حوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة
نموذج مقترح

Information technology governance to reduce cyber risks and enhance the security of accounting information in Libyan public institutions

أ. إبتسام محمود القصير
أستاذ مساعد/ كلية العلوم التقنية مصراتة
EMG@etsm.edu.ly

استلمت الورقة بتاريخ 2024/08/24، وقبلت بتاريخ 2024/09/04، ونشرت بتاريخ 2024/09/07

الكلمات المفتاحية:
حوكمة ، تقنية المعلومات، المخاطر السيبرانية، المراجع الداخلي .

الملخص

هدفت الدراسة لاقتراح نموذج لحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة واتبعت الدراسة المنهج الوصفي التحليلي من خلال مراجعة الدراسات السابقة والتقارير والنماذج وأفضل الممارسات والأدبيات ذات العلاقة، وخلصت الدراسة أن حوكمة تقنية المعلومات لها دور إيجابي في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية وتمثلت أهم ركائز النموذج المقترح في : الحوكمة ولجنة حوكمة تقنية المعلومات وآلياتها واستقلالية المراجع الداخلي مع التأكيد على كل من إدارة المخاطر، الرقابة النشطة والمستمرة، الشفافية والمساءلة وأوصت الدراسة بضرورة تبني المؤسسات الليبية العامة الحوكمة وحوكمة تقنية المعلومات.

Abstract

The study aimed to propose a model for information technology governance to reduce cyber risks and enhance the security of accounting information in Libyan public institutions. The study followed the descriptive analytical approach by reviewing studies, reports, models and best practices. The study concluded that information technology governance has a positive role in reducing cyber risks and enhancing the security of accounting information. The most important pillars of the proposed model were: governance, the IT Governance Committee and its mechanisms, and the independence of the internal auditor, with an emphasis on risk management, continuously monitor, transparency and accountability. The study recommended the need for Libyan public institutions to adopt governance and IT governance.

المقدمة:-

جاء غياب الأمن السيبراني في المرتبة الرابعة من بين أبرز 10 مخاطر متوقعة في العامين المقبلين والتي تصدرت تقرير المخاطر العالمية 2024م الصادر عن منتدى دافوس العالمي في يناير 2024م والذي شمل استطلاع آراء أكثر من 1400 من خبراء المخاطر العالميين وصناع السياسات وقادة القطاعات، وكانت المرتبة الأولى من نصيب المخاطر المتعلقة بالمعلومات الخاطئة والمضللة المعززة بالذكاء الإصطناعي وهي تعد كذلك من المخاطر الإلكترونية(WEF,2024)، وفي ظل التطور التقني المتسارع في استخدام الحاسوب والإنترنت في المعاملات المالية وفي أنظمة المعلومات المحاسبية بصفة عامة تزايد معه احتمال تعرض أمن المعلومات المحاسبية للمخاطر السيبرانية، وفي المقابل فإن حوكمة تقنية المعلومات تعد إحدى الأدوات الأساسية للتحكم وتوجيه تقنية المعلومات لتحقيق استراتيجية وأهداف المؤسسة وبما قد يساهم في الحد من المخاطر التقنية والتي من بينها المخاطر السيبرانية .

2.مشكلة الدراسة:-

الأمن السيبراني هو أمن الفضاء الإلكتروني و يدخل في نطاقه أمن كافة المعلومات الإلكترونية بما فيها أمن المعلومات المحاسبية، وبالتالي فإن الحد من التهديدات والمخاطر السيبرانية يساهم في تعزيز الأمن السيبراني وهذا ينعكس ايجابا على تعزيز أمن المعلومات المحاسبية والعكس صحيح، ولقد احتلت المخاطر السيبرانية المركز الأول في الإستبيان

العالمي لأعلى المخاطر المتوقعة في 2024م والذي أجراه المعهد الدولي للمراجعين الداخليين، ووفقا للعدد 22 من (يورومسكو) الصادر من المعهد الأوروبي للبحر المتوسط في يوليو 2021م فإنه من ضمن التحديات التي تواجه منطقة الشرق الأوسط وشمال أفريقيا تحديث مؤسساتها العامة لمواجهة التهديدات الجديدة في الفضاء السيبراني، ولقد تحصلت ليبيا على معدل متدني جدا في مؤشر الأمن السيبراني العالمي لسنة2020م الصادر من الإتحاد الدولي للإتصالات التابع للأمم المتحدة، كما عقد مؤتمرين دوليين في ليبيا عن الأمن والمخاطر السيبرانية في كل من بنغازي وطرابلس وذلك في يناير 2023م وتم التأكيد في كلا المؤتمرين على أهمية الأمن السيبراني كركيزة للأمن القومي وعلى ضرورة إنشاء بنية تحتية للتحول الرقمي وبناء استراتيجية وطنية للأمن السيبراني، وبالتالي فإن هناك حاجة ماسة للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة، وتعد حوكمة تقنية المعلومات إحدى الأدوات الهامة لتفعيل دور ادارة المخاطر وأنظمة الرقابة على تقنية المعلومات بما قد يساهم في الحد من المخاطر التقنية وتعزيز أمن المعلومات المحاسبية، ووفقا لما سبق يمكن صياغة مشكلة الدراسة كالتالي:-

التساؤل الأول:- ما هي أهم المخاطر السيبرانية التي يمكن أن يتعرض لها أمن المعلومات المحاسبية؟

التساؤل الثاني:- ما مفهوم حوكمة تقنية المعلومات؟ وما دور الحوكمة وحوكمة تقنية المعلومات في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية؟

التساؤل الثالث:- ما مكونات النموذج المقترح لحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة؟

3.أهداف الدراسة:-

الهدف الأول : التعرف على أهم المخاطر السيبرانية التي يمكن أن يتعرض لها أمن المعلومات المحاسبية.

الهدف الثاني : التعريف بحوكمة تقنية المعلومات والتعرف على دور الحوكمة وحوكمة تقنية المعلومات في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية .

الهدف الثالث: إقتراح نموذج لحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة.

4.أهمية الدراسة:-

مع تزايد اعتماد المؤسسات بمختلف أنواعها على التقنية تزايدت تبعا لذلك المخاطر السيبرانية التي تواجهها وأصبح الأمن السيبراني والمخاطر السيبرانية موضوع الساعة، وفيما يتعلق بالدولة الليبية فإن مستوى المخاطر السيبرانية مرتفع وذلك بناءا على دراسات وتقارير العديد من المنظمات الدولية ومع ملاحظة ندرة البحوث والدراسات في هذا المجال في البيئة الليبية جاءت هذه الدراسة لملء الفراغ النظري واقتراح نموذج لحوكمة تقنية المعلومات في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية.

5.منهجية الدراسة:- لتحقيق أهداف الدراسة تم اتباع منهجية التحليل الوصفي من خلال مراجعة الدراسات والتقارير والنماذج وأفضل الممارسات والأدبيات ذات العلاقة.

5.الإطار النظري:-

لتحقيق أهداف الدراسة تم تقسيم الإطار النظري إلى خمسة مباحث وفيما يتعلق بمراجعة الدراسات السابقة ولمنع التكرار وجلبا للفائدة تم تقسيمها إلى فئتين الفئة الأولى تتمثل في الدراسات السابقة عن حوكمة تقنية المعلومات في القطاع العام وتم إدراجها ضمن المبحث الثاني، أما الفئة الثانية فتتناول دور حوكمة تقنية المعلومات في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية وتم إدراجها في المبحث الثالث.

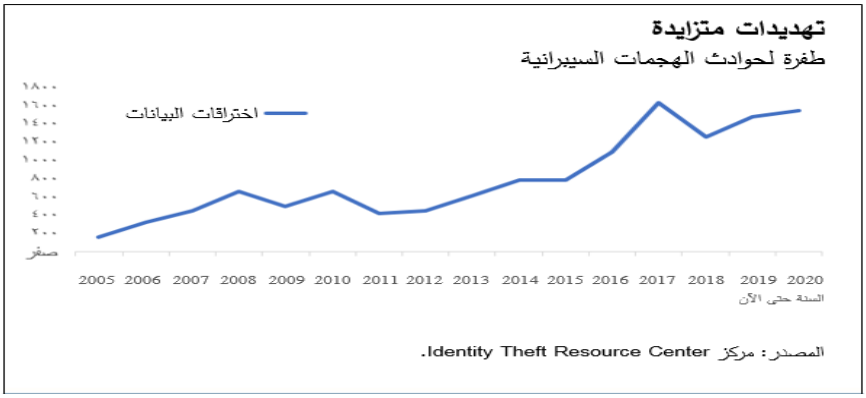
1.5.أمن المعلومات المحاسبية الإلكترونية والمخاطر السيبرانية :-

وصف دليل مراجعة تقنية المعلومات للرقابة العليا لمجموعة الإنتوساي أمن المعلومات بأنه بمثابة حارس البوابة الذي يحمي الأصول المعلوماتية في المؤسسة وعرفه بأنه قدرة النظام على حماية المعلومات وموارد النظام فيما يتعلق بالسرية والسلامة(WGITA،2014)، ووفقا لمعيار الآيزوIEC /17799 فإن المعلومات تعد من الأصول مثل الأصول التجارية الهامة الأخرى وبالتالي هي تحتاج إلى الحماية المناسبة ولقد عرف المعيار أمن المعلومات بأنه حماية المعلومات من مجموعة واسعة من التهديدات من أجل ضمان استمرارية الأعمال وتقليل المخاطر وتعظيم العائد على الاستثمارات(ISO/IEC1779 ، 2005) ومن هنا يمكن تعريف أمن المعلومات المحاسبية بأنه حماية المعلومات المحاسبية وموارد النظام المحاسبي فيما يتعلق بالسرية والسلامة والتوافر من أجل ضمان استمرارية الأعمال وتقليل المخاطر.

ومع تطور الأعمال وانتشار الإنترنت واتساع استخدام الحاسوب والأنظمة الإلكترونية في مختلف الأنشطة الإقتصادية ظهر ما يعرف بالأمن السيبراني والمخاطر السيبرانية، والسيبرانية مصطلح مرادف ل(الفضاء الإلكتروني)، ولقد عرف المعهد الوطني للمعايير والتقنية في الولايات المتحدة الأمريكية الأمن السيبراني بأنه عملية حماية المعلومات عن طريق منع الهجمات والكشف عنها والإستجابة لها(NIST ،2018)، وبصورة أكثر تفصيلية فإن الأمن السيبراني هو"كل

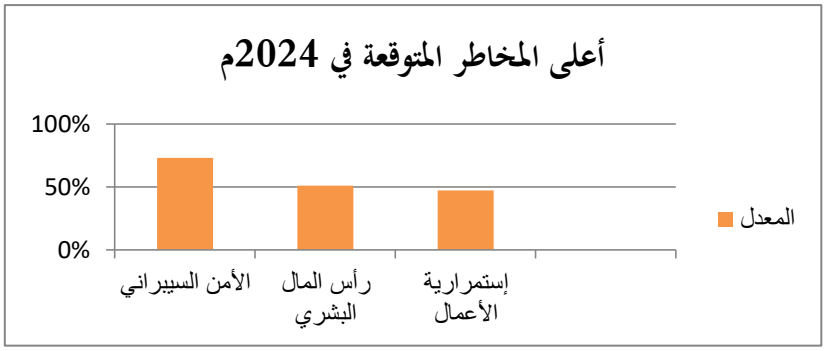
الإجراءات التي تتخذ لحماية الإتصالات والشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من برمجيات وأجهزة، وما تقدمه من خدمات، وما تحتويه من بيانات، سواء كانت حماية سابقة وقائية بواسطة وضع أنظمة حماية من المخاطر المحتملة أو حماية لاحقة من أي هجوم سيبراني أو اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع ويشمل أيضا المحافظة على البني التحتية الحساسة للدولة من هجمات الروبوتات وغيرها وسواء ارتكبت الجريمة السيبرانية عن طريق الجهات الحكومية أو غير الحكومية"(المطيري، 2022 : 999)، كما أن المخاطر السيبرانية هي الأخطار المحتمل وقوعها وتتمثل في الهجمات السيبرانية كالقرصنة واختراق البرمجيات المشفرة والفيروسات وسرقة وتزوير البيانات والمعلومات، وهذه الهجمات لم تعد تقتصر على الهواة والنشطاء والقراصنة بل تتم عبر حروب سيبرانية منظمة تشرف عليها دول ومنظمات وقد تؤدي إلى زعزعة الثقة وتسبب أحيانا في خسائر مادية كبيرة (شحادة، 2022)، ويختلف الأمن السيبراني عن أمن المعلومات في كون الأخير يختص بحماية المعلومات عامة سواء كانت إلكترونية أم غيرها أما الأمن السيبراني فهو كافة العمليات والإجراءات المتبعة لحماية البيئة الإلكترونية والتي تشمل المعلومات والإتصالات والشبكات والأجهزة والبرمجيات وبالتالي فإن نقطة تلاقيهما هي حماية أنظمة المعلومات الإلكترونية وعلى رأسها نظم المعلومات المحاسبية الإلكترونية والتي تأثرت كغيرها بالتطور التقني الحاصل، ولقد ساعد هذا في توفير الوقت والجهد وكذلك في تحسين مستوى الكفاءة والدقة في إعداد وتجهيز وتوصيل المعلومات المحاسبية إلى الإدارة وأصحاب المصالح إلا أن هذا التطور واكبه ارتفاع مستوى المخاطر السيبرانية.

ولقد تزايدت عواقب المخاطر السيبرانية خطورة ولاتزال العناوين الرئيسية مليئة بالتقارير عن الوكالات الحكومية والشركات الكبرى التي وقعت ضحية للهجمات السيبرانية بالرغم من الزيادات الكبيرة في الإنفاق على الأمن السيبراني حيث بلغ حوالي 150 مليار دولار سنويا على مستوى العالم وأكثر من ذلك على المنتجات والخدمات السيبرانية(Chertoff،2023)، ومن المتوقع أن تنمو تكلفة الجرائم السيبرانية - بما في ذلك تكلفة التعافي والمعالجة - إلى 10.5 تريليون دولار سنويًا بحلول عام 2025 (Zeijlemaker et al،2023). ووفقا لموقع صندوق النقد الدولي فإن عدد الهجمات السيبرانية تضاعف ثلاث مرات على مدار العقد الماضي مع تزايد الاعتماد على الخدمات المالية الإلكترونية وهي الأكثر استهدافا ونظرا لقوة الروابط المالية والتقنية المتبادلة، فإن أي هجمة ناجحة على مؤسسة مالية كبرى أو نظام أساسي أو خدمة يستخدمها الكثيرون يمكن أن تنتشر تداعياتها سريعا في النظام المالي بأسره، والشكل التالي يبين عدد الهجمات السيبرانية المتزايدة في الفترة [2005- 2020] على مستوى العالم :-



الشكل (1) ارتفاع مستوى المخاطر السيبرانية المصدر:- صندوق النقد الدولي

ووفقا للاستبيان العالمي الذي أجراه المعهد الدولي للمراجعين الداخليين عن المخاطر المتوقعة على مستوى العالم لسنة 2024م التي تواجه مؤسسات الأعمال، والذي قسم على ستة مناطق هي: أفريقيا، آسيا والمحيط الهادئ، أمريكا الجنوبية والبحر الكاريبي، أوروبا، أمريكا الشمالية، الشرق الأوسط والذي شمل استطلاع آراء 4207 من الرؤساء التنفيذيين للمراجعة الداخلية ومديرو ادارات المراجعة الداخلية فإنه كشف أن هناك إجماع عالمي على المجالات الثلاث الأكثر خطورة بالنسبة للمؤسسات تصدرتها مخاطر الامن السيبراني وجاءت المخاطر المتعلقة بالرأس المال البشري في المرتبة الثانية أما المرتبة الثالثة فكانت لمخاطر استمرارية الأعمال(المعهد الدولي للمراجعين الداخليين، 2024). والشكل (2) يوضح ذلك:



الشكل(2) أعلى المخاطر المتوقعة في 2024م المصدر: من إعداد الباحثة بالإعتماد على بيانات(معهد المراجعين الداخليين IIA ، 2024).

والمخاطر السيبرانية قد تكون مخاطر غير مقصودة ناجمة عن ارتكاب أخطاء أوعدم دراية كافية باستخدام التقنية ومخاطر مقصودة يسعى مرتكبوها للحصول على كسب مادي أو سرقة البيانات والمعلومات أو الإضرار بسمعة المؤسسة ولقد صنفها البعض من حيث المصدر إلى مخاطر داخلية ومخاطر خارجية مثل (بن سعيد، 2018; Zhou،2022): فالمخاطر الداخلية تنشأ من داخل المؤسسة حيث يتمتع الموظفون بسهولة الوصول إلى المعلومات علاوة على ذلك فهم على دراية بالسياسات الأمنية للمؤسسة أم المخاطر الخارجية فتنشأ من قبل أطراف من خارج المؤسسة كالقراصنة والدول، ولقد حدد (IIA، 2016) خمس مصادر للتهديدات السيبرانية وهي: الدول ، مجرمو الإنترنت، القراصنة، المطلعون ومقدمو الخدمات، المطورون للمنتجات والخدمات دون المستوى، ، إلا أن التصنيف العام للمخاطر السيبرانية والذي اعتمدته العديد من الدراسات هو تصنيفها وفقا لأساسيات الأمن السيبراني الثلاثة وهي : - السرية، النزاهة، التوافر أو القدرة على الوصول (IIA،2016 ; Muravskyi،2021 ; Stefanescu.et al،2019):-

1. اختراق السرية بحيث يتم كشف البيانات والمعلومات والإطلاع عليها من قبل أشخاص غير مصرح لهم بالحصول عليها، فأغلب المؤسسات تمتلك بيانات ومعلومات سرية والكشف عنها أو سرقتها قد يسبب ضرر كبير على القيمة السوقية أو الإيرادات أو الميزة التنافسية للمؤسسة.
2. المخاطر التي تسبب ضررا فيما يتعلق بالنزاهة وتتمثل في تزوير وسرقة البيانات والإحتيال.
3. المخاطر المتعلقة بعدم إمكانية الوصول إلى الأنظمة الإلكترونية للمستخدمين المصرح لهم متى وأينما يحتاجون إليها وبالشكل المطلوب ومن أمثلتها تعطيل الأنظمة وعدم القدرة على أداء الخدمة.

بالإضافة إلى ذلك فإن من ظواهر التطور التقني للأنظمة المحاسبية المحاسبة السحابية والتي يتم التعامل من خلالها ونقل وتخزين البيانات والمعلومات عبر الإنترنت وإن كانت تتصف بدرجة عالية من الآمان من حيث حماية البيانات من الفقد أو الحرائق أو السرقة وغيرها وذلك بحكم أن تخزينها والتعامل معها بإجراء النسخ الإحتياطي التلقائي وغيره يتم من خلال طرف آخر عبر الإنترنت وبعيدا جدا عن مقر المؤسسة إلا أن هذا لا يمنع تعرضها للمخاطر السيبرانية فالبرامج الضارة وأخطاء الموظفين وتعطل الأجهزة كلها تؤثر على النظام المحاسبي سواء السحابي أو غيره وهوما أوضحه اتحاد محاسبي أوروبا (FEE ،2016) وأكد أنه من الضروري على المؤسسات أن تتحقق من أن السحابة توفر إجراءات أمنية كافية.

وبين كل من (Laichuk et al،2023; FEE ، 2016) أن استخدام المحاسبة السحابية قد يمكن أشخاص غير مصرح لهم بالإطلاع على البيانات كما أن المعلومات المحاسبية معرضة للتهديدات السيبرانية من خلال عدم القدرة على استخدام الإصدارات القديمة للبرامج والإعتماد الكبير على جودة الخدمات المقدمة من قبل مقدمي الخدمة والافتقار إلى الحماية القانونية المناسبة لحقوق المعلومات في البيئة السحابية إضافة إلى أن النسخ الإحتياطي التلقائي قد يوفر أمانا أفضل من أنظمة سطح المكتب إلا أن المؤسسة لا تتحكم في نظام النسخ الإحتياطي وكم مدة الحفظ وكيفية الوصول إليه.

وفي دراسة أجرتها شركة MCAfee أظهرت أن واحد من كل أربعة مشاركين في استطلاع 2018م أبلغو عن سرقة بيانات من مستخدمي السحابة، وواحد من كل خمسة تعرضوا لهجوم على السحابة الخاصة بهم ولذا فالمؤسسات يجب أن لاتفترض أن السحابة ستوفر لهم مستوى فعال من الأمن(ACCA et al.،2019).

كذلك ظهرت تقنية البلوك تشين في مجال المحاسبة وهي عبارة عن مجموعة من الأجهزة المترابطة ببعضها على هيئة كتل سلاسل عبر الإنترنت وتخزن فيها البيانات والمعلومات وتتم المعاملات والتبادل بين المشاركين بحيث أن كل معلومة يتم تسجيلها تشفر ولايمكن تعديلها وكافة المشاركين يكونون مطلعين على كافة البيانات وبالتالي توفر مستوى عالي من الشفافية إلا أن هذه التقنية في نفس الوقت تتمتع بمستوى منخفض من الخصوصية وسرية البيانات المتعلقة بأنشطة المؤسسة فضلا عن التخزين الزائد لدى أجهزة تخزين البيانات(Laichuk et al.،2023).

2.5. ماهية حوكمة تقنية المعلومات :-

الحوكمة بمفهومها الإداري والمحاسبي تتمثل في وجود مجلس إدارة فعال مسؤوليته الإشراف والتوجيه والمراقبة على الإدارة التنفيذية من أجل الحفاظ على حقوق أصحاب المصالح وتحقيق أهداف المؤسسة وذلك من خلال تفويض الصلاحيات وتشكيل لجان تتبعه ويشترط في مجلس الإدارة الفعال أن يتضمن أعضاء مستقلين عن الإدارة التنفيذية، ويتوجب أن يقوم بمسؤولياته كلها في نطاق الشفافية والإفصاح، ومع اتساع استخدام التقنية في مجال الأعمال ومختلف أنواع المؤسسات وتزايد المخاطر التي تتبعها ظهرت عدة أنواع من الحوكمة وجميعها وبدون استثناء هي جزء من الحوكمة الشاملة للمؤسسة مثل حوكمة البيانات والحوكمة السيبرانية إلا أن أشهرها وأكثرها انتشارا هي حوكمة تقنية المعلومات.

ظهر مصطلح حوكمة تقنية المعلومات لأول مرة في بداية التسعينات من القرن الماضي، ولقد عرفتها مجموعة عمل الانتوساي لمراجعة تقنية المعلومات ومبادرة الإنتوساي للتنمية بأنها " الإطار العام الذي يوجه عمليات تقنية المعلومات في المؤسسة لضمان تلبية احتياجات العمل في الوقت الحاضر، ويشتمل على خطط للنمو والإحتياجات المستقبلية وهي تعتبر جزءا لا يتجزأ من مشروع الحوكمة الشامل"(WGITA,2014:p18) كما عرفها De Haes&Grembergen بأنها جزء لا يتجزأ من حوكمة الشركات، يمارسها مجلس الإدارة، بحيث يشرف على تحديد وتنفيذ العمليات والهياكل والآليات في المؤسسة التي تمكن كل من رجال الأعمال وموظفي تقنية المعلومات من تنفيذ مسؤولياتهم في دعم الأعمال التجارية لمواءمة تقنية المعلومات وخلق قيمة الأعمال من خلال الاستثمار في تقنية المعلومات (Haes&Grembergen,2015)، وعرفت كذلك من قبل معهد حوكمة تقنية المعلومات بأنها"مسئولية مجلس الإدارة والإدارة التنفيذية، وهي تعد عنصرا أساسيا في حوكمة الشركات وتتضمن قيادة العمليات والهياكل التنظيمية التي تؤكد أن تقنية المعلومات بالمؤسسة تدعم وتساند في تحقيق أهداف واستراتيجيات المؤسسة"(ISACA, 2009)، ومما سبق يمكن تعريف حوكمة المعلومات وتقنية بأنها جزء من حوكمة الشركات ومسؤوليتها تقع على عاتق مجلس الإدارة والإدارة التنفيذية مع وجوب التنسيق الكامل بين أهداف تقنية المعلومات وأهداف المؤسسة.

1.2.5 عناصر حوكمة تقنية المعلومات:

وتتمثل عناصر حوكمة تقنية المعلومات أو المجالات التي تركز عليها فيما يلي(ISACA,2009):-

1. التوافق الإستراتيجي:- وهي عملية تهدف فيها حوكمة تقنية المعلومات أن يكون هناك انسجام وتوافق بين استراتيجية تقنية المعلومات واستراتيجية المؤسسة من خلال التعاون والمشاركة في القضايا والفرص المتعلقة بالتقنية بين مستويات الإدارة داخل المؤسسة .

2. تسليم القيمة:- تتمثل القيمة في تقديم الخدمات والحلول المناسبة في الوقت المحدد وفي حدود الميزانية وتحقيق الفوائد المالية والغير المالية المقصودة من خلال التركيز على استثمارات تقنية المعلومات الحالية التي تضيف قيمة وزيادتها والتخلص من أصول تقنية المعلومات التي لا تضيف قيمة .

3 . إدارة المخاطر:- وتتمثل في معالجة المخاطر المتعلقة بتقنية المعلومات والتي من المحتمل أن تؤثر في أعمال المؤسسة وبالتالي فهي تركز على الحفاظ على القيمة.

4. .إدارة الموارد:- تتمثل في توفير وضمان وجود القدرات والموارد المناسبة لتنفيذ استراتيجية تقنية المعلومات كما تركز على توفير التدريب وضمان كفاءة موظفي تقنية المعلومات.

5. قياس الأداء:- بدون إنشاء ومراقبة مقاييس الأداء فمن غير المرجح أن تحقق المجالات السابقة النتائج المرجوة، ويتضمن القيام بأنشطة التقييم في مجال تقنية المعلومات والتركيز على التحسين المستمر.

وتوجد عدة أطر استخدمت كإطار عمل لحوكمة المعلومات والتقنية كمعاييرISO وإطار ITIL إلا أن أكثرها انتشارا وتطبيقا إطار COBIT للرقابة الداخلية.

2.2.5حوكمة تقنية المعلومات في القطاع العام :-

لم يحض القطاع العام بنفس القدر من الإهتمام الذي حضي به القطاع الخاص في مجال الدراسات التي تناولت حوكمة تقنية المعلومات ومن بينها دراسة(Wiedenhoft et al, 2017) وهدفت التعرف على أثر إضفاء الطابع المؤسسي لحوكمة تقنية المعلومات على النتائج المحققة من تقنية المعلومات بدراسة سلوك الأفراد وأظهرت النتائج أن إضفاء الطابع المؤسسي لحوكمة تقنية المعلومات يساعد المديرين على القيام بالمهام المرتبطة بتقنية المعلومات، دراسة (Ali et al , 2022) هدفت إلى تحديد ممارسات حوكمة تقنية المعلومات في القطاع العام الباكستاني ذات الصلة بعوامل النجاح من خلال مراجعة الأدبيات ذات العلاقة وكذلك دراسة لعدد 8 مؤسسات عامة في الباكستان وأشارت النتائج أن القطاع العام الباكستاني يمارس خمسة مجالات تتبع حوكمة تقنية المعلومات هي: التوافق الإستراتيجي ، تحقيق القيمة، إدارة المخاطر،

إدارة الموارد، قياس الأداء. وهدفت دراسة (Tambotoh et al, 2020) التعرف على ما يمكن أن يساهم في تحسين قدرات حوكمة تقنية المعلومات بناءا على آلياتها من خلال مراجعة 41 دراسة اهتمت بدراسة تنفيذ حوكمة تقنية المعلومات في القطاع العام وخلصت إلى أن هناك العديد من الممارسات لآليات حوكمة تقنية المعلومات، وحاولت دراسة (Ai Qassimi & Rusu,2015)التعرف على كيفية تنفيذ حوكمة تقنية المعلومات في المؤسسات العامة في البلدان النامية من خلال دراسة حالة تتمثل في مؤسسة عامة حكومية لدولة نامية وخلصت أن هناك تنفيذ غير مقصود لحوكمة تقنية المعلومات مع الحاجة للتحسين.

بعض الدراسات حاولت اقتراح نموذج لحوكمة تقنية المعلومات في القطاع العام ومن بينها دراسة(Tonelli et al, 2015) التي هدفت اقتراح نموذج مفاهيمي لحوكمة تقنية المعلومات للتعريف بأثر آليات حوكمة تقنية المعلومات على تقنية المعلومات والأداء التنظيمي للمؤسسات العامة وتم جمع البيانات بإجراء مسح شمل 146 مؤسسة عامة برازيلية وأظهرت النتائج أن أداء تقنية المعلومات يرتبط ارتباطا ايجابيا بالأداء التنظيمي من خلال حوكمة تقنية المعلومات. كذلك دراسة (Ghildyal&Chang,2017)هدفت اقتراح نموذج لحوكمة تقنية المعلومات في القطاع العام وذلك لموائمة استراتيجية الأعمال وتقنية المعلومات مع الأداء التنظيمي لاستدامة القدرات وذلك من خلال مراجعة الأدبيات والدراسات في ذات المجال وبينت الدراسة أن شفافية اتخاذ القرار في المؤسسات العامة لها أثر في فاعلية حوكمة تقنية المعلومات كما خلصت إلى أن التوافق بين تقنية المعلومات والأعمال أمر مهم فيما يتعلق بتنفيذ تقنية المعلومات.كما سعت دراسة(Tambotoh.2017)إلى اقتراح نموذجا يصف العلاقة بين آليات حوكمة تقنية المعلومات والتوافق الإستراتيجي لتقنية المعلومات وتوصلت الدراسة إلى أن النموذج المقترح من الممكن أن يساهم في خلق القيمة العامة من خلال الإستغلال الأمثل لتقنية المعلومات، وفيما يتعلق بالبيئة المحلية دراسة (الصيد وآخرون ، 2022) وهدفت التعرف على أثر حوكمة تقنية المعلومات في أداء الجامعات الليبية واستطاعت تجميع 3006 استمارة استبيان إلكترونية وخلصت إلى وجود علاقة طردية تربط بين حوكمة تقنية المعلومات وأداء الجامعات الليبية.

مما سبق ومن خلال الدراسات السابقة التي تم تناولها في مجال حوكمة تقنية المعلومات في القطاع العام يمكن استخلاص أن حوكمة تقنية المعلومات لها دور ايجابي في تحسين أداء المؤسسات العامة.

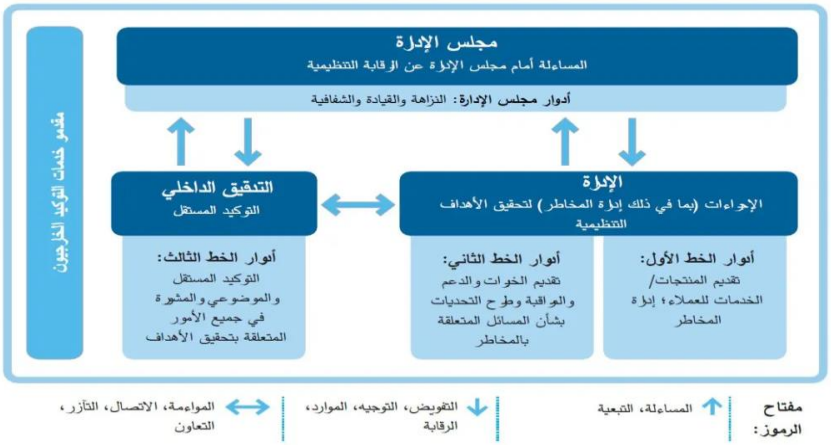
3.5.الحوكمة وحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية الإلكترونية :-

بداية يتوجب التعرف على العلاقة بين الحوكمة وإدارة المخاطر والرقابة الداخلية، ولقد اصدر الإتحاد الدولي للمحاسبين سنة 2012م دليل تقويم وتحسين الرقابة الداخلية للمؤسسات ذكر فيه أن الرقابة الداخلية يمكن أن تكون أكثر فاعلية عندما تكون جزءا لا يتجزأ من نظام إدارة المخاطر، وبدورهما يمثلان جزءا لا يتجزأ من الحوكمة، وتجدر الإشارة إلى أن الحوكمة تركز على الإدارة الفعالة للمخاطر بشكل أكبر من تركيزها على الرقابة الداخلية(IFAC,2012). وما يؤكد أهمية الحوكمة في هذا المجال هناك ثلاثة أطر تتعلق بالأمن السيبراني وإدارة المخاطر والرقابة الداخلية لتقنية المعلومات حضيت على المستوى الدولي بانتشار واهتمام كبيرين وتعد الحوكمة العنصر الأساسي فيها وهذه الأطر هي :-

أولا-إطار الأمن السيبراني :- هو إطار غير ملزم هدفه تقديم التوجيهات وأفضل الممارسات لمواجهة مخاطر الأمن السيبراني وصدرت النسخة المحدثة منه في 26 فبراير 2024م من قبل المعهد الوطني للمعايير والتقنية NIST في الولايات المتحدة الأمريكية حيث تمت إضافة الحوكمة، وأصبحت الوظائف التي يشملها ستة تتقدمها الحوكمة ويمكن باختصار التعريف بهذه الوظائف كالتالي (NIST,2024):-

1- الحوكمة :-ومن خلالها يتم وضع استراتيجة وسياسة إدارة المخاطر للأمن السيبراني للمؤسسة وكذلك التوقعات ومراقبتها، والحوكمة تعد ضرورية لدمج الأمن السيبراني في استراتيجية إدارة المخاطر للمؤسسة.
2- التحديد:- تؤكد هذه الوظيفة على التعرف والفهم الجيد لوظائف وأعمال المؤسسة ومن تم التركيز على المخاطر السيبرانية التي يمكن أن تكون مصدر تهديد للمؤسسة.
3- الحماية :- وهي القيام بالإجراءات المناسبة لحماية المعلومات وضمان عدم تعرضها للمخاطر السيبرانية.
4- الكشف:- وتتمثل في كافة الإجراءات والأنشطة التي تمكن من اكتشاف الهجوم السيبراني في أسرع وقت.
5- الإستجابة :- وهي كافة الأنشطة التي يتوجب القيام بها عند اكتشاف هجوم سيبراني.
6- الإستعادة:- وتتركز في القيام بما يلزم للحفاظ على الأعمال واستمرارها بعد حدوث الهجوم السيبراني.

ثانيا- نموذج الخطوط الثلاثة:- وهو يعد نموذج شامل للحوكمة وإدارة المخاطر والرقابة ولقد أصدر معهد المراجعين الداخليين IIA النسخة المحدثة منه في 2021م ويتكون من ستة مبادئ الحوكمة أولها ويتمثل الخط الأول في الإدارات التشغيلية التي تقوم بالأعمال الروتينية ومهمته الأساسية تتركز في تحديد المخاطر ومنها المخاطر السيبرانية بشكل أولي والخط الثاني يتمثل في إدارات الدعم والتي تساند الخط الأول في الأنشطة التي يقوم بها مثل إدارة المخاطر وإدارة أمن المعلومات والرقابة المالية أما الخط الثالث فهو المراجعة الداخلية ومهمته تقييم مدى كفاءة وفاعلية الخطين الأول والثاني ويشترط أن يتمتع بالإستقلالية عن مسؤوليات الإدارة التنفيذية من خلال المساءلة أمام مجلس الإدارة والوصول غير المقيد إلى الأشخاص والموارد والبيانات اللازمة لإنجاز عمله(معهد المراجعين الداخليين IIA ، 2020)، والشكل(3) يوضح ذلك:-



الشكل(3) نموذج الخطوط الثلاثة المصدر: (معهد المراجعين الداخليين IIA، 2020)

ثالثا COBIT كإطار تنفيذي لحوكمة تكنولوجيا المعلومات:-

وهو اختصارا ل(Control Objectives for Information and related Technology)، وظهرت النسخة الأولى من COBIT سنة 1996م كدليل لتنفيذ المراجعة في بيئة تقنية المعلومات وقامت بإصداره جمعية المراجعة والرقابة على نظم المعلومات (ISACA) وبعد ذلك تم تطوير إطار COBIT وظهرت عدة نسخ منه أشهرها COBIT5 والتي صدرت في 2012م، وينصب التركيز الرئيسي لCOBIT وهو الإطار التنفيذي لحوكمة تقنية المعلومات على التخفيف من المخاطر السيبرانية وتحقيق الأهداف المنشودة، وآخر الإصدارات COBIT19 وتضمنت هذه النسخة مجموعتين من المبادئ تمثلت الأولى في ستة مبادئ تصف المتطلبات الأساسية لحوكمة تقنية المعلومات وهي :-

تزويد أصحاب المصلحة بالقيمة- المنهج الشامل لنظام الحوكمة-نظام حوكمة ديناميكي بما يعني قابلية نظام الحوكمة للتعديل والتغيير - التمييز أو الفصل بين الحوكمة والإدارة - التناسب مع احتياجات المؤسسة-

نطاق عمل الحوكمة يشمل المؤسسة من بدايتها إلى نهايتها(ISACA,2018). بينما المجموعة الثانية تمثلت في ثلاثة مبادئ لإطار نظام الحوكمة أولا أن يعتمد إطار الحوكمة على نموذج مفاهيمي يحدد المكونات الرئيسية والعلاقات بين المكونات، وثانيا أن يكون الإطار مفتوحًا ومرنًا ، وثالثا أن يتماشى إطار الحوكمة مع المعايير والأطر واللوائح ذات الصلة (ISACA,2018).

ومع تنامي دور تقنية المعلومات في المؤسسات وارتفاع مستوى المخاطر والتهديدات السيبرانية أصبحت الحوكمة وتقييم المخاطر السيبرانية شرطا أساسيا لأداء الأعمال الناجح (Zeijlemaker et al. , 2023). وجاءت الحاجة لحوكمة تقنية المعلومات لضمان تحقيق أهداف تقنية المعلومات في المؤسسات والحد من المخاطر السيبرانية التي تواجهها Levestek et al., 2018). فالغرض الأساسي من حوكمة تقنية المعلومات يتمثل في أمرين الأول هو المساعدة في تحقيق الإستخدام الأمثل لتقنية المعلومات والثاني الحد من المخاطر المتعلقة بتقنية المعلومات ويتحقق ذلك من خلال التوافق بين استراتيجية تقنية المعلومات والأعمال وتوفير الموارد اللازمة وإدارتها وقياس الأداء لتقييم مدى التقدم نحو الأهداف المرجوة ISACA, (2009). ولقد اقترحت منظمة التعاون الإقتصادي والتنمية لمواجهة المخاطر السيبرانية اعتماد آلية الحوكمة المحلية الذي يسند إليها دور تعزيز الأمن الرقمي للأنشطة الحيوية (OECD, 2021). وأشار دليل مراجعة تقنية المعلومات لأجهزة الرقابة العليا الصادر من قبل مجموعة الإنتوساي لمراجعة تقنية المعلومات أن من الجوانب الأساسية لحوكمة تقنية المعلومات هو أمن المعلومات لضمان التوافر والسرية والتكامل والتي يعتمد عليها كل شئ(WGITA, 2014).

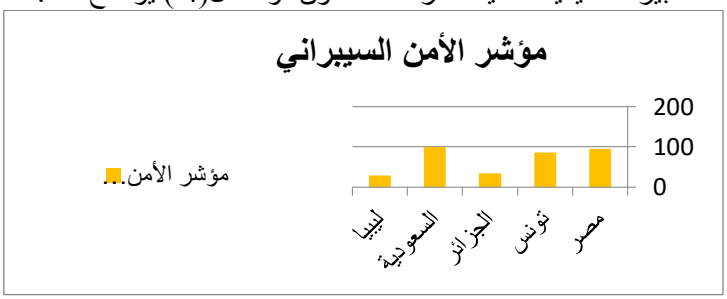
وتوجد العديد من الدراسات التي تناولت حوكمة تقنية المعلومات وبينت الدور الإيجابي لها في الحد من المخاطر السيبرانية وتعزيز أمن وجودة المعلومات المحاسبية ومن بينها دراسة (رحماني و جودي، 2012) التي أشارت أن الإستثمار في تقنية المعلومات يتطلب من المؤسسات اعتماد حوكمة تقنية المعلومات للتقليل من مخاطر أمن المعلومات والإتصالات. وقامت دراسة (Mangalaraj et al ,2014) بمراجعة الدراسات المتعلقة ب COBIT وحاولت البحث في أهداف حوكمة تقنية المعلومات المرتبطة بإطار COBIT وخلصت الدراسة إلى أن أغلب الدراسات ركزت على أمرين هما إما التطوير أو المقارنة بين عدة مجالات مرتبطة ب COBIT مثل الأمن وإدارة المخاطر وفاعلية الرقابة الداخلية كما أظهرت الدراسة زيادة نطاق إطار COBIT بحيث يشمل العديد من المجالات المرتبطة بأمن المعلومات. وخلصت دراسة (Fazlida&Said , 2015) والتي هدفت اقتراح إطار لمخاطر أمن المعلومات وحوكمة تقنية المعلومات إلى أن أمن المعلومات يعد جزءا مكملا لحوكمة تقنية المعلومات في ترسيخ أساسيات الأمن السيبراني.

دراسة (Wolden&Valverde,et.al,2015) هدفت التعرف على أثر COBIT5 كإطار عمل لحوكمة تقنية المعلومات في الحد من مخاطر الهجمات السيبرانية على نظام التوريد وتم توزيع الإستبيان على مديرين المؤسسات المتعلقة بالتوريد وكشفت الدراسة أن COBIT ساهم في وضع إجراءات صارمة لمنع الهجمات السيبرانية. كما أوضحت دراسة Ghidyal&

(Chang,2017) أن حوكمة تقنية المعلومات هي في الواقع مجموعة من العمليات التي تقلل من مخاطر تقنية المعلومات وذلك من خلال التحكم في استثمارات تقنية المعلومات من أجل إضافة قيمة إلى المؤسسة. وتناولت دراسة(الحسناوي وآخرون، 2017) دور حوكمة تقنية المعلومات في تقليل مخاطر مراجعة نظم المعلومات المحاسبية الإلكترونية في ظل إطار عمل COBIT للرقابة الداخلية في المصارف الأهلية العراقية، واستخدمت الدراسة الإستبيان كأداة لجمع البيانات وخلصت إلى أن تطبيق آليات حوكمة تقنيةالمعلومات في المصارف الأهلية العراقية يمكن أن يؤدي إلى تقليل مخاطر المراجعة ودعم أمن المعلومات الإلكترونية. ومن بين الدراسات كذلك التي تناولت دور حوكمة تقنية المعلومات في الحد من المخاطر السيبرانية دراسة (البردان و شحاته ، 2021) وعنوانها: أثر تفعيل حوكمة تقنية المعلومات في ظل استراتيجيات الرقمنة على الحد من الهجمات السيبرانية في البيئة المصرية، وخلصت الدراسة إلى ضرورة قيام المؤسسات ومنها الحكومية في الإستفادة من حوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز شفافية التقارير وإنشاء إدارة للأمن السيبراني تكون مستقلة عن إدارة تقنية المعلومات. دراسة (خليفة وآخرون ، 2021)هدفت التعرف على أثر حوكمة تقنية المعلومات على الحد من مخاطر نظام المعلومات المحاسبي في ظل التطور التقني: دراسة ميدانية على عينة من المحاسبين ، وخلصت إلى أن تفعيل آليات حوكمة تقنية المعلومات بشكل متكامل سيؤدي حتما إلى التقليل من المخاطر التي تواجه نظام المعلومات المحاسبية وهذا ينعكس طبعا على جودة المعلومات المحاسبية. دراسة (Qyssar,et.al, 2021)هدفت إلى استكشاف دور تطبيق حوكمة تقنية المعلومات باستخدام إطار COBIT5 في تحسين أمن أنظمة المعلومات المحاسبية في مصرف التجارة العراقي وأظهرت الدراسة أن تطبيق آليات حوكمة تقنية المعلومات باستخدام COBIT يقلل من مخاطر معالجة البيانات ويحسن أمن نظم المعلومات المحاسبية الآلية. وكشفت دراسة (العازمي ، 2022) والتي هدفت التعرف على دور حوكمة تقنية المعلومات في تأمين المعلومات المحاسبية من المخاطر الإلكترونية في المصارف التجارية الكويتية أن هناك تأثير معنوي لتفعيل حوكمة تقنية المعلومات على تأمين المعلومات المحاسبية من المخاطر الإلكترونية في المصارف التجارية الكويتية، من جانب آخر بعض الدراسات تناولت العلاقة بين حوكمة تقنية المعلومات وجودة المعلومات المحاسبية ومنها(نشوان وآخرون، 2018; رشوان ، 2017 ; بن سعيد ، 2015) وأظهرت هذه الدراسات أن حوكمة تقنية المعلومات لها دور الإيجابي في تحسين جودة المعلومات المحاسبية، مما سبق يتضح أن الحوكمة وحوكمة تقنية معلومات لها دور إيجابي في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية للمؤسسات.

4.5. الجهود والتشريعات في البيئة الليبية في مجال الحوكمة والأمن السيبراني:-

الأمن السيبراني في المؤسسات الليبية العامة يكاد يكون معدوما وبالتالي فإن مستوى المخاطر السيبرانية فيها مرتفع جدا فكلما انخفض مستوى الأمن السيبراني كلما ازدادت المخاطر والتهديدات السيبرانية ولقد فاقم الوضع ما تعانيه ليبيا من انقسام سياسي ووضع أمني هش، ووفقا لمؤشر الأمن السيبراني العالمي لسنة2020م الصادر من الإتحاد الدولي للإتصالات التابع للأمم المتحدة تحصلت ليبيا على معدل متدني جدا مقارنة ببعض الدول العربية كالسعودية التي تحصلت على معدل 99.48 بينما معدل ليبيا بلغ 28.78 فقط ، ويقيس هذا المؤشر خمس مجالات للأمن السيبراني وهي :- التشريعات المتعلقة بالأمن السيبراني – التدابير التقنية – التدابير التنظيمية- تنمية القدرات- التعاون، والشكل(4) يوضح ذلك:-



الشكل (4) مؤشر الأمن السيبراني المصدر: من إعداد الباحثة بالإعتماد على بيانات (ITU)الإتحاد الدولى للإتصالات

أما فيما يتعلق بالجهود والتشريعات في البيئة الليبية في مجال الحوكمة والأمن السيبراني فهي لاترقى لإحتياجات الدولة ولا متطلبات المرحلة والجدول(1) يوضح مايمكن اعتباره أهم التشريعات بالخصوص:-

التشريعات الليبية بشأن الحوكمة والأمن السيبراني الجدول (1)

التشريع	سنة الإصدار
القانون رقم 11 بشأن سوق الأوراق المالية	2010م
لائحة قواعد الإدارة الرشيدة (الحوكمة)	2010م
دليل الحوكمة للقطاع المصرفي	2010م
القانون رقم 23 (القانون التجاري)	2010م
دليل حوكمة تقنية المعلومات للقطاع المصرفي	2023م

المصدر: من إعداد الباحثة

في أغسطس 2023م صدر دليل حوكمة تقنية المعلومات للمؤسسات المالية الليبية من قبل مصرف ليبيا المركزي وهو اطار عام لحوكمة وإدارة المعلومات والتقنية والمجالات الفرعية لها، حيث ألزم بتكوين لجنة لحوكمة تقنية المعلومات والعديد من الإدارات المرتبطة بإدارة تقنية المعلومات مثل إدارة الحوادث، إدارة الخدمات، إدارة مشاريع تقنية المعلومات، إدارة النسخ الإحتياطي للبيانات، إدارة التغيير وغيرها، وهذا الإطار هو جيد من حيث الإجراءات العملية كأساس إلا أن الهيكل العام لإطار حوكمة تقنية المعلومات غير واضح والركائز الأساسية كأدوار مجلس الإدارة وإدارة المخاطر واستقلالية المراجع الداخلي تاهت بين التفاصيل.

و" تعاني ليبيا تاريخيا من غياب الحوكمة ومبادئها، أبرزها المساءلة والشفافية، إذ تشير معضم التقارير الدولية إلى تدني عدد كبير من مؤشراتها في ليبيا مقارنة بدول أخرى"(الأمم المتحدة الإسكوا ، 2020). ومع ذلك فإن ليبيا لديها الإمكانيات التي تجعلها تغير الواقع وتصنع مستقبل زاهر فهي " أكبر اقتصاد نفطي في أفريقيا من حيث احتياطيات النفط المؤكدة تليها نيجيريا والجزائر، وهي أيضا أحد أغنى الاقتصاديات في العالم من حيث نسبة احتياطيات النفط إلى حجم السكان"(البنك الدولي ، 2020: ص7). في المقابل هناك طموحات كبيرة من قبل الدولة الليبية في السير قدما نحو التحول الرقمي مما يخلق في المقابل مزيدا من التهديدات والمخاطر السيبرانية، وفيما يلي بعض الجهود المبذولة في مجال الأمن السيبراني في ليبيا:-

بعض الجهود المبذولة في ليبيا فيما يتعلق بالفضاء السيبراني الجدول(2)

المبادرة	الرؤية أو الهدف
قيام مصرف ليبيا المركزي في 2021م بإطلاق مشروع سايبر ليبيا	**إرساء بنية تشريعية للتحول الرقمي وفتح المجال أمام الإستثمار الآمن في الفضاء السيبراني.**
وضع الاستراتيجية الوطنية للإتصالات والمعلوماتية(2023-2027)من قبل الهيئة العامة للإتصالات والمعلوماتية	**خلق قطاع رقمي مستدام وآمن من أجل مجتمع معرفي متصل وتحويل ليبيا إلى مركز اتصالات ومعلوماتية في أفريقيا.**
مقترح استراتيجية التحول الرقمي الحكومي لدولة ليبيا(2022)	**بحلول نهاية عام 2030، سيتمكن الجميع في دولة ليبيا من التمتع بخدمات حكومية عالمية المستوى بطريقة سلسة وسهلة وآمنة.**

المصدر: من إعداد الباحثة

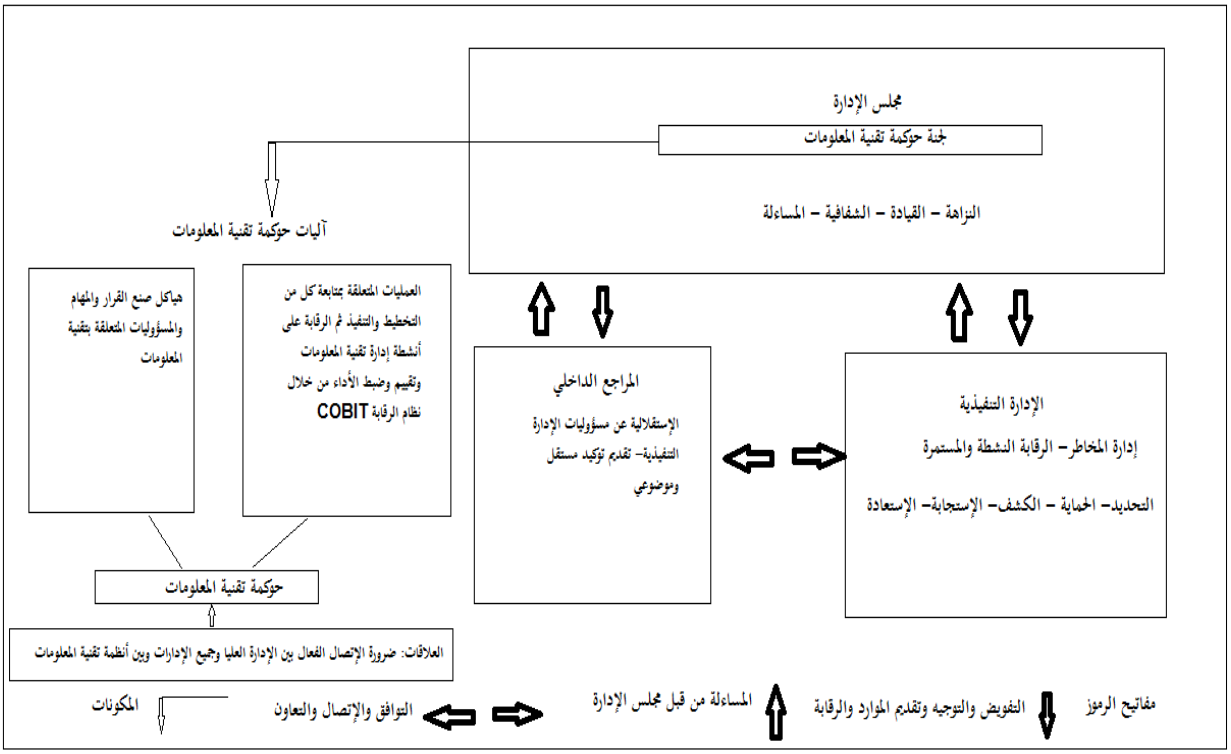
وبناءا لما سبق فإن سمات الفضاء السيبراني للمؤسسات الليبية العامة تتمثل فيما يلي:-

1- التوجه الحثيث نحو التحول الرقمي.
2- ارتفاع كبير في مستوى المخاطر السيبرانية.
3- ضعف أو إنعدام الحوكمة.
4- الإفتقار إلى الأطر والتشريعات القانونية المتعلقة بالفضاء السيبراني.

ومن هنا فإن هناك حاجة ماسة لأطر وتشريعات تساهم في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية ومن بينها نموذج لحوكمة تقنية المعلومات في المؤسسات الليبية العامة.

5.5. نموذج مقترح للهيكل العام لحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة:-

بالأخذ في الإعتبار سمات الفضاء السيبراني للمؤسسات الليبية العامة بحثت الدراسة في النماذج التي تمثل أفضل الممارسات وتحدد بوضوح وبشكل مبسط خطوط المسؤوليات والإتصال فوجدت أن أنسب هذه النماذج هو نموذج الخطوط الثلاثة المعتمد من معهد المراجعين الداخليين (IIA) وجعلته كأساس للنموذج المقترح وفيما يلي النموذج المقترح :-



الشكل (5) الهيكل العام للنموذج المقترح لحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة

وتتمثل الركائز الأساسية للنموذج المقترح فيما يلي:

1- الحوكمة :- يؤكد النموذج على أن حوكمة تقنية المعلومات جزء لا يتجزأ من الحوكمة المؤسسية "الحوكمة الفعالة بمثابة صخرة في المشهد السيبراني المتغير باستمرار" (ACCA et al, 2019:p29).
وتتجسد الحوكمة في النموذج من خلال مجلس الإدارة الذي يعتلي أعلى هرم السلطة في المؤسسة و يتمتع بالإستقلالية عن الإدارة التنفيذية التي تتم مساءلتها من قبله ويمارس أدواره المتمثلة في : النزاهة ، القيادة، الشفافية والمساءلة والعمل على تحقيق التوافق بين استراتيجية تقنية المعلومات واستراتيجية المؤسسة .

2- لجنة حوكمة تقنية المعلومات يقوم بتشكيلها مجلس الإدارة ومسؤليتها تقع على عاتقه وعلى الإدارة التنفيذية.

3- آليات حوكمة تقنية المعلومات المتعارف عليها ثلاثة وقد تناولتها العديد من الدراسات ومن أشهرها (Grembergen, De Haes,2008) وهي الهياكل والعمليات والعلاقات وتتمثل الهياكل في هيكلية صنع القرار المتعلقة بتقنية المعلومات وتحديد الأدوار والمسؤوليات، أما العمليات فهي الإجراءات التنفيذية متمثلة في تخطيط ومتابعة تنفيذ الأنشطة المرتبطة بتقنية المعلومات ثم تقييم الأداء من قبل أنظمة الرقابة على تقنية المعلومات والتي أشهرها COBIT. وآلية العلاقات تتمثل في ضرورة تواجد خطوط اتصال فعالة من خلال اجتماعات دورية بين مجلس إدارة المؤسسة والإدارة التنفيذية والعاملين في أنظمة تقنية المعلومات وكذلك كافة الإدارات ذات الصلة بأنظمة تقنية المعلومات وأمنها.

4- التأكيد على الدور الفعال لإدارة مخاطر تقنية المعلومات في الحد من المخاطر السيبرانية وتطبيق إطار الأمن السيبراني والمتمثل في: الحوكمة- التحديد – الحماية- الكشف- الإستجابة-الإستعادة.

5- التأكيد على استقلالية المراجع الداخلي عن مسؤوليات الإدارة التنفيذية بحيث تكون مساءلته من قبل مجلس الإدارة ويقوم بتقييم أداء الإدارة لتقديم توكيد على مدى سلامة وفاعلية السياسات والإجراءات الرقابية في الحد من المخاطر السيبرانية إلى لجنة حوكمة تقنية المعلومات وكذلك الإدارة التنفيذية.

6- التأكيد على أهمية الرقابة المستمرة في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية حيث أكد دليل تقويم وتحسين الرقابة الداخلية الصادر من قبل الإتحاد الدولي للمحاسبين أن الرقابة الداخلية عنصر مهم في نظام حوكمة المؤسسة والقدرة على إدارة المخاطر(IFAC,2012) . كما أن المراقبة المستمرة ضرورية لتحديد ما إذا كانت استراتيجية إدارة المخاطر السيبرانية تعمل على النحو المنشود(Zeijlemaker et al,2023). إضافة على ذلك تعد المراقبة النشطة أمرا بالغ الأهمية ذلك أنه إذا تمكن المهاجم من الوصول إلى النظام فمن المرجح أن يحصل خط الهجوم التالي على امتيازات إدارية تغطي مساراته(IIA, 2016).

7- الشفافية والإفصاح والمساءلة:- جاء في دليل مراجعة تقنية المعلومات لأجهزة الرقابة العليا الصادر عن مجموعة الإنتوساي المعنية بمراجعة تقنية المعلومات (WGITA) أن الشفافية والمساءلة هما من العناصر الهامة للحوكمة وتعتبر الشفافية قوة هائلة ومتابعة تطبيقها يساعد في محاربة الفساد وتحسين الحوكمة وتعزيز المساءلة (WGITA,2014). إن

الشفافية بشأن الأمن السيبراني لا تعد من أفضل الممارسات فحسب، بل أصبحت الآن مطلبًا للشركات الأمريكية إذ أصدرت هيئة الأوراق المالية في الولايات المتحدة قواعد الأمن السيبراني تطالب فيه الشركات المدرجة في البورصة بالإفصاح وتقديم التقارير عن حالة الأمن السيبراني لديها بما فيها إشراف مجلس الإدارة على المخاطر السيبرانية، ووصف دور الإدارة في تقييم وإدارة المخاطر السيبرانية، والخبرة ذات الصلة لهذه الإدارة، ودور الإدارة في تنفيذ سياسات وإجراءات واستراتيجيات الأمن السيبراني للمؤسسة(Zeijlemaker et al,2023). وأظهرت تجارب المجتمعات النامية أن الشفافية لابد أن تقترن بالمساءلة كما أن فوائدها لاتظهر إلا على المدى الطويل(Thompson,2018).

وتؤكد الباحثة أن الحد من المخاطر السيبرانية في المؤسسات الليبية العامة هي مسألة إدارية قبل أن تكون تقنية ويؤيد ذلك ما جاء في دراسة جمعية المحاسبين المعتمدين العالمية إذ أوضحت أن المخاطر السيبرانية ليست مجرد مشكلة تقنية وموظفوا تقنية المعلومات هم فقط جزء من الحل فالأمر ليس مجرد علاجا فنيا وإنما يجب أن يكون نشاطا تنظيميا(ACCA,2019).

6.5 تحديات ومتطلبات التنفيذ:-

التحديات التي تواجه تنفيذ النموذج المقترح هي ذاتها التي تواجه تنفيذ الحوكمة بصفة عامة في ليبيا، فحوكمة المصارف على سبيل المثال لم تنفذ فعليا حتى هذه اللحظة بالرغم من صدور دليل لحوكمة المصارف الليبية منذ 2010م، ويعد استشراء الفساد المالي والإداري هو العائق الأكبر في تنفيذ الحوكمة في ليبيا ووفقا لمؤشر مدركات الفساد (CPI)لسنة 2023 الصادر من قبل منظمة الشفافية الدولية في يناير 2024م جاءت ليبيا في المرتبة العاشرة في قائمة الدول الأكثر فسادا في العالم (منظمة الشفافية الدولية CPI،2024). وفي رأي الباحثة فإن ممارسات الفساد التي تعاني منها ليبيا منذ عقود أصبحت مع مرور الزمن هي القواعد وأخذت الطابع المؤسسي مما أدى إلى خلق جبهة قوية داخل المؤسسات الليبية معارضة للتغيير ولتنفيذ الحوكمة والإمتثال إذ تعتبر ذالك تهديدا لمصالحها وهذا الرأي يتوافق مع آراء العالمان John Burns & Robert W.Scapens الذين أوضحا أن الأعمال الروتينية في المؤسسة تصبح مع مرور الزمن هي القواعد وتأخذ الطابع المؤسسي بل تصبح المؤسسة ذاتها (Burns& W.Scapens , 2000)، ويرى العالمان وتتفق معهما استراتيجيات التغير المؤسسي أنه لإنجاح التغيير المنشود لابد من خلق قوة داعمة للتغيير داخل المؤسسات وتتمتع بنفوذ أكبر من القوى المعارضة، ووفقا لذلك فإن متطلبات تنفيذ النموذج المقترح هي:-

1- وجود إرادة حقيقية من قبل السلطات العليا في الدولة الليبية لتنفيذ الحوكمة وحوكمة تقنية المعلومات ويترجم ذلك من خلال وضع استراتيجية على مستوى الدولة ذات أهداف واضحة وتوقيت زمني محدد حتى يمكن قياس مدى التقدم المحرز.
2- ايجاد مستوى معين من البنية التحتية لتقنية المعلومات.
3- خلق قوة داعمة لتنفيذ الحوكمة داخل المؤسسات الليبية تكون من بينها كوادر مؤهلة في مجال الرقابة وإدارة المخاطر والأمن السيبراني وتحضى بدعم السلطات العليا وتتمتع بنفوذ يفوق نفوذ القوى المعارضة للتغيير وتنفيذ الحوكمة والإمتثال.

6. الإستنتاجات:-

1- حوكمة تقنية المعلومات هي جزء من الحوكمة الشاملة وتقع مسؤليتها على عاتق مجلس الإدارة والمديرين التنفيذيين وهدفها التوجيه والرقابة على تقنية المعلومات للحد من المخاطر التقنية وتحقيق أهداف المؤسسة.
2- حوكمة تقنية المعلومات لها دور ايجابي في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية.
3- تتمثل سمات الفضاء السيبراني للمؤسسات الليبية العامة في: التوجه الحثيث نحو التحول الرقمي، ارتفاع كبير في مستوى المخاطر السيبرانية، غياب الحوكمة، الإفتقار إلى الأطر والتشريعات المتعلقة بالأمن السيبراني.
4- الركائز الأساسية للنموذج المقترح : الحوكمة، لجنة حوكمة تقنية المعلومات وآلياتها، إدارة مخاطر تقنية المعلومات، استقلالية المراجع الداخلي عن الإدارة التنفيذية، الرقابة المستمرة، الشفافية والإفصاح والمساءلة.
5- يتطلب تنفيذ النموذج المقترح وجود إرادة حقيقية للسلطات العليا للدولة للتنفيذ ووضع استراتيجية ذات أهداف واضحة وتوقيت زمني محدد، وكذلك وجود مستوى من البنية التحتية لتقنية المعلومات وكوادر مؤهلة خصوصا في مجال الرقابة وإدارة المخاطر والأمن السيبراني، كما يتطلب نجاح التنفيذ وتحقيق التغيير المطلوب خلق قوة داعمة للتنفيذ داخل المؤسسات الليبية تتمتع بنفوذ يفوق نفوذ القوى المعارضة.

7. التوصيات:-

1- ضرورة تبني الحوكمة وحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية.
2- من الضروري وجود إرادة حقيقية للسلطات العليا للدولة الليبية لتنفيذ الحوكمة وحوكمة تقنية المعلومات وتوفير مستوى من البنية التحتية لتقنية المعلومات .
3-توصي الدراسة لإنجاح تنفيذ الحوكمة وحوكمة تقنية المعلومات خلق قوة داعمة داخل المؤسسات الليبية العامة تكون من بينها كوادر مؤهلة في مجال الرقابة وادارة المخاطر والأمن السيبراني تحضي بدعم من السلطة العليا وتتمتع بنفوذ يفوق نفوذ القوى المعارضة.
4- توصي الدراسة بتكثيف البحوث في مجال حوكمة تقنية المعلومات وتعزيز الأمن السيبراني والحد من مخاطره.

8. المراجع :-

أولاً المراجع العربية:-

[1] الإسكوا (2020)، دراسة تمهيدية عن الحوكمة والمؤسسات في ليبيا: الوقائع والتحديات والآفاق، الأمم المتحدة.

[2]البردان، محمد و شحاته، محمد(2021)، أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل استراتيجيات الرقمنة على الحد من مخاطر الهجمات السيبرانية بالبيئة المصرية، المؤتمر الدولي الثالث: الرقمنة ضمان جودة التعليم العالي، مصر، 2-3 أكتوبر.

[3] البنك الدولي (2020)، مراجعة القطاع المالي في ليبيا.

[4] الحسناوي، عقيل و الموسوي، إنعام (2017)، دور حوكمة تكنولوجيا المعلومات في تقليل مخاطر تدقيق نظم المعلومات المحاسبية الإلكترونية في ظل إطار عمل COBIT للرقابة الداخلية، مجلة كلية الإدارة والإقتصاد للدراسات الإقتصادية والإدارية والمالية (الكوفة: جامعة الكوفة)، المجلد 9، العدد 3، ص1-24.

[5] الصيد ، وريث و أبوشناف، عبد الله و التويقري، خالد(2022)، أثر حوكمة تكنولوجيا المعلومات في أداء الجامعات الليبية: من وجهة نظر أعضاء هيئة التدريس، مجلة البحوث الإقتصادية والإستراتيجية، العدد التاسع.

[6] العازمي، عبد الله الفالح(2022)، تفعيل حوكمة تكنولوجيا المعلومات في تأمين المعلومات المحاسبية من المخاطر الإلكترونية في ظل عصر الرقمنة : دراسة تطبيقية على البنوك التجارية الكويتية، المجلةالعلمية للدراسات والبحوث المالية والإدارية، المجلد 13، العدد2، مارس، ص 1115-1155.

[7] المطيري، خالد ظاهر (2022)، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية ، العدد 38.

[8] بن سعيد ، أمين(2015)، أثر حوكمة تكنولوجيا المعلومات على جودة وموثوقية القوائم المالية ، مجلة الدراسات الإقتصادية والمالية ، جامعة الوادي، العدد الثامن ، المجلد الثالث ، الجزائر.

[9] بن سعيد، أمين و عبد الرحيم، نادية و مخلوف، أحمد(2018)، مستقبل نظم المعلومات المحاسبية في ظل تكنولوجيا الحوسبة السحابية، مجلة الميادين الإقتصادية، العدد1، المجلد1،ص7-20.

[10]خليفة، أحمد و ضيف الله، محمد و زين، عبد المالك(2021)، أثر حوكمة تكنولوجيا المعلومات على الحد من مخاطر نظام المعلومات المحاسبي: دراسة ميدانية لعينة من المحاسبين، مجلة الدراسات المالية والمحاسبية والإدارية، العدد1، المجلد8.

[11] رحماني، موسى و جودي، سامية (2012)، حوكمة تقنية المعلومات أداة استراتيجية لحماية أمن المعلومات، محبر مالية بنوك وإدارة اعمال، الملتقى الوطني حول:حوكمة الشركات كآلية للحد من الفساد المالي والإداري ، 6-7 مايو.

[12] رشوان، عبد الرحمن محمد(2017)، تحليل العلاقة بين تطبيق حوكمة الشركات وحوكمة تكنولوجيا المعلومات وأثرها على زيادة جودة المعلومات المحاسبية، مجلة الدراسات المالية والمحاسبية والإدارية، العدد الثامن، ديسمبر.

[13] شحادة، مها (2022)،تأثير أبعاد التحول الرقمي في النضج الرقمي للمصارف الإسلامية : بحث تطبيقي في البنوك الإسلامية الأردنية، مجلة الجامعة القاسمية للإقتصاد الإسلامي، المجلد 2، العدد1.

[14] معهد المراجعين الداخليينIIA (2023)،التركيز على المخاطر 2024، مؤسسة المراجعين الداخليين.

[15] معهد المراجعين الداخليين IIA (2020)، نموذج الخطوط الثلاثة: نسخة محدثة من نموذج خطوط الدفاع الثلاثة.

[16] منظمة الشفافية الدولية(2024)، مؤشر مدركات الفساد CPIلسنة 2023.

[17] نشوان، إسكندر و الطويل، عصام و شحادة، محمد(2018)، دور حوكمة تكنولوجيا المعلومات في تحسين جودة المعلومات المحاسبية المنشورة في التقارير المالية: دراسة ميدانية على الشركات الخدمية الفلسطينية، مجلة جامعة الازهر، غزة، عدد خاص، المجلد 20، ص 639-676.

[18] يمني لبن، ألكسندرا(2021)، الإقتصاد الرقمي والجرائم السيبرانية، مجلة يوروميسكو، المعهد الأوروبي للبحر الأبيض المتوسط، العدد 22.

ثانيا المراجع الأجنبية :-

[1] ACCA, Chartered Accountants Australia and New Zealand, Macquarie university and Optus (2019), Cyber and the CFO, The Association of chartered Certified Accountants, May.

[2]Ali. Amanat, Khattak.Muhammad,Arfeen.Muhammad,Yousuf.Laiba, Chaudhary.Muhammad(2022),Exploration of information Technology Governance practices in the public sector: ADeveloping country s perspective, IJCSNS International Journal of Computer Science and Network Security,Vol.22,No.1,pp523-529.

[3]Burns.John, W.Scapens .Robert (2000), Conceptualizing management accounting change: an institutional framework, Elsevier, Vol.11, No.1,pp3-25.

[4] Chertoff, Michael,(2023).Here’s How Companies Can Keep Up . Harvard Business Review, April, 3, available at:

https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up?ab=at_art_art_1x4_s022#
[5]Fazlida, M.R. ,and Said. J (2015), Information Security: Risk, Governance and Implementation Setback, Procedia Economics and Finance, Vol. 28, pp. 243–248.
[6]FEE- federation of European Accountants (2016), Moving to the cloud : Information paper- SMPs ,September.
[7] George Managalarai. Anil Singh. Aakash Taneja(2014), IT Governance Frame works and COBIT- ALiteratur Review,Twenteith Americas Conference on Information Systems, Savannah.
[8]Ghildyal.Amit,Chang.Elizaabeth (2017),IT Governance and Benefit Models: Literature Review and proposal of a Novel Approach,International Journal of e- Education,e-Business,e- Management and e-Learning,Vol.7,No.2,June.
[9]Ghildyal. Amit,Chang.Elizaabeth(2017),ITGovernance,IT BusinessAlinment and Organization performance for public sctors,Journal of Economics,Business and Management,Vol.5,No.6, June, pp255-260.
[10] IFAC-International Federation of Accountants(2012),Evaluating and Improving Internal Control in Organizations.
[11] IIA-The Institute of Internal Auditors (2016),Assessing Cyber Security Risk: Roles of the three Lines of Defense.
[12] ISACA (2009),Implementing and Cotinually Improving ITGovernance,USA.
[13] ISO/ IEC17799,International Standard (2005),Information technology-Security techniques- Code of Practice for Information Security Management.
[14] Laichuk. Svitlana, Maksym. Yatsko, Koval.Liubor,Dovzhyk. Olena,Harkusha. Serhii(2023),Ensuring Cyber Security in Accounting in the Digital Economy ERA,Financial and Credit Activity: problems of theory and practice, Vol.6(53).pp 145-157.
[15]Levstek. Ales, Hovelja.Tomaz,Pucihar. Andreja (2018),ITGovernance Mechanisms and Contingency Factors:Towards an Adaptive it Governance Model, Sciendo, Organizacija, Vol.51, Issue 4, November.
[16] Muravskyi, Volodymyr(2021), Accounting and Cybersecurity: Monograph Kindle Publishing , KDP , Seattle. USA.
[17] NIST-National Institute of Standards and Technology (2018),Framework for Improving Critical Infastructure Cyberseurity. https://doi.org/10.6028/NIST.CSWP.04162018
[18] NIST-National Institute of Standards and Technology (2024), The NIST Cyber Security Framework (CSF) 2.0, February,26.
[19] OECD .Bernat, L. (2021), "Enhancing the digital security of critical activities", Going Digital Toolkit Note, No. 17,
https://goingdigital.oecd.org/data/toolkitnotes/No17_ToolkitNote_DigitalSecurity. pdf
[20]Qassimi. Najla & Rusu.Lazar (2015),IT Governance in public organization in Developing Country:Acase Study of a Governmental Organization,Conference on Enterprise Information systems ,International Conferrnce on Project Management.

[21] Qyssar Alfatlawi.Dawood Al farttoosi. Akeel Almagtome (2021), Accounting Information Security and It Governance Under COBIT 5 framework:ACase Study(Webology , Special Issue on Inforrmation Retrieval and web Search) V.18,April.
[22]Stefanescu. Cristina,Comanescu. Loredana, Buhusi. Ciprian, Bilcan.George (2019), Cyber Security for Cyber Accounting:Tool for the Digital Enterprise, Academic Journal of Economic Studies, Vol.5,No.3,September,pp138-143.
[23] Steven DE Haes and Wim Van Grembergen(2015),Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT5, Springer.

[24] Tambotoh. Johan,Prabowo.Harjanto,Isa.Sani, Pudjianto. Bonifasius (2020),Key Practices Of Information Technology Governance Mechanisms For Public Sector: A systematic Literature Review, International Journal of Advanced Science and Technology, Vol.29,No.7,pp2172-2183.
[25]Tambotoh.Johan, Supangkat.Suhono, Pudjianto. Bonifasius (2017), A Coceptual Model for Creating Effective Public Value Through Key Practices in Information Technology Governance Mechanisms,International Conference of Information Management and Technology,Indonesia, November,15-17.
[26] Thompson. Dennis (2018),Theories of Instetutional Corruption, Annual Review of Plitical Science,Harvard Library Office for Scholarly Communication.
[27] Tonelli. Adriano, Bermejo.Paulo,Santos.Pamela, Zuppo.Larissa, Zambald.Andre (2015), IT Governance in Public Sector: aconceptual model, Springer Science+Business Media, New york.
[28] Van Grembergen, W., and De Haes, S (2008). Implementating Information Technology Governance : Models, Practices, and Cases", IGI Global.
[29]WEF-World Economic Forum(2024),Global Risks Report 2024, Geneva,Switzerland.
[30] WGITA-INTOSAI Working Group on ITAudit,IDI-INTOSAI Aevelopment Initiative (2014), IT Audit for Supreme Audit Institutions,February.
[31] Wiedenhoft.Guilherme, Luciano. Edimara, Pereira.Gabriela (2017), Institutionalization of Information Technology Governance and the Behavior of Individuals in the Public Organizations Cotext, Twenty-Fifth European Confrerence on Information Systems (ECIS),Guimaraes,Portugal.
[32]Woden, M,Valverde,R,&Talla,M,(2015),The Effectiveness of COBIT5 Information Security Framwork for Reducing Cyber attacks on Subbly Chain Management System,IFAC-Papers Online , 48(3),1846-1852.
[33] Zeijlemaker, Sander., Hetner, Chris., Siegel, Michael,(2023). 4 Areas of Cyber Risk That Boards Need to Address. Harvard Business Review, June, 2: https://hbr.org/2023/06/4-areas-of-cyber-risk-that-boards-need-to-address#
[34] Zhou.Ping (2022),Risks in the Design Analysis of Accounting Systems, 7th International Conference on Social Sciences and Economic Development.

ثالثا المواقع الإلكترونية:-

[1] الإتحاد الدولي للإتصالات ، مؤشر الأمن السيبراني العالمي (2020):-
https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
[2] صندوق النقد الدولي ،إليوت. جينيفر، جينكينسون.نايجل(2020)، المخاطر السيبرانية ..التهديد الجديد للإستقرار المالي:-
https://www.imf.org/ar/Blogs/authors?author=Jennifer%20Elliott