لمتطلبات الجهة المقدمة للتدقيق
- ISO 27007 إرشادات لتدقيق أنظمة إدارة أمن المعلومات
- ISO 27008 إرشادات للمراجعين حول ضوابط نظم إدارة أمن المعلومات

د. منشورات متعلقة بتسيير المشروعات والرقابة الداخلية والحوكمة

- إصدار دليل PMBOK الدليل العملي لإدارة المشروعات.
- إصدار COSO للرقابة الداخلية. (IIA IPPF, 2017)
- إطار حوكمة تكنولوجيا المعلومات الخاص بأهداف التحكم في المعلومات والتكنولوجيا المتعلقة بها (COBIT). (ISACA, 2019, 20: 25)

وعلى المستوى الأوروبي، قامت منظمة EUROSAI بنشر تقارير تدقيق واستطلاعات قد تساعد في تنفيذ تدقيقات تكنولوجيا المعلومات في مختلف المجالات. أحد أهداف مجموعة العمل الأوروبية EUROSAI لتكنولوجيا المعلومات هو مساعدة أجهزة التدقيق الأوروبية في تدقيقاتها لتكنولوجيا المعلومات.

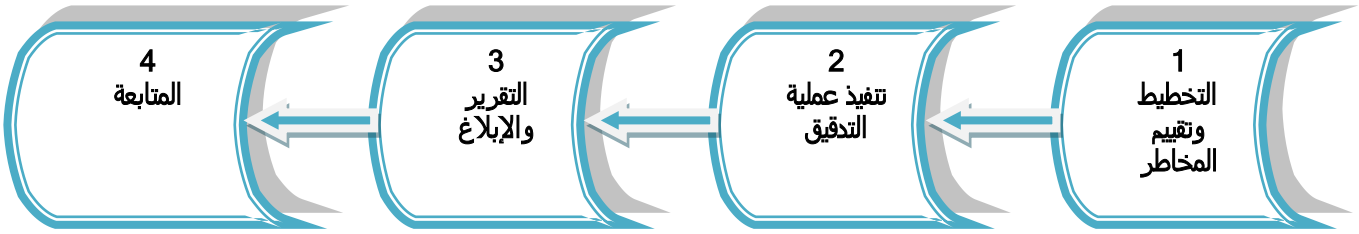
كذلك قامت الوكالة الأوروبية لأمن المعلوماتية (ENISA) بنشر إرشادات ودراسات قد تكون ذات صلة بتدقيقات تكنولوجيا المعلومات.(EUROSAI ITWG, 2023)

وعلى المستوى العربي قامت منظمة أرابوساي من خلال لجنة الرقابة على تكنولوجيا المعلومات بإبرام مذكرة تعاون مع مجموعة عمل اليوروساي لتكنولوجيا المعلومات لتبادل المعارف والخبرات والمشروعات المشتركة في مجال تدقيق تكنولوجيا المعلومات، بالإضافة إلى قيامها بعقد ندوة علمية عن تكنولوجيا المعلومات على هامش الاجتماع الثالث للجنة الرقابة على تكنولوجيا المعلومات الذي عقد في تونس في أكتوبر ٢٠٢٣، وقيام منظمة أرابوساي بعقد مؤتمر علمي عن الأساليب الحديثة في الرقابة على الأنظمة المعلوماتية والذي استضافة الجهاز المركزي للمحاسبات في القاهرة في يوليو ٢٠٢٤,

١/١/١١ مسار تدقيق أنظمة تكنولوجيا المعلومات والاتصال

يجب على المدقق قبل الشروع في التدقيق أن يأخذ بالاعتبار تحضير عملية اختيار المحاور الجوهرية لعملية التدقيق، وفهم البيئة المعلوماتية للمؤسسة والتأقلم معها، وفهم وتحليل البيانات في إطار القانون، والأخذ بالاعتبار استرجاع المعلومات والتنبه لمخاطر البرمجيات. (جمعة، ٢٠١٩، ٢٩: ٣٠)

شكل رقم (٣) يوضح مسار تدقيق تكنولوجيا المعلومات



المصدر: من إعداد الباحث

ويتضمن المسار العام لتدقيق أنظمة تكنولوجيا المعلومات والاتصال مجموعة من الخطوات التي تظهر كما يلي:

أولًا: التخطيط وتقييم المخاطر

يُعتبر تخطيط التدقيق في تكنولوجيا المعلومات أهم مرحلة، نظرًا لكون هذه الخطوة تحدد المسار العام لعملية التدقيق، وتضمن القيام بالمهمة بجودة عالية، وبطريقة اقتصادية، وفعالة وكفؤة، ومتوافقاً مع أهداف المنظمة، فهو مرحلة حاسمة تؤسس لتقييم ناجح لبنية المنظمة التحتية لتكنولوجيا المعلومات والعمليات والضوابط.

يتضمن تخطيط تدقيق أنظمة تكنولوجيا المعلومات، **التدقيق الاستراتيجي** وهو تخطيط طويل الأمد يضعه الجهاز الأعلى للرقابة في الدولة، **التخطيط الكلي** وهي مخططات يقوم بها المدقق لعمليات التدقيق التي يقوم بها خلال السنة، **والتدقيق الجزئي** وهو التخطيط لكل عملية على حدة.

وفيما يلي نظرة عامة على عملية التخطيط، أنواع التخطيط، تقييم المخاطر، ومفهوم التدقيق القائم على المخاطر (INTOSAI WGITA, IDI, 2022, 9: 14).

أ. أنواع التخطيط

تتضمن عملية التخطيط الأنواع التالية: (محمد، ٢٠١٧، ٥٨: ٦٥)

١. التخطيط الأولي

- **تحديد الأهداف:** تحديد غرض التدقيق، ويشمل ذلك فهم الأهداف التجارية والأهداف المحددة لتدقيق تكنولوجيا المعلومات.
- **تحديد النطاق:** تحديد حدود التدقيق، ويتضمن ذلك تحديد الأنظمة والعمليات والإدارات التي سيتم تدقيقها.
- **تخصيص الموارد:** تخصيص الموارد اللازمة، بما في ذلك أعضاء فريق التدقيق والأدوات والتقنيات المطلوبة للتدقيق.

٢. **التخطيط التفصيلي**

- **تقييم المخاطر:** إجراء تقييم تفصيلي للمخاطر لتحديد الأولويات.
- **تطوير برنامج التدقيق:** إنشاء خطة منظمة توضح إجراءات التدقيق والجداول الزمنية والمعالم الرئيسية.
- **جمع المعلومات:** جمع الوثائق ذات الصلة، مثل سياسات تكنولوجيا المعلومات، والإجراءات، وتقارير التدقيق السابقة، ومحاضر الاجتماعات، والمتطلبات التنظيمية، وصف الحالة التقنية للمؤسسة ومختلف التطورات فيها، الاطلاع على العقود المتعلقة بالاستفادة من خدمات الطرف الثالث.

٣. **تخطيط الاتصال**

- **مشاركة الأطراف المعنية:** تحديد الأطراف الرئيسية وإبلاغهم بخطة التدقيق والأهداف والتوقعات.
- **تنسيق الاجتماعات:** جدولة الاجتماعات مع الأطراف المعنية لمناقشة خطة التدقيق ومعالجة أي مخاوف.

ب. <u>تقييم المخاطر</u>

يُعد تقييم المخاطر جزءاً مهمًا من عملية تخطيط التدقيق في تكنولوجيا المعلومات، ويتضمن ذلك تحديد التهديدات المحتملة لبيئة تكنولوجيا المعلومات وتقييم تأثيرها المحتمل واحتمال حدوثها، ويتضمن ذلك مايلي: (INTOSAI WGITA, IDI, 2022, 9: 14) (بالقاسم، وحسين، ٢٠١٧، ٢٥: ٥٥)

١. **تحديد المخاطر:** تحديد المخاطر المتعلقة بأنظمة تكنولوجيا المعلومات، مثل خروقات البيانات، وفشل النظام، وعدم الامتثال للأنظمة.
٢. **تقييم التأثير والاحتمال:** تقييم التأثير المحتمل لكل خطر على عمليات المنظمة واحتمال حدوثه.
٣. **تحديد الأولويات:** تصنيف المخاطر بناءً على تأثيرها وتقييم احتمالها للتركيز على التهديدات الأكثر أهمية.
٤. **استراتيجيات التخفيف:** تحديد الضوابط والاستراتيجيات القائمة للحد من هذه المخاطر.

ج. <u>التدقيق القائم على المخاطر</u>

يركز نهج التدقيق القائم على المخاطر على تحديد الأولويات لأنشطة التدقيق بناءً على مستوى المخاطر. يضمن هذا النهج تخصيص موارد التدقيق للمناطق ذات الأهمية الكبرى، ويشمل ذلك: (حسن، ٢٠١٧، ٣٠: ٣٥)

١. **تقييم المخاطر:** إجراء تقييم شامل للمخاطر لتحديد وتقييم المخاطر.
٢. **تخطيط التدقيق:** تطوير خطة التدقيق بناءً على المخاطر المحددة، مع التركيز على المناطق عالية المخاطر.

٣. **تقييم الضوابط:** تقييم فعالية الضوابط الموجودة في تخفيف المخاطر المحددة.
٤. **إجراءات التدقيق:** تصميم إجراءات التدقيق التي تستهدف المناطق عالية المخاطر، لضمان فحص دقيق للضوابط والعمليات الحيوية.
٥. **التقرير:** تقديم نتائج وتوصيات مفصلة، مع التركيز على المناطق التي لم تُدار فيها المخاطر بشكل كافٍ.

د. تصميم التدقيق

يمكن اعتبار تصميم التدقيق جزءًا من مرحلة التخطيط لتدقيق تكنولوجيا المعلومات. يتضمن ذلك تطوير نهج منظم لكيفية إجراء التدقيق. ويتداخل ذلك في كافة إجراءات التخطيط السابقة، وفيما يلي العناصر التي تقع عادةً ضمن تصميم التدقيق في مرحلة التخطيط (INTOSAI WGITA, IDI, 2022, 14: 17)

١. **تحديد الأهداف:** توضيح ما يسعى التدقيق لتحقيقه بشكل واضح.
٢. **تحديد النطاق:** تحديد المناطق والأنظمة والعمليات التي سيتم فحصها، ويكون ذلك على أساس الحاجة ووفقًا لعمليات الفحص الأولية المنفذة، ويتضمن نطاق التدقيق أنظمة الرقابة المتعلقة باستعمال وحماية موارد تكنولوجيا المعلومات والاتصال بمفهومها الواسع، والتي تضم البيانات، أنظمة التشغيل، التكنولوجيا، الترخيصات، الأشخاص وحوكمة تكنولوجيا المعلومات؛ وغير ذلك من الأمور المرتبطة بتكنولوجيا المعلومات.
٣. **تقييم المخاطر:** تقييم المخاطر المحتملة لتحديد أولويات مناطق التركيز.
٤. **تطوير المنهجية:** وضع الأساليب والإجراءات التي سيتم استخدامها لجمع وتحليل البيانات.
٥. **تخصيص الموارد:** تحديد الأفراد والأدوات والتقنيات المطلوبة للتدقيق.
٦. **تحديد الجدول الزمني والمعالم الرئيسية:** تحديد جدول زمني مع المواعيد النهائية والمعالم الرئيسية .
٧. **إنشاء برنامج التدقيق:** صياغة برنامج تدقيق مفصل يحدد الخطوات والإجراءات لإجراء التدقيق.

يتضمن التخطيط الفعال لتدقيق تكنولوجيا المعلومات تخطيطاً أولياً وتفصيلياً شاملاً، وتقييماً شاملاً للمخاطر، وتبني نهج التدقيق القائم على المخاطر، ومن خلال التركيز على المناطق عالية المخاطر وضمان التواصل القوي مع الأطراف المعنية، ويضمن ذلك تصميم التدقيق بحيث يكون منهجيًا وشاملاً ومنظمًا وفعالًا ومتوافقًا مع أهداف المنظمة ومخاطرها، ويحمي أصولها التكنولوجية والمعلوماتية.

ثانيًا: تنفيذ عملية التدقيق

إن تنفيذ عملية التدقيق يمر عبر مجموعة من المراحل الأساسية والمتمثلة في جمع الأدلة، المعاينات والزيارات الميدانية لتنتهي بالتقرير الأولي ثم التقرير النهائي. وتتضمن هذه المراحل إجراءات فحص

وتقييم نظام الرقابة الداخلية وجمع البيانات والمعلومات الأكثر تفصيلًا لتحديد نواحي الضعف الهامة والتي يركز عليها المدقق في اختباراته.

ويمكن توضيح هذه الخطوات كما يلي: (INTOSAI, WGITA, IDI, 2022, 18:22) (البري، ٢٠٢٣، ٤٥: ٥٥) (أبو عمرو، ٢٠٢٣، ٣١: ٣٥) (جمعة، ٢٠١٩، ٣٠: ٣٥)

أ. جمع أدلة التدقيق

يقوم المدقق بجمع الأدلة قبل مرحلة الزيارة الميدانية للمؤسسة، وتتضمن هذه المرحلة الفحص المعمق للسياسات والإجراءات المتعلقة بالمجالات التي تم تحديدها في نطاق التدقيق ليتم تدقيقها، ويشمل ذلك الوثائق الخاصة بسياسات حماية البيانات، الدليل العملي للإجراءات المتعلقة بالبيانات الحساسة، نماذج التدريب على حماية البيانات، سجلات المخاطر، سجلات الأصول المتعلقة بالمعلومات، بنية حوكمة المعلومات وغيرها.

ويهدف هذا الإجراء للتأكد، من أن المرحلة الموالية المتمثلة في الزيارة الميدانية ستكون فعالة وذلك من خلال تحديد الأشخاص الذين سيتم استجوابهم والعمليات التي سيتم فحصها؛

ب. الزيارة الميدانية

تأخذ هذه المرحلة عادة يومين إلى ثلاثة أيام من وقت المهمة، وتبدأ الزيارة الميدانية بالاجتماع مع أعضاء مجلس الإدارة من أجل أن يتم شرح عملية التدقيق لهم ولتتم مناقشة المشاكل والقضايا المتعلقة بالتدقيق والإجابة على الأسئلة التى لديهم حول عملية تدقيق أنظمة تكنولوجيا المعلومات.

كما يتم خلال هذه المرحلة القيام بعدة إجراءات للحصول على أدلة الإثبات، وهي تتعدد ما بين:

١. **التقييم الأولي لضوابط تكنولوجيا المعلومات:** وتشمل الضوابط العامة وضوابط التطبيقات لاستنباط فهم للتأكيد على أنها موثوقة وكافية لتحقيق هدف التدقيق.
٢. **الاختبارات الموضوعية:** بناء على تقييم الضوابط، قد يحدد المدققون المجالات ذات الأولوية للاختبارات الموضوعية والتي تتضمن اختبارات تفصيلية للضوابط.
٣. **الفحص المادي:** ويقصد به عملية الجرد أو الفحص الفعلي الذي يقوم به المدقق على الأصول الملموسة للمؤسسة؛
٤. **المصادقات:** ويقصد بها أن يتم جمع الأدلة من مصدر آخر غير المنظمة محل التدقيق، وهو ما يصطلح بالطرف الثالث، حيث يرسل إليه المدقق المعلومات التى يريد التأكد منها، ليقوم هذا الطرف بالمصادقة عليها أو نفيها؛
٥. **التثبت:** ويقصد به فحص مستندات ووثائق المؤسسة؛
٦. **الإجراءات التحليلية:** وتتمثل الإجرءات التحليلية في القيام بمقارنات وعلاقات لتحديد منطقية معلومة ما؛

٧. **الاستفسار من العميل:** ويقصد به الحصول على معلومات من العميل، ويقصد بالعميل المنظمة محل الفحص، ويمكن في هذا الإطار استعمال موقع المنظمة أو البريد الإلكتروني للحصول على هذه المعلومات كوسيلة لاقتصاد الوقت والتكلفة؛

٨. **إعادة التشغيل:** ويقصد به أن يقوم المدقق بإعادة تشغيل جزء من النظام للحكم على كفاءة تشغيل النظام وفعالية الإجراءات الرقابية.

٩. **توثيق التدقيق:**هو سجل أعمال التدقيق المنفذة والأدلة الداعمة للنتائج والاستنتاجات، ويجب أن يتوافق مع متطلبات الموثوقية والاكتمال والكفاية والدقة.

يرى الباحث أن المرور بالمراحل السابقة يُمكن المدقق من التعرف على المشاكل الأساسية في أنظمة تكنولوجيا المعلومات والاتصال في المؤسسة.

ثالثًا: تقرير التدقيق والإبلاغ

تعتبر مرحلة التقرير والإبلاغ من أهم مراحل تدقيق تكنولوجيا المعلومات، حيث تختتم جهود التدقيق ويتم تقديم النتائج والتوصيات إلى أصحاب المصالح والجهات المعنية، ويُمثل التقرير المنتج النهائي لعملية التدقيق، كما يعد أداة اتصال وتبليغ نتائج التدقيق، ويشترط أن يكون هذا التبليغ يتضمن نتائج مهمة التدقيق، وأهدافها ونطاق عملية التدقيق والنتائج التي تم الوصول إليها، ويجب أن يتم تبليغ هذه النتائج بشكل دقيق، موضوعي، واضح، موحد، بنّاء وكامل، كما يجب أن تصدر في الوقت المناسب.

ونظرًا لخصوصية تدقيق أنظمة تكنولوجيا المعلومات والاتصال، لابد من احتواء تقرير مدقق أنظمة تكنولوجيا المعلومات على: (INTOSAI WGITA, IDI, 2022, 23:25)

أ. **بيان نطاق التدقيق:** حيث على المدقق أن يحدد بشكل دقيق ما هي المحاور الأساسية والمجالات التي تم فحصها وإدراجها بعملية التدقيق، كما يمكن توضيح ما هي المجالات التي لم يتم إدراجها في المهمة، وتساعد هذه الفقرة على تجاوز سوء الفهم؛

ب. **ملخص تنفيذي لعملية التدقيق:** يجب على مدقق تكنولوجيا المعلومات والاتصال كتابة ملخص تنفيذي يتضمن سرد القضايا المعالجة بالتفصيل وتوضيح مخططات العمل، ويقصد بسرد الملخص للقضايا تسليط الضوء على القضايا ذات المعنوية أو الأهمية النسبية مقارنة بغيرها. ويشترط في هذا الملخص أن يكون:

- معبرًا عن المهمة بحيث يتسنى لمن ليس لديه وقت لقراءة كافة التفاصيل الاعتماد عليه وفهم المهمة بشكل مجمل بما في ذلك الإجراءات الرقابية وبيئة العمل انطلاقًا من الملخص؛
- بمثابة وثيقة إعلامية للمطلع عليه حتى مع فصله عن بقية أجزاء التقرير؛
- يتضمن معلومات متعلقة بنتائج التدقيق بشكل عام؛

ج. **قائمة القضايا وخطط العمل:** تعد هذه القائمة العنصر الأساسي في التقرير، نظرًا لكونها تتضمن التفاصيل حول القضايا الهامة التي تم اكتشافها وما هي الإجراءات التي تتخذ لحلها. ويجب أن

يكون هذا العنصر مفهومًا بحيث يوفر فهما للأفراد الذين يتعاملون مع المجال الذي تم تدقيقه فهمًا مناسبًا للقضايا المدققة، كما يوفر لمجلس الإدارة معلومات حول المخاطر وأسباب الحاجة لتخفيفها؛

د. **عناصر إضافية (اختيارية):** توجد بعض العناصر الإضافية التي لا تعد أساسية في التقرير، ولكن قد تظهر الحاجة لسردها في التقرير، ويتعلق الأمر بـ:

- **الضوابط الرقابية الأساسية:** إذا لاحظ المدقق بعض الضوابط الرقابية ذات الأهمية في المنطقة أو المجال الذي تم تدقيقه، فيمكن له أن يوردها في التقرير مع المشكلة التي تمت معالجتها، وذلك لتشجيع الإجراءات الجيدة والتعليق على الضوابط غير الملائمة وذلك للفت انتباه المسؤولين لتحسينها؛
- **العناصر المغلقة:** إذا قامت المنظمة بحل بعض القضايا أثناء فترة التدقيق، تعتبر هذه العناصر مغلقة أي بمعنى أنه تمت معالجتها، وفي هذه الحالة لابد من الإشارة لها في التقرير وذلك تقديرًا للجهود الاستباقية للمؤسسة، وضمانًا لإعطاء التقرير صورة كاملة عن المشاكل في وقت عرضه؛
- **القضايا البسيطة:** قد يجد مدقق تكنولوجيا المعلومات والاتصال بعض القضايا أو المشاكل التي تعد بسيطة، أو لا تشكل خطرًا كبيرًا، وبالتالي ليس هناك داع لوضع خطط لها أو إصدار قرارات بشأنها، ولكن يمكن للمدقق إدراجها في التقرير على سبيل لفت الانتباه لها، وكنوع من إعلام المسيرين بها وترك القرار لهم.

إنّ إعداد التقرير الأولي لا يعني نشره بشكل مباشر، حيث يسمح المدقق للمؤسسة بالاطلاع على التقرير الأولي مع إمكانية تعليقهم عليه قبل صدوره، وبعد إعداد التقرير الأولي ومراجعته يمكن إصدار التقرير النهائي ورفعه لمجلس الإدارة، أو للمجلس ولجنة التدقيق وذلك حسب الحالة.

رابعًا: المتابعة

تعد مرحلة المتابعة جزءًا حيويًا وأساسيًا من نجاح عملية تدقيق تكنولوجيا المعلومات حيث تضمن تنفيذ التوصيات المقدمة في تقرير التدقيق بشكل فعال ومعالجة أي قضايا تم تحديدها بشكل مناسب. تساعد هذه المرحلة في إغلاق دورة عملية التدقيق وتضمن التحسين المستمر في ضوابط وعمليات تكنولوجيا المعلومات في المنظمة، وأن المنظمة تحافظ على بيئة ضوابط قوية وفعالة. (INTOSAI WGITA, IDI, 2022, 23).

١/١/١٢ تأثير أنظمة تكنولوجيا المعلومات والاتصال على إجراءات التدقيق

حسب البيانين الدوليين ١٠٠١ و١٠٠٢ للتدقيق، فإن بيئة الحاسب تؤثر على إجراءات التدقيق كما يلي:

أ. إن بيئة الحاسب تجعل من الصعب والمكلف توفير الضوابط الرقابية الكافية، لذا فإن المدقق يفترض بأن مخاطر الرقابة عالية في هذه الحالة. ويجب في هذه الحالة عند تقدير المدقق للمخاطر أن يخطط لتقليل أخطاء الاكتشاف بما أن المخاطر الرقابية عالية. (كرسوع، ٢٠٢٣، ٣٠: ٤٩)

ب. إن من الملائم للمدقق في هذه الحالة أن يقوم بعد حصوله عل فهم بيئة الرقابة وتدفق المعاملات أن يركز على الاختبارات الجوهرية عند اقتراب أو في نهاية السنة المالية، وهو ما يتطلب زيادة الفحص المادي والمصادقات بالنسبة للموجودات، وكذلك زيادة الاختبارات التفصيلية وتوسيع حجم العينات، واستخدام طرق التدقيق باستخدام الحاسب كلما كان ذلك ممكنًا وملائمًا؛

ج. قد تتضمن طرق التدقيق باستخدام الحاسب استخدام المدقق برمجيات خاصة به، كما قد يستخدم برمجيات المنظمة ويقارن نتائج معالجة المعلومات، وقد يطور طريقة خاصة للتدقيق؛

د. تتضمن الإجراءات الرقابية التي يأخذها المدقق بعين الاعتبار: (طه، وأخرون، ٢٠١٦، ٢٧١: ٢٨٤) (علي، وشحاته، ٢٠١٥، ١٥: ٢٧) (مانيش، وأخرون، ٢٠١٨، ٤٣ :٤٥)

١) **الفصل بين المهام وضوابط الترصيد:** ويتضمن ذلك فصل المهام وتدويرها بين الموظفين، إضافة لمراجعة الإدارة للتقارير والجداول التي تحدد الموظفين المستخدمين للنظام والمهام الموكلة إليهم؛

٢) **الوصول إلى الحاسب والملفات:** ويتضمن ذلك وضع الحاسب على مرأى من الشخص المسؤول عن مراقبته وذلك لتسهيل وصوله إليه، واستخدام المفاتيح لإقفال الحاسب والأجهزة الفرعية، واستخدام كلمات السر لتقييد الوصول للبرامج وملفات البيانات، ووضع قيود على برامج المنفعة العامة. وينص البيان ١٠٠٢ للتدقيق على أن ضوابط الوصول للبيانات تهدف لاكتشاف ومنع أي وصول أو تغيير أو استخدام البيانات والبرامج بشكل غير مرخص؛

٣) **استخدام برمجيات الطرف الثالث:** عند شراء المنظمة لبرامج من طرف آخر، فإنه يجب القيام بفحص هذه البرامج قبل اقتنائها، والتأكد من وظائفها وسعتها وضوابطها، والاختيار الملائم للبرمجيات والتعديلات عليها قبل الاستخدام، كما يجب القيام بتقييم مستمر للبرمجيات للتأكد من وفائها بمتطلبات الزبائن؛

٤) **توفير ضوابط لتطوير وصيانة الأنظمة:** ويتضمن ذلك إجراءات التأكد من أن الضوابط الضرورية للتطبيقات المباشرة ككلمات السر وضوابط الوصول وتدقيق صحة البيانات المباشرة وإجراءات استئناف التشغيل، قد تم إدراجها ضمن النظام خلال تطويره وصيانته؛

٥) **توفير ضوابط البرمجة:** وتتضمن إجراءات مصممة لمنع أو اكتشاف تغييرات غير مناسبة لبرامج الحاسب، والتي تم الوصول إليها من خلال الأجهزة الفرعية المباشرة. وفي هذا الإطار ينبغي تقييد الوصول للبرامج وتوثيق كل التغييرات التي تطرأ على البرامج؛

هـ. هناك بعض الضوابط التطبيقية في أنظمة تكنولوجيا المعلومات والاتصال وهي:

١) **الترخيص السابق للمعالجة:** مثل استعمال البطاقة المصرفية مع رقم التعريف الشخصي قبل إجراء السحب النقدي من خلال الآلة؛

٢) **إجراء التدقيق بشكل دوري لمدخلات النظام ونتائج المعالجة:** للتأكد من اكتمال ودقة ومعقولية أدلة الإثبات والمعطيات المعالجة؛

٣) **إجراءات القطع:** وهي إجراءات للتأكد من أن العمليات قد تمت معالجتها في الفترة المحاسبية المناسبة؛

٤) **ضوابط الملفات:** وهي إجراءات خاصة تضمن استعمال ملفات البيانات الصحيحة في المعالجات المباشرة؛

٥) **ضوابط الملف الرئيسي:** حيث أن أهمية الملف الرئيسي تفرض إجراءات أكثر صرامة من بقية الملفات والمعالجات؛

٦) **الموازنة:** وهي إجراء لإنشاء مجاميع التحكم على البيانات المقسمة للمعالجة من خلال الأجهزة الفرعية المباشرة، ومقارنة مجاميع التحكم خلال وبعد المعالجة، لضمان انتقال البيانات بشكل كامل ودقيق، لكل مرحلة من مراحل المعالجة.

١/١/١٣ أدوات وتقنيات تدقيق تكنولوجيا المعلومات

يستخدم مدققو تكنولوجيا المعلومات بصفة عامة مجموعة متنوعة من الأدوات والتقنيات والبرامج لتدقيق تكنولوجيا المعلومات في الجهات الخاضعة لرقابتهم، منها على سبيل المثال: (غنيمي، ٢٠١٧، ٤٢٠: ٤٩٠) (Chris & others, 2015, 99: 120)

١. **أدوات مسح الضعف:** تستخدم لتحليل البنية التحتية للشبكة والأنظمة لتحديد الثغرات الأمنية المحتملة.

٢. **أدوات اختبار الاختراق:** يُستخدم لاختبار أمان النظم والتطبيقات من خلال تقليد هجمات حقيقية لتحديد الثغرات الأمنية وتقديم توصيات لتصحيحها.

٣. **أدوات مراقبة السلامة والأمان:** تُستخدم لمراقبة النشاطات غير المصرح بها والمطابقة لسياسات الأمان والتوجيهات القانونية.

٤. **أنظمة إدارة الحماية:** تقوم بإدارة ورصد الأمان والحماية من خلال تحليل السياسات والتقارير وتقديم توصيات لتحسينها.

٥. **أنظمة إدارة الحوادث والاستجابة للأمان:** تُستخدم للتعامل مع الحوادث الأمنية والتحقيق فيها واستجابتها بشكل فعال.

٦. **أنظمة مراقبة الوصول والتحقق من الهوية:** تستخدم لإدارة الوصول إلى البيانات والموارد بشكل آمن وفعال.

٧. **أدوات تحليل السجلات والمراقبة:** تستخدم لمراقبة وتحليل سجلات الأنشطة للكشف عن أنماط غير طبيعية أو مشتبه بها.

يرى الباحث أن هذه الأدوات والتقنيات المستخدمة تختلف بناءً على احتياجات التدقيق المحددة ومتطلبات الأمان لكل جهة.

١/١/١٤ مجالات تدقيق تكنولوجيا المعلومات

تشمل عملية تدقيق تكنولوجيا المعلومات مجموعة واسعة من المجالات التي تهدف إلى تقييم فعالية وكفاءة وضوابط نظم تكنولوجيا المعلومات في المنظمة. فيما يلي بعض مجالات التدقيق الأساسية:

(INTOSAI WGITA, IDI, 2022, 26: 95) (Pandzo &Taljanovic, 2013, 288: 294)

(الوردات، ٢٠١٩، ٦٥، ٧٠) (البري، ٢٠٢٣، ٢٠: ٢٨) (الظاظا، ٢٠١٦، ٢٢٠: ٢٣٠)

أ. أمن المعلومات والأمن السيبراني

يشير **أمن المعلومات** إلى مجموعة من التدابير والإجراءات التي تهدف إلى حماية المعلومات من التهديدات والمخاطر المحتملة، سواء كانت ذات طابع فعلي مثل الاختراقات والتسريبات، أو طابع غير فعلي مثل الأخطاء البشرية والطبيعية. ويهدف إلى ضمان سلامة وسرية المعلومات، سلامة الأنظمة، وتوفير الوصول المناسب للمستخدمين المخولين فقط.

بينما يشير **الأمن السيبراني** إلى فرع محدد من أمن المعلومات يركز بشكل خاص على حماية الأنظمة والشبكات الرقمية من الهجمات السيبرانية، والتي قد تشمل الاختراقات الإلكترونية، والبرمجيات الخبيثة، والتصيّد الاحتيالي، وغيرها من الهجمات عبر الإنترنت.

وبشكل عام، يعتبر الأمن السيبراني جزءًا من أمن المعلومات، حيث يركز على حماية البنية الرقمية والأنظمة من التهديدات الإلكترونية، بينما يشمل أمن المعلومات جميع الجوانب المتعلقة بالحفاظ على سلامة وسرية المعلومات بشكل عام.

إن تدقيق أمن المعلومات وتدقيق الأمن السيبراني يمكن أن يكونا جزءًا من تدقيق تكنولوجيا المعلومات، حيث يتم تقييم الأنظمة والتقنيات المستخدمة لحماية المعلومات والبيانات والأنظمة الرقمية في سياق أوسع.

فيركز**تدقيق تكنولوجيا المعلومات** على تقييم وتدقيق جميع جوانب التكنولوجيا المستخدمة في المؤسسة، ويشمل ذلك الأجهزة والبرمجيات والشبكات وأنظمة قواعد البيانات والتخزين وما إلى ذلك. ومن بين جوانب التكنولوجيا التي يتم تدقيقها يمكن أن تكون أمن المعلومات والأمن السيبراني جزءًا مهمًا.

ب. تدقيق عمليات تشغيل النظام

يركز تدقيق عمليات تشغيل النظام على تقييم كفاءة وفعالية العمليات التشغيلية للنظم المعلوماتية. ويشمل ذلك التحقق من:

- **أداء النظام:** التأكد من أن الأنظمة تعمل بكفاءة وتلبي احتياجات المستخدمين.
- **إدارة الحوادث:** تقييم كيفية التعامل مع الحوادث والمشاكل التقنية واستجابات الطوارئ.
- **إدارة النسخ الاحتياطي والاستعادة:** التحقق من وجود واستدامة إجراءات النسخ الاحتياطي واستعادة البيانات.
- **الأمن:** فحص الضوابط الأمنية المطبقة لحماية البيانات والمعلومات من الوصول غير المصرح به.

ج. تدقيق حوكمة تكنولوجيا المعلومات

يركز تدقيق حوكمة تكنولوجيا المعلومات على تقييم السياسات والإجراءات التي تحكم استخدام وإدارة تكنولوجيا المعلومات داخل المنظمة. ويشمل ذلك:

- **هيكل الحوكمة:** تقييم هيكل الحوكمة لتكنولوجيا المعلومات والتأكد من أنه يتماشى مع أهداف المنظمة.
- **إدارة المخاطر:** فحص العمليات المستخدمة لتحديد وتقييم وإدارة مخاطر تكنولوجيا المعلومات.
- **الامتثال:** التأكد من أن المنظمة تلتزم باللوائح والقوانين والمعايير ذات الصلة بتكنولوجيا المعلومات.
- **المساءلة والشفافية:** تقييم مدى وضوح الأدوار والمسؤوليات المتعلقة بتكنولوجيا المعلومات داخل المنظمة.

د. تدقيق الاستثمار في تكنولوجيا المعلومات

يهدف تدقيق الاستثمار في تكنولوجيا المعلومات إلى تقييم كيفية إدارة الموارد والاستثمارات في تكنولوجيا المعلومات لضمان تحقيق العائد المرجو منها. ويشمل ذلك:

- **تحليل التكلفة والفائدة:** التحقق من أن الاستثمارات في تكنولوجيا المعلومات تتم بعد إجراء تحليلات شاملة للتكلفة والفائدة.
- **إدارة المشاريع:** تقييم عمليات إدارة المشاريع لضمان تنفيذها ضمن الجدول الزمني والميزانية المحددة.
- **التخطيط الاستراتيجي:** فحص مدى توافق الاستثمارات في تكنولوجيا المعلومات مع الاستراتيجية العامة للمنظمة.
- **مراقبة الأداء:** التأكد من وجود آليات لمراقبة وتقييم أداء الاستثمارات في تكنولوجيا المعلومات لضمان تحقيق الأهداف المحددة.

هـ. تدقيق صيانة أنظمة تكنولوجيا المعلومات

يهدف تدقيق صيانة أنظمة المعلومات إلى تقييم العمليات والإجراءات المتعلقة بصيانة وتحديث النظم المعلوماتية. ويشمل ذلك:

- **إدارة التغيير**: تقييم العمليات المتبعة لإدارة تغييرات النظام والتأكد من أنها تتبع ممارسات معترف بها.
- **إجراءات التحديث والترقيات**: التحقق من أن عمليات التحديث والترقيات تتم بطريقة منهجية وآمنة.
- **الدعم الفني والصيانة**: فحص كيفية تقديم الدعم الفني والصيانة للنظم والتأكد من كفاءتها.
- **التوثيق**: التأكد من أن كافة عمليات الصيانة موثقة بشكل مناسب ومحدثة.

إن تدقيق مجالات تكنولوجيا المعلومات المختلفة، بما في ذلك أمن المعلومات والأمن السيبراني، يلعب دوراً حاسماً في تعزيز أمان وكفاءة وفعالية نظم تكنولوجيا المعلومات، مما يدعم تحقيق أهداف المنظمة.

١/١/١٥ دور الأجهزة العليا للرقابة في مجال تدقيق تكنولوجيا المعلومات

يتمثل دور الأجهزة العليا للرقابة في مجال تدقيق تكنولوجيا المعلومات في عدة جوانب أهمها مايلي:

(EUROSAI ITWG, 2023, Training course) (INTOSAI WGITA, IDI, 1: 9)

١. **وضع السياسات والتوجيهات**: تلعب الأجهزة العليا للرقابة دورًا مهمًا في وضع السياسات والتوجيهات المتعلقة بتدقيق تكنولوجيا المعلومات في المنظمات الحكومية. يتمثل هذا الدور في تحديد المعايير والمتطلبات الأمنية وتوجيه المؤسسات بشأن كيفية تطبيقها بشكل فعال.

٢. **المراجعة والتقييم**: تقوم الأجهزة العليا للرقابة بمراجعة وتقييم أداء المنظمات الحكومية في مجالات تدقيق تكنولوجيا المعلومات، ويشمل ذلك تقييم مدى الامتثال للسياسات والمعايير الأمنية وفعالية الإجراءات الأمنية المعمول بها.

٣. **توجيه الإصلاحات والتحسينات**: استنادًا إلى نتائج التقييمات والمراجعات، توجه الأجهزة العليا للرقابة الإصلاحات والتحسينات الضرورية في مجالات التدقيق الأمني في المؤسسات الحكومية، ويهدف ذلك إلى تعزيز الأمان السيبراني وحماية البيانات والأنظمة الحيوية للدولة.

٤. **التوجيه والدعم الفني**: تقدم الأجهزة العليا للرقابة التوجيه والدعم الفني للمؤسسات الحكومية في مجالات تدقيق تكنولوجيا المعلومات، ويشمل ذلك توفير المشورة والتوجيه الفني لتطبيق أفضل الممارسات واعتماد أحدث التقنيات الأمنية.

٥. **التوعية والتثقيف الأمني**: تقوم الأجهزة العليا للرقابة بدور هام في نشر الوعي الأمني والتثقيف بشأن أهمية التدقيق الأمني ومكافحة التهديدات السيبرانية، ويهدف ذلك إلى تعزيز الثقافة الأمنية داخل المؤسسات الحكومية وتعزيز قدرتها على التصدي للتهديدات الأمنية.

٦. **التنسيق بين الجهات الحكومية:** تلعب الأجهزة العليا للرقابة دورًا مهمًا في تعزيز التنسيق بين الجهات الحكومية المختلفة المعنية بالأمان السيبراني، مما يسهم في تحقيق الشمولية وتقليل الثغرات والتهديدات السيبرانية.

يرى الباحث أن الأجهزة العليا للرقابة تلعب دورًا حيويًا في ضمان أمان المعلومات والحفاظ على استقرار الأنظمة الحكومية، وتعزيز قدرتها على التصدي للتهديدات السيبرانية المتزايدة. وتحتاج هذه الجهات إلى التحديث المستمر والتعاون الوثيق مع المؤسسات الحكومية والقطاع الخاص لتحقيق أقصى استفادة من جهودها في هذا الصدد.

ويرى الباحث أنه لتعزيز قدرات الأجهزة العليا للرقابة في مجال تدقيق تكنولوجيا المعلومات، يمكن اتباع مايلي:

١. **تعزيز التخصص والكفاءة الفنية:** يجب توفير التدريب المناسب والتطوير المهني للموظفين في الأجهزة العليا للرقابة لتعزيز معرفتهم ومهاراتهم في مجالات تدقيق تكنولوجيا المعلومات وأمن المعلومات والأمن السيبراني.
٢. **استخدام التقنيات المتقدمة:** يجب توفير الموارد اللازمة لاعتماد واستخدام التقنيات الحديثة وأدوات التحليل الضخم لتعزيز فعالية عمليات التدقيق والرصد.
٣. **توفير التدريب والتطوير المهني المستمر:** لتعزيز القدرات المهنية للمدققين في مجال تدقيق تكنولوجيا المعلومات وأمن المعلومات والاستفادة من التكنولوجيا الحديثة في مجال الرقابة.
٤. **تعزيز الشراكات والتعاون:** يجب تعزيز التعاون مع الجهات الحكومية الأخرى والمؤسسات الأكاديمية، والمنظمات المهنية والأجهزة النظيرة والقطاع الخاص لتبادل المعرفة والخبرات وتطوير حلول مشتركة لتعزيز الأمن السيبراني.
٥. **تحسين البنية التحتية والموارد:** يجب توفير الموارد اللازمة، سواء كانت بنية تحتية تكنولوجية أو بشرية، لتمكين الأجهزة العليا للرقابة من أداء واجباتها بشكل فعّال.
٦. **تبادل الخبرات والمعرفة:** من خلال المشاركة في فرق ومجموعات العمل واللجان المعنية بتدقيق تكنولوجيا المعلومات والبيانات الضخمة وتأثير العلوم والتكنولوجيا على التدقيق في نطاق مجتمع الانتوساي.
٧. **تطوير السياسات والمعايير:** يجب تطوير وتحديث السياسات والمعايير الخاصة بتدقيق تكنولوجيا المعلومات بشكل دوري لضمان مواكبتها للتطورات التكنولوجية والتهديدات السيبرانية.
٨. **تعزيز الوعي والتثقيف الأمني:** يجب توعية المجتمع والمنظمات بأهمية الأمن السيبراني وكيفية التصدي للتهديدات السيبرانية من خلال حملات تثقيفية وتوعوية مستمرة.
٩. **تطوير قدرات الرصد والتحليل:** يجب تطوير قدرات الأجهزة العليا للرقابة في مجالات الرصد والتحليل لتمكينها من اكتشاف ومواجهة التهديدات السيبرانية بشكل فعال.

١٠. **توفير التوجيه والدعم المستمر:** يجب توفير التوجيه والدعم المستمر للمنظمات الحكومية في مجالات تدقيق تكنولوجيا المعلومات وأمن المعلومات والأمن السيبراني من قبل الأجهزة العليا للرقابة.

١١. **تعزيز الشفافية والمساءلة:** يجب العمل على تعزيز الشفافية والمساءلة في عمليات التدقيق والرقابة لضمان استقامة العمل ومواكبته للمعايير والمتطلبات القانونية والأمنية.

يرى الباحث أنه من خلال تبني هذه الخطوات والتركيز على التطوير المستمر والتعاون المشترك، يمكن للأجهزة العليا للرقابة تعزيز قدراتها في مجال تدقيق تكنولوجيا المعلومات بشكل فعّال.

١/١/١٦ تجارب الأجهزة العليا للرقابة في تدقيق تكنولوجيا المعلومات

نتناول في هذا الجزء بعض الحالات العملية لتدقيقات تكنولوجيا المعلومات عن طريق الأجهزة العليا للرقابة وذلك على النحو التالي: (EUROSAI ITWG, 2023, IT audit training course)

١. **تدقيق الجهاز الاعلى للرقابة في ألمانيا حول التحول الرقمي في الإدارة عام ٢٠٢٣**

يتطلب قانون الوصول الإلكتروني الألماني من الإدارة العامة في ألمانيا توفير معظم خدماتها بشكل رقمي بحلول نهاية عام ٢٠٢٢. ووزارة الداخلية هي منسقة لانتشار التكنولوجيا الرقمية في الإدارة العامة.

يشير تدقيق الجهاز الأعلى للرقابة في ألمانيا حول التحول الرقمي في الإدارة إلى أن الوزارة قامت بإعداد برنامجين لتنفيذ قانون الوصول الإلكتروني. كان أحد البرامج مخصصًا للخدمات الإدارية المقدمة على الصعيد الفيدرالي وبرنامج آخر للخدمات الإدارية المقدمة بمشاركة الحكومات الفيدرالية والولائية والمحلية. تم تخصيص مبلغ ٣,٥ مليار يورو لتنفيذ قانون الوصول الإلكتروني. بحلول نهاية عام ٢٠٢٢، لم يتم استخدام حوالي ٥٢% من هذه الأموال وكانت نسبة ١٩% من الخدمات الإدارية الممكن تطبيقها رقميًا متوفرة على الإنترنت.

يلاحظ التدقيق أن الوزارة قضت ما يقرب من نصف فترة التنفيذ القانوني لتحديد الخدمات الإدارية التي يجب أن تصبح رقمية، فضلاً عن مدى وترتيب هذه الخدمات. جاءت المواصفات التقنية والمتطلبات والحلول الرئيسية لتكنولوجيا المعلومات بتأخير، مما أدى إلى تطوير مزدوج ومتعدد.

يوصي التدقيق، بين أمور أخرى، بأن الوزارة ينبغي أن تنسق بشكل أفضل تنفيذ قانون الوصول الإلكتروني ويجب أن تضمن توفر المواصفات التقنية والمتطلبات في الوقت المناسب. يجب أن تسهم توفير الحلول المركزية لتكنولوجيا المعلومات في تجنب التطوير المتزامن. يحتاج الحكومة الفيدرالية إلى العمل نحو استراتيجية رقمية وتكنولوجية في الحكومة الفيدرالية.

٢. **تدقيق الجهاز الأعلى للرقابة في بريطانيا حول تحول الخدمات الحكومية عام ٢٠٢٣**

تناول التقرير الصادر عن المدقق العام في بريطانيا عام ٢٠٢٣ العقبات التي تعترض كفاءة التحول الرقمي في الحكومة. يشير إلى أنه في عام ٢٠٢١، أنشأ مجلس الوزراء مكتب البيانات الرقمية المركزي (CDDO) لقيادة وظيفة التكنولوجيا الرقمية والبيانات عبر الحكومة.

في عام ٢٠٢٢، نشر مكتب البيانات الرقمية المركزي خريطة الطريق للبيانات الرقمية للفترة من ٢٠٢٢ إلى ٢٠٢٥ تسلط الضوء على ست مهام حكومية مشتركة، بما في ذلك مهمة إنشاء خدمات عامة محولة تحقق النتائج المطلوبة. وفقًا لهذه المهمة، يجب نقل ٥٠ على الأقل من بين أفضل ٧٥ خدمة حكومية مدرجة في ملحق خريطة الطريق إلى معيار "ممتاز". يتطلب المعيار "ممتاز" أن تقلل الخدمات من الوقت والجهد والتكلفة غير الضرورية لكل من مستخدميها والإدارات التي تقدمها.

وفقًا للتحليل الأولي الذي أجراه مكتب البيانات الرقمية المركزي، فقد وصل ١٠% من الخدمات المدرجة في خريطة الطريق إلى هذا المعيار في وقت نشر تقريرالجهاز الأعلى للرقابة اعتبارًا من عام ٢٠٢٣، كان مكتب البيانات الرقمية المركزي يعمل على فهم مدى كفاءة عمل الخدمات الـ ٧٥ المدرجة في الاستراتيجية وإعداد خط الأساس لأداء جميع هذه الخدمات، مع التركيز على قياس الأداء بالنسبة للمستخدمين الرئيسيين لهذه الخدمات.

كجزء من مجموعة المعايير الوظيفية لتوجيه العاملين في الحكومة البريطانية ومعها، طور مكتب البيانات الرقمية المركزي المعيار الوظيفي الحكومي GovS 005:الرقمي ويركز على إدارة الخدمات والتكنولوجيا والبيانات، وكذلك على ممارسات الإدارة الرقمية.

يوصي تقرير، من بين أمور أخرى، بأن يحتفظ مكتب البيانات الرقمية المركزي بنطاق أنشطة خريطة الطريق تحت مراجعة دائمة لضمان توافقها مع الموارد المتاحة، مع تحديد الأولويات عند الحاجة.

٣. تدقيق الجهاز الأعلى للرقابة في استراليا حول مخاطر سلسلة التوريد الأمنية عام ٢٠٢٢

قام الجهاز الأعلى للرقابة في أستراليا عام ٢٠٢٢ بالتحقيق في كيفية امتثال ثلاث كيانات حكومية، وهي شرطة أستراليا الفيدرالية، مكتب الضرائب الأسترالي، ووزارة الشؤون الخارجية والتجارة، للمتطلبات الأمنية المنشأة فيما يتعلق بالموردين.

أوضح التقرير أن مؤسسات الحكومة الأسترالية تعتمد على سلاسل التوريد من المؤسسات والأشخاص والأنشطة والمعلومات وغيرها من الموارد، لتقديم الخدمات الرقمية وللحفاظ على أمانها. ولتقديم هذه الخدمات، يجب عليها تطبيق إطار سياسة الأمن الوقائي (PSPF) كسياسة حكومية أسترالية. يشمل مبادئ ونتائج وستة عشر سياسة، بما في ذلك السياسة رقم ٦ التي تتعامل مع الحوكمة الأمنية لمقدمي السلع والخدمات المتعاقدين.

في التقرير المذكور أعلاه، تم اختيار عقود لكل كيان محقق لدعم تقييم الالتزام بمتطلبات السياسة رقم ٦. وجد المدققون، بين أمور أخرى، أن الموردين المتعاقدين قد نفذوا العديد من العمليات والضوابط ولكن ليس كلها وفقًا لـPSPF .

على سبيل المثال، قد نفذ أحد مقدمي العقود، شركة تلسترا أستراليا، تدابير أمنية لتقييد الامتيازات الإدارية لبعض أجهزة الشبكة المحددة. ومع ذلك، لم تقم تلسترا بتنفيذ تصحيحات لأنظمة التشغيل على أجهزة الشبكة وفقًا لمتطلبات PSPF وكانت هيتاشي فانتارا، مقدم العقود الآخر، قد نفذت عمليات إدارة التصحيح لأنظمة التشغيل والتطبيقات، لكن الشرطة الفيدرالية الأسترالية لم تقم بتنفيذ عمليات إدارة التصحيح للتطبيقات على خوادم هيتاشي.

لم يحدد أي من الكيانات المدققة البنود والشروط المتعلقة بإدارة عدم الامتثال بالنسبة إلى PSPF ومتطلبات السياسة الداخلية للكيان.

وكانت من توصيات المدقق، بين أمور أخرى، بأن الكيانات المدققة يجب أن تنفذ عمليات للتحقق من موثوقية معلومات الأداء وإدارة عدم الالتزام لمقدمي العقود ضد PSPF ومع دليل أمان المعلومات لمركز أمن الإنترنت الأسترالي، وكذلك مع متطلبات السياسة الداخلية للكيان. ووافقت الكيانات الثلاثة على هذا التوصية.

٤. <u>تدقيق الجهاز الأعلى للرقابة في هولندا لاختبار الأمن السيبراني عام ٢٠٢٠</u>

تضمن تدقيق الجهاز الأعلى للرقابة في الأمن السيبراني للضوابط الحدودية في مطار أمستردام الضوابط التي يديرها حرس الحدود الهولندي. ركز التدقيق على ثلاثة أنظمة تقنية تدعم الفحوصات المسبقة للركاب القادمين، والفحوصات التي يتم إجراؤها في مكاتب جوازات السفر، والفحوصات التي تُجرى عند بوابات جوازات السفر الذاتية الخدمة في مطار سخيبول أمستردام. كان وزير الدفاع مسؤولاً عن الأمن السيبراني للنظامين الأولين، وكان وزير العدل والأمن مسؤولاً عن أمان النظام الثالث.

وفقًا للتدقيق، تتطلب سياسة الأمان الخاصة بوزارة الدفاع إجراء اختبارات أمان سنوية، لكن هذا المطلب لم يُتبع في الواقع. رتب المدققون اختبارًا لنظام تكنولوجيا المعلومات المستخدم في الفحوصات المسبقة في نوفمبر ٢٠١٩.

كشف هذا الاختبار عن إحدى عشرة ثغرة، بما في ذلك استخدام كلمات مرور قياسية، وإمكانية إرسال رسائل بريد إلكتروني مزيفة باسم مسؤولي وزارة الدفاع، واستخدام برامج قديمة. هذه الثغرات قد تسمح لموظف في وزارة الدفاع لديه وصول إلى شبكة الوزارة لكنه غير مصرح له بالدخول إلى نظام الفحص المسبق، بالتسلل إلى النظام والتلاعب في عملياته. يلاحظ تقرير التدقيق أن وزارة الدفاع اتخذت إجراءات لمنع مثل هذا الهجوم.

وكانت وزارة العدل والأمن قد استعانت بمقاول في عام ٢٠١٨ لإجراء تحليل أمني للنظام الذاتي الخدمة، ومع ذلك خلص تحقيق التدقيق إلى أن هذا التحليل لم يكشف عن أي مخاطر حرجة.

في عام ٢٠١٨، كلفت وزارة الدفاع إحدى إداراتها، فريق الاستجابة للطوارئ الحاسوبية للدفاع (DefCERT)، بإجراء اختبارات أمان على نظام بوابات جوازات السفر الذاتية الخدمة. حدد هذا الاختبار وجود ثغرة واحدة مصنفة على أنها "عالية المخاطر" وسبع ثغرات مصنفة على أنها "متوسطة المخاطر". خلص DefCERT إلى أن هناك حاجة لإجراء اختبارات إضافية لتقديم توصيات حول الحالة العامة لمشروع النظام الذاتي الخدمة. تم إزالة الثغرات التي وُجدت في هذا الاختبار بعد التدقيق.

أوصى المدققون، من بين أمور أخرى، بأن يقوم وزير الدفاع ووزير العدل والأمن بإجراء اختبارات أمان سنوية للأنظمة الثلاثة لتكنولوجيا المعلومات المستخدمة في الضوابط الحدودية وضمان تنفيذ التوصيات الناتجة عن الاختبارات.

استجاب وزير الدفاع ووزير العدل والأمن بأن الأنظمة الحرجة الأربعة عشر لوزارة الدفاع سيكون مطلوبًا منها اجتياز اختبار أمان وتنفيذ التدابير بناءً على توصياته كل ثلاث سنوات. وكان من المخطط أن يبدأ الاختبار السنوي لنظام الخدمة الذاتية في عام ٢٠٢١.

١/١/١٧ الملاحظات الشائعة في تدقيق تكنولوجيا المعلومات

يمكن تبويب أهم الملاحظات الشائعة التي يتم اكتشافها عند تدقيق نظم المعلومات الإلكترونية، والمخاطر المرتبطة بها على النحو التالي: (Gantz, 2014, 50:60) (EUROSAI ITWG, 2023, IT training course)

أ- <u>ملاحظات تتعلق بالأمان والوصول</u>

١. عدم تغيير كلمات المرور بصورة دورية، ويمكن أن يؤدي إلى وصول غير مصرح به للبيانات والموارد.
٢. عدم وجود سجلات مراقبة لحركات المستخدمين، مما يعيق الكشف عن الأنشطة غير المعتادة والاحتمالية لحوادث الأمان.
٣. استخدام كلمات مرور ضعيفة أو قصيرة أو عدم تطبيق سياسات تعقيد كلمات المرور، مما يزيد من مخاطر الوصول غير المصرح به.
٤. عدم تنفيذ إجراءات تأمين متعددة العوامل لتعزيز الحماية من الوصول غير المصرح به.
٥. عدم تحديد مستويات الوصول، مما يمكن معه زيادة تعرض النظام لمخاطر الاختراق.

ب-<u>ملاحظات تتعلق بإدارة المستخدمين</u>

١. عدم وجود مراجعات دورية لصلاحيات المستخدمين، ويمكن أن يؤدي ذلك إلى صلاحيات غير ملائمة ومخاطر انتهاك الأمان.
٢. عدم تدريب المستخدمين على ممارسات الأمان، مما يسهم في زيادة مخاطر الاختراق.

٣. التأخر في تعطيل حسابات المستخدمين بعد تركهم العمل أو وصولهم إلى سن التقاعد، مما يزيد من مخاطر الوصول غير المصرح به.
٤. عدم تحديد مسؤوليات المستخدمين بشكل واضح، مما يؤدي إلى تداخل الصلاحيات وزيادة مخاطر الأمان.

ج- ملاحظات تتعلق بالبنية التحتية التقنية

١. استخدام أنظمة وبرامج وأجهزة غير مدعمة، مما يؤدي إلى مشكلات توافق وأمان.
٢. تحديثات غير مختبرة للبرامج والتطبيقات، مما قد يسبب مشاكل في الأمان والاستقرار.
٣. عدم تنفيذ إجراءات احتياطية منتظمة واختبارها، مما قد يؤدي إلى فقدان البيانات في حالة الكوارث.
٤. استخدام أجهزة قديمة وغير محدثة، مما يتيح الفرصة للمهاجمين للاستفادة من ثغرات معروفة.
٥. عدم تقديم تدريب منتظم للموظفين المسؤولين عن البنية التحتية التقنية، مما يؤدي إلى قرارات غير صحيحة فيما يتعلق بالأمان والصيانة.

د- ملاحظات تتعلق بالسجلات والمراقبة

١. عدم تفعيل ضوابط الرقابة في مراكز البيانات وعدم وجود سجلات للزائرين يمكن أن يؤدي إلى ضعف الأمان المادي، عدم وجود سجلات دقيقة لحركات المستخدمين.
٢. تأخر في مراجعة وتحليل سجلات الأمان يمكن أن يتسبب في عدم اكتشاف الأحداث الغير معتادة في الوقت المناسب.
٣. استخدام أنظمة مراقبة غير فعّالة يمكن أن يؤدي إلى تفويت أحداث هامة في عملية المراقبة.
٤. عدم وجود سياسات وإجراءات واضحة لمراقبة الأمان والاستجابة للحالات الأمنية يمكن أن يزيد من مخاطر فقدان البيانات والاختراق.

ذ- ملاحظات تتعلق بالبيانات المالية

١. عدم اكتمال دفتر الأستاذ في النظام الإلكتروني، والقيام بإدخال ومعالجة المعاملات خارج نظام المعلومات.
٢. وجود فروق في الأرقام التسلسلية لإدخال المعاملات في نظام المعلومات الإلكتروني.
٣. وجود أخطاء في إدخال بيانات المعاملات اليومية على سبيل المثال الخطأ في إدخال أسعار صرف العملات الأجنبية.
٤. وجود تحويلات مالية لبعض الموردين دون وجود عمليات شراء مقابلة لها في نظام المعلومات.

ر- **ملاحظات تتعلق بالتخطيط الاستراتيجي والانفاق على تكنولوجيا المعلومات**

١. ضغط الوقت أو الجدول الزمني غير الواقعي يؤدي إلى التأخيرفي التسليم وتنفيذ أنظمة غير مختبرة مع تجاهل أو تأجيل أمن المعلومات.

٢. إهمال متطلبات أمن المعلومات خلال مرحلة المفهوم والتصميم، اهمال نقاط الضعف في أمن المعلومات مما يؤدي الاضطرابات والتأخير في إصلاح نقاط الضعف في أمن المعلومات

٣. ضعف التنسيق بين أصحاب المصلحة في مجال تكنولوجيا المعلومات والأعمال مما يؤدي إلى زيادة تكاليف المشروع بسبب عدم الكفاءة

٤. عدم وجود خطة استراتيجية متعددة السنوات لتكنولوجيا المعلومات. فبدون خطة طويلة الأجل، لا تتماشى استثمارات تكنولوجيا المعلومات مع أهداف العمل، مما يؤدي إلى الإسراف في الإنفاق وتخصيص الموارد دون المستوى الأمثل.

١/١/١٨ التحديات التي تواجه تدقيق تكنولوجيا المعلومات

يواجه تدقيق تكنولوجيا المعلومات عدة تحديات تتعلق بالموارد والتقنيات والتطورات السريعة في مجال التكنولوجيا، يتمثل بعضها فيمايلي: (كرسوع، ٢٠٢٤، ٣٠: ٤٩) (Engel, 2024, 265; 290) (Hernan, 2019,240: 250) (Davis, 2021, 230: 260)

١. **تطور التهديدات والهجمات السيبرانية:** مع تزايد تطور التهديدات السيبرانية وظهور تقنيات هجومية جديدة، يصعب على فرق التدقيق مواكبة جميع النقاط الضعيفة المحتملة في الأنظمة والشبكات.

٢. **التعقيد التقني:** تزداد تعقيدات البنى التحتية الرقمية وأنظمة المعلومات مع تطور التكنولوجيا، مما يجعل تحليل الأمان والتدقيق أكثر صعوبة وتعقيدًا.

٣. **نقص الموارد البشرية المتخصصة:** قلة الخبرات والمهارات في مجال الأمن السيبراني وتدقيق التكنولوجيا يمثل تحديًا، حيث يصعب إيجاد الكوادر المؤهلة لتنفيذ العمليات بكفاءة.

٤. **ضغط الوقت والجدولة:** تحديد الجداول الزمنية لعمليات التدقيق وإتمامها في الوقت المحدد يمثل تحديًا، خاصةً في ظل الحاجة الملحة للحفاظ على أمان البيانات والأنظمة.

٥. **الامتثال للمعايير واللوائح:** مع تزايد قيود الامتثال القانونية والتشريعات الأمنية، يصبح تأمين الامتثال لهذه المعايير واللوائح تحديًا إضافيًا لعمليات التدقيق.

٦. **التعامل مع حجم البيانات الكبير:** تحديات تدقيق التكنولوجيا المعلوماتية تشمل أيضًا التعامل مع حجم البيانات الكبير وتحليلها بشكل فعال للكشف عن الثغرات والتهديدات.

٧. **تكامل التقنيات والأنظمة:** تعقيدات التكامل بين التقنيات المختلفة وأنظمة المعلومات يمكن أن تجعل من التحقق من الأمان أمرًا أكثر تعقيدًا.

٨. **التحديات القانونية والتشريعات الدولية:** التغيرات في القوانين والتشريعات الدولية قد تتطلب منظورًا جديدًا لعمليات التدقيق، مما يضيف تحديات إضافية للمؤسسات.

يرى الباحث أن تلك التحديات تتطلب استراتيجيات واضحة وتعاونًا قويًا بين الأقسام المختلفة داخل المنظمة، بالإضافة إلى الاستثمار في التقنيات والأدوات اللازمة للتعامل معها بشكل فعال.

١/١/١٩ مواجهة التحديات التي تواجه تدقيق تكنولوجيا المعلومات

يرى الباحث أنه للتغلب على التحديات التي تواجه عمليات تدقيق تكنولوجيا المعلومات، يمكن اتباع استراتيجيات متعددة تشمل مايلي:

١. **تعزيز القدرات المهنية للمدققين:** وذلك بتشجيعهم للحصول على الشهادات المهنية في مجال تدقيق تكنولوجيا المعلومات مثل شهادة مدقق تكنولوجيا معلومات معتمد، وكذلك المشاركة في فرق العمل واللجان المعنية بتدقيق تكنولوجيا المعلومات في مجتمع الانتوساي واليوروساي والأرابوساي، كذلك المشاركة في المبادرات التي تصدرها المنظمات الدولية والمهنية لتعزيز مهارات المدققين بصفة عامة ومدققي تكنولوجيا المعلومات بصفة خاصة مثل الحصول على شهادة تدقيق تكنولوجيا المعلومات لغير مدققي تكنولوجيا المعلومات التي أصدرتها منظمة اليوروساي خلال عام ٢٠٢٣، وكذلك حضور اللقاءات العلمية والتدريبية في مجال تدقيق تكنولوجيا المعلومات على سبيل المثال اللقاء العلمي الذي نظمته منظمة أرابوساي بعنوان الأساليب الحديثة في الرقابة على النظم المعلوماتية خلال يوليو ٢٠٢٤.

٢. **توعية وتدريب الموظفين:** تعتبر التوعية الأمنية وتدريب الموظفين أمرًا حيويًا للتصدي للتهديدات السيبرانية، ويمكن أن يشمل التدريب مواضيع مثل التعرف على الهجمات السيبرانية وكيفية التصدي لها وممارسات الأمان السيبراني.

٣. **استخدام التقنيات المتقدمة:** استخدام التقنيات المتقدمة مثل الذكاء الصناعي وتحليل البيانات الضخمة في عمليات التدقيق يمكن أن يزيد من كفاءة وفعالية عمليات التحقق من الأمان.

٤. **تبسيط العمليات والإجراءات:** تبسيط العمليات والإجراءات الأمنية يمكن أن يسهل عملية التدقيق ويقلل من الأخطاء الإنسانية وزيادة الامتثال للسياسات واللوائح.

٥. **تحسين الشفافية والتواصل:** تعزيز التواصل الداخلي والخارجي وتعزيز الشفافية في العمليات الأمنية يمكن أن يسهل عمليات التدقيق ويساهم في تحقيق أهدافها بشكل أفضل.

٦. **تعزيز التعاون والتنسيق:** تشجيع التعاون والتنسيق بين الأقسام المختلفة داخل المنظمة ومع الجهات الخارجية يمكن أن يعزز فعالية عمليات التدقيق وتوجيه الجهود بشكل أفضل.

٧. **تبني ثقافة الامتثال والمسؤولية:** تشجيع ثقافة الامتثال للسياسات الأمنية والمسؤولية الفردية تجاه الأمن السيبراني يمكن أن يعزز الوعي الأمني ويقلل من مخاطر الاختراقات.

٨. **الاستثمار في التحديث والتطوير المستمر:** الاستثمار في التحديث والتطوير المستمر للأنظمة والتقنيات الأمنية يمكن أن يساعد في التصدي للتهديدات السيبرانية المتطورة وتحسين قدرة المنظمة على التكيف مع التغيرات.

كما يرى الباحث أن تنفيذ هذه الاستراتيجيات بشكل فعّال يمكن أن يسهم في تعزيز أمن المعلومات والتأكد من أن عمليات التدقيق تلبي الأهداف المحددة بشكل كامل.

المبحث الثاني
مخاطر نظم المعلومات الإلكترونية

١/٢/١ تمهيد

في عصرنا الحالي، أصبحت نظم المعلومات الإلكترونية لبنة أساسية في البنية التحتية في غالبية المنظمات والمجتمعات، وتعد هذه النظم المعقدة منصة حيوية لتخزين ومعالجة ونقل البيانات والمعلومات. ومع تزايد التبادل الإلكتروني للمعلومات، فإن أهمية تأمين هذه النظم وحمايتها تزداد بشكل كبير.

نظرًا لأهمية قطاع المؤسسات الحكومية وما تقدمه من دور هام في عملية التنمية الاقتصادية والاجتماعية والإدارية بما توفره من بيانات تسهم فى إعداد الخطط والموازنات وقرارات تسهم في حل المشكلات في ظل التحديات التي تواجهها من ظروف بيئية وسياسية محيطة، والتقدم التكنولوجي الذي شهده هذا القطاع من تطورات أدت إلى تحويل إجراءات العمل اليدوية إلى آلية، فقد اعتمدت هذه المنظمات على نظم تكنولوجيا المعلومات. (ضيف الله، ٢٠١٧، ٢٠١: ٢٢٠)

تواجه نظم المعلومات الإلكترونية مجموعة متنوعة من المخاطر، بدءًا من التهديدات الإلكترونية البسيطة مثل البرامج الضارة والفيروسات، وصولًا إلى التهديدات الأكثر تطورًا مثل الاختراقات الهجومية والاختراقات الهجينة، وتتنوع هذه المخاطر أيضًا لتشمل الاختراقات من قبل المتسللين الداخليين، والتهديدات المتعلقة بالاحتيال وسرقة البيانات، وحتى التهديدات الجيوسياسية التي تشمل الهجمات السيبرانية الدولية. ومن المهم أن ندرك أن هذه المخاطر لا تقتصر على الأنظمة الكبيرة فقط، بل تمتد أيضًا إلى الأفراد والأسر، خاصة مع تزايد استخدام الأجهزة المتصلة بالإنترنت في حياتنا اليومية، ويتطلب تأمين نظم المعلومات الإلكترونية اهتمامًا جادًا وجهودًا متواصلة من جميع الأطراف المعنية، وأن تتضمن هذه الجهود استراتيجيات فعالة للوقاية من الهجمات السيبرانية، وتعزيز الوعي الأمني.

١/٢/٢ مفهوم نظم المعلومات الإلكترونية

يمكن تعريف نظام المعلومات الإلكترونية بأنه نظام يهدف إلى إدارة وتنظيم المعلومات بشكل إلكتروني في كافة المجالات، ويشمل نظام المعلومات الإلكترونية استخدام التكنولوجيا لتخزين البيانات، وإدخالها، واسترجاعها، ومعالجتها، ونقلها بشكل فعال وفي الوقت المناسب.

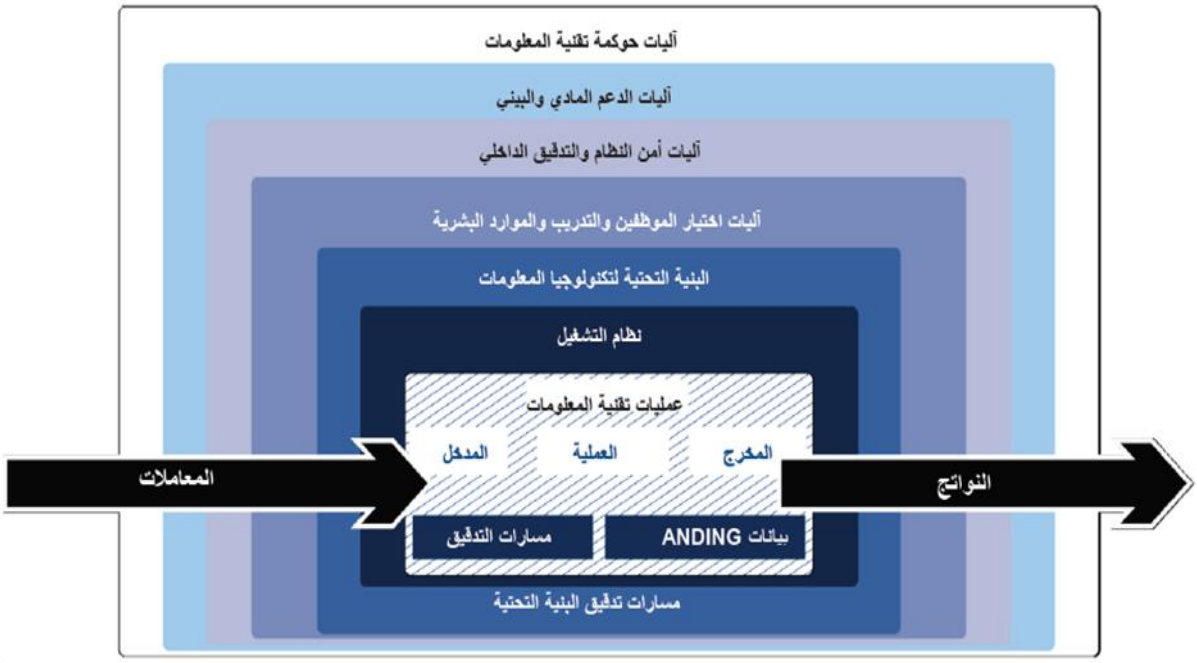
كما يشير إلى الأنظمة والتقنيات التي تُستخدم لجمع وتخزين ومعالجة ونقل المعلومات بشكل إلكتروني تتضمن هذه الأنظمة مجموعة متنوعة من البرمجيات والبنية التحتية التكنولوجية التي تدعم تبادل المعلومات بين المستخدمين والأنظمة. (الغبور، وأخرون، ٢٠١٩، ٣٦٠: ٤٠٨) (Al-Fatlawi, 2021, 25: 27)

إن نظم المعلومات الإلكترونية تشمل العديد من العناصر، من أهمها:

(مداح، ٢٠٢١، ٢٠: ٢٥) (المري، ٢٠٢٣، ١٣٠٣، ١٣٧٣) (أبورمان، ٢٠٢١، ٣٢: ٣٠)

١. **البرمجيات:** تتضمن برمجيات إدارة المحتوى ونظم إدارة العلاقات مع العملاء ونظم تخزين البيانات وبرمجيات الأمان والحماية، والتي تُستخدم لإدارة ومعالجة المعلومات بشكل فعال.
٢. **الأجهزة:** تشمل الخوادم وأجهزة التخزين والأجهزة الشبكية والأجهزة النهائية (مثل الحواسيب والأجهزة اللوحية والهواتف الذكية)، والتي تعمل معًا لتمكين تشغيل وإدارة النظم الإلكترونية.
٣. **الشبكات:** توفر البنية التحتية اللازمة لتوصيل الأجهزة وتبادل المعلومات بينها، سواء كانت شبكات محلية داخلية أو شبكات واسعة النطاق عبر الإنترنت.
٤. **تقنيات التخزين وقواعد البيانات:** تُستخدم لتخزين البيانات بشكل آمن وفعال، وتسمح بالوصول السريع إلى المعلومات وإدارتها بشكل منظم.
٥. **تقنيات التواصل والتبادل:** تتضمن التقنيات التي تمكن تبادل المعلومات بين المستخدمين، مثل البريد الإلكتروني والدردشة والمنصات الاجتماعية وأنظمة المشاركة في المستندات.
٦. **أنظمة إدارة الأمان والحماية:** تُستخدم لحماية البيانات والمعلومات من التهديدات الأمنية، وتتضمن تقنيات الحماية من الفيروسات والبرامج الضارة والاختراقات السيبرانية.

شكل رقم (٤) يوضح نظام المعلومات الإلكتروني



المصدر: دليل مبادرة الإنتوساي لتدقيق تكنولوجيا المعلومات، ٢٠٢٢

١/٢/٣ أهداف نظم المعلومات الإلكترونية

تهدف نظم المعلومات الإلكترونية إلى تحقيق مجموعة متنوعة من الأهداف التي تسهم في تحسين أداء المنظمة وتعزيز فعالية العمليات الداخلية والخارجية، ويعد من الأهداف الرئيسية لنظم المعلومات

الإلكترونية مايلي: (المطيري، ٢٠٢٣، ١: ٢٧) (النقبي، والمصعبي، ٢٠٢٣، ١٨١٥: ١٩٠٧) (علي، وشحاتة، ٢٠١٥، ١٠: ١٥)

١. **تحسين الوصول إلى المعلومات:** يهدف نظام المعلومات الإلكترونية إلى توفير وصول سريع وسهل إلى المعلومات المهمة والضرورية للموظفين والإدارة والعملاء والشركاء.
٢. **زيادة كفاءة العمليات:** يعمل نظام المعلومات الإلكترونية على تبسيط العمليات اليومية وتحسين تنظيمها، مما يسهم في زيادة كفاءة العمل وتقليل الوقت والجهد المبذول.
٣. **تحسين التواصل والتعاون:** يسهم نظام المعلومات الإلكترونية في تعزيز التواصل بين مختلف أقسام المنظمة وبين العاملين بها، كما يسهل التعاون وتبادل المعلومات والموارد بين الأعضاء.
٤. **توفير الدعم لاتخاذ القرار:** يسهم نظام المعلومات الإلكترونية في تحليل البيانات وتوليد التقارير والإحصائيات التي تساعد في اتخاذ القرارات الاستراتيجية والتكتيكية بشكل أفضل وأكثر دقة.
٥. **تحسين خدمة العملاء:** من خلال توفير وصول سريع إلى المعلومات حول المنتجات والخدمات ومعالجة طلبات العملاء بفعالية، يسهم نظام المعلومات الإلكترونية في تحسين رضا العملاء وتعزيز العلاقات معهم.
٦. **تحسين إدارة الموارد:** يساعد نظام المعلومات الإلكترونية في إدارة الموارد المالية والبشرية والمواد بشكل أفضل، مما يسهم في تقليل التكاليف وزيادة الكفاءة.
٧. **زيادة التنافسية:** يهدف نظام المعلومات الإلكترونية إلى تعزيز تنافسية المنظمة عبر تحسين العمليات وتوفير فرص جديدة للابتكار والتطوير.
٨. **تحسين جودة المنتجات والخدمات:** يمكن لنظام المعلومات الإلكترونية أن يسهم في مراقبة جودة المنتجات والخدمات وتحسينها من خلال مراقبة العمليات وجمع الملاحظات وتحليلها.
٩. **زيادة الرضا لدى الموظفين:** من خلال توفير أدوات وموارد تقنية متطورة، يمكن لنظام المعلومات الإلكترونية زيادة رضا الموظفين وتحسين بيئة العمل.
١٠. **تحسين الأمان والسرية:** يسعى نظام المعلومات الإلكترونية إلى حماية المعلومات الحساسة وضمان سرية البيانات من خلال تطبيق إجراءات الأمان والتشفير ومراقبة الوصول.
١١. **تحسين العلاقات مع الشركاء والموردين:** يمكن لنظام المعلومات الإلكترونية تسهيل التواصل وتبادل المعلومات مع الشركاء والموردين، مما يعزز التعاون ويسهم في تحسين العلاقات التجارية.

هذه هي بعض الأهداف الرئيسية لنظم المعلومات الإلكترونية، ويمكن تخصيصها وفقًا لاحتياجات وأهداف كل مؤسسة أو منظمة

١/٢/٤ خصائص نظم المعلومات الإلكترونية

لكي تتمكن الإدارة من النهوض بمسؤلياتها وتحقيق الأهداف التي تسعى إليها لابد من توفير المعلومات الضرورية بالنوعية والوقت والتكلفة ويتم ذلك من خلال نظم المعلومات، وهناك العديد من السمات التي

تجعل نظم المعلومات الإلكترونية قادرة على تحقيق الأهداف المرجوة بشكل فعّال، وفيما يلي بعض الخصائص الرئيسية لنظم المعلومات الإلكترونية: (المطيري، ٢٠٢٣، ١: ٢٧) (أبورمان، ٢٠٢١، ٣٠)

١. **تخزين البيانات:** تتميز نظم المعلومات الإلكترونية بالقدرة على تخزين كميات كبيرة من البيانات بشكل آمن ومنظم.
٢. **سهولة الوصول:** توفر نظم المعلومات الإلكترونية وسائل سهلة للوصول إلى البيانات والمعلومات، سواء كان ذلك عبر واجهات مستخدم رسومية أو أنظمة بحث فعّالة.
٣. **مشاركة المعلومات:** تمكّن نظم المعلومات الإلكترونية من مشاركة البيانات والمعلومات بين مختلف الأقسام والأفراد داخل المؤسسة.
٤. **توفير الأمان والسرية:** تضمن نظم المعلومات الإلكترونية تطبيق إجراءات الأمان المناسبة لحماية البيانات وضمان سرية المعلومات الحساسة.
٥. **التكاملية:** تسمح نظم المعلومات الإلكترونية بالتكامل مع أنظمة أخرى داخل المنظمة مثل أنظمة إدارة العلاقات مع العملاء وأنظمة إدارة الموارد البشرية.
٦. **التحليل والتقرير:** تتيح نظم المعلومات الإلكترونية إمكانية تحليل البيانات وإنشاء التقارير والإحصائيات التي تدعم عمليات اتخاذ القرار.
٧. **المرونة والتوسع:** تتميز نظم المعلومات الإلكترونية بالمرونة والقدرة على التوسع لمواكبة احتياجات المنظمة المتغيرة.
٨. **التنسيق والتنظيم:** تساعد نظم المعلومات الإلكترونية في تنسيق وتنظيم العمليات والبيانات بشكل فعّال لتحسين كفاءة العمل لا يوجد نظام واحد يصلح للتطبيق في كافة المنظمات وذلك لأن النظام وإن كان له هيكل عام متشابه إلا أن المكونات الداخلية تختلف من منشأة إلى أخرى.

<u>وبالرغم من هذه الخصائص إلا أنه:</u>

- يجب ألا يبقى نظام المعلومات جامدًا في تطبيقه في المنظمة الواحدة وينبغى أن يتعدل كلما استدعى الأمر ذلك.
- يجب أن يتم تقييم استخدام نظم المعلومات الإلكترونية من فترة لإستكشاف نقاط القوة لتعيمها ونقاط الضعف لتلافيها.
- كما أن التغذية العكسية في نظم المعلومات هي العنصر الأساسي لضمان استمرار تطبيقة بفعالية.

١/٢/٥ دور نظم المعلومات الإلكترونية في صنع واتخاذ القرار

تلعب نظم المعلومات الإلكترونية دورًا حيويًا في عملية صنع واتخاذ القرار في المؤسسات، حيث توفر البيانات والمعلومات اللازمة لاتخاذ القرارات الاستراتيجية والتكتيكية بشكل مستنير ومبني على الأدلة، وذلك على النحو التالي: (النقبي، والمصعبي، ٢٠٢٣، ١٨١٥: ١٩٠٧) (أبورمان، ٢٠٢١، ٢٠: ٢٥)

١. **توفير البيانات والمعلومات:** تقوم نظم المعلومات الإلكترونية بجمع وتخزين وتنظيم البيانات والمعلومات من مختلف مصادرها داخل المؤسسة، مما يسهل على صناع القرار الوصول إلى المعلومات اللازمة.

٢. **التحليل والتقييم:** تتيح نظم المعلومات الإلكترونية إمكانية تحليل البيانات والمعلومات بشكل شامل ودقيق، مما يساعد في فهم الوضع الحالي وتقييم الخيارات المتاحة.

٣. **توليد التقارير والإحصائيات:** تتيح نظم المعلومات الإلكترونية إنشاء التقارير والإحصائيات المتعلقة بالمعلومات المحددة، مما يسهل على صناع القرار استخلاص النتائج والمعلومات الهامة.

٤. **دعم عمليات اتخاذ القرار:** توفر نظم المعلومات الإلكترونية الدعم اللازم لصناع القرار من خلال تقديم البيانات والتحليلات اللازمة لاتخاذ القرارات السليمة والمبنية على الأدلة.

٥. **التنبؤ والتخطيط:** تساعد نظم المعلومات الإلكترونية في التنبؤ بالاتجاهات المستقبلية وتطوير الخطط والاستراتيجيات الملائمة للتعامل معها.

٦. **التواصل والتنسيق:** تسهم نظم المعلومات الإلكترونية في تحسين التواصل والتنسيق بين أعضاء المنظمة المختلفين، مما يسهل عملية تبادل المعلومات واتخاذ القرارات المشتركة.

يرى الباحث أن نظم المعلومات الإلكترونية تعمل على دعم عملية صنع القرارات من خلال توفير البيانات والتحليلات والتواصل بين الأقسام المختلفة، مما يساعد على اتخاذ قرارات فعالة ومبنية على الحقائق.

١/٢/٦ نظم المعلومات المحاسبية الإلكترونية

تعتبر نظم المعلومات المحاسبية جزءًا أساسيًا من نظم المعلومات الإلكترونية في المنظمات، وتهدف هذه النظم إلى تنظيم ومعالجة وتقديم المعلومات المحاسبية والمالية بشكل فعّال ودقيق، وتلبية احتياجات المنظمة في مجال التقارير المالية وإدارة الأموال وتحليل البيانات المالية، وفيمايلي بعض الجوانب الرئيسية لنظم المعلومات المحاسبية كجزء من نظم المعلومات الإلكترونية: (قرداش، وقنصوة، ٢٠٢٣، ١: ٢١) (المنيزل، ٢٠٢٢، ٣٦: ٤٠) (أبو الهيجاء، ٢٠١٧، ٢٥: ٢٧)

١. **تسجيل المعاملات المالية:** تقوم نظم المعلومات المحاسبية بتسجيل وتوثيق جميع المعاملات المالية التي تتم في المؤسسة، مثل العمليات الشرائية والمبيعات والمدفوعات والاستحقاقات.

٢. **إعداد التقارير المالية:** تمكن نظم المعلومات المحاسبية من إعداد التقارير المالية اللازمة للمنظمة، مثل قوائم الدخل والميزانية العمومية وقوائم التدفقات النقدية والموازنات والحسابات الختامية، بشكل دقيق وفي الوقت المناسب.

٣. **إدارة الحسابات:** تتيح نظم المعلومات المحاسبية إدارة الحسابات المالية والميزانيات والقوائم المالية بشكل فعّال، مما يسهل على الإدارة اتخاذ القرارات المالية الصائبة.

٤. **التقارير التحليلية:** تساعد نظم المعلومات المحاسبية في تحليل البيانات المالية وإعداد التقارير التحليلية التي تساهم في فهم أداء المنظمة وتحديد الاتجاهات والتوجهات المستقبلية.

٥. **الامتثال والتقييم الضريبي:** تلتزم نظم المعلومات المحاسبية بمعايير الامتثال الضريبي والمحاسبي، وتساعد في إعداد التقارير اللازمة للتقييم الضريبي والتوافق مع القوانين واللوائح المالية المعمول بها.

٦. **التحكم الداخلي:** تقدم نظم المعلومات المحاسبية آليات للتحكم الداخلي وضمان دقة وسلامة المعلومات المالية، من خلال تطبيق سياسات وإجراءات محاسبية مناسبة.

يرى الباحث أن نظم المعلومات المحاسبية تعد جزءًا حيويًا من نظم المعلومات الإلكترونية، وتسهم في إدارة المعلومات المالية وتوفير البيانات اللازمة لاتخاذ القرارات المالية الصائبة وضمان الامتثال للمعايير المحاسبية والضريبية.

١/٢/٧ أنواع المخاطر التى تواجه نظم المعلومات الإلكترونية

تعرف مخاطر تكنولوجيا المعلومات بأنها كل ما ينتج عنه وجود خطأ أو خلل في تكنولوجيا المعلومات تؤدي إلى تأثير سلبي على أعمال المنظمة، ونظم المعلومات الخاصة بها.

وفى هذا السياق يمكن تبويب وتصنيف مخاطر أمن نظم المعلومات الإلكترونية من وجهات نظر مختلفة على النحو التالي: (أبو شيبة، الفطيمى،٢٠١٧، ٨٠: ٩٨) (الجربوع، ٢٠٢٣، ١٣٦٣: ١٤٣٠)

أ- من حيث مصدرها

- **المخاطر الداخلية:** ويعتبر موظفي المنظمات هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات الإلكترونية وذلك لكونهم على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق ونقاط القوة والضعف فيه لدى المنظمة، ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولذلك فإن موظفي المنظمة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تعديلها.
- **المخاطر الخارجية:** ويمثل قراصنة المعلومات والكوارث الطبيعية أهم مصادر المخاطر الخارجية، وعادة مايستغل قراصنة المعلومات مهاراتهم العالية فى الحاسب وتكنولوجيا المعلومات فى الدخول غير القانونى إلى النظم والبرامج بهدف التلاعب فى البيانات أو تدميرها أو بهدف السرقة والإختلاس، وقد يحاولون اختراق الضوابط الرقابية والأمنية بهدف الحصول على معلومات سرية عن المنظمة، بينما قد تسفر بعض الكوارث الطبيعية مثل الزلزال والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المنظمة .

ب- من حيث المتسبب فيها

- **مخاطر ناتجة عن العنصر البشرى** والتى قد تكون نتيجة بعض التصرفات البشرية غير المتعمدة (نتيجة الخطأ أو السهو) أو المتعمدة بقصد الغش والتلاعب.

- **مخاطر ناتجة عن العنصر غير البشري** والتى ليس للإنسان دخل فيها والتي تكون نتيجة الكوارث الطبيعية والمتعلقة بأعطال التيار الكهربائي والحرائق.

ج-من حيث العمدية

- **مخاطر ناتجة عن تصرفات متعمدة:** وتعتبر هذه المخاطر من المخاطر المؤثرة جدًا على النظام مثل الإدخال المتعمد لبيانات غير صحيحة أو التدمير المتعمد للبيانات فى بعض الملفات الهامة أو أجزاء منها، وعادة ما يكون ذلك بإلغاء أو تعديل أو تحريف بيانات بعض السجلات والملفات أو خلق معلومات مضللة أو غير صحيحة بغرض إخفاء آثار حالات الغش والتلاعب وسرقة بعض الأموال أو بعض البيانات الهامة.
- **مخاطر نتيجة تصرفات عفوية وغير متعمدة:** وهى تصرفات يقوم بها الأشخاص نتيجة الجهل وعدم الخبرة الكافية كإدخالهم للبيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق إدخالها أو السهو أو الخطأ، وهذه المخاطر في معظم الأحيان يمكن تصحيحها أو تفاديها بمزيد من التدريب للموظفين وحسن الإشراف عليهم.

د- من حيث الآثار الناتجة عنها

- **مخاطر ينتج عنها أضرار مادية** للنظام وأجهزة الحاسب أو التدمير المادي لوسائل تخزين البيانات، والتي قد تنتج من بعض الظواهر الطبيعية كالفيضانات والزلازل أو إنقطاع التيار الكهربائي أو الحرائق، أومن سقوط النظم أوالشبكات لفترات معينة.
- **مخاطر فنية أو منطقية:** والتي قد تصيب البيانات الموجودة في ذاكرة الحاسب أو على الشرائط الممغنطة، وقد يكون ذلك بتحريف البرامج وإدخال فيروسات للكمبيوتر والتي قد تؤثر سلبًا على مدى إتاحة البيانات عند الحاجة اليها، وذلك بحجبها عن الأشخاص المصرح لهم حق الإطلاع عليها أو إستخدامها أو إفشاء البيانات السرية لأشخاص غير مصرح لهم بالإطلاع عليها والتي قد تؤثر على تكامل البيانات والبرامج داخل النظام.

هـ-من حيث علاقتها بمراحل النظام

- **مخاطر المدخلات:** وتتمثل المخاطر المتعلقة بأمن المدخلات فى خلق بيانات غير حقيقية- تعديل أو تحريف بيانات المدخلات من خلال التلاعب في المدخلات والمستندات الأصلية بعد اعتمادها من قبل المسئول وقبل إدخالها إلى النظام- حذف بعض المدخلات قبل إدخالها إلى الكمبيوتر- تكرار إدخال البيانات أكثر من مرة.
- **مخاطر تشغيل البيانات:** وينصب تأثير تلك المخاطر على البيانات المخزنة في ذاكرة الكمبيوتر والبرامج التي تقوم بتشغيل تلك البيانات، وتتمثل مخاطر تشغيل البيانات في تعديل وتحريف البرامج -عمل نسخ غير قانونية من البرامج - إستخدام البرنامج بطريقة غير مصرح أو مرخص بها -

إدخال القنابل الموقوتة والفيروسات إلى أجهزة الحاسب- تحريف وتعديل البرامج بإستخدام حصان طروادة أو غيره من الأساليب التي تحتاج إلى خبرات متخصصة في الكمبيوتر والبرمجة.

- **مخاطر المخرجات:** ويقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية التشغيل، إن مخاطر مخرجات الكمبيوتر تتمثل في سرقة مخرجات الكمبيوتر أو طمس أو تدمير بنود معينة من المخرجات أو خلق مخرجات زائفة وغير صحيحة أو إساءة إستخدامها أو عمل نسخ غير مصرح بها من المخرجات أو توجيهها إلى أشخاص غير مصرح لهم بإستلامها أو الاطلاع عليها نظرًا لسريتها أو لأنهم غير مخول لهم صلاحيات الإطلاع عليها ولا تتوافر فيهم المقومات الأمنية، بالإضافة الى خلق بيانات زائفة.

ويمكن تصنيف المخاطر المتعلقة بنظم المعلومات الإلكترونية على النحو الآتي (حسين، ٢٠٢٠، ٢٠:٥٠):

أ) مخاطر البنية التحتية المتعلقة بتكنولوجيا المعلومات وتتمثل في الآتي:

١- عدم كفاية التشفير للبيانات والمعلومات.

٢- عدم ملاءمة إجراءات منع السرقة والوصول غير المشروع للمعلومات.

٣- غياب أو عدم سلامة إجراءات الدعم والمساندة.

٤- مواجهة المخاطر المادية كالحرائق.

٥- غياب إجراءات النسخ الاحتياطي.

ب) مخاطر متعلقة بتطبيقات تكنولوجيا المعلومات وتشمل:

١- عدم كفاية إجراءات تأمين البرمجيات المتصلة بأمن البنية التحتية لتكنولوجيا المعلومات.

٢- عدم كفاية ضوابط الإدخال واستخراج البيانات.

٣- الخلل أو الأخطاء في تطبيقات تكنولوجيا المعلومات.

٤- التغيرات غير المصرح بها في البرامج المستخدمة.

ج) مخاطر تتعلق بالتجارة الإلكترونية:

يشير معهد المحاسبين القانونيين الأمريكي إلى أن مخاطر التجارة الإلكترونية ترجع إلى الآسباب الآتية (Gantiz, 2014, 35:50) (Davis, 2021, 25:30):

١- **الهجمات المتعمدة:** وتحدث بواسطة قراصنة الإنترنت أو منافسي المنظمة بهدف الوصول إلى المعلومات السرية للشركة، كأرقام بطاقات اعتماد العملاء مثلاً، والمعلومات السرية المتعلقة بالعملاء، وحجم المبيعات، وأمور كثيرة قد يصعب حصرها.

٢- **خصوصية التعامل:** تعد التعاملات الإلكترونية التي تتم بين الأفراد والشركة ذات طابع معلوماتي مهم جدًا، وذلك لأنها تحفظ على ذاكرة النظام الرقمية، وهي معلومات قيمة جداً، قد يتمكن أحد من معرفتها أو

حتى تتبعها واختراقها وبالتالي سيفقد العميل الثقة بالشركة التي تعامل معها من منطلق أنها لم تتمكن من حماية خصوصيته.

٣- **فقدان الثقة:** يقصد بها فقدان ثقة المنظمة بمعلومات عميلها، فمن المتعارف عليه أن العميل يستخدم ما يسمى التوقيع الرقمي الخاص به لدخول نظام المنظمة وذلك لإتمام عمليته المرغوب فيها، فكيف إذا تمكن الشخص غير الصحيح بالدخول مستخدمًا توقيع العميل.

٤- **فشل عملية التحويل:** على الرغم أن عملية الشراء الإلكترونية تتم بسرعة كبيرة جدًا، إلا أنها عرضه لخطر فشل عملية التحويل، فمن المتعارف عليه أن عملية الشراء عبر التجارة الإلكترونية تتم من خلال عدة خطوات، فيبدأ المستهلك بملء النموذج الابتدائي وخطوات أخرى قد تكون ضرورية وفقاً لسياسات الشركة، ففي كل مرحلة تفتح صفحة جديدة عبر موقع المنظمة ولأسباب تقنية أو أخرى، قد تفشل إحدى الخطوات، وهنا ستظهر مشكلة جديدة وهي عدم التأكد من إتمام العملية.

٥- **غياب التوثيق:** يتم في التجارة التقليدية عادة توثيق الصفقة بأوراق ثبوتية مرسومة بشعار المنظمة وموقعة من قبل الشخص المناسب، وبواسطة اتصال شخصي ومباشر بين البائع والمشتري، ولكن تعد جميع تلك الأمور في التجارة الإلكترونية شبه مفقودة بالكامل، وهذه الحقيقة تزيد من احتمالية التعامل مع الشخص غير الصحيح.

٦- **سرقة الهوية:** مع غياب التوثيق المناسب كما في التجارة التقليدية أصبح من السهل على المجرمين انتحال شخصية الغير والقيام بالعمليات دون علمه.

٧- **تزوير الحقائق:** سوف تكون خدمات بعض مسوقي ومزودي خدمات الحماية، خدمات تجميلية فقط في غياب آلية معينة تؤكد مصداقيتهم وفاعلية خدماتهم.

٨- **آثار ضغوط الاقتصاد:** أدى النمو المتسارع للتجارة الإلكترونية، إلى أن أصبحت سوقًا تنافسيًا، كما أصبحت قوة المتنافس الحقيقية تكمن في نجاح آليات الآمان والموثوقية المتعلقة بنظامه المحاسبي، فكل من يستطيع توفير هذه الآليات يكون نصيبه أكبر في هذا السوق التكنولوجي العالمي.

د) مخاطر متعلقة بالإختراقات التى تتم عبر شبكة الإنترنت

وترجع أسباب صعوبة تعقب الاختراقات التي تتم عبر شبكة الإنترنت فيمايلي:

١- سرعة العملية، قد لا يحتاج الدخيل (المخترق) إلى أكثر من بعض دقائق لاختراق موقع معين والتلاعب به ومغادرة الموقع قبل أن يتم تعقبه.

٢- عدم وجود هوية محددة، لا يمكن معرفة ماهية المخترق، ولا بأي شكل من الأشكال.

٣- تباعد المسافات، قد يكون المخترق لموقع ما يبعد آلاف الكيلومترات وفي بلد آخر، فشبكة الإنترنت صممت بشكل عالمي.

٤- إمكانية الدخول من عدة أماكن، فالمتعامل عبر الإنترنت لا يحتاج إلى مكان محدد لدخول الشبكة، فأي شخص يمكنه الدخول إلى الشبكة من أي مكان يوجد فيه جهاز كمبيوتر وخط اتصال، مثل مقاهي الإنترنت ومختبرات الجامعات والمدارس.

٥- عدم وجود قوانين دولية، فشبكة الإنترنت شبكة عالمية ذات معايير موحدة للاستخدام فقط ولو أننا افترضنا اكتشاف أحد المخترقين بدولة مغايرة لدولة المنظمة التي تم اختراقها، فإنه ليس من الضرورة وجود قوانين موحدة للتعامل مع المخترق.

٦- إمكانية إتلاف بيانات جهاز الكمبيوتر في حالة شعور أي مخترق بإمكانية تعقبه تستطيع إتلاف جهازه بضغطه زر بسيطة، مما يجعل عملية تعقبه عديمة الجدوى والفائدة.

١/٢/٨ أسباب المخاطر التى تواجه نظم المعلومات الإلكترونية

تتعرض مقومات نظام المعلومات الإلكترونية (الأفراد، الإجراءات، البيانات، البرامج، البنية التحتية لتكنولوجيا المعلومات، الرقابة الداخلية، متطلبات أمن المعلومات) للمخاطر لأى سبب من الأسباب التالية: (خليل، وابراهيم، ٢٠١٤) (أبو رمان، ٢٠٢١، ٣٠: ٣٥) (المنيزل، ٢٠٢١، ٤٠: ٤٥)

١- زيادة خبرة الافراد بإستخدام الكمبيوتر ومعرفة نقاط الضعف فى النظام الذى يمكن اختراقه من خلالها من قبل موظفي المنظمة .

٢- عدم توافر الحماية الكافية ضد مخاطر الفيروسات والقرصنة.

٣- عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمي، وعدم فصل المهام والوظائف المتعلقة بنظم المعلومات لدى المنظمة .

٤- عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات لدى المنظمة .

٥- عدم تطبيق مبادئ ومعايير حوكمة أمن المعلومات

٦- ضعف وعدم كفاءة النظم الرقابية المطبقة على اكتشاف تلك المخاطر فى حالة حدوثها.

٧- اشتراك البعض من موظفى المنظمة فى استخدام كلمات السر ذاتها للدخول إلى النظام.

٨- التقدم التكنولوجى وتطور البرامج السريع فى صناعة الحاسبات.

١/٢/٩ مدى حاجة بيئة الأعمال الحديثة لإجراءات وقائية لنظم المعلومات الإلكترونية

إن عدم وجود ضوابط وإجراءات ملاءمة تتيح فرص التلاعب والتخريب في نظم المعلومات الإلكترونية بواسطة أشخاص غير مسئولين من داخل أو خارج الشركة.

وبشكل عام، يُطلب من مدقق تكنولوجيا المعلومات اختبار الضوابط المتعلقة بالتكنولوجيا، وكحد أدنى، يتعين على جميع المدققين فهم البيئة الرقابية للمؤسسة الخاضعة للتدقيق من أجل تقديم ضمانات بشأن الضوابط الداخلية العاملة في المنظمة. وفقًا للمبادئ الأساسية للمعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة للرقابة على القطاع العام، فإنه يجب على المدققين الحصول على فهم لطبيعة الجهة

أو القسم أو البرنامج الذي سيتم تدقيقه، ويتضمن ذلك فهم الضوابط الداخلية، بالإضافة إلى الأهداف والعمليات والبيئة التنظيمية والأنظمة والعمليات التجارية المعنية.

وتتمثل الإجراءات الرقابية (مقومات نظام الرقابة الداخلية الفعال) في ظل نظم المعلومات الإلكترونية في ثلاث مجموعات رئيسية هي: (المنيزل، ٢٠٢١، ٢٣ :٢٥) (الوهيب، ٢٠٢٢، ٣٦: ٥١)

١- الإجراءات الرقابية العامة.

٢- الإجراءات الرقابية على التطبيقات.

٣- الإجراءات الرقابية على قاعدة البيانات

وفيما يلي عرضاً موجزاً لهذه الإجراءات:

١- الإجراءات الرقابية العامة:

هي الإجراءات التي تتصل بجميع أو معظم التطبيقات التي تتم بواسطة الحاسب الآلي وتتعلق تلك الإجراءات بالرقابة على ما يلي:

أ- **الفصل بين الوظائف:**

يجب أن يتم فصل الوظائف في قسم المعالجة الإلكترونية للبيانات والوظائف في الأقسام المستخدمة للمعلومات وتزداد أهمية هذا الفصل في حالة الوظائف المتعلقة بكل من:

١. الصلاحيات بالتفويض

٢. التنفيذ والتسجيل

٣. المحافظة على الأصول

٤. المسئولية المحاسبية

فقسم المعالجة الإلكترونية يجب أن يكون مسئولاً فقط عن وظيفة التسجيل وتكون الوظائف الأخرى من مسئوليات الأقسام الأخرى داخل المنظمة .

ب-صلاحيات تفويض وتصديق عمليات تطوير، وشراء، وتغيير البرامج قبل استخدامها في معالجة البيانات:

وتشمل هذه الصلاحيات ما يلي:

١. يجب أن تتم مشاركة الأقسام المستخدمة للمعلومات في تصميم النظم جنبًا إلى جنب مع قسم المعالجة الإلكترونية.

٢. يجب أن يشارك موظفو الأقسام المستخدمة للمعلومات مع موظفي قسم المعالجة الإلكترونية في تجربة النظم الجديدة.

٣. يجب الحصول على موافقة كل من إدارة المنظمة , الأقسام المستخدمة للمعلومات، وقسم المعالجة الإلكترونية على إدخال النظم الجديدة قبل البدء في استخدام تلك النظم.

٤. يجب إحكام الرقابة على نقل أو نسخ الملف الرئيسي أو بعض ملفات العمليات وذلك لمنع التغيير غير المسموح به في محتوياتها ولضمان دقة النتائج عند استخدام تلك الملفات.
٥. يجب أن يتم التوثيق بصورة جيدة للبرامج والنظم وكذلك التغييرات التي تحدث فيها.
٦. يجب توثيق مقترحات التغيير التي تتقدم بها الأقسام المستخدمة للمعلومات أو يتقدم بها قسم المعالجة الإلكترونية.
٧. يجب أن يقوم مدير قسم نظم المعلومات بدراسة وتقييم جميع التغييرات التي تتم في البرامج والنظم.
٨. يجب أن يتم اختبار البرامج التي يتم تعديلها باستخدام بيانات الاختبار.
٩. يجب أن تتم مقارنة البرامج التي يتم تشغيلها مع النسخ المحفوظة من تلك البرامج بغرض اكتشاف أي تغييرات غير مصرح بها في تلك البرامج.

ج- صلاحيات الوصول إلى ملفات البيانات:

وتشمل هذه الصلاحيات ما يلي:

١. يجب تحديد صلاحية الوصول إلى البرامج وملفات البيانات وأجهزة الحاسب فقط في الأشخاص المفوضين بالتعامل معها كموظفي التشغيل والمشرفين عليهم وغيرهم من المسموح لهم بالوصول إلى الأجهزة والبرامج والبيانات.
٢. يجب التحكم في الدخول إلى غرفة الحاسب الآلي لمنع غير المصرح لهم من دخولها.
٣. يجب الاحتفاظ بسجل للزوار الذين يقومون بزيارة غرفة الحاسب الآلي بعد الإذن لهم بذلك وبمرافقته أحد الأشخاص المصرح لهم.
٤. يجب استخدام الرمز الشخصي أو كلمة المرور لحصر الوصول إلى البرامج في الأشخاص المفوضين بذلك.
٥. استخدام نظام الاستدعاء لتحديد وتمييز الأشخاص المفوضين بالدخول على نظام الحاسب.
٦. يجب ترميز البيانات عند تخزينها في الملفات أو عند نقلها من المواقع القديمة إلى نظام الحاسب عبر الشبكات أو غيرها.
٧. منح مشغلي البرامج حرية الوصول إلى أدلة التشغيل التي تحتوي على تعليمات المعالجة مع حجب تفاصيل البرامج عنهم.
٨. يجب أن يقوم فريق المراقبة بمراقبة نشاطات المشغلين وجدولة أعمالهم.

د- الإجراءات الرقابية العامة المبنية في النظام نفسه

هناك إجراءات رقابية عامة مبنية في نظام الحاسب الآلي وهذه الإجراءات تضفى على الحاسب ثقة قصوى من جانب من يستخدمه وترجع هذه الثقة بشكل أساسي إلى تقدم وتطور تقنية الرقائق والإجراءات المبنية في نظام الحاسب عبارة عن وسائل تشخيص ذاتي لاكتشاف ومنع أعطال الأجهزة، **وفيما يلي استعراض لبعض تلك الإجراءات:**

- **أجهزة وبرامج التشخيص:** هي عبارة عن أجهزة وبرامج التي يوفرها صانعوا الحاسبات الآلية مع تلك الحاسبات لاستخدامها في فحص العمليات وأساليب المعالجة الإلكترونية داخل نظام الحاسب الآلي.
- **حماية نطاق التشغيل:** في معظم وحدات المعالجة المركزية يتم إجراء عدة عمليات تشغيل في وقت واحد ولكي يتم التأكد من أن العمليات التي يتم تشغيلها في آن واحد لن تتداخل على بعضها البعض (مما يتسبب في التلف أو التغيير) فإن البرامج تحتوى على إجراءات لحماية نطاق كل عملية تشغيل.

هـ-إجراءات رقابية عامة أخرى

هناك إجراءات رقابية عامة أخرى، تتمثل فيما يلي:

١. استخدام نظام الاحتفاظ بملفات احتياطية لاسترجاع البيانات عند التلف، للمحافظة على السجلات والقدرة على تصحيح حالات الخطأ أو الفشل المفاجئ.
٢. المعالجة في الحالات الطارئة، ووضع خطط تفصيلية لمقابلة أي فشل في النظام تفصل هذه الخطط مسئوليات الأفراد وتوضح مواقع التشغيل البديلة التي يمكن استخدامها عند الحاجة.
٣. بطاقات التمييز، عبارة عن ديباجة ورقية لاصقة توضع على وسيلة تخزين البيانات لتمييز الملف.

٢- الإجراءات الرقابية على التطبيقات

يتعلق هذا النوع من الإجراءات الرقابية باستخدام الحاسب الآلي للقيام بتطبيقات محددة ويمكن أن تكون هذه الإجراءات إجراءات يدوية أو إجراءات إلكترونية، **وتنقسم هذه الإجراءات إلى ثلاث أنواع هي:**

أ- **الإجراءات الرقابية على المدخلات:** حيث يتم التأكد على أن البيانات التي يتم استلامها للمعالجة بالحاسب الآلي تمثل عمليات تم التصديق عليها بصورة سليمة وأن البيانات دقيقة وصحيحة ومكتملة لحظة إدخالها في الحاسب.

ب-**الإجراءات الرقابية على التشغيل (المعالجة):** الغرض من هذه الإجراءات التأكيد على مصداقية ودقة المعالجة الإليكترونية للبيانات الخاصة بالتطبيق المعين وبالتحديد تهدف تلك الإجراءات إلى التأكيد بأن جميع العمليات قد تمت معالجتها بموجب تفويض محدد، وأن

جميع العمليات التي تم التصديق على معالجتها آلياً قد تمت معالجتها ولم يحذف منها شيء، وأنه لم يتم إضافة أي عمليات غير مصرح بمعالجتها إلى العمليات التي تم التصريح بمعالجتها **وتتخذ الإجراءات الرقابية على التشغيل أشكالاً عديدة منها:**

١. **استخدام المجاميع الرقمية:** عبارة عن مجموع رقابي لا معنى له للأغراض المالية ولكنه مجموع رقمي يستخدم لأغراض الرقابة.

٢. **رقم الاختبار:** يستخدم كوسيلة للتأكد من صحة الأرقام التي تميز حقول السجلات فعلى سبيل المثال: استخدام رقم اختبار للتأكد من صحة أرقام حسابات العملاء في البنك.

ج- **الإجراءات الرقابية على المخرجات:** تهدف إلى:

١. التأكد من مصداقية وصحة المخرجات (المعلومات) التي يتم إنتاجها بعد المعالجة الإليكترونية للبيانات.

٢. التأكيد بأن تلك المخرجات قد تم تسليمها إلى الموظفين المفوضين باستخدامها فقط وليس إلى أشخاص غير مصرح لهم باستخدامها.

٣- <u>الإجراءات الرقابية على قاعدة البيانات:</u>

هناك بعض الإجراءات الرقابية الخاصة بنظم قاعدة البيانات، ومنها:

أ- وجود إجراءات رقابية تحدد حرية الوصول إلى قاعدة البيانات فقط عن طريق الأشخاص المصرح لهم.

ب-تنسيق أنشطة مستخدمي قاعدة البيانات والتحكم فيها بحيث تكون الرقابة على البيانات متناسبة مع أهمية تلك البيانات.

ج- يقتضي اشتراك عدد كبير من المستخدمين في نفس ملفات البيانات أن تكون هناك رقابة محكمة على تلك الملفات لمنع التغيير أو الضياع.

د- اتخاذ الإجراءات الاحتياطية اللازمة للمحافظة على استمرار النظام مثل:

١. استخدام برامج الحماية اللازمة مثل الجدار الناري لمنع اقتحام الشبكة من جانب المتطفلين، وبرامج الحماية من الفيروسات.

٢. وجود بيانات وبرامج احتياطية محفوظة خارج موقع العمل.

٣. إجراءات محددة تتخذ في الحالات الطارئة مثل حالات السرقة والضياع للبيانات أو البرامج.

٤. توفير المعالجة من خارج المنظمة في حالات حدوث كوارث.

ملخص الفصل الأول

يتطلب تدقيق تكنولوجيا المعلومات والاتصالات اتباع نهج شامل يشمل الجوانب المالية وجوانب الأداء والامتثال. ورغم أن الكفاءة من حيث التكلفة والامتثال تعتبر اعتبارات أساسية، فمن المهم بنفس القدر تقييم ما إذا كانت تكنولوجيا المعلومات والاتصالات تحقق النتائج المقصودة، وما إذا كانت تقدم القيمة مقابل المال، وما إذا كانت تلبي احتياجات المواطنين وأصحاب المصلحة. ونظرًا للطبيعة المترابطة للبنية التحتية لتكنولوجيا المعلومات والاتصالات والنمو السريع للخدمات المشتركة والمبادرات المشتركة بين الوكالات، يجب على المدققين العمل بشكل وثيق مع الكيانات ذات الصلة لضمان اتباع نهج موحد وشامل لكل من الرقابة الداخلية والخارجية. ومن خلال تعزيز التعاون وتبادل المعلومات، يمكن للمدققين تعزيز تأثير عمليات التدقيق التي يقومون بها وتعزيز المساءلة عبر النظام البيئي لتكنولوجيا المعلومات والاتصالات.

وقد استعرض الفصل أهمية تدقيق تكنولوجيا المعلومات ونظم المعلومات الإلكترونية، مشيرًا إلى أهمية فحص وتقييم الأمان والسلامة والتوافق مع القوانين واللوائح. كما تناول الفصل أيضًا الضوابط المتبعة في هذا المجال وأهمية تطبيقها الصارم، مع التركيز على مخاطر الأمان المحتملة وسبل التصدي لها والوقاية منها.

تمحور الفصل أيضًا حول مسار تدقيق تكنولوجيا المعلومات وأساليب تقييم المخاطر وتحليل الثغرات في أنظمة المعلومات، بما في ذلك التهديدات الداخلية والخارجية. كما شمل الفصل أمثلة على الملاحظات الشائعة في تقارير تدقيق تكنولوجيا المعلومات، وكذلك دور التدقيق في الحفاظ على سرية وموثوقية المعلومات وضمان توافرها وتنفيذ سياسات الأمان بفعالية.

كما يُسلط الضوء على أهمية توثيق عمليات التدقيق وتقديم التوصيات لتحسين الأمان وتقليل المخاطر المحتملة، وتسليط الضوء على التحديات والحلول في مجال تدقيق تكنولوجيا المعلومات ونظم المعلومات الإلكترونية.

الفصل الثاني

الدراسة التطبيقية

الفصل الثاني
الدراسة التطبيقية

٢/١ المقدمة

هدف هذا البحث إلى تحليل تأثير سياسات تدقيق أمن المعلومات على تقليل مخاطر نظم المعلومات الإلكترونية في البنوك المصرية، وتقديم التوصيات اللازمة لتعزيز أمان المعلومات والبيانات في هذه البنوك، وذلك من خلال توصيف البيانات الأولية التي حصل عليها الباحث عن طريق إعداد وتوزيع قائمة الاستبيان التي اعتمد عليها في جمع البيانات، بالإضافة إلى اختبار فرضيات البحث والحصول على النتائج وتقديم التوصيات التي تعزز من أمن المعلومات في البنوك المصرية.

٢/٢ فرضيات الدراسة

انطلاقاً من الأهداف السابق ذكرها، سعت الدراسة إلى اختبار مدى صحة الفرضية الرئيسية التالية:

يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية.

والفرضيات الفرعية التالية:

١. يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر الإدخال في البنوك.
٢. يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر التشغيل في البنوك.
٣. يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر المخرجات في البنوك.
٤. يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من المخاطر البيئية في البنوك.

٢/٣ الأساليب الإحصائية المستخدمة في الدراسة

ولتحقيق أهداف الدراسة اعتمد الباحث على بعض الأساليب الإحصائية الوصفية، وبعض الأساليب الإحصائية الاستدلالية.

أ. الأساليب الإحصائية الوصفية:

تم الاعتماد على بعض المقاييس الوصفية لوصف بيانات البحث كما يلي:

١- الوسط الحسابي:

هو مؤشر لتحديد الأهمية النسبية لكل عنصر من عناصر السؤال، والأوزان النسبية التي تم تخصيصها لردود مفردات العينة على أسئلة الاستقصاء باستخدام المعادلة الرياضية التالية:

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

حيث:

$\bar{x}$: الوسط الحسابي للأوزان النسبية.

$\sum_{i=1}^{n} x$: مجموع الأوزان النسبية التي تم تحديدها بالردود.

n : حجم العينة.

٢- الانحراف المعياري:

هو أحد مقاييس التشتت، ويستخدم كمؤشر لتحديد انحرافات القيم عن وسطها الحسابي ويحسب بالجزر التربيعي لمتوسط مربعات القيم عن وسطها الحسابي، ويفيد في قياس التشتت أو التجانس بين الآراء، ويزيد التجانس بين الآراء عندما يقل الانحراف المعياري، ويزيد التشتت بين الآراء عندما يزيد الانحراف المعياري، ويحسب كالتالي:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x - \bar{x})^2}{n}}$$

حيث تشير (σ) إلى الانحراف المعياري

ب. الأساليب الإحصائية الاستدلالية:

اختبار "ت" T Test:

وهو اختبار يستخدم في معرفة الفرق المعنوي للوسط الحسابي المحسوب للعينة، من حيث كونه معنوياً أو غير معنوي، فإذا كانت مستوى المعنوية P-Value أقل من ٠,٠٥ فيكون هناك اختلاف أو فروق معنوية، أما إذا كانت قيمة الدلالة أكبر من ٠,٠٥ فلا يكون هناك يوجد اختلاف أو فروق معنوية.

وبرنامج SPSS إصدار ٢٥ يعطي قيمة الدلالة P-Value، حيث يتم مقارنتها بقيمة المعنوية ٥%، فإذا كانت قيمة الدلالة أصغر من قيمة المعنوية ٥% يتم قبول الفرض القائل بوجود علاقة بين المتغيرين والعكس صحيح.

٢/٤ قائمة الاستقصاء

في ضوء البيانات اللازمة لاختبار فرضيات الدراسة قام الباحث بتصميم قائمة استبيان، والتي شملت مجموعة من العبارات التي تقيس دور سياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية، بالاعتماد على مجموعة من العبارات معتمدة على مقياس ليكرت الخماسي.

٢/٥ مجتمع وعينة البحث

تألف مجتمع الدراسة من أعضاء الجهاز الجهاز الأعلى للرقابة في مصر وموظفي القطاع المالي وقطاع تكنولوجيا المعلومات وقطاع المراجعة الداخلية في أحد البنوك المصرية، تم توزيع أداة الدراسة على عينة ملائمة وممثلة لمجتمع الدراسة، وتم أخذ عينة عشوائية من مجتمع الدراسة حيث تمثلت وحدة المعاينة بـ (المدراء، المدققين الخارجيين، والمحاسبين، ورؤساء الأقسام والمدققين الداخلين ومساعديهم، موظفي تكنولوجيا المعلومات) وزعت عليهم (٥٠) استبانة، تم استردادها منهم بالكامل بنسبة ١٠٠%.

تمت مراجعة كل قائمة من القوائم المستلمة من المستقصى منهم، للتأكد من اكتمالها وصلاحيتها لإدخالها في التحليل الإحصائي، والجدول التالي يوضح ذلك:

الجدول رقم (١)

بيان بقوائم الاستقصاء الموزعة والمستلمة والصالحة للتحليل الإحصائي

بيان	القوائم الموزعة	القوائم غير المستلمة	القوائم المستلمة	القوائم المستبعدة	القوائم الصالحة
العدد	٥٠	٠	٥٠	٠	٥٠
%	١٠٠	٠	١٠٠	٠	١٠٠

يتضح من خلال الجدول السابق أن نسبة الاستجابة تصل إلى (١٠٠%)، وكانت القوائم الصالحة لتحليل الإحصائي تبلغ (١٠٠%) من إجمالي القوائم الموزعة والبالغ عددها (٥٠) استمارة.

٢/٦ الجداول التكرارية والنسبية

استخدم الباحث هذه الجداول لاستنتاج عدد ونسب الاستجابات من المبحوثين ووضعها في جدول من عمودين يمثل الأول التكرارات والثاني النسبة من حجم العينة كما هو موضح في الجداول التالية:

جدول رقم (٢)

يوضح عدد ونسبة المبحوثين في العينة

المتغيرات الديموغرافية		التكرارات	النسبة (%)
المؤهل	بكالوريوس	٤٢	٨٤
	عضوية جمعيات مهنية	٢	٤
	ماجستير	٤	٨
	دكتوراه	٢	٤
	الإجمالي	٥٠	100
النوع	ذكر	٣٠	٦٠
	أنثى	٢٠	٤٠
	الإجمالي	٥٠	100
الخبرة العملية	من ٥ سنة وأقل من ١٠	٢	٤
	من ١٠ سنة وأقل من ٢٠	٣	٦
	٢٠ سنة فأكثر	٤٥	٩٠
	الإجمالي	٥٠	100
المسمى الوظيفي	مدير مالي	٥	١٠
	مدير رقابة	١٠	٢٠
	مدققون داخليون / خارجيون / محاسبون	٢٠	٤٠
	موظفي تكنولوجيا معلومات	١٥	٣٠
	الإجمالي	٥٠	١٠٠

٢/٧ الإحصاءات الوصفية

وصف أبعاد المتغير المستقل سياسات تدقيق أمن المعلومات

يهدف هذا الجزء إلى استخراج المتوسطات الحسابية والانحرافات المعيارية وبيان درجة الأهمية وترتيب

الفقرات لوصف اتجاهات عينة الدراسة نحو أبعاد سياسات تدقيق أمن المعلومات.

البعد الأول: صلاحية النظام

جدول (٣): المتوسط الحسابي والانحراف المعياري لاستجابة أفراد عينة الدراسة عن بعد صلاحية النظام

رقم الفقرة	الفقرات	المتوسط الحسابى	الانحراف المعياري	درجة الموافقة	النسية المئوية	الرتبة
1	توفر بنوك القطاع العام محل البحث حماية لأمن وسلامة جميع مكونات النظام.	3.61	0.914	متوسطة	72.2	5
2	تحرص بنوك القطاع العام محل البحث وبشكل دوري على إخضاع مستخدمي الأنظمة إلى محاضرات إرشادية.	3.49	0.980	متوسطة	69.8	6
3	تقوم بنوك القطاع العام محل البحث بالفصل بين مهام كل من محللي النظم، ومشغلي النظم، وموظفي قسم الحاسوب.	3.63	0.981	متوسطة	72.6	3
4	تمنح بنوك القطاع العام الصلاحية المناسبة والكافية لطاقم تدقيق أمن المعلومات.	4.28	0.775	مرتفعة	85.6	1
5	تعمل بنوك القطاع العام على اجراء الصيانة الدورية للمكونات المادية لنظام المعلومات.	3.61	0.974	متوسطة	72.2	4
٦	يحرص المدراء في بنوك القطاع العام على توفير الصلاحيات للمدقق الداخلي لإجراء عملية التدقيق.	٣,٧٠	٠,٨٦٧	مرتفعة	٧٤	٢
	المؤشر الكلى	**٣,٧٢**	**٠,٥٧٣**	**مرتفعة**	**%٧٤,٤**	

يشير الجدول السابق إلى أن هذا البعد حقق وسطاً حسابياً (٣,٧٢) وبنسبة (٧٤,٤%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٥٧٣)، وهو ما يشير إلى أن مستوى صلاحية النظام قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد عينة الدراسة، ويعود السبب إلى أن بنوك القطاع العام تمنح الصلاحية المناسبة والكافية لطاقم تدقيق أمن المعلومات، كذلك يحرص المدراء في هذه البنوك على توفير الصلاحيات للمدقق الداخلي لإجراء عملية التدقيق.

البعد الثاني: واجبات فريق التدقيق

جدول (٤): المتوسط الحسابي والانحراف المعياري الاستجابة أفراد عينة الدراسة عن بعد واجبات فريق التدقيق

رقم الفقرة	الفقرات	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	النسية المئوية	الرتبة
7	يتمتع المدققين الداخليين في بنوك القطاع العام بالتأهيل العلمي اللازم لممارسة مهامهم بكفاءة	3.98	0.698	مرتفعة	79.6	3
8	تحدد بنوك القطاع العام مهام وواجبات فريق التدقيق وتحدد الصلاحيات الموكلة إليهم	4.01	0.691	مرتفعة	80.2	1

9	تمنح بنوك القطاع العام الثقة للأشخاص الذين يتولون مهمة الفحص والتأكد من صحة أمن وسلامة المعلومات	3.97	0.765	مرتفعة	79.4	4
10	يتعاون موظفي الإدارات في في بنوك القطاع العام مع المدققين الداخليين في التعامل مع أدوات حفظ أمن المعلومات	3.84	0.915	مرتفعة	76.8	6
11	توجه إدارات البنوك المدققين الداخليين على استخدام أدوات تكنولوجية حديثة	3.99	0.886	مرتفعة	79.8	2
12	يحرص مدققي الحسابات على حضور الندوات والمؤتمرات الخاصة ببيئة أمن وسلامة المعلومات والحصول على الشهادات المهنية في مجال تكنولوجيا المعلومات والتدقيق	3.85	0.999	مرتفعة	77	5
	المؤشر الكلي	**3.94**	**0.607**	**مرتفعة**	**%78.8**	

يشير الجدول (٤) إلى أن هذا البعد حقق وسطاً حسابياً (٣,٩٤) وبنسبة (٧٨,٨%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٦٠٧)، وهو ما يشير إلى أن مستوى واجبات فريق التدقيق قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد عينة الدراسة، ويعود السبب إلى أن بنوك القطاع العام تحدد كل من مهام وواجبات وصلاحيات فريق التدقيق، وكذلك يقوم موظفي الإدارات المختلفة بالتعاون مع المدققين الداخليين لإيجاد وسيلة التعامل مع أدوات حفظ أمن المعلومات.

البعد الثالث: تقارير نظام التدقيق الداخلي

جدول (٥): المتوسط الحسابي والانحراف المعياري لإجابات أفراد عينة الدراسة نحو بعد تقارير نظام التدقيق الداخلي

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
13	توجه إدارات البنوك المدققين إصدار تقرير المدقق الداخلي كأحد سياسات أمن المعلومات.	4.60	0.628	مرتفعة	92	1
14	يحرص فريق تدقيق أمن المعلومات على إصدار تقرير بنتائج التدقيق لمعالجة أي انحرافات أو أخطاء.	4.14	0.687	مرتفعة	82.8	2
15	ترفع تقارير التدقيق الداخلي لمدير القسم من أجل متابعة الإجراءات الالزامية لمعالجة أي استثناءات.	3.97	0.730	مرتفعة	79.4	4
16	يحرص فريق تدقيق أمن المعلومات على توفير تقارير التدقيق الداخلي وقت الحاجة.	3.85	0.921	مرتفعة	77	5
17	يقدم قسم التدقيق الداخلي تقرير لمجلس الإدارة عن المخاطر التي تتعرض لها البنوك وكيفية تجنبها.	4.10	0.788	مرتفعة	82	3
18	يحرص فريق تدقيق أمن المعلومات على مراجعة وتدقيق كافة المعاملات المالية لدى بنوك القطاع العام.	3.68	0.887	مرتفعة	73.6	6
	المؤشر الكلي	**4.06**	**0.539**	**مرتفعة**	**%81.2**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٤,٠٦) وبنسبة (٨١,٢) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٥٣٩)، وهو ما يشير إلى أن مستوى تقارير نظام التدقيق

الداخلي قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد عينة الدراسة، ويعود السبب إلى أن إدارات بنوك القطاع العام تقوم بتوجيه المدققين لإصدار تقرير يمثل نتائج عملية التدقيق لمعالجة أي انحرافات أو أخطاء، وحرص فريق تدقيق أمن المعلومات في في تلك البنوك على تدقيق ومراجعة كافة المعاملات المالية لديها.

البعد الرابع: التوثيق والأدلة

جدول (٦): المتوسط الحسابي والانحراف المعياري لإجابات أفراد عينة الدراسة نحو بعد التوثيق والأدلة

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
19	تحرص بنوك القطاع العام على وضع التعليمات الخاصة بتوثيق عملية التدقيق.	3.99	0.756	مرتفعة	79.8	1
٢٠	تحرص بنوك القطاع العام على وضع ضوابط رقابية على المستندات وتسلسل إجراءات إدخال البيانات للنظام.	3.78	0.912	مرتفعة	75.6	5
21	تقوم بنوك القطاع العام بتجميع الأدلة من مصدرها الرئيسي والتثبت من دقة المعلومات الواردة فيها.	3.93	0.824	مرتفعة	78.6	3
22	تحتفظ البنوك بنسخة من برامج المعالجة في مكان مناسب وتسجل مخرجات النظام كوسيلة رقابية.	3.64	0.863	متوسطة	72.8	6
23	تؤكد بنوك القطاع العام على ضرورة توثيق كافة الإجراءات والآليات المتبعة خلال العمل على تدقيق أمن المعلومات.	3.95	0.901	مرتفعة	79	2
24	تحرص البنوك على التأكد من مدى ملائمة الأدلة وكفايتها للحصول على تقرير أمن المعلومات.	3.91	0.905	مرتفعة	78.2	4
	المؤشر الكلي	**3.87**	**0.649**	**مرتفعة**	**%77.4**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٣,٨٧) وبنسبة (٧٧,٤%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٦٤٩)، وهو ما يشير إلى أن مستوى التوثيق والأدلة قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد عينة الدراسة، ويعود السبب إلى أن تلك البنوك تعمل على وضع تعليمات مختصة بتوثيق عملية التدقيق لديها، واحتفاظها بنسخة من برامج المعالجة في أماكن مناسبة، وتسجيل مخرجات النظام.

البعد الخامس: ميثاق السلوك الخاص بتدقيق امن المعلومات

جدول (٧): المتوسط الحسابي والانحراف المعياري لإجابات أفراد عينة الدراسة نحو بعد ميثاق السلوك الخاص بتدقيق أمن المعلومات

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
25	تلتزم بنوك القطاع العام بميثاق السلوك الخاص بتدقيق أمن المعلومات.	3.74	0.844	مرتفعة	74.8	5

26	يحرص مدققي الحسابات الداخليين بالبنوك على أداء الواجبات الموكلة إليهم بشكل هادف وعناية فائقة.	3.75	0.734	مرتفعة	75	4
27	يتقيد مدققي الحسابات الداخليين في البنوك بالمحافظة على سرية وخصوصية المعلومات التي تم جمعها.	3.68	1.027	مرتفعة	73.6	6
28	يحرص مدققي الحسابات الداخليين في البنوك على تقديم نتائج دقيقة لعملية التدقيق بأكملها.	3.82	0.894	مرتفعة	76.4	2
29	تدعم بنوك القطاع العام الجهود التوعوية التي تهدف إلى مساعدة المتعاملين معها لتطوير فهمهم لأمن وإدارة نظم المعلومات.	3.80	0.750	مرتفعة	76	3
30	تخضع بنوك القطاع العام لعقوبات رادعة وصارمة في حال إخفاق المدقق بالعمل في ميثاق السلوك الخاص بتدقيق أمن المعلومات.	4.06	0.937	مرتفعة	81.2	1
	المؤشر الكلي	**3.81**	**0.670**	**مرتفعة**	**%76.2**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٣,٨١) وبنسبة (٧٦,٢%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٦٧٠)، وهو ما يشير إلى أن مستوى ميثاق السلوك الخاص بتدقيق أمن المعلومات قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد عينة الدراسة، ويعود السبب إلى أن البنوك تعمل على وضع تعليمات مختصة بتوثيق عملية التدقيق لديها، واحتفاظها بنسخة من برامج المعالجة في أماكن مناسبة، وتسجيل مخرجات النظام.

البعد السادس: التدقيق الخارجي

جدول (٨): المتوسط الحسابي والانحراف المعياري لإجابات أفراد عينة الدراسة نحو بعد التدقيق الخارجي لتكنولوجيا المعلومات

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
٣١	التدقيق الخارجي لتكنولوجيا المعلومات في البنك يتم بصفة دورية مناسبة من ٢إلى ٥ سنوات	3.74	0.844	مرتفعة	74.8	5
٣٢	يحرص مدققي تكنولوجيا المعلومات الخارجيين على أداء واجباتهم بشكل هادف وعناية فائقة.	3.75	0.734	مرتفعة	75	4
٣٣	يحرص مدققي تكنولوجيا المعلومات الخارجيين على اتباع المعايير والأدلة والإرشادات المتعلقة بتكنولوجيا المعلومات والصادرة من المنظمات المهنية الدولية والمحلية.	3.68	1.027	مرتفعة	73.6	6
٣٤	يحرص مدققي تكنولوجيا المعلومات الخارجيين على تقديم نتائج دقيقة لعملية التدقيق بأكملها.	3.82	0.894	مرتفعة	76.4	2
٣٥	يقدم تقرير المدقق الخارجي لتكنولوجيا المعلومات توصيات تفيد في الحد من المخاطر التي تتعرض لها أنظمة المعلومات بالبنوك	3.80	0.750	مرتفعة	76	3
٣٦	يساعد التدقيق الخارجي لتكنولوجيا المعلومات من تعزيز أمن المعلومات والأمن السيبراني ويحد من مخاطر المدخلات ومخاطر التشغيل ومخاطر	4.06	0.937	مرتفعة	81.2	1

	المخرجات والمخاطر البيئية					
	المؤشر الكلي	**3.81**	**0.670**	**مرتفعة**	**%76.2**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٣,٨١) وبنسبة (٧٦,٢%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٦٧٠)، وهو ما يشير إلى أن مستوى التدقيق الخارجي لتكنولوجيا المعلومات قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد عينة الدراسة، ويعود السبب إلى أن التدقيق الخارجي لتكنولوجيا المعلومات يساعد في تعزيز أمن المعلومات والأمن السيبراني ويحد من مخاطر المدخلات ومخاطر التشغيل ومخاطر المخرجات والمخاطر البيئية، كما يحرص مدققي تكنولوجيا المعلومات الخارجيين على تقديم نتائج دقيقة لعملية التدقيق.

ثانيا: مخاطر نظم المعلومات الإلكترونية

المجال الأول: مخاطر الادخال

جدول (٩): المتوسط الحسابي والانحراف المعياري لاستجابة أفراد عينة الدراسة عن مخاطر الادخال

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
٣٧	تحرص بنوك القطاع العام على عقد دورات تدريبية لتوعية مدخلي البيانات بكيفية وأهمية الحفاظ على أمن المعلومات.	3.68	0.768	مرتفعة	73.6	6
٣٨	عدم اشتراك الموظفين بنفس كلمة السر وإجبار كل موظف في البنوك على تغييرها بشكل دوري	3.97	0.858	مرتفعة	79.4	4
٣٩	تعمل نظم المعلومات في البنوك على مراجعة المدخلات والتأكد من صحتها والحد من إدخال البيانات الخاطئة.	4.25	0.720	مرتفعة	85	1
٤٠	تحرص البنوك على ضبط عملية إدخال البيانات وتعديلها إلا من قبل الموظفين المخول لهم بذلك.	4.11	0.787	مرتفعة	82.2	2
٤١	تستفيد البنوك دائما من التطورات التكنولوجية في مجالات برامج حماية أنظمة المعلومات مثل برامج التشفير.	3.73	0.785	مرتفعة	74.6	5
٤٢	تستخدم البنوك أجهزة إنذار تنبيهيه في حال الدخول غير المصرح بإدخال البيانات.	4.04	0.886	مرتفعة	80.8	3
	المؤشر الكلي	**3.96**	**0.635**	**مرتفعة**	**79.2**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٣,٩٦) وبنسبة (٧٩,٢%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٦٣٥)، وهو ما يشير إلى أن مستوى الحد من مخاطر إدخال البيانات قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد العينة.

المجال الثاني: مخاطر التشغيل

جدول (١٠) المتوسط الحسابي والانحراف المعياري لإجابات أفراد عينة الدراسة نحو مخاطر التشغيل

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
٤٣	تمتلك بنوك القطاع العام نظم معلومات تمنع تعديل البيانات من قبل الأفراد غير المصرح لهم.	4.00	0.848	مرتفعة	80	5
٤٤	توفير الحماية الكافية في البنوك من خلال استخدام البرامج المضادة للفيروسات والجدران النارية.	4.33	0.694	مرتفعة	86.6	3
٤٥	التواصل مع مزود خدمة الإنترنت لاسترجاع الخدمة بأسرع ما يمكن في حال قطعها عن البنوك.	4.73	0.450	مرتفعة	94.6	1
٤٦	فحص البرامج والأقراص الممغنطة الجديدة قبل إدخالها إلى أجهزة الكمبيوتر بشكل دوري.	4.06	0.689	مرتفعة	81.2	4
٤٧	تمتلك البنوك نظم معلومات قادرة على التنبؤ بمخاطر التشغيل والحد منها.	3.57	0.816	متوسطة	71.4	6
٤٨	تحرص البنوك على معالجة البيانات الكترونياً دون تدخل العنصر البشري بذلك.	4.54	0.688	مرتفعة	90.8	2
	المؤشر الكلي	**4.21**	**0.476**	**مرتفعة**	**84.2**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٤,٢١) وبنسبة (٨٤,٢%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٤٧٦)، وهو ما يشير إلى أن مستوى الحد من مخاطر التشغيل قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد العينة.

المجال الثالث: مخاطر المخرجات

جدول (١١): المتوسط الحسابي والانحراف المعياري لإجابات أفراد عينة الدراسة نحو مخاطر المخرجات

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
٤٩	تتبع مخرجات كل عملية وإرفاقها المستندات الثبوتية المعززة لوجودها في البنوك محل البحث.	3.89	0.760	مرتفعة	77.8	2
٥٠	تمنع نظم المعلومات المحاسبية لدى البنوك محل البحث تعديل التقارير الصادرة من النظام أو تزويرها.	3.05	0.922	متوسطة	61	6
٥١	تمتلك المؤسسات الحكومية نظم معلومات محاسبية قادرة على منع إمكانية خلق مخرجات غير حقيقية من قبل العاملين.	3.78	0.764	مرتفعة	75.6	4
٥٢	الاحتفاظ بمخرجات النظام الورقية في أماكن آمنة ومحكمة الإغلاق والقيام بأرشفتها لمنع ضياعها أو سرقتها أو إتلافها.	3.59	0.893	متوسطة	71.8	5
٥٣	وضع قواعد وأنظمة تحدد مسا ارت توزيع التقارير الناتجة عن النظام في البنوك محل البحث.	3.80	0.820	مرتفعة	76	3

٥٤	إصدار نسخ سرية لمخرجات نظم المعلومات في البنوك محل البحث لتسهيل عمليات الفحص والتقييم ومواجهة حالات السرقة أو التزوير.	3.90	0.781	مرتفعة	78	1
	المؤشر الكلي	**3.67**	**0.597**	**مرتفعة**	**%73.4**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٣٦٧) وبنسبة (٧٣,٤%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٥٩٧)، وهو ما يشير إلى أن مستوى الحد من مخاطر المخرجات قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد العينة.

المجال الرابع: مخاطر بيئية

جدول (١٢): المتوسط الحسابي والانحراف المعياري لإجابات أفراد عينة الدراسة نحو المخاطر البيئية

رقم الفقرة	الفقرات	المتوسط الحسابي	الإنحراف المعياري	درجة الموافقة	النسبة المئوية	الرتبة
55	هنالك وعي كاف بكيفية التعامل مع حالات الطوارئ عند حدوث الكوارث الطبيعية في البنوك محل الدراسة.	4.80	0.420	مرتفعة	96	1
56	تقوم البنوك بوضع خطة واضحة للتنبؤ بالأضرار الناجمة عن المخاطر البيئية وكيفية معالجتها والوقاية منها.	4.16	0.598	مرتفعة	83.2	3
57	تقوم إدارة المؤسسات الحكومية بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا.	4.08	0.670	مرتفعة	81.6	5
58	يستطيع المدقق الداخلي إصدار توجيهات لإدارة بضرورة تحمل إدارة البنوك جزء من مخاطر البيئة الخارجية الناتجة عن سوء الإدارة.	4.57	0.610	مرتفعة	91.4	2
59	تحرص البنوك محل الدراسة على وضع خطط لمواجهة العوامل البيئية مثل الزلازل والأعاصير والفيضانات والحرائق التي تؤثر على امن وسالمة نظم المعلومات الإلكترونية.	4.10	0.607	مرتفعة	82	4
60	تقوم البنوك محل الدراسة بعقد دو ارت تدريبية عن امن وسالمة نظم المعلومات الالكترونية في حال حدوث كوارث طبيعية أو كوارث غير طبيعية التي قد تؤثر على عمل النظام.	3.87	0.806	مرتفعة	77.4	6
	المؤشر الكلي	**4.26**	**0.393**	**مرتفعة**	**%85.2**	

يشير الجدول السابق إلى أن هذا البعد حقق متوسطاً حسابياً (٤,٢٦) وبنسبة (٨٥,٢%) من مساحة المقياس الكلي، وبانحراف معياري قدره (٠,٣٩٣)، وهو ما يشير إلى أن مستوى الحد من المخاطر البيئية قد جاء ضمن المستوى المرتفع وذلك من وجهة نظر أفراد العينة.

٢/٨ الإحصاءات الاستدلالية

١. اختبار أثر سياسات تدقيق أمن المعلومات بأبعادها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية

جدول (١٣): نتائج اختبار أثر سياسات تدقيق امن المعلومات بأبعادها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية

Coefficient						ANOVA			Model Summery		المتغير التابع
T Sig	T	Beta	الخطأ المعياري	B	البيان	Df	F Sig	F	R2	R	
*0.00	5.501	0.239	0.033	0.179	صالحية النظام	280/5	*0.00	110.291	0.663	0.814	الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية
0.911	0.122	0.006	0.041	0.005	واجبات فريق التدقيق						
*0.00	5.318	0.322	0.048	0.257	تقارير نظام التدقيق الداخلي						
*0.00	3.625	0.196	0.036	0.130	التوثيق والأدلة						
*0.00	3.688	0.206	0.036	0.132	ميثاق السلوك الخاص بتدقيق أمن لمعلومات						
*معنوي عند مستوى معنوية α≥0.05											
قيمة T الجدولية= ١,٩٦						قيمة F الجدولية= ٢,٢١					

يشير الجدول السابق إلى وجود أثر ذي دلالة إحصائية لسياسات تدقيق أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية من خلال قيمة F والبالغة (١١٠,٢٩١) وهي أكبر من قيمتها الجدولية والبالغة (٢,٢١) ومعنوية عند مستوى دلالة (a≤٠,٠٥). كما بلغ معامل الارتباط (٨١٤) مما يشير إلى وجود علاقة قوية بين سياسات تدقيق أمن المعلومات والحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

٢. نتائج اختبار الفرضية الفرعية الأولى:

جدول (١٤): نتائج اختبار أثر سياسات تدقيق امن المعلومات بأبعادها في الحد من مخاطر الادخال

Coefficient						ANOVA			Model Summery		المتغير التابع
T Sig	T	Beta	الخطأ المعياري	B	البيان	Df	F Sig	F	R2	R	
*0.00	4.784	0.248	0.057	0.272	صالحية النظام						
0.847	0.193	0.013	0.072	0.014	واجبات فريق التدقيق						
*0.001	3.331	0.241	0.085	0.284	تقارير نظام التدقيق الداخلي						
0.442	0.770	0.050	0.063	0.049	التوثيق والأدلة						الحد من مخاطر

الادخال	0.721	0.520	60.691	*0.00	280/5	ميثاق السلوك الخاص بتدقيق امن المعلومات	0.369	0.063	0.390	5.835	*0.00
						التدقيق الخارجي	0.369	0.063	0.390	5.835	*0.00
*معنوي عند مستوى معنوية α≥0.05											
قيمة F الجدولية= 2.21						قيمة T الجدولية= 1.96					

يمثل الجدول (١٤) نتائج الاختبار الإحصائي لنموذج هذه الفرضية والمتمثل بوجود مجموعة من المتغيرات المستقلة وهي صلاحية النظام واجبات فريق التدقيق تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي ومتغير تابع واحد يمثل الحد من مخاطر الإدخال. ويشير الجدول إلى وجود أثر ذي دلالة إحصائية لسياسات تدقيق أمن المعلومات في الحد من مخاطر الإدخال من خلال قيمة F والبالغة (٦٠,٦٩١) وهي اكبر من قيمتها الجدولية والبالغة (٢٢١) ومعنوية عند مستوى دلالة (٠,٠٥). كما بلغ معامل الارتباط (٧٢,١%) مما يشير إلى وجود علاقة قوية بين سياسات تدقيق أمن المعلومات والحد من مخاطر الإدخال.

٣. **<u>نتائج اختبار الفرضية الفرعية الثانية:</u>**

جدول (١٥): نتائج اختبار أثر سياسات تدقيق امن المعلومات بأبعادها في الحد من مخاطر التشغيل

Coefficient								ANOVA	Model Summery		المتغير التابع
T Sig	T	Beta	الخطأ المعياري	B	البيان	Df	F Sig	F	R2	R	
*0.00	3.894	0.216	0.046	0.179	صالحية النظام	280/5	*0.00	45.945	0.451	0.671	الحد من مخاطر التشغيل
0.532	0.625	0.046	0.058	0.036	واجبات فريق التدقيق						
*0.004	2.941	0.228	0.068	0.201	تقارير نظام التدقيق الداخلي						
*0.00	4.605	0.318	0.051	0.233	التوثيق والأدلة						
0.815	0.234	0.017	0.051	0.012	ميثاق السلوك الخاص بتدقيق امن المعلومات						
0.815	0.234	0.017	0.051	0.012	التدقيق الخارجي						
معنوي عند مستوى معنوية α≥0.05											
قيمة F الجدولية= 2.21						قيمة T الجدولية= 1.96					

يمثل الجدول (١٥) نتائج الاختبار الإحصائي لنموذج هذه الفرضية والمتمثل بوجود مجموعة من المتغيرات (صلاحية النظام واجبات فريق التدقيق تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق

السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي ومتغير تابع واحد يمثل الحد من مخاطر التشغيل. ويشير الجدول إلى وجود أثر ذي دلالة إحصائية لسياسات تدقيق أمن المعلومات في الحد من مخاطر التشغيل من خلال قيمة F والبالغة (٤٥,٩٤٥) وهي أكبر من قيمتها الجدولية والبالغة (٢,٢١) ومعنوية عند مستوى دلالة (a≤٠,٠٥). كما بلغ معامل الارتباط (٦٧,١%) مما يشير إلى وجود علاقة قوية بين سياسات تدقيق أمن المعلومات والحد من مخاطر التشغيل.

٤. **نتائج اختبار الفرضية الفرعية الثالثة:**

جدول (١٦): نتائج اختبار أثر سياسات تدقيق أمن المعلومات بأبعادها في الحد من مخاطر المخرجات

Coefficient						ANOVA			Model Summery		المتغير التابع
T Sig	T	Beta	الخطأ المعياري	B	البيان	Df	F Sig	F	R2	R	
*0.00	3.863	0.214	0.058	0.222	صلاحية النظام	28/50	*0.00	46.706	0.455	0.674	الحد من مخاطر المخرجات
0.867	0.168	0.012	0.072	0.012	واجبات فريق التدقيق						
*0.001	3.490	0.269	0.085	0.298	تقارير نظام التدقيق الداخلي						
0.096	1.672	0.115	0.063	0.106	التوثيق والأدلة						
*0.007	2.731	0.194	0.063	0.173	ميثاق السلوك الخاص بتدقيق امن المعلومات						
*0.007	2.731	0.194	0.063	0.173	التدقيق الخارجي						
*معنوي عند مستوى معنوية α≥0.05											
قيمة T الجدولية= 1.96						قيمة F الجدولية= 2.21					

يمثل الجدول (١٦) نتائج الاختبار الإحصائي لنموذج هذه الفرضية والمتمثل بوجود مجموعة من المتغيرات المستقلة وهي صلاحية النظام واجبات فريق التدقيق تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي ومتغير تابع واحد يمثل الحد من مخاطر المخرجات. ويشير الجدول إلى وجود أثر ذي دلالة إحصائية لسياسات تدقيق أمن المعلومات في الحد من مخاطر المخرجات من خلال قيمة والبالغة (٤٦,٧٠٦) وهي أكبر من قيمتها الجدولية والبالغة (٢,٢١) ومعنوية عند مستوى دلالة (a≤٠,٠٥). كما بلغ معامل الارتباط (٦٤,٥%) مما يشير إلى وجود علاقة قوية بين سياسات تدقيق أمن المعلومات والحد من لمخاطر البيئة.

٥. **<u>نتائج اختيار الفرضية الفرعية الرابعة</u>**

جدول (١٧): نتائج اختبار أثر سياسات تدقيق امن المعلومات بأبعادها في الحد من المخاطر البيئية

Coefficient						ANOVA			Model Summery		
T Sig	T	Beta	الخطأ المعياري	B	البيان	Df	F Sig	F	R2	R	المتغير التابع
0.304	1.030	0.059	0.039	0.040	صلاحية النظام	28/50	*0.00	39.830	0.416	0.645	الحد من المخاطر البيئية
0.375	0.889	0.067	0.049	0.044	واجبات فريق التدقيق						
*0.00	4.210	0.336	0.058	0.245	تقارير نظام التدقيق الداخلي						
*0.00	5.307	0.378	0.043	0.229	التوثيق والأدلة						
0.981	0.024	0.002	0.043	0.001	ميثاق السلوك الخاص بتدقيق امن المعلومات						
0.981	0.024	0.002	0.043	0.001	التدقيق الخارجي						
• معنوي عند مستوى معنوية α≥0.05											
قيمة T الجدولية= 1.96						قيمة F الجدولية= 2.21					

يمثل الجدول (١٧) نتائج الاختبارالإحصائي لنموذج هذه الفرضية والمتمثل بوجود مجموعة من المتغيرات المستقلة وهي صلاحية النظام واجبات فريق التدقيق تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي، ومتغير تابع واحد يمثل الحد من مخاطر البيئة. ويشير الجدول إلى وجود أثر ذو دلالة إحصائية لسياسات تدقيق أمن المعلومات في الحد من المخاطر البيئية من خلال قيمة F والبالغة (٣٩,٨٣) وهي اكبر من قيمتها الجدولية والبالغة (٢,٢١) ومعنوية عند مستوى دلالة (٠,٠٥). كما بلغ معامل الارتباط (٦٤,٥%) مما يشير إلى وجود علاقة قوية بين سياسات تدقيق أمن المعلومات والحد من لمخاطر البيئة.

من نتائج التحليل الإحصائي للفرضية الرئيسية والفرضيات الفرعية يتضح أنه يوجد دور لسياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية، وعلاقة قوية بين متغيرات الدراسة.

الفصل الثالث

النتائج والتوصيات

الفصل الثالث
النتائج والتوصيات

تناول **الباحث** في هذا الجزء النتائج والتوصيات التي توصل إليها، ولذلك فقد تم تقسيم هذا الجزء إلى ما يلي:

٣/١: النتائج.

٣/٢: التوصيات.

٣/١ النتائج

في ضوء ما أسفرت عنه نتائج تحليل بيانات الدراسة التطبيقية التي قام بها **الباحث**، يمكن عرض **النتائج** كما يلي:

١- توجد علاقة ذات دلالة إحصائية بين سياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق السلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) والحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية.

٢- أظهرت الدراسات أن تطبيق عمليات تدقيق نظم تكنولوجيا المعلومات بشكل منتظم يمكن أن يقلل بشكل كبير من مخاطر الأمن السيبراني وانتهاكات البيانات. وتشير الأمثلة العملية إلى أن تقنيات مثل الفحص الدوري للثغرات، وتقييم التهديدات، وتنفيذ إجراءات التصحيح اللازمة يمكن أن تساهم في تعزيز أمان النظم الإلكترونية.

٣- أهمية وجود إطار تنظيمي قوي ومستقل للرقابة على أنظمة المعلومات، حيث يمكن للأجهزة العليا للرقابة أن تلعب دوراً رئيسياً في تحديد المعايير والممارسات الأمنية، ومراقبة تنفيذها، وتوجيه الشركات والمؤسسات لتحسين أمان وموثوقية أنظمتهم. كما أن التعاون بين القطاعين العام والخاص يمكن أن يسهم في تعزيز فعالية جهود الرقابة وتحسين أمن المعلومات.

٤- يتعين على الشركات والمؤسسات التعامل مع تحديات متنوعة تتعلق بتدقيق تكنولوجيا المعلومات، مثل تطور التهديدات السيبرانية والتشريعات الجديدة المتعلقة بحماية البيانات. ومن الفرص المهمة الاستفادة من تطورات التكنولوجيا الحديثة لتعزيز قدرة الجهات المعنية على اكتشاف والتصدي للتهديدات الأمنية.

٥- يجب على الشركات والمؤسسات تطبيق استراتيجيات متعددة لتحسين عمليات تدقيق تكنولوجيا المعلومات، بما في ذلك توظيف الكوادر المؤهلة واعتماد تقنيات تحليل البيانات الكبيرة والتعاون مع مزودي الخدمات الأمنية المتخصصين.

٦- إن تقييم فعالية عمليات تدقيق تكنولوجيا المعلومات يمكن أن يساعد في تحديد نقاط القوة والضعف وتحديد المجالات التي تحتاج إلى تحسين. ومن المهم أيضًا تبادل الخبرات والمعرفة بين الشركات والمؤسسات لتعزيز الفهم المشترك لأفضل الممارسات في مجال تدقيق تكنولوجيا المعلومات.

٧- إن تنفيذ عمليات تدقيق تكنولوجيا المعلومات يمكن أن يسهم في تعزيز الامتثال للتشريعات واللوائح القانونية المتعلقة بحماية البيانات وأمان المعلومات. وقد يؤدي ذلك إلى تقليل المخاطر القانونية والتبعات المالية للانتهاكات الأمنية.

٨- يمكن أن يسهم تدقيق تكنولوجيا المعلومات في تعزيز الاتصال والتوعية بمخاطر الأمن السيبراني داخل المؤسسات، وتشجيع الموظفين على المشاركة في جهود حماية البيانات والتبليغ عن أية استفسارات أو انتهاكات محتملة.

٩- من خلال تدقيق تكنولوجيا المعلومات، يمكن تحسين استعداد المؤسسات للاستجابة لحوادث الأمان مثل اختراقات البيانات أو الهجمات السيبرانية. وتشمل هذه الاستراتيجيات التخطيط المسبق والتمارين الدورية لمواجهة حوادث الأمان وتقديم الاستجابة الفعالة.

١٠-يمكن لتدقيق تكنولوجيا المعلومات أن يسهم في بناء الثقة والمصداقية في الأنظمة الرقمية، سواء كانت داخل المؤسسات أو بين العملاء والشركاء التجاريين. ويمكن أن يؤدي هذا إلى تعزيز التفاعلات الإلكترونية وزيادة الثقة في استخدام التكنولوجيا.

١١-يمكن أن يؤدي تطبيق عمليات تدقيق تكنولوجيا المعلومات إلى تحسين كفاءة وفعالية العمليات التجارية، من خلال تقليل الانقطاعات والتوقفات غير المخطط لها نتيجة لمشاكل الأمان، وتعزيز التواصل وتبادل المعلومات الآمن بين الأقسام المختلفة في المؤسسة.

٣/٢ التوصيات

في ضوء ما توصل إليه الباحث من نتائج التحليل الوصفي، واستعراض الدراسات والمراجع والأبحاث، يقدم الباحث مجموعة من التوصيات تتلخص فيما يلي:

١- **تعزيز توعية الموظفين وتدريبهم:** يجب على المؤسسات تعزيز توعية موظفيها بأهمية أمان المعلومات وممارسات التكنولوجيا الآمنة، وتقديم تدريب مستمر لهم حول التهديدات السيبرانية وكيفية التعامل معها.

٢- **تطبيق إجراءات تدقيق دورية:** ينبغي على المؤسسات تنفيذ عمليات تدقيق دورية لأنظمتها وتقنياتها للتأكد من مواكبتها لأحدث معايير الأمان والامتثال للتشريعات واللوائح.

٣- **تعزيز التعاون مع الجهات العليا للرقابة:** ضرورة قيام الشركات والمؤسسات بتعزيز التعاون مع الأجهزة العليا للرقابة والاستفادة من الإرشادات والتوجيهات التي تقدمها لتحسين أمن المعلومات.

٤- **تبني أفضل الممارسات والتقنيات الحديثة:** ينبغي على المؤسسات استخدام أفضل الممارسات واعتماد التقنيات الحديثة في تطبيق عمليات التدقيق وتأمين الأنظمة الإلكترونية.

٥- **تطوير استراتيجيات استجابة لحوادث الأمان:** يجب على المؤسسات وضع استراتيجيات محددة وفعالة للاستجابة لحوادث الأمان، وإجراء تدريبات دورية لفحص استجابتها وتحسينها.

٦- **الاستفادة من تحليل البيانات والذكاء الصناعي:** يمكن للشركات والمؤسسات استخدام تقنيات تحليل البيانات والذكاء الصناعي لتعزيز قدرتها على اكتشاف التهديدات الأمنية وتحليل السلوكيات الغير معتادة داخل الأنظمة الإلكترونية.

٧- **التحديث الدوري لسياسات الأمان والإجراءات الداخلية:** ينبغي على المؤسسات ضرورة تقييم وتحديث سياسات الأمان والإجراءات الداخلية بانتظام لضمان استمرار توافقها مع تطورات التهديدات السيبرانية والمتطلبات القانونية.

المراجع

المراجــع

أولًا: المراجع باللغة العربية

أدلة ومعايير دولية

١. الإنتوساي، ٢٠٢٢، دليل مبادرة تنمية الانتوساي بخصوص تدقيق تقنية المعلومات لمؤسسات التدقيق العليا.

٢. الإنتوساي، ٢٠١٩، إطار انتوساي للتوجيهات المهنية.

٣. الاتحاد الدولي للمحاسبين، ٢٠١٩، معايير المراجعة الدولية.

٤. المعهد الأمريكي للمراجعين الداخليين، ٢٠١٧، المعايير الدولية للممارسة المهنية للتدقيق الداخلي.

الكتب:

١. الذيبة، زياد عبد الحليم وآخرون، ٢٠١٤، نظم المعلومات في الرقابة والتدقيق، دار المسيرة، عمان،الأردن.

٢. الصرن، رعد حسن، ٢٠٢١، **أنظمة إدارة الجودة والبيئة**، جامعة الشام، سوريا.

٣. الظاظا، ناجي شكري، ٢٠١٦، تكنولوجيا الاتصال والمعلومات: البنية والحماية، دار القدس للطباعة والتوزيع، غزة، فلسطين.

٤. الواردات، خلف عبد الله، ٢٠١٩، **دليل التدقيق الداخلي وفق المعايير الدولية الصادرة عن IIA** (الوراق للنشر والتوزيع، عمان، الأردن.

٥. أنور، أحمد، 2017، **مقدمة في تكنولوجيا المعلومات وأساسيات استرجاع المعلومات**، دار الثقافة العلمية، الإسكندرية، مصر.

٦. جمعة، أحمد حلمي، ٢٠١٩، **المدخل إلى التأكيد المعقول وفقا للمعايير الدولية للمراجعة**، دار صفاء للنشر والتوزيع، عمان، الأردن، الطبعة الثالثة.

٧. سليمان، أحمد فؤاد، ٢٠١٧، تكنولوجيا المعلومات للاعمال، المركز العربي للدراسات والبحوث العلمية، مصر.

٨. صادق، دلال، و الفتال، حميد ناصر،٢٠١٩، **أمن المعلومات**، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن.

٩. على، عبد الوهاب نصر، وشحاتة، شحاته السيد، **نظم المعلومات المحاسبية (مدخل دورات المعاملات وتكنولوجيا المعلومات)**، قسم المحاسبة كلية التجارة – جامعة الاسكندرية، ٢٠١٥.

١٠. كراسنة، إبراهيم، ٢٠١٧، **أطر أساسية ومعاصرة في الرقابة على البنوك وإدارة المخاطر**، معهد السياسات الاقتصادية، صندوق النقد العربي، أبو ظبي، الإمارات، الطبعة الثانية.

١١. مانيش، أغروال، وآخرون، ٢٠١٨، **أمن المعلومات وإدارة مخاطر تقنية المعلومات**، ترجمة: جعفر بن أحمد العلوان، مركز البحوث والدراسات – معهد الإدارة العامة، المملكة العربية السعودية.
١٢. يونس، زين، ومصطفى، عوادي، ٢٠١٥، **المراجعة الداخلية وتكنولوجيا المعلومات وفق معاير المراجعة الدولية**، مطبعة سخري، الوادي، الجزائر.

<u>الرسائل العلمية</u>

١.أبو الهيجاء، أحمد عدنان، ٢٠١٧، أثر موثوقية نظم المعلومات المحاسبية في ظل تطبيق حوكمة تكنولوجيا المعلومات على ربحية البنوك الأردنية المدرجة في بورصة عمان، **رسالة دكتوراه**، جامعة العلوم الإسلامية العالمية، كلية الدراسات العليا ،عمان، ٢٠١٧.
٢.أبو رمان، إيناس فوزي، ٢٠٢١، دور التدقيق في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية في البنوك التجارية الأردنية، **رسالة ماجستير**، كلية الدراسات العليا، جامعة البلقاء، الأردن.
٣.أبو عمرو، إيمان حسين حسن، ٢٠٢٣، أثر تدقيق تكنولوجيا المعلومات في فاعلية نظم المعلومات المحاسبية في البنوك التجارية الأردنية، **رسالة دكتوراة**، كلية الدراسات العليا، جامعة العلوم الاسلامية العالمية، عمان، الأردن.
٤.البري، ولاء عواد جازي، ٢٠٢٣، أثر تدقيق تكنولوجيا المعلومات في الحد من مخاطر التدقيق الخارجي في البنوك المدرجة في بورصة عمان، **رسالة ماجستير**، جامعة ال البيت، عمان، الأردن
٥.العوامري، عبير عيسى، ٢٠٢٢، أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الالكترونية، **رسالة ماجستير**، كلية التجارة، جامعة بنها، مصر.
٦.العلمى، حسام أحمد محمد، ٢٠١٥، دور نظم المعلومات المحاسبية المحوسبة في كفاءة وفعالية التدقيق الخارجي، **رسالة ماجستير**، كلية التجارة، الجامعة الإسلامية، غزة، فلسطين.
٧.السعداوى، محمد عبد الله فرج، ٢٠١٧، تفعيل أثر حوكمة نظم المعلومات فى الحد من مخاطر نظم المعلومات: دراسة ميدانية، **رسالة ماجستير**، كلية التجارة – جامعة عين شمس، مصر.
٨.المنيزل، محمد حسن مفلح، ٢٠٢١، أثر نظم المعلومات المحاسبية المحوسبة في تعزيز فاعلية الرقابة الداخلية لدى البنوك التجارية الأردنية، **رسالة ماجستير**، كلية الدراسات العليا، جامعة جرش، الأردن.
٩.الوهيب، عبدالوهاب مبارك، ٢٠٢٢، أثر تطبيق إطار عمل **COBIT5** في الحد من تهديدات أمن نظم المعلومات المحاسبية المحوسبة في البنوك العاملة في الكويت، **رسالة ماجستير**، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية، الأردن.

١٠.حسن، يسري التميمي، ٢٠١٧، دور المراجع الداخلي فى تقييم أمن نظم المعلومات المحاسبية في ضوء حوكمة تقنية المعلومات بالتطبيق علي هيئة قناة السويس ببورسعيد، رسالة ماجستير، كلية التجارة، جامعة بورسعيد، مصر.
١١.محمد، ميرغنى الشيخ عمر، ٢٠١٧، أساليب مراجعة نظم المعلومات المحاسبية الالكترونية وأثرها على جودة المراجعة الخارجية: دراسة ميدانية، **رسالة ماجستير**، كلية الدراسات العليا، جامعة النيلين، السودان.

المقالات:

١.أبو شيبة، إبراهيم على، الفطيمى، محمد مفتاح، ٢٠١٧، مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية: دراسة ميدانية على المصارف التجارية فى بلدية مصراتة، **مجلة دراسات الإقتصاد والأعمال، كلية الإقتصاد والعلوم السياسية**، جامعة مصراتة، السنة الخامسة، عدد خاص.
٢.الجربوع، عبدالله محمد، ٢٠٢٣، جرائم الاعتداء المتعمد على سلامة نظم المعلومات الإلكترونية وفقاً للنظام السعودي (دراسة تحليلية تطبيقية)، **مجلة البحوث الفقهية والقانونية**، المجلد ٣٥، العدد ٤٣، كلية الشريعة والقانون، جامعة الأزهر الشريف، مصر.
٣.العازمي، عبد الله فالح، ٢٠٢٢، دور تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات المحاسبية من المخاطر الالكترونية في ظل عصر الرقمنة، **المجلة العلمية للدراسات والبحوث المالية والإدارية**، المجلد الثالث عشر، العدد الثانى، كلية التجارة، جامعة مدينة السادات، مصر.
٤.الطيب، الصادق محمد السالم، والصديق، بابكر إبراهيم، ٢٠١٤، جودة المراجعة الخارجية في ظل بيئة التشغيل الإلكتروني للبيانات المالية "دراسة نظرية"، **مجلة العلوم الاقتصادية**، العدد ١٥(٢)، جامعة السودان للعلوم و التكنولوجيا.
٥.المري، راشد محمد، ٢٠٢٣، أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية، **مجلة البحوث الفقهية والقانونية**، المجلد ٣٥، العدد ٤٠، كلية الشريعة والقانون، جامعة الأزهر الشريف، مصر.
٦.المطيري، فهد خالد، ٢٠٢٣، أثر التكامل بين موثوقية نظم المعلومات المحاسبية الإلكترونية وتطبيق آليات الحوكمة على ربحية البنوك التجارية الكويتية (دراسة ميدانية)، **المجلة العلمية للدراسات والبحوث المالية والإدارية**، المجلد ١٥، العدد ٣، كلية التجارة، جامعة مدينة السادات، مصر.
٧.النقبي، جمال محمد، والمصعبي، سلطان محمد، ٢٠٢٣، الجوانب التقنية والقانونية لنظم المعلومات الإلكترونية، **مجلة المعهد العالي للدراسات النوعية**، المجلد ٣، العدد ٤، مصر.
٨.بالقاسم، أمحارب سعد سليمان، حسين، أحمد محمد سليم، ٢٠١٧، واقع مخاطر أمن نظم المعلومات المحاسبية الإلكترونية بالمصارف التجارية الليبية بمدينة البيضاء، **المؤتمر العلمى الدولى الأول:**

التحوط وإدارة الخطر فى الصناعة المالية الإسلامية، مركز السنابل للبحث وتطوير الموارد البشرية ومركز بيان للهندسة المالية الإسلامية، عمان، الأردن.

٩. حبيب، سمر، ٢٠٢٢، دور المحاسبة ومعايير التدقيق السحابي في تأكيد أمن البيانات والمعلومات: دراسة ميدانية من وجهة نظر مدققي الحسابات الخارجيين في سورية، **مجلة جامعة تشرين للعلوم الاقتصادية والقانونية**، المجلد ٤٤، العدد ٦، جامعة تشرين، سوريا.

١٠. حسين، محمود عبد الرحيم، ٢٠٢٠، الدور التأثيرى لحوكمة تكنولوجيا المعلومات كمتغير وسيط فى العلاقة بين المراجعة الداخلية كنشاط مضيف للقيمة والحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، **مجلة الدراسات والبحوث المحاسبية**، كلية التجارة، جامعة بنها – العدد الثاني.

١١. ضيف الله، محمد الهادي، ٢٠٢١، أثر حوكمة تكنولوجيا المعلومات على الحد من مخاطر نظام المعلومات المحاسبي، **مجلة الدراسات المالية والمحاسبية والإدارية**، المجلد ٨، العدد١، جامعة أم البواقي، الجزائر.

١٢. غنيمى، سامى محمد احمد، "نحو معيار محاسبي لحوكمة تكنولوجيا المعلومات فى ضوء تطور تكنولوجيا الإتصالات وتبادل المعلومات – دراسة ميدانية، **مجلة الفكر المحاسبي**، قسم المحاسبة والمراجعة، كلية التجارة، جامعة عين شمس، العدد الثالث– الجزء الأول، اكتوبر ٢٠١٧.

١٣. قرداش، عباس، وقانصوة، حسن، ٢٠٢٣، اثر نظم المعلومات المحاسبية المحوسبة في اتخاذ القرارات الاستثمارية، **المجلة العربية للعلوم الإنسانية والاجتماعية**، العدد ٢١، مركز السنبلة للبحوث والدراسات، عمان – الأردن.

١٤. كرسوع، أرزاق أيوب، ٢٠٢٣، معوقات تدقيق نظم المعلومات المحاسبية الالكترونية من وجهة نظر مدققي الحسابات العاملين في البريد ووزارة المالية في ظل جائحة كورونا بغزة، **المجلة الأفروآسيوية للبحث العلمي**، المجلد الأول، العدد الرابع، الأكاديمية الإفريقية للدراسات المتقدمة، تركيا.

١٥. هبه جمال هاشم علي، ٢٠٢٣، منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل، **المجلة العلمية للدراسات والبحوث المالية والتجارية**، المجلد ٤، العدد ٢، كلية التجارة، جامعة قناة السويس، مصر.

ثانيًا: المراجع باللغة الإنجليزية

Books:

1. Chris, Davis, and others, 2011, **IT Auditing: using controls to protect information assets**, Mc Graw Hill, 2011, second édition.

2. Davis, Robert E., 2021, **Auditing Information and Cyber Security Governance: A Controls-Based Approach**, CRC Press, Taylor & Francis Group, LLC, New York, USA.
3. Engel, Barak, 2024, **Why CISOs Fail (Internal Audit and IT Audit)**, CRC Press, Taylor & Francis Group, LLC, New York, USA.
4. Gantz, Stephen D., 2014, **The Basics of IT Audit. Purposes, Processes, and Practical Information**, Syngress
5. Hernan, Murdock, 2019, **Auditor essentials 100 concepts, tips, tools, and techniques for success**, CRC Press, Taylor & Francis Group, LLC, New York, USA.
6. ISACA, CISA Review Manual, 2019, 27 th edition, USA.

Periodecals:

1. Al-Fatlawi Q.Ali, Salman, Dawood, Almagtome, Akeel, 2021, Accounting Information Security and IT Governance Under COBIT5 Framework: A Case Study, **Faculty of Administration and Economics**, University of Kufa, Najaf, Iraq, Vol.18.
   Available at: https://www.researchgate.net, Retrieved at: 30-2-2024.
2. Alsaleem, Enas Amjed, & Husin, Norhayati Mat, 2023, The Impact of Information Technology Governance Under Cobit-5 Framework on Reducing the Audit Risk in Jordanian Companies, **International Journal of Professional Business Review**, Volume 8, Issue 2, Miami, USA.
3. Bradford, M., et al, 2020, Using generalized audit software to detect material misstatements, control deficiencies and fraud: How financial and IT auditors perceive net audit benefits, **Managerial Auditing Journal**, Vol. 35 No. 4. https://doi.org/10.1108/MAJ-05-2019-2277
4. Hossin, Adel M.& Ayedh, Abdellah M., 2016, The Risks of Electronic Accounting Information System in the Centeral Bank of Libya, **South East Asia Journal of Contemporary Business, Economic & Law**, Vol.1, No.1.

5. Hussain, M. Ali, 2013, A Study of Information Security in E-Commerce Application, **International Journal of Computer Engineering Science (IJCES),** Vol.3, Issue3.
6. Institute of Internal Auditors (IIA), 2016, International Standards for the Professional Practice of Internal Auditing Standards.
7. Krishna, D Jadhav, 2023, The Role of Cybersecurity Audits in Managing Company Systems and Applications,
8. Mirwali Azizi, Hakimi, M., Frishta Amiri, & Amir Kror Shahidzay, 2024, The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. **Open Access Indonesia Journal of Social Sciences**, volume 7, issue 2.
9. Mohammad Aljanabi & et al, 2023, The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment, **Mesopotamian journal of Cybersecurity**, vol.2023.
10. Pandzo, Alica, & Taljanovic, Kemal, 2013, IT Governance and IT Auditing Practice in Commercial Banks in Bosnia and Herzegovina, **Recent Advances in Information Science Jounal**.
11. Richard, Brisebois, 2015, What is IT Governence and why is it important for the IS auditor, **research journal of recent sciences**, vol. 09, issue 15, Information Systems Audit and Control Association (ISACA).
12. Rabii, Hamza, 2023, The Contribution of IT Audit to Data Governance, **Journal of Namibian Studies**, V. 36, issue S 2, Society of Cultural Studies and Social Sciences, Hong Kong
13. Slapnicar, Sergeja, & et al, 2022, Effectiveness of cybersecurity audit, **International Journal of Accounting Information Systems**, Volume 44, Issue 8, Elsevier Inc.

14. Taherdoost, Hamed, 2022, Understanding Cybersecurity Frameworks and Information Security Standards: A Review and Comprehensive Overview, Volume 11, Issue 14, **MDPI**, Basel, Switzerland.

15. Yohannes, Kurniawan & Archie Mulyawan, 2023, The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting, **Journal of System and Management Sciences**, Vol. 13, No. 1.

Training Course:

1- EUROSAI, ITWG, 2023, IT audit for non IT auditors, Training Course.

الملاحق

الملحق

نموذج استبيان

الرقابة على نظم المعلومات والأمن السيبراني

بحث مقدم للاشتراك في مسابقة البحث العلمي الرابعة عشر في مجال الرقابة للمنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة أرابوساي

إعداد الباحث

محاسب/ د. سامي علي محمد زغلول

مدير عام بالإدارة المركزية للرقابة على البنوك

الجهاز المركزي للمحاسبات

جمهورية مصر العربية

يمثل هذا الاستبيان أحد الجوانب الهامة في البحث، ويهدف إلى دراسة دور سياسات تدقيق أمن المعلومات بأبعادها (صـــلاحية النظام، واجبات فريق التدقيق، تقارير نظام التدقيق الداخلي، التوثيق والأدلة، ميثاق الســـلوك الخاص بتدقيق أمن المعلومات، التدقيق الخارجي) في الحد من مخاطر نظم المعلومات الإلكترونية في البنوك المصرية.

أرجو التكرم بالإجابة على الأسـئلة المطروحة وتزويد الباحث بآرائكم القيمة من خلال وضــع إشــارة (✓) على الإجابة التي ترونها ملائمة ، كما يأمل الباحث أن تغني إجاباتكم وترفع من المسـتوى البحثي العلمي لهذا البحث.

يرجى العلم أن جميع الأسئلة المطروحة ضمن هذا الاستبيان لأغراض البحث العلمي وأن إجاباتكم ستكون محاطة بالسرية الكاملة والعناية العلمية الفائقة.

شكرا لتعاونكم وحسن استجابتكم....

الباحث

د. سامي علي محمد زغلول

أولاً: المعلومات العامة:

يرجى الإجابة على الأسئلة التي تتضمن معلومات عامة بوضع إشارة (✓)

1- الاسم: .....(اختياري)

2- المؤهل العلمي:

[ ] بكالوريوس

[ ] عضو جمعية مهنية

[ ] ماجستير/ شهادات مهنية

[ ] دكتوراه

3- النوع:

[ ] ذكر

[ ] أنثى

4- الخبرة العملية:

[ ] من 5 سنة وأقل من 10

[ ] من10 سنة وأقل من 20

[ ] أكثر من 20

5- الوظيفة:

[ ] مدير مالي

[ ] مدير رقابة

[ ] مدققون خارجيون / مدققون داخليون / محاسبون

[ ] موظفي تكنولوجيا معلومات

ثانياً: وصف أبعاد المتغير المستقل سياسات تدقيق أمن المعلومات:

م	البعد الأول: صلاحية النظام	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
1	توفر بنوك القطاع العام محل البحث حماية لأمن وسلامة جميع مكونات النظام.					
2	تحرص بنوك القطاع العام محل البحث وبشكل دوري على إخضاع مستخدمي الأنظمة إلى محاضرات إرشادية.					
3	تقوم بنوك القطاع العام محل البحث بالفصل بين مهام كل من محللي النظم، ومشغلي النظم، وموظفي قسم الحاسوب.					
4	تمنح بنوك القطاع العام الصلاحية المناسبة والكافية لطاقم تدقيق أمن المعلومات.					
5	تعمل بنوك القطاع العام على اجراء الصيانة الدورية للمكونات المادية لنظام المعلومات.					
6	يحرص المدراء في بنوك القطاع العام على توفير الصلاحيات للمدقق الداخلي لإجراء عملية التدقيق.					

م	البعد الثاني: واجبات فريق التدقيق	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
7	يتمتع المدققين الداخليين في بنوك القطاع العام بالتأهيل العلمي اللازم لممارسة مهامهم بكفاءة					
8	تحدد بنوك القطاع العام مهام وواجبات فريق التدقيق وتحدد الصلاحيات الموكلة إليهم					
9	تمنح بنوك القطاع العام الثقة للأشخاص الذين يتولون مهمة الفحص والتأكد من صحة أمن وسلامة المعلومات					
10	يتعاون موظفي الإدارات في في بنوك القطاع العام مع المدققين الداخليين في التعامل مع أدوات حفظ أمن المعلومات					
11	توجه إدارات البنوك المدققين الداخليين على استخدام أدوات تكنولوجية حديثة					
12	يحرص مدققي الحسابات على حضور الندوات والمؤتمرات الخاصة ببيئة أمن وسلامة المعلومات والحصول على الشهادات المهنية في مجال تكنولوجيا المعلومات والتدقيق					

م	البعد الثالث: تقارير نظام التدقيق الداخلي	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
1	توجه إدارات البنوك المدققين إصدار تقرير المدقق الداخلي كأحد سياسات أمن المعلومات.					
2	يحرص فريق تدقيق أمن المعلومات على إصدار تقرير بنتائج التدقيق لمعالجة أي انحرافات أو أخطاء.					
3	ترفع تقارير التدقيق الداخلي لمدير القسم من أجل متابعة الإجراءات الالزامية لمعالجة أي استثناءات.					
4	يحرص فريق تدقيق أمن المعلومات على توفير تقارير التدقيق الداخلي وقت الحاجة.					
5	يقدم قسم التدقيق الداخلي تقرير لمجلس الإدارة عن المخاطر التي تتعرض لها البنوك وكيفية تجنبها.					
6	يحرص فريق تدقيق أمن المعلومات على مراجعة وتدقيق كافة المعاملات المالية لدى بنوك القطاع العام.					

م	البعد الرابع: التوثيق والادلة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
19	تحرص بنوك القطاع العام على وضع التعليمات الخاصة بتوثيق عملية التدقيق.					
20	تحرص بنوك القطاع العام على وضع ضوابط رقابية على المستندات وتسلسل إجراءات إدخال البيانات للنظام.					
21	تقوم بنوك القطاع العام بتجميع الأدلة من مصدرها الرئيسي والتثبت من دقة المعلومات الواردة فيها.					
22	تحتفظ البنوك بنسخة من برامج المعالجة في مكان مناسب وتسجل مخرجات النظام كوسيلة رقابية.					
23	تؤكد بنوك القطاع العام على ضرورة توثيق كافة الإجراءات والآليات المتبعة خلال العمل على تدقيق أمن المعلومات.					
24	تحرص البنوك على التأكد من مدى ملائمة الأدلة وكفايتها للحصول على تقرير أمن المعلومات.					

م	البعد الخامس: ميثاق السلوك الخاص بتدقيق أمن المعلومات.	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
25	تلتزم بنوك القطاع العام بميثاق السلوك الخاص بتدقيق أمن المعلومات.					
26	يحرص مدققي الحسابات الداخليين بالبنوك على أداء الواجبات الموكلة إليهم بشكل هادف وعناية فائقة.					
27	يتقيد مدققي الحسابات الداخليين في البنوك بالمحافظة على سرية وخصوصية المعلومات التي تم جمعها.					
28	يحرص مدققي الحسابات الداخليين في البنوك على تقديم نتائج دقيقة لعملية التدقيق بأكملها.					
29	تدعم بنوك القطاع العام الجهود التوعوية التي تهدف إلى مساعدة المتعاملين معها لتطوير فهمهم لأمن وإدارة نظم المعلومات.					
30	تخضع بنوك القطاع العام لعقوبات رادعة وصارمة في حال إخفاق المدقق بالعمل في ميثاق السلوك الخاص بتدقيق أمن المعلومات.					

م	البعد السادس: التدقيق الخارجي	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
31	التدقيق الخارجي لتكنولوجيا المعلومات في البنك يتم بصفة دورية مناسبة من 2إلى 5 سنوات					
32	يحرص مدققي تكنولوجيا المعلومات الخارجيين على أداء واجباتهم بشكل هادف وعناية فائقة.					
33	يحرص مدققي تكنولوجيا المعلومات الخارجيين على اتباع المعايير والأدلة والإرشادات المتعلقة بتكنولوجيا المعلومات والصادرة من المنظمات المهنية الدولية والمحلية.					
34	يحرص مدققي تكنولوجيا المعلومات الخارجيين على تقديم نتائج دقيقة لعملية التدقيق بأكملها.					
35	يقدم تقرير المدقق الخارجي لتكنولوجيا المعلومات توصيات تفيد في الحد من المخاطر التي تتعرض لها أنظمة المعلومات بالبنوك					
36	يساعد التدقيق الخارجي لتكنولوجيا المعلومات من تعزيز أمن المعلومات والأمن السيبراني ويحد من مخاطر المدخلات ومخاطر التشغيل ومخاطر المخرجات والمخاطر البيئية					

ثانياً: وصف مجالات مخاطر نظم المعلومات الإلكترونية:

م	المجال الأول: مخاطر الإدخال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
37	تحرص بنوك القطاع العام على عقد دورات تدريبية لتوعية مدخلي البيانات بكيفية وأهمية الحفاظ على أمن المعلومات.					
38	عدم اشتراك الموظفين بنفس كلمة السر وإجبار كل موظف في البنوك على تغييرها بشكل دوري					
39	تعمل نظم المعلومات في البنوك على مراجعة المدخلات والتأكد من صحتها والحد من إدخال البيانات الخاطئة.					
40	تحرص البنوك على ضبط عملية إدخال البيانات وتعديلها إلا من قبل الموظفين المخول لهم بذلك.					
41	تستفيد البنوك دائما من التطورات التكنولوجية في مجالات برامج حماية أنظمة المعلومات مثل برامج التشفير.					
42	تستخدم البنوك أجهزة إنذار تنبيهيه في حال الدخول غير المصرح بإدخال البيانات.					

م	المجال الثاني: مخاطر التشغيل	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
43	تمتلك بنوك القطاع العام نظم معلومات تمنع تعديل البيانات من قبل الأفراد غير المصرح لهم.					
44	توفير الحماية الكافية في البنوك من خلال استخدام البرامج المضادة للفيروسات والجدران النارية.					
45	التواصل مع مزود خدمة الإنترنت لاسترجاع الخدمة بأسرع ما يمكن في حال قطعها عن البنوك.					
46	فحص البرامج والأقراص الممغنطة الجديدة قبل إدخالها إلى أجهزة الكمبيوتر بشكل دوري.					
47	تمتلك البنوك نظم معلومات قادرة على التنبؤ بمخاطر التشغيل والحد منها.					
48	تحرص البنوك على معالجة البيانات الكترونياً دون تدخل العنصر البشري بذلك.					

م	المجال الثالث: مخاطر المخرجات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
49	تتبع مخرجات كل عملية وإرفاقها المستندات الثبوتية المعززة لوجودها في البنوك محل البحث.					
50	تمنع نظم المعلومات المحاسبية لدى البنوك محل البحث تعديل التقارير الصادرة من النظام أو تزويرها.					
51	تمتلك المؤسسات الحكومية نظم معلومات محاسبية قادرة على منع إمكانية خلق مخرجات غير حقيقية من قبل العاملين.					
52	الاحتفاظ بمخرجات النظام الورقية في أماكن آمنة ومحكمة الإغلاق والقيام بأرشفتها لمنع ضياعها أو سرقتها أو إتلافها.					
53	وضع قواعد وأنظمة تحدد مسا ارت توزيع التقارير الناتجة عن النظام في البنوك محل البحث.					
54	إصدار نسخ سرية لمخرجات نظم المعلومات في البنوك محل البحث لتسهيل عمليات الفحص والتقييم ومواجهة حالات السرقة أو التزوير.					

م	المجال الرابع: المخاطر البيئية	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		5	4	3	2	1
55	هنالك وعي كاف بكيفية التعامل مع حالات الطوارئ عند حدوث الكوارث الطبيعية في البنوك محل الدراسة.					
56	تقوم البنوك بوضع خطة واضحة للتنبؤ بالأضرار الناجمة عن المخاطر البيئية وكيفية معالجتها والوقاية منها.					
57	تقوم إدارة المؤسسات الحكومية بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا.					
58	يستطيع المدقق الداخلي إصدار توجيهات لإدارة بضرورة تحمل إدارة البنوك جزء من مخاطر البيئة الخارجية الناتجة عن سوء الإدارة.					
59	تحرص البنوك محل الدراسة على وضع خطط لمواجهة العوامل البيئية مثل الزلازل والأعاصير والفيضانات والحرائق التي تؤثر على امن وسالمة نظم المعلومات الإلكترونية.					
60	تقوم البنوك محل الدراسة بعقد دو ارت تدريبية عن امن وسالمة نظم المعلومات الالكترونية في حال حدوث كوارث طبيعية أو كوارث غير طبيعية التي قد تؤثر على عمل النظام.					