Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. Special Issue, Part (1): 374-393
Doi: www.doi.org/10.25130/tjaes.19.SP3.1.22

Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
ISSN: 1813-1719 (Print)

Cybersecurity in Compliance with COBIT Requirements

Adel Sobhi Abdel Qader Al-Basha*
Department of Accounting, College of Administration and Economics. Iraqi University

Keywords:
COBIT2019, cyber security, IT governance.

Article history:
Received 03 May. 2023
Accepted 07 May. 2023
Available online 30 Aug. 2023

*Corresponding author:
Adel Sobhi Abdel Qader Al-Basha
Department of Accounting, College of Administration and Economics. Iraqi University

Abstract: The research aims to study and analyze the relationship between compliance with COBIT requirements and cyber security through a scientific analysis of the concept of the COBIT 2019 framework and the basic principles adopted by it and its mechanism of action, and to identify the foundations of knowledge for the concept of cyber security and its basic dimensions, where awareness of information security has become an urgent necessity because today in almost every home there is At least one device is connected to the Internet and is exposed to one of the electronic threats or exposure to one of the types of viruses, and because information security enhances the awareness of the user of the danger of using technology indiscriminately and thus exposure to penetration and harm to the user. Therefore, awareness of information security is the basis for preserving user privacy despite the use of software Protection and antiviruses, and to achieve the objectives of the research, the researcher prepared a questionnaire consisting of 28 questions distributed to a group of university professors, holders of higher degrees, and a group of those interested in the subject of cybersecurity, as the number of distributed questionnaires reached 54 questionnaires, and the program (SPSS) was used to find the relationship between the variables The researcher reached a set of conclusions, the most important of which was that the COBIT system is used to improve business performance in a balanced framework to create value for information technology and reduce potential risks, and thus improve the level of performance of the economic unit and to increase transparency and maximize vision in the future of economic units in a manner that guarantees the confidence of stakeholders. The recommendations were to pay attention to information security, information technology oversight and governance, and better risk management, in a way that contributes to strengthening the entire corporate governance system.

Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. Special Issue, Part (1): 374-393
Doi: www.doi.org/10.25130/tjaes.19.SP3.1.22

الامن السيبراني في ظل الالتزام بمتطلبات COBIT

عادل صبحي عبد القادر الباشا
قسم المحاسبة، كلية الادارة والاقتصاد، الجامعة العراقية

المستخلص

يهدف البحث إلى القيام بدراسة وتحليل العلاقة بين الالتزام بمتطلبات COBIT والأمن السيبراني من خلال تحليل علمي لمفهوم اطار COBIT2019 والمبادئ الأساسية التي اعتمدها وآلية عمله، وتحديد المرتكزات المعرفية لمفهوم الأمن السيبراني وأبعاده الاساسية ، حيث اصبحت التوعية بأمن المعلومات ضرورة ملحة لأن اليوم في كل منزل تقريبا هناك جهاز واحد على الأقل متصل بالأنترنيت وهو معرض لإحدى التهديدات الالكترونية أو التعرض لأحد أنواع الفيروسات ولأن أمن المعلومات يقوم بتعزيز الوعي لدى المستخدم بخطورة استخدام التكنولوجيا بشكل عشوائي وبالتالي التعرض للاختراق والأضرار بالمستخدم لذلك فإن التوعية بأمن المعلومات هي أساس الحفاظ على خصوصية المستخدم بالرغم من استخدام برامج الحماية ومضادات الفيروسات، ولتحقيق أهداف البحث فقد قام الباحث بإعداد استبانة مكونه من 28 سؤال توزعت على مجموعة من أساتذة الجامعات وحملة الشهادات العليا ومجموعة من المهتمين بموضوع الأمن السيبراني حيث بلغ عدد الاستبانات الموزعة 54 استبانة، وقد تم استخدام برنامج (SPSS) لإيجاد العلاقة بين المتغيرات، وقد توصل الباحث إلى مجموعة من الاستنتاجات كان من أهمها أن نظام COBIT يستخدم لتحسين أداء الأعمال بإطار متوازن لخلق قيمة لتقنية المعلومات وخفض المخاطر المحتملة منها وبالتالي الارتقاء بمستوى اداء الوحدة الاقتصادية ولزيادة الشفافية وتعظيم الرؤية في مستقبل الوحدات الاقتصادية وبما يضمن ثقة اصحاب المصلحة، اما اهم التوصيات فكانت العمل على الاهتمام بأمن المعلومات والرقابة على تقنية المعلومات وحوكمتها وادارة المخاطر بشكل افضل وبما يسهم في تدعيم نظام الحوكمة المؤسسية بالكامل.

الكلمات المفتاحية: COBIT2019، الامن السيبراني، حوكمة تقنية المعلومات.

المقدمة

المبحث الأول: منهجية البحث (Research Methodology)

المقدمة (Introduction)

يعد موضوع الأمن السيبراني جزء أساسي من أمن الوحدة الاقتصادية، حيث يرتبط بالمسائل المتعلقة بحماية المعلومات على جميع أنظمة الحوسبة والشبكات الإلكترونية، ولعظم أهمية الأمن السيبراني وحاجة الناس إليه ولارتباطه بواقعنا المعاصر، باتت عملية حماية الفضاء السيبراني ضرورة لا غني عنها لأن الأمر أصبح بمثابة حرب باردة عبر القارات، وهي من أخطر الحروب، وتزداد خطورتها كلما زاد التقدم في المجال المعلوماتي والتكنولوجي، فالدمار الذي تلحقه هذه الحرب على الوحدة الاقتصادية بصورة عامة أشد وطأة وشراسة من المنافسة التقليدية، فكان لابد من وجود متطلبات يتم الالتزام بها لتحقيق هذه الحماية وهي متطلبات اطار COBIT2019 لحماية الأصول المختلفة للوحدة الاقتصادية حيث يعد من أفضل الاطار المطبقة حاليا لنظام الرقابة الداخلية داخل الوحدات الاقتصادية المتطورة من حيث استخدام وتطبيق جميع أنظمة الحوسبة والشبكات الإلكترونية وتكنولوجيا المعلومات.

أولاً. مشكلة البحث (Research problem): يمكن تحديد مشكلة البحث من خلال الإجابة عن السؤال الآتي "هل هناك تأثير للالتزام بمتطلبات COBIT بكل ما تمتلكه من مميزات على الأمن السيبراني للوحدة الاقتصادية من خلال توفير المستلزمات المناسبة"

ثانياً. هدف البحث (Research goal): يهدف هذا البحث إلى تحقيق الآتي:

1. تحليل علمي لمفهوم إطار COBIT2019 والمبادئ الاساسية التي اعتمدها وآلية عمله.
2. تحديد المرتكزات المعرفية لمفهوم الأمن السيبراني وأبعاده الأساسية.
3. دراسة وتحليل العلاقة بين الالتزام بمتطلبات COBIT والأمن السيبراني

ثالثاً. فرضية البحث (Research hypothesis): ينطلق البحث من فرضية مفادها أن هناك إمكانية للاستفادة من الالتزام بمتطلبات COBIT بكل ما تمتلكه من مميزات وتسخير ذلك لخدمة الأمن السيبراني من خلال توفير المستلزمات المناسبة ويستند البحث إلى الفرضية الرئيسة الآتية:

الفرضية الرئيسة الأولى: "هناك علاقة احصائية ذات دلالة معنوية بين الالتزام بمتطلبات COBIT والأمن السيبراني، وتنبثق من هذه الفرضية الفروض الفرعية الآتية:

الفرضية الفرعية الأولى: "هناك علاقة ارتباط ذات دلالة معنوية بين الالتزام بمتطلبات COBIT والأمن السيبراني.

الفرضية الفرعية الثانية: هناك علاقة تأثير ذات دلالة معنوية بين الالتزام بمتطلبات COBIT والأمن السيبراني.

رابعاً. أهمية البحث (Research importance): تنطلق أهمية البحث من أهمية موضوع الأمن السيبراني ونتائج عدم الاهتمام به كون الموضوع جزء أساسي من أمن الوحدة الاقتصادية، حيث يرتبط بالمسائل المتعلقة بحماية المعلومات على جميع أنظمة الحوسبة والشبكات الإلكترونية وعملية الابلاغ المالي الالكتروني للوحدة الاقتصادية وتزداد خطورة تداعيات عدم الاهتمام بموضوع الأمن السيبراني كلما زاد التقدم في المجال المعلوماتي والتكنولوجي، فالدمار الذي تلحقه هذه الحرب على الوحدة الاقتصادية بصورة عامة أشد وطأة وشراسة من المنافسة التقليدية.

خامساً. مجتمع البحث (Research Community): تم اختيار عينة البحث بصورة عشوائية اقتصرت على مجتمع من أساتذة الجامعات وحملة الشهادات العليا ومجموعة من المهتمين بموضوع الأمن السيبراني.

المبحث الثاني: مفهوم وخصائص الأمن السيبراني

The concept and characteristics of Cybersecurity

أولاً. مفهوم الأمن السيبراني وأبعاده. تند تقنية بلوك تشين

أصبحت شبكة المعلومات الإلكترونية المتصلة جزءًا لا يتجزأ من حياتنا اليومية. حيث تستخدم جميع أنواع الوحدات، مثل المؤسسات الطبية والمالية والتعليمية، هذه الشبكة للعمل بفاعلية. إنهم يستخدمون الشبكة من خلال جمع كميات هائلة من المعلومات الرقمية ومعالجتها وتخزينها ومشاركتها. ومع جمع المزيد من المعلومات الرقمية ومشاركتها، أصبحت حماية هذه المعلومات أكثر أهمية لأمننا القومي واستقرارنا الاقتصادي.

وقد تزايد استخدام الناس للإنترنت بوتيرة سريعة جدًا في العقود الماضية، حيث أفاد تقرير حديث صادر عن Statista أن ما يقرب من 62٪ من سكان العالم و94٪ في أوروبا الغربية يستخدمون الإنترنت اعتبارًا من كانون الثاني 2022، وفيما يتعلق بأجهزة الحوسبة التي يستخدمونها

للوصول إلى الإنترنت، تقرير آخر سابق لعام 2021 من Statista وجد أن ما يقرب من 91٪ من المستخدمين العالميين يستخدمون الهواتف الذكية، يليهم 71٪ يستخدمون أجهزة الكمبيوتر المحمولة و/ أو أجهزة الكمبيوتر المكتبية، و30٪ من أجهزة التلفزيون الذكية، و14٪ من الأجهزة المنزلية الذكية الأخرى، وقد أظهر نفس التقرير أيضًا أن معظم (65٪) المستخدمين العالميين وصلوا إلى الإنترنت من أجهزة الحوسبة الخاصة بهم، بينما استخدم جزء كبير (30٪) أجهزة العمل. ومع الاستخدام الواسع للإنترنت وأنواع مختلفة من أجهزة الحوسبة، تتزايد أيضًا مشكلات الأمن السيبراني والخصوصية، وقد طور العديد من مستخدمي الإنترنت بعض الوعي بهذه المشكلات، خاصةً فيما يتعلق بالتصيد الاحتيالي والأدوات الضارة (Johnson, 2021: 1).

وقد شهد القرن الحالي تطورا هائلا في وسائل الاتصال ومقابل التباين بين مستخدمي الشبكة ظهرت استخدامات غير مشروعة، مما أدى إلى ظهور جرائم مختلف عن الجرائم التقليدية عابرة للقارات وقد سميت بالجرائم المعلوماتية أو الإلكترونية أو جرائم الانترنت لمكافحة هذه الجرائم كان لابد من قيام نظام يكافحها ُ لذا أنشيء الأمن السيبراني، ويمكن تعريف الأمن السيبراني بأنه أمن الشبكات، والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنت وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية، المفروض اتخاذها أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، للحد من آثارها في اقسى واسوء الظروف والأحوال (جبور، 2021: 25)

ويتزايد الاعتراف بممارسة الأمن السيبراني على أنها أكثر من مجرد ممارسة تكنولوجية، حيث أصبح تطبيق وجهات النظر الاجتماعية والسياسية على هذه الممارسة، لا سيما في الوحدات الأكثر شيوعًا، وغالبًا ما يوصف الأمن السيبراني بانه مصدر للخوف، حيث تكون التهديدات الإلكترونية دائمة ومتطورة (Joseph, 2022: 1)

ويطاول الأمن السيبراني جميع المسائل الاقتصادية والاجتماعية والسياسية والانسانية، لذا لابد من التوقف عند أبعاد الأمن السيبراني وهي كالاتي: (جبور، 2021: 28-31)

1. **الابعاد العسكرية**: تتراكم الأمثلة التي يمكن سوقها هذا المجال لتوضيح الأبعاد العسكرية للأمن السيبراني وخطورة الهجمات السيبرانية منها ما حصل في كوريا الجنوبية وجورجيا وغيرها من الدول، لا سيما وإن التقاعس عن معالجة هذه الابعاد قد تكون كلفتها كارثية ونتائج ذلك أكثر دراماتيكية.
2. **الأبعاد الاجتماعية**: تسمح طبيعة الانترنيت المفتوح عبر المدونات والشبكات الاجتماعية لكل مواطن ان يعبر عن تطلعاته السياسية منها وطموحاته الاجتماعية مما يتيح فرصة الاطلاع عل كل هذه الامور، لذلك لابد من العمل حماية المجتمع من مخاطر الفضاء السيبراني والتعامل بحد أدنى من قواعد السلامة مع إدراك للعواقب القانونية التي يمكن أن تترتب على بعض التصرفات التي تمارس في الفضاء السيبراني.
3. **الأبعاد السياسية**: وتتمثل في حق الدولة في حماية نظامها السياسي ومصالحها الاقتصادية وواجبها في السعي إلى تحقيق رفاهية شعبها في وقت تؤثر فيه التقنيات التكنولوجية الحديثة في موازين القوى حيث أصبح بإمكان اي فرد في المجتمع أن يتحول إلى لاعب سياسي في اللعبة السياسية كما أصبح بإمكانه الاطلاع على خلفيات ومبررات القرارات السياسية.

4. **الابعاد الاقتصادية**: يرتبط الامن السيبراني ارتباطا وثيقا بالاقتصاد فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات وعلى كل المستويات كذلك تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لبلدان كثيرة عبر افادتها من فرص الاستخدام التي توفرها وتقدمها الشركات الدولية الكبرى.
5. **الابعاد القانونية:** يرتب النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني نتائج قانونية وموجبات تستدعي اهتمام لحل النزاعات التي يمكن أن تنشا عنها لذلك لا بد مراعاة بعض التحولات التي رافقت ظهور مجتمع المعلومات.

ويرى الباحث إن الأمن السيبراني Cybersecurity هو الجهد المستمر من قبل الوحدة الاقتصادية بكافة هياكلها التنظيمية لحماية هذه الأنظمة المتصلة بالشبكة وجميع البيانات من الاستخدام غير المصرح به أو الأذى وعلى المستوى الشخصي، تحتاج إلى حماية هويتك وبياناتك وأجهزة الكمبيوتر الخاصة بك، وعلى مستوى الوحدة الاقتصادية، فتقع على عاتق جميع العاملين داخل الوحدة الاقتصادية كونها مسؤولية حماية سمعة الوحدة الاقتصادية وبياناتها وزبائنها، وعلى مستوى الدولة، فإن الأمن القومي وسلامة المواطنين ورفاهيتهم على المحك.

ثانياً. انواع الهاكر والمتطلبات الاساسية للأمن السيبراني: تختلف أنواع التهديدات التي تواجه الوحدة الاقتصادية باختلاف من يقوم بها من مهاجمون سيبرانيون حيث نجد أن هناك أنواع مختلفة من المهاجمون أو ما يطلق عليه بالهاكر (Hackers) وكالآتي: (النجار، 2020: 12)

1. **هاكر ذو القبعة البيضاء**: وهو العاكر الاخلاقي الذي يوجه مهاراته لاكتشاف الثغرات ومواطن الضعف في الوحدات والاجهزة المتصلة بها وهو يحمل شهادات متخصصة ليمارس عمله بشكل قانوني.
2. **هاكر ذو القبعة الرمادي**: هو خليط بين ذو القبعة البيضاء والسوداء فهو في بعض الأحيان يقوم باكتشاف الثغرات والتبليغ عنها واصلاحها وفي احيان أخرى يقوم بالاختراق بهدف الابتزاز.
3. **هاكر ذو القبعة السوداء**: وهو الذي يقوم بعمليات الاختراق والذي يستهدف المصارف والشركات الكبيرة بمختلف أنواعها.
4. **هاكر ذو قبعة حمراء:** ومعظمهم يعملون في جهات أمنية يقومون باختراق الهاكر والمتخصصين الاخرين واجهزة التحكم وهم يتلقون الدعم من أجهزة مختلفة.

ويجب أن يتمتع محترفو الأمن السيبراني بنفس مهارات المهاجمين السيبرانيين، ولكن يجب على المتخصصين في الأمن السيبراني العمل ضمن حدود القانون المحلي والوطني والدولي. ويجب على محترفي الأمن السيبراني أيضًا استخدام مهاراتهم بشكل أخلاقي.

وفيما يتعلق بالمتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات (Threats) الداخلية والخارجية وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية وهي (الهيئة الوطنية للأمن السيبراني)

- ❖ سرية المعلومة (Confidentiality)
- ❖ سلامة المعلومة (Integrity)
- ❖ توافر المعلومة (Availability)

وتأخذ هذه الضوابط بالاعتبار المحاور الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

- ❖ الإستراتيجية (Strategy)
- ❖ الأشخاص (People).
- ❖ الإجراء (Process).
- ❖ التقنية (Technology).

المبحث الثالث... إطار عمل COBIT
The COBIT framework

أولاً. مفهوم حوكمة تقنية المعلومات والحاجة لها: إن المفهوم الضمني لإطار COBIT وهو الرقابة في تكنولوجيا المعلومات من خلال البحث عن المعلومات التي تكون ناتجة عن الاستخدام الموحد للموارد المتعلقة بتكنولوجيا المعلومات والتي بحاجة إلى إدارة من خلال عمليات تكنولوجيا المعلومات ولغرض تلبية أهداف الوحدة الاقتصادية يتطلب الأمر أن تكون المعلومات متوافقة مع معايير معينة يشير إليها بـ COBIT على أنها متطلبات الوحدة للمعلومات. وعند وضع قائمة بالمتطلبات، يوجد COBIT المبادئ الضمنية وهي متطلبات الجودة والتي تشمل الجودة والكلفة والتسليم ومتطلبات ائتمانية وتشمل الكفاءة والثقة والمطابقة مع القوانين ومتطلبات الحماية والتي تشمل السرية والنزاهة وتوافر المعلومات (خالد، 2014: 343).

تعد حوكمة تقنية المعلومات جزء من حوكمة الشركات التي تسهم في الرقابة على تقنية المعلومات وادارة المخاطر بشكل أفضل وإن استعمال إطار COBIT لحوكمة تقنية المعلومات يساهم في تدعيم نظام الحوكمة المؤسسية بالكامل (العبيدي والجوهر، 2019: 35).

وفي ضوء التحول الرقمي، أصبحت المعلومات والتكنولوجيا (I & T) حاسمة في دعم واستدامة ونمو الوحدات الاقتصادية، ففي السابق، كان بإمكان مجالس الإدارة والإدارة العليا تفويض أو تجاهل أو تجنب القرارات المتعلقة بـ I & T. والان في معظم القطاعات والصناعات، أصبحت هذه المواقف غير متوقعة فغالبًا ما يكون خلق قيمة أصحاب المصلحة (أي تحقيق الفوائد بتكلفة مثالية للموارد مع تحسين المخاطر) مدفوعًا بدرجة عالية من الرقمنة في نماذج الأعمال الجديدة والعمليات الفعالة والابتكار الناجح وما إلى ذلك، ونظرًا لمركزية I&T في إدارة مخاطر المؤسسة وتوليد القيمة، فقد ظهر تركيز خاص على إدارة المؤسسات للمعلومات والتكنولوجيا (EGIT) على مدى العقود الثلاثة الماضية وبذلك اصبحت EGIT جزء لا يتجزأ من حوكمة الشركات حيث يتم ممارستها من قبل مجلس الإدارة الذي يشرف على تحديد وتنفيذ العمليات والهياكل والآليات العلائقية في المؤسسة والتي تمكن كل من رجال الأعمال وتكنولوجيا المعلومات من تنفيذ مسؤولياتهم لدعم الأعمال التجارية وكذلك العمل على مواءمة تكنولوجيا المعلومات وخلق قيمة الأعمال (ISACA, 2019: 11).

ويمكن القول إن حوكمة تقنية المعلومات تمثل جميع الهياكل التنظيمية والاجراءات التنفيذية والقيادية بمختلف أنواعها والتي تضمن تقنية المعلومات والعمل على توسيعها لاستراتيجية الوحدة الاقتصادية وأهدافها (Gherman & Edurado, 2006: 1). لذلك يرى البعض أن حوكمة تقنية المعلومات هي من مسؤولية مجلس الادارة والمديرين التنفيذين وإن هدفها الأساس هو تحقيق الانسجام الكامل بين استراتيجية تقنية المعلومات واستراتيجية الوحدة الاقتصادية وإنها جزء من نظام أشمل واوسع هو الحوكمة للوحدة الاقتصادية (العبيدي والجوهر، 2019: 17).

وتتضمن فوائد إدارة المعلومات والتكنولوجيا الاتي: - (ISACA, 2019: 11-12):

1. تحقيق الفوائد من خلال خلق قيمة للوحدة الاقتصادية.
2. تحسين المخاطر من خلال المحافظة على ما تم خلقه من قيمة.
3. تحسين الموارد من خلال ضمان وجود القدرات المناسبة لتنفيذ الخطة الإستراتيجية وتوفير الموارد الكافية والمناسبة والفاعلة.

ثانياً. مفهوم وأهمية إطار COBIT المحدث ومراحل تطوره COBIT اختصار لـ

Control Objectives for Information and Related Technology

وتعني أهداف الرقابة على المعلومات والتقنيات المتعلقة بها حيث يعرف دوليا على أنه وصف لمجموعة من الممارسات الجيدة لمجلس الادارة والادارة التنفيذية والأعمال التشغيلية ومديري تكنولوجيا المعلومات حيث يحدد مجموعة عمليات الرقابة على تكنولوجيا المعلومات وينظمها حول إطار عمل منطقي لعمليات تكنولوجيا المعلومات للوحدة (De Haes & Van, 2015: 129).

تستخدم إرشادات COBIT مصطلحات حوكمة معلومات المؤسسة والتكنولوجيا، وحوكمة المؤسسات للمعلومات والتكنولوجيا، وحوكمة تكنولوجيا المعلومات وحوكمة تكنولوجيا المعلومات بالتبادل (ISACA, 2018: 18).

ويمكن القول إن COBIT هو إطار عمل لحوكمة وإدارة معلومات وتقنية المؤسسة، يستهدف المؤسسة بأكملها. I&T الوحدة الاقتصادية يعني كل التقنيات ومعالجة المعلومات التي تضعها المؤسسة لتحقيق أهدافها، بغض النظر عن مكان حدوث ذلك في المؤسسة. بمعنى آخر، لا تقتصر شركة I & T على قسم تكنولوجيا المعلومات في وحدة اقتصادية ما، ولكنها تتضمنها بالتأكيد (ISACA, 2018: 14).

وفيما يخص مراحل تطور اصدار إطار COBIT فقد تضمن المراحل الآتية: (L.H. Atrinawati et al., 2021: 2)

1. في عام 1996 تم اصدار ونشر النسخة الأولى الأصلية من إطار COBIT موجه للمدققين للانتقال بشكل أفضل في بيئة تكنولوجيا المعلومات.
2. في عام 1998 تم اصدار النسخة 2 ليتضمن المزيد من الارشادات لإدارة تكنولوجيا المعلومات.
3. في عام 2000 ركز الاصدار 3 على توفير الأدوات وأفضل الممارسات والأهداف القابلة للتطبيق وعوامل النجاح الاساسية ونماذج النضج لعمليات تكنولوجيا المعلومات.
4. في عام 2005 تم اصدار النسخة 4 التي تضمن العديد من المفاهيم التي توضح آليات الحوكمة والادارة الحديثة.
5. في عام 2012 تم اصدار النسخة 5 حيث يوفر إطار أكثر شمولية في مساعدة الوحدات على تحقيق أهدافها في مجالات الحوكمة وادارة تكنولوجيا المعلومات فيها
6. في عام 2018 تم نشر الاصدار الأخير المحدث من قبل ISACA ليتم تسميته (COBIT2019) وليكون الاصدار الأكثر شمولية والممكن تطبيقه من قبل جميع الوحدات بغض النظر عن حجمها واهدافها كونه يعالج أفضل تكنولوجيا متغيرة بسرعة عالية مع توافر المزيد من التحديثات المتكررة.

ويعمل COBIT 2019 على تحسين الإصدارات السابقة من اطار COBIT في المجالات الآتية: (ISACA ,2018: 18)

- ❖ المرونة والانفتاح: حيث يسمح تعريف واستخدام عوامل التصميم بتصميم COBIT من أجل مواءمة أفضل مع سياق المستخدم الخاص، كما تتيح بنية COBIT المفتوحة إضافة مجالات تركيز جديدة أو تعديل المجالات الحالية، دون آثار مباشرة على هيكل ومحتوى النموذج الأساسي COBIT.

- العملة والأهمية: حيث يدعم نموذج COBIT الإشارة والمواءمة مع المفاهيم الناشئة في مصادر أخرى (على سبيل المثال، أحدث معايير تكنولوجيا المعلومات ولوائح الامتثال).
- التطبيق الوصفي: ويمكن أن تكون نماذج مثل COBIT وصفية وتعليمية، حيث تم بناء النموذج المفاهيمي COBIT وتقديمه بحيث يُنظر إلى تجسيده (أي تطبيق مكونات حوكمة COBIT المصممة خصيصًا) على أنه وصفة لنظام حوكمة تكنولوجيا المعلومات المصمم خصيصًا.
- إدارة أداء تكنولوجيا المعلومات: تم دمج هيكل نموذج إدارة أداء COBIT في النموذج المفاهيمي. ليتم تقديم مفاهيم النضج والقدرات من أجل مواءمة أفضل مع CMMI.

ثالثاً. مبادئ ومكونات COBIT2019: يمكن القول إن اطار COBIT2019 يمثل أحد الأطر والأساليب الحديثة للرقابة على استخدام التقنيات الحديثة والاجهزة الالكترونية التي تدخل في عمليات الوحدة بصورة سليمة من خلال مجموعة أهداف يضعها الاطار لتقييم كفاءة نظام الرقابة الداخلية على استخدام تكنولوجيا المعلومات وزيادة فاعلية الأنشطة المرتبطة بها لذلك يعتمد أسلوب حوكمة وإدارة تقنية المعلومات في إطار COBIT2019 على ستة مبادئ: (ISACA, 2018: 18).

1. توفير قيمة أصحاب المصلحة
2. منهج شمولي
3. نظام الحوكمة الديناميكي
4. حوكمة متميزة عن الإدارة.
5. مصممة خصيصا لاحتياجات المؤسسة.
6. نظام الحوكمة الشامل.

وهذا الامر هو توسيع للمبادئ الخمسة الموجودة في COBIT 5 المتضمنة:

1. تلبية احتياجات أصحاب المصلحة.
2. تغطية المؤسسات المستخدِمة من البداية إلى النهاية.
3. تطبيق إطار واحد متكامل.
4. تمكين نهج شمولي.
5. فصل الحكم عن الإدارة.

وتظهر أهمية COBIT2019 من خلال اضافة قيمة للوحدات الاقتصادية التي تستخدم تكنولوجيا المعلومات من خلال التنسيق والموازنة بين المنافع المستهدفة والرقابة على استخدام الموارد وادارة المخاطر وتحديد الأولويات من أجل التركيز على القضايا الرئيسة وربط احتياجات الوحدة الاقتصادية بأصحاب المصلحة لتجنب تعارض المصالح وضمان تحقيق الأهداف وزيادة فاعلية الأنشطة المتعلقة بتكنولوجيا المعلومات من خلال توفير ارشادات عامة لجميع العمليات التي يتم فيها عرض لأنشطة تكنولوجيا المعلومات بالتفصيل وشرح كيفية تنفيذها (Thabit H et al., 2020: 12).

أما مكونات COBIT2019 فقد لتلبية أهداف الحوكمة والإدارة، حيث تحتاج كل وحدة اقتصادية إلى إنشاء وتكييف واستدامة نظام حوكمة مبني من عدد من المكونات التي تمثل العوامل التي تساهم، بشكل فردي وجماعي، في العمليات الجيدة لنظام إدارة الوحدة الاقتصادية عبر تقنية المعلومات والاتصالات حيث تتفاعل المكونات مع بعضها البعض، مما يؤدي إلى نظام حوكمة شامل للإنترنت والتكنولوجيا ويمكن أن تكون المكونات من أنواع مختلفة الأكثر شيوعا هي العمليات. ومع ذلك، فإن مكونات نظام الحكم تشمل أيضًا الهياكل التنظيمية؛ السياسات والإجراءات؛ عناصر

المعلومات؛ الثقافة والسلوك. المهارات والكفاءات؛ والخدمات والبنية التحتية والتطبيقات وكما يأتي: (ISACA, 2018: 14).

1. العمليات: حيث مجموعة منظمة من الممارسات والأنشطة لتحقيق أهداف معينة وإنتاج مجموعة من المخرجات التي تدعم تحقيق الأهداف العامة المتعلقة بتكنولوجيا المعلومات.
2. الهياكل التنظيمية هي الكيانات الرئيسية لصنع القرار في المؤسسة.
3. المبادئ والسياسات والأطر تترجم السلوك المرغوب فيه إلى إرشادات عملية للإدارة اليومية.
4. المعلومات: وهي منتشرة في جميع أنحاء أي منظمة وتشمل جميع المعلومات التي تنتجها وتستخدمها المؤسسة. يركز COBIT على المعلومات المطلوبة للتشغيل الفعال لنظام إدارة المؤسسة.
5. غالبًا ما يتم الاستهانة بثقافة وأخلاقيات وسلوك الأفراد والمؤسسات بعدّها عوامل في نجاح أنشطة الحوكمة والإدارة.
6. مطلوب الأشخاص والمهارات والكفاءات لاتخاذ قرارات جيدة وتنفيذ الإجراءات التصحيحية والانتهاء بنجاح من جميع الأنشطة.
7. تشمل الخدمات والبنية التحتية والتطبيقات البنية التحتية والتكنولوجيا والتطبيقات التي تزود الوحدة بنظام إدارة لمعالجة تقنيات المعلومات والاتصالات.

المبحث الرابع: عرض وتحليل نتائج الاستبيان

اولاً. نتائج الإحصاء الوصفي: يسعى هذا المبحث إلى عرض نتائج الدراسة الميدانية التي أجراها الباحث، وتحليلها، وذلك باستعمال أدوات الإحصاء الوصفي والمتمثلة بالوسط الحسابي لتحديد مدى اتفاق العينة المختارة مع أسئلة الاستبيان، كما تم استعمال الانحراف المعياري لتقدير التشتت المطلق لإجابات أفراد العينة عن الوسط لتقدير التشتت النسبي، وذلك بهدف رسم صورة أو أطار عام لتفضيل المستجيبين وتوجهاتهم العامة فيما يتعلق بمتغيرات البحث، وذلك من خلال مقياس ليكارت (Likart) الخماسي والذي هو مقياس ترتيبي، والأرقام التي تدخل في البرنامج الإحصائي (SPSS) تعبر عن الأوزان والتي هي (اتفق تماما"=5، اتفق=4، محايد=3، لا اتفق=2، لا اتفق تماماً=1) وحدد الباحث مستوى الإجابات في ضوء المتوسطات الحسابية من خلال تحديد انتمائها لأي فئه، ولكون استبانة البحث تعتمد على مقياس ليكارت الخماسي فأنه يتم تحديد الوسط الحسابي (الوسط المرجح) للمقياس من تحديد طول الفترة أولاً وهي مساوية إلى حاصل قسمة 4 على 5، إذ أن 4 تمثل عدد المسافات (من 1 إلى 2 مسافة أولى، ومن 2 إلى 3 مسافة ثانية، ومن 3 إلى 4 مسافة ثالثة، ومن 4 إلى 5 مسافة رابعة) بينما يمثل الرقم 5 عدد الاختيارات، وعند قسمة 4 على 5 ينتج طول الفترة (الفئة) ويساوي 0.8 ويصبح التوزيع وفقاً للجدول رقم (1).

الجدول (1): فقرات مقياس ليكارت

ت	الوسط المرجح	المستوى
1	من 1 إلى 1.79	لا اتفق تماما
2	من 1.8 إلى 2.59	لا اتفق
3	من 2.6 إلى 3.39	محايد
4	من 3.4 إلى 4.19	اتفق
5	من 4.2 إلى 5	اتفق تماما

المصدر: اعداد الباحث

Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. Special Issue, Part (1): 374-393
Doi: www.doi.org/10.25130/tjaes.19.SP3.1.22

وتألفت الاستبانة من (28) سؤالاً توزعت على محورين، المحور الأول كان للمتغير الأول والموسوم (الالتزام بمتطلبات COBIT) والذي تضمن (14) أسئلة، في حين تضمن المحور الثاني منها المتغير الثاني والموسوم (الامن السيبراني) تضمن (14) أسئلة، وقد تم استلام (54) استبانة من خلال اعداد استبيان تم تصميمه الكترونياً. وقد كان الوسط الحسابي والانحراف المعياري لإجمالي المتغيرات كما هو موضح بالجدول رقم (2).

الجدول (2): الأوساط الحسابية والانحرافات المعيارية الإجمالية

المقاييس / المتغيرات	الوسط الحسابي	الانحراف المعياري	النتيجة
الالتزام بمتطلبات COBIT	4.242	0.368	اتفق
الامن السيبراني	4.198	0.408	اتفق

المصدر: اعداد الباحثان بالرجوع الى برنامج SPSS.

ومن خلال ملاحظة الجدول رقم (2) نجد أن الوسط الحسابي للبعد الأول (الالتزام بمتطلبات COBIT) والبعد الثاني (الأمن السيبراني) كان (4.242) و(4.198) على التوالي، وهما أعلى من الوسط الفرضي والبالغ (3)*، وبانحراف معياري كان (0.368) و(0.408) على التوالي، والنتائج تؤكد على وجود اتفاق عام بين أفراد العينة حول الأسئلة المطروحة فيها، وذلك من خلال نتائج الوسط الحسابي لكلا المتغيرين، فضلاً عن تشتت منخفض في إجابة أفراد العينة من خلال نتيجة الانحراف المعياري لكل المحاور ايضاً.

اولاً. عرض وتفسير نتائج الوسط الحسابي والانحراف المعياري للمحور الأول الموسوم بـ (الالتزام بمتطلبات COBIT)، حيث يوضح الجدول رقم (3) الأوساط الحسابية ومدى ابتعاد الإجابة عن وسطها الحسابي من خلال الانحرافات المعيارية للمحور الأول من الاستبانة الموزعة على أفراد العينة.

الجدول (3): النسب والتكرارات والأوساط الحسابية والانحرافات المعيارية للمحور الأول

ت	الأسئلة	المقياس	اتفق تماما	اتفق	محايد	لا اتفق	لا اتفق تماما	الوسط الحسابي	الانحراف المعياري	النتيجة
1	يمثل نظام COBIT أداة بيد الوحدة الاقتصادية لإدارة وحوكمة تقنية المعلومات وبما يضمن اضافة قيمة للوحدة الاقتصادية.	التكرار	9	36	9	0	0	4.000	0.583	اتفق
		النسبة	%16.7	%66.7	%16.7	%0	%0			
2	يُستخدم نظام COBIT لتحسين أداء الأعمال بإطار متوازن لخلق قيمة لتقنية المعلومات وخفض المخاطر المحتملة منها وبالتالي الارتقاء بمستوى اداء الوحدة.	التكرار	36	18	0	0	0	4.670	0.476	اتفق تماما
		النسبة	%66.7	%33.3	%0	%0	%0			
3	يساعد نظام COBIT في إدارة وإيجاد حلول للمخاطر المتعلقة بتقنية المعلومات وبما يضمن تحقيق اهداف الوحدة الاقتصادية.	التكرار	21	27	6	0	0	4.280	0.656	اتفق تماما
		النسبة	%39.9	%50	%11.1	%0	%0			
4	يحرص نظام COBIT على التأكيد بأن على الوحدة الاقتصادية ان تُدرك قيمة استثمارها في مجال تكنولوجيا الأعمال والعمل على تطوير هذه الاستثمارات.	التكرار	24	27	3	0	0	4.330	0.752	اتفق تماما
		النسبة	%44.4	%50	%5.6	%7	%0			
5	يُستخدم نظام COBIT لزيادة الشفافية وتعظيم الرؤية في مستقبل الوحدات الاقتصادية وبما يضمن ثقة اصحاب المصلحة.	التكرار	12	39	0	3	0	4.110	0.664	اتفق
		النسبة	%22.2	%72.2	%0	%5.6	%0			

*: الوسط الفرضي = مجموع أوزان البدائل ÷ عدد البدائل = (1+2+3+4+5) ÷5=3

ت	الأسئلة	المقياس	اتفق تماما	اتفق	محايد	لا اتفق	لا اتفق تماما	الوسط الحسابي	الانحراف المعياري	النتيجة
6	يحرص نظام COBIT على توفير اعلى مستويات الامان في الوحدات الاقتصادية مما ينعكس على توفير نظرة مستقبلية ثاقبة.	التكرار	15	33	3	3	0	4.110	0.744	اتفق
		النسبة	%27.8	%61.1	%5.6	%5.6	%0			
7	لبناء نظام إدارة وحوكمة تقنية المعلومات فاعل وكفوء على نظام COBIT ان يوفر خمسة مكونات اساسية لا يمكن الاستغناء عنها (الاطار، التعريف واوصاف العمليات، اهداف الرقابة، ارشادات الادارة ونماذج النضج).	التكرار	18	36	0	0	0	4.330	0.476	اتفق تماما
		النسبة	%33.3	%66.7	%0	%0	%0			
8	يساعد نظام COBIT على تلبية احتياجات أصحاب المصلحة المختلفة.	التكرار	30	24	0	0	0	4.506	0.502	اتفق تماما
		النسبة	%55.6	%44.4	%0	%0	%0			
9	يمتلك نظام COBIT القدرة على التوافق أو الاندماج مع أحدث الأطر والمعايير ذات الصلة مما يساعد على التوافق وعلى جميع المستويات.	التكرار	18	30	6	0	0	4.220	0.634	اتفقت ماما
		النسبة	%33.3	%55.6	%11.1	%0	%0			
10	يعمل نظام COBIT على التمييز الواضح بين الحوكمة والإدارة حيث إن كل قسم مطلوب منه أنواع مختلفة من الأنشطة تتطلب هياكل تنظيمية مختلفة تخدم أغراض مختلفة.	التكرار	21	21	9	0	3	4.060	1.036	اتفق
		النسبة	%38.9	%38.9	%16.7	%0	%5.6			
11	أصبحت تقنية المعلومات شيء أساسي يجب توافره في الوحدات بغض النظر عن حجمها ونشاطها، سواء كانت تجارية أو غير ربحية أو من القطاع العام، لتعزيز كفاءتها وجودة منتجاتها/ خدماتها.	التكرار	24	30	0	0	0	4.440	0.502	اتفق تماما
		النسبة	%44.4	%55.6	%0	%0	%0			
12	يعمل نظامCOBIT على تحديد إمكانات التطور التدريجي لمعالجة ما تشهده تكنولوجيا المعلومات من تقلبات مستمرة وبالتالي المحافظة على قدرة مواجهة التقلبات.	التكرار	18	30	3	3	0	4.170	0.771	اتفق
		النسبة	%33.3	%55.6	%5.6	%5.6	%0			
13	يستخدم نظام COBIT نموذجًا مفتوح المصدر يسمح بجمع التعليقات من المجتمع العالمي لمتخصصي إدارة وإدارة تكنولوجيا المعلومات لتحسين المنهجية وبالتالي القدرة على التكيف مع الفرص الجديدة في المستقبل.	التكرار	18	33	0	3	0	4.220	0.718	اتفق تماما
		النسبة	%33.3	%61.1	%0	%5.6	%0			
14	يحدد نظام COBIT عوامل التصميم التي يجب أن تأخذها الوحدة الاقتصادية في الاعتبار لبناء أفضل نظام حوكمة مناسب لجميع احتياجات اصحاب المصلحة.	التكرار	6	42	0	3	3	3.890	0.816	اتفق
		النسبة	%11.1	%77.8	% 0	%5.6	%5.6			

اعداد الباحث بالرجوع الى برنامج SPSS

يتبين من الجدول رقم (3) أن نسبة المتفقين تماما على مستوى أسئلة المحور كانت (35.71%) مقابل نسبة غير المتفقين (لا اتفق + لا اتفق تماما) البالغة (2.79%) أما الإجابات المحايدة فقد كانت بنسبة (5.16%) وقد كان إجمالي الوسط الحسابي لفقرات هذا المتغير (4.242) للمحور الأول وهو أعلى من الوسط الفرضي البالغ (3) من أصل (5) وبانسجام مقبول في الإجابات من خلال قيمة الانحراف المعياري بمعدل (0.368) وهذه النتيجة تدل على ان هناك اتفاق حول تأثير الالتزام بمتطلبات COBIT في الامن السيبراني وفي أدناه الجدول رقم (4) يوضح التكرارات والنسب الإجمالية للمحور الأول.

Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. Special Issue, Part (1): 374-393
Doi: www.doi.org/10.25130/tjaes.19.SP3.1.22

الجدول (4): التكرارات والنسب الإجمالية للمحور الأول

المقياس	اتفق تماما	اتفق	محايد	لا اتفق	لا اتفق تماما	المجموع
التكرار	270	426	39	15	6	756
النسب	%35.71	%56.34	%5.16	%1.99	%0.8	%100

اعداد الباحث بالرجوع الى برنامج SPSS.

ثانياً. عرض وتفسير نتائج الوسط الحسابي والانحراف المعياري للمحور الثاني الموسوم بـ (الأمن السيبراني)، حيث يوضح الجدول (5) الأوساط الحسابية ومدى ابتعاد الإجابة عن وسطها الحسابي من خلال الانحرافات المعيارية للمحور الثاني من الاستبانة الموزعة على أفراد العينة.

الجدول (5): النسب والتكرارات والأوساط الحسابية والانحرافات المعيارية للمحور الثاني

ت	الأسئلة	المقياس	اتفق تماما	اتفق	محايد	لا اتفق	لا اتفق تماما	الوسط الحسابي	الانحراف المعياري	النتيجة
1	يمكن أن تكون كل الأدوار جزءًا من عملك في مجال الأمن السيبراني المثير والمتغير باستمرار والمطلوب بشدة.	التكرار	12	39	3	0	0	4.170	0.505	اتفق
		النسبة	%22.2	%72.2	%5.6	%0	%0			
2	أصبحت شبكة المعلومات الإلكترونية المتصلة جزءًا لا يتجزأ من حياة الوحدة الاقتصادية من خلال جمع كميات هائلة من المعلومات الرقمية ومعالجتها وتخزينها ومشاركتها	التكرار	15	39	0	0	0	4.280	0.452	اتفق تماما
		النسبة	%27.8	%72.2	%0	%0	%0			
3	مع قضاء العاملين في الوحدة الاقتصادية المزيد من الوقت على الإنترنت، يمكن أن تؤثر هويتهم، سواء عبر الإنترنت أو في وضع عدم الاتصال، على امن الوحدة الاقتصادية لذلك يجب توخي الحذر.	التكرار	18	33	0	3	0	4.220	0.718	اتفق تماما
		النسبة	%33.3	%61.1	%0	%5.6	%0			
4	تتضمن بيانات الشركة معلومات مختلفة عن الموظفين والملكية الفكرية والقوائم المالية ويمكن اعتبار هذه الملكية الفكرية سرًا تجاريًا؛ ويمكن أن يكون فقدان هذه المعلومات كارثيًا على مستقبل الوحدة	التكرار	24	24	0	6	0	4.220	0.925	اتفق تماما
		النسبة	%44.4	%44.4	%0	11.1 %	%0			
5	مع ظهور إنترنت الأشياء (IoT)، هناك الكثير من البيانات التي يجب على الوحدة الاقتصادية إدارتها وتأمينها	التكرار	15	39	0	0	0	4.280	0.452	اتفق تماما
		النسبة	%27.8	%72.2	%0	%0	%0			
6	مع السرعة والحجم وتنوع البيانات التي تم إنشاؤها بواسطة إنترنت الأشياء والعمليات اليومية للأعمال، أصبحت سرية هذه البيانات وسلامتها وتوفرها حيوية لبقاء الوحدة الاقتصادية	التكرار	18	27	9	0	0	4.170	0.694	اتفق
		النسبة	%33.3	%50	%16.7	%0	%0			
7	تعد السرية والنزاهة والتوافر، والمعروفة باسم ثالوث CIA، بمثابة دليل لأمن المعلومات للوحدة الاقتصادية حيث تضمن السرية خصوصية البيانات عن طريق تقييد الوصول من خلال تشفير المصادقة وتضمن النزاهة أن المعلومات دقيقة وجديرة بالثقة ويضمن التوافر أن المعلومات في متناول الأشخاص المصرح لهم	التكرار	21	24	6	3	0	4.170	0.841	اتفق
		النسبة	%38.9	%44.4	%11.1	%5.6	%0			

Doi: www.doi.org/10.25130/tjaes.19.SP3.1.22

8	يجب أن تقيد سياسات الوحدة الاقتصادية الوصول إلى المعلومات للأفراد المصرح لهم وأن تضمن عدم عرض هذه البيانات إلا للأشخاص المصرح لهم من خلال تقسيم البيانات وفقًا لمستوى الأمان أو الحساسية للمعلومات.	التكرار	18	24	9	3	0	4.060	0.856	اتفق
		النسبة	%33.3	%44.4	%16.7	%5.6	%0			
9	يجب عدم تغيير البيانات أثناء النقل وعدم تغييرها من قبل الوحدات غير المصرح لها.	التكرار	18	33	3	0	0	4.280	0.564	اتفق تماما
		النسبة	%33.3	%61.1	%5.6	%0	%0			
10	إن حماية وحدة اقتصادية ما من كل هجوم إلكتروني محتمل غير ممكن، وذلك لعدة منها ان الخبرة اللازمة لإنشاء شبكة آمنة وصيانتها قد تكون باهظة الثمن	التكرار	15	33	6	0	0	4.170	0.607	اتفق
		النسبة	%27.8	%61.1	%11.1	%0	%0			
11	سيستمر المهاجمون دائمًا في إيجاد طرق جديدة لاستهداف الشبكات وفي النهاية سينجح الهجوم الإلكتروني المتقدم والمستهدف لذلك ستكون الأولوية بعد ذلك هي مدى سرعة استجابة فريق الأمان للهجوم لتقليل فقدان البيانات ووقت التعطل والإيرادات.	التكرار	24	27	3	0	0	4.390	0.596	اتفق تماما
		النسبة	%44.4	%50	%5.6	%0	%0			
12	قد يقوم المتسلل (أو مجموعة القرصنة) بتخريب موقع الوحدة الاقتصادية على الويب من خلال نشر معلومات غير صحيحة وإفساد سمعتها التي استغرق بناؤها سنوات لذلك فقد تبدو الشركة غير موثوقة وربما تفقد مصداقيتها.	التكرار	18	33	3	0	0	4.280	0.564	اتفق تماما
		النسبة	%33.3	%61.1	%5.6	%0	%0			
13	إذا تم اختراق موقع الوحدة الاقتصادية أو الشبكة، فقد يؤدي ذلك إلى تسريب مستندات سرية وكشف أسرار تجارية وملكية فكرية مما يؤدي فقدان كل هذه المعلومات إلى إعاقة نمو الشركة وتوسعها.	التكرار	15	30	6	3	0	4.060	0.787	اتفق
		النسبة	%27.8	%55.6	%11.1	%5.6	%0			
14	التكلفة المالية للخرق أعلى بكثير من مجرد استبدال أي أجهزة مفقودة أو مسروقة لذلك هناك حاجة ماسة للاستثمار في الأمان الحالي وتعزيز الأمن المادي لمبنى ومعدات ومعلومات الوحدة الاقتصادية.	التكرار	6	45	3	0	0	4.060	0.408	اتفق
		السبة	%11.1	%83.3	%5.6	%0	%0			

اعداد الباحث بالرجوع الى برنامج SPSS

يتبين من الجدول رقم (5) أن نسبة المتفقين (اتفق + اتفق تماما) على مستوى أسئلة المحور كانت (90.87%) مقابل نسبة غير المتفقين البالغة (2.38 %) أما الإجابات المحايدة فقد كانت بنسبة (6.75 %) وقد كان إجمالي الوسط الحسابي لفقرات هذا المتغير (4.198) للمحور الثاني وهو أعلى من الوسط الفرضي البالغ (3) من أصل (5) وبانسجام متوسط في الإجابات من خلال قيمة الانحراف المعياري بمعدل (0.408) وهذه النتيجة تدل على أن هناك اتفاق حول تأثير الالتزام بمتطلبات COBIT في الامن السيبراني وفي أدناه الجدول رقم (6) يوضح التكرارات والنسب الإجمالية للمحور الثاني.

الجدول (6): التكرارات والنسب الإجمالية للمحور الثاني

المقياس	اتفق تماما	اتفق	محايد	لا اتفق	لا اتفق تماما	المجموع
التكرار	237	450	51	18	0	756
النسب	%31.35	%59.52	%6.75	%2.38	%0	%100

اعداد الباحث بالرجوع الى برنامج SPSS

ثانياً. اختبار وتحليل علاقة الارتباط بين متغيرات البحث: إن أول خطوه في تحديد العلاقة بين المتغيرات تتمثل بتحديد متغيرات البحث الأساسية وطبيعة العلاقة بينهما، إذ إن لدينا متغيرين الأول هو المتغير الرئيس (المستقل) والمتمثل بالالتزام بمتطلبات COBIT، والمتغير الثاني وهو ما يسمى بالمتغير المعتمد (التابع) والمتمثل بالأمن السيبراني، وقد جرى التحقق من صحة فرضيات البحث المتعلقة بعلاقات الارتباط بين متغيّرات البحث والتي تم صياغتها استناداً إلى مشكلة البحث، وقد استعملت الوسائل الإحصائية الخاصة بمعامل الارتباط (بيرسون) لتحديد نوع العلاقات بين متغيّرات البحث والبرنامج الإحصائي (SPSS) والذي يختبر علاقات الارتباط بين المتغيّرات الرئيسة. والجدول رقم (7) يوضح نتائج قيم معامل الارتباط بيرسون لمتغيرات البحث التي تم افتراضها.

الجدول (7): معامل الارتباط (بيرسون) بين متغيرات البحث

المتغير المعتمد / المتغير المستقل	الامن السيبراني	مستوى المعنوية
الالتزام بمتطلبات COBIT	0.788	0.194

المصدر: اعداد الباحث بالرجوع الى برنامج SPSS.

ومن الجدول رقم (7) يتضح بأن معامل الارتباط بلغ بين المتغير المستقل المتمثل بـ (الالتزام بمتطلبات COBIT) والمتغير التابع والمتمثل بـ (الامن السيبراني) ما قيمته (0.788) بمستوى معنوية بلغت (0.194) وهي أكبر من مستوى المعنوية البالغ (0.05) وتشير إلى وجود علاقة ارتباط طردية قوية بين متغيرات البحث حيث بلغت نسبة معامل الارتباط بيرسون 78.8%.

ثالثاً. اختبار وتحليل علاقة الانحدار بين متغيرات البحث الرئيسة: لقد جرى التحري عن علاقة التأثير وفقاً لمعادلة الانحدار المتعدد بين المتغير المستقل المتمثل بـ (الالتزام بمتطلبات COBIT) والمتغير التابع المتمثل بـ (الامن السيبراني) ويتضح من الجدول رقم (8) نتائج قيم معادلة الانحدار التي تم التوصل إليها من نتائج الاستبيان الذي تم إجراءه من قبل الباحث.

الجدول (8): قيم معامل الانحدار

المتغير المستقل / المتغير التابع	الامن السيبراني			
الالتزام بمتطلبات COBIT	المؤشرات الإحصائية			
	β	Sig	R^2	F
	0.788	0.194	6060.	79.986

المصدر: اعداد الباحث بالرجوع الى برنامج SPSS.

ومن خلال الجدول رقم (8) تبين قيمة F المحسوبة قد بلغت (79.986) وهي أكبر من قيمة F الجدولية البالغة (4.96) عند مستوى معنوية (0.194) وهذه النتيجة تشير إلى وجود تأثير للمتغير

المستقل (الالتزام بمتطلبات COBIT) في المتغير المعتمد (الامن السيبراني) وإنَّ قيمة (R^2) قد بلغت (0.606) وهي توضح ان المتغير المستقل المتمثل بـ (الالتزام بمتطلبات COBIT) قد فسر ما قيمته 60.6 % من التغير الذي يطرأ على المتغير التابع والمتمثل (الأمن السيبراني) أمّا النسبة المتبقية البالغة (39.94 %) فَتُعزى إلى إسهام متغيرات أخرى غير داخلة في أنموذج الانحدار لم يتم تناولها من قبل الباحث، أما قيمة معامل الميل الحدي لزاوية الانحدار (β) والبالغة (0.788) والتي تبين أن أي تغيير بنسبة وحدة واحدة سوف يعادله تغيير ما قيمته 78.8 %، أما مستوى المعنوية فقد بلغت (0.194) وهي أكبر من مستوى المعنوية (0.05) وهذه النتيجة تشير إلى معنوية معلمة النموذج وتوكد على عدم وجود علاقة تأثير للمتغير التفسيري في المتغير المعتمد.

رابعاً. اختبار الفروض: من النتائج التي تم عرضها في أعلاه يصار إلى رفض الفرضية الرئيسية التي كان مفادها:

الفرضية الرئيسة الأولى: "هناك علاقة احصائية ذات دلالة معنوية بين الالتزام بمتطلبات COBIT والأمن السيبراني، وتنبثق من هذه الفرضية الفروض الفرعية الآتية:

الفرضية الفرعية الأولى: " هناك علاقة ارتباط ذات دلالة معنوية بين الالتزام بمتطلبات COBIT والأمن السيبراني

الفرضية الفرعية الثانية: "هناك علاقة تأثير ذات دلالة معنوية بين الالتزام بمتطلبات COBIT والأمن السيبراني

المبحث الرابع: الاستنتاجات والتوصيات
(Conclusions and Recommendations)

أولاً. الاستنتاجات (Conclusions):

1. إن نظام COBIT يستخدم لتحسين أداء الأعمال بإطار متوازن لخلق قيمة لتقنية المعلومات وخفض المخاطر المحتملة منها وبالتالي الارتقاء بمستوى أداء الوحدة الاقتصادية ولزيادة الشفافية وتعظيم الرؤية في مستقبل الوحدات الاقتصادية وبما يضمن ثقة اصحاب المصلحة.
2. أصبحت تقنية المعلومات شيء أساسي يجب توافره في الوحدات بغض النظر عن حجمها ونشاطها، سواء كانت تجارية أو غير ربحية أو من القطاع العام، لتعزيز كفاءتها وجودة منتجاتها/ خدماتها.
3. يستخدم نظام COBIT نموذجًا مفتوح المصدر يسمح بجمع التعليقات من المجتمع العالمي لمتخصصي إدارة وإدارة تكنولوجيا المعلومات لتحسين المنهجية وبالتالي القدرة على التكيف مع الفرص الجديدة في المستقبل.
4. مع السرعة والحجم وتنوع البيانات التي تم إنشاؤها بواسطة إنترنت الأشياء والعمليات اليومية للأعمال، أصبحت سرية هذه البيانات وسلامتها وتوفرها حيوية لبقاء الوحدة الاقتصادية في المنافسة الشرسة والحرب الباردة التي تعيشها الاسواق العالمية.
5. سيستمر المهاجمون دائمًا في إيجاد طرق جديدة لاستهداف الشبكات وفي النهاية سينجح الهجوم الإلكتروني المتقدم والمستهدف لذلك ستكون الأولوية بعد ذلك هي مدى سرعة استجابة فريق الأمان للهجوم لتقليل فقدان البيانات ووقت التعطل والتكاليف المترتبة على ذلك والإيرادات التي من المتوقع أن تفقد.
6. قد يقوم المتسلل (أو مجموعة القرصنة او الهاكر) بتخريب موقع الوحدة الاقتصادية على الويب من خلال نشر معلومات غير صحيحة وإفساد سمعتها التي استغرق بناؤها سنوات لذلك فقد تبدو الشركة

غير موثوقة وربما تفقد مصداقيتها او قد يقوم بالتلاعب بالمعلومات التي تم الابلاغ عنها من قبل الوحدة الاقتصادية.

7. إذا تم اختراق موقع الوحدة الاقتصادية أو الشبكة، فقد يؤدي ذلك إلى تسريب مستندات سرية وكشف أسرار تجارية وملكية فكرية مما يؤدي فقدان كل هذه المعلومات إلى إعاقة نمو الشركة وتوسعها وفقدان ثقة اصحاب المصالح وعدم القدرة على تحقيق اهداف الوحدة الاقتصادية.

ثانياً. التوصيات (Recommendations):

1. العمل على الاهتمام بأمن المعلومات والرقابة على تقنية المعلومات وحوكمتها وادارة المخاطر بشكل أفضل وبما يسهم في تدعيم نظام الحوكمة المؤسسية بالكامل.
2. نشر ثقافة ومتطلبات الأمن السيبراني بكافة تفاصيلها المختلفة لكافة الأفراد العاملين داخل الوحدات الاقتصادية.
3. العمل على اشراك المتخصصين في مجال الابلاغ المالي الالكتروني بالدورات الضرورية والخاصة بمعالجة أي هجوم سيبراني او على أقل تقدير الاستجابة السريعة ومعالجة تداعيات الهجوم السيبراني.
4. توفير المستلزمات الضرورية للعاملين في مجال الابلاغ المالي الالكتروني من قبل الوحدات الاقتصادية للقيام بحوكمة تقنية المعلومات وذلك من خلال الاستعانة بمتخصصين بمجال الأمن السيبراني.
5. العمل على دعم كافة الدراسات المحاسبية المختصة في مجال الأمن السيبراني وأنظمة الرقابة الداخلية المتطورة (COBIT2019).

المصادر (Resources)

اولاً. المصادر العربية:

1. العبيدي، احمد جاسم، الجوهر، كريمة علي، قياس اداء حوكمة تقنية المعلومات على وفق إطار COBIT باستعمال بطاقة العلامات المتوازنة، مجلة دراسات محاسبية ومالية، المجلد 14 العدد 47، بغداد، جمهورية العراق، 2019.
2. جبور، منى الاشقر، السيبرانية هاجس العصر، جامعة الدول العربية، 2021، WWW.carjj.org
3. خالد، وليد، الرقابة على انظمة المعلومات باستخدام COBIT، مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الاربعون، بغداد، جمهورية العراق، 2014.
4. نجار، شهاب، مقدمة في امن المعلومات، مجلة الكترونية لأمن المعلومات والخصوصية الرقمية، العدد الاول، 2020.

ثانياً. المصادر الأجنبية:

1. De Haes, S., & Van Grembergen, W., Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5 Second Edition, Springer International Publishing Switzerland.2015.
2. Johnson, J., 2021. Share of online adults worldwide who can identify key cybersecurity terms as of 2020. https://www-statista.com.chain.kent.ac.uk/statistics/1147391/online-adults-identify cybersecurity-terms/ .
3. Joseph Da Silva, Cyber security and the Leviathan, journal homepage: www.elsevier.com/locate/cose, 2022.

4. ISACA, COBIT 2019 FRAMEWORK Introduction and Methodology, www.isaca.org/COBITuse. 2018.
5. Gherman, M. and Eduardo, P. "The COBIT 4.0 Strategic Assessment", Modulo Security Risks Manager, 2006.
6. L H Atrinawati, E Ramadhani, T P Fiqar, Y T Wiranti, A I N F Abdullah, H M J Saputra, and D B Tandirau, "Assessment of Process Capability Level in University XYZ Based on COBIT 2019", Journal of Physics: Conference Series ,2021.
7. Thabit H. Thabit, Heba S. Ishhadat, Omar T. Abdulrahman, "Applying Data Governance Based on COBIT2019 Framework to Achieve Sustainable Development Goals", Journal of Techniques, ISSN: 2708-8383, Vol. 2, No. 3, 2020

الملحق (1): حضرة الأستاذ الفاضل المحترم

م/ استبانة

تحية شكر وامتنان...

الاستبانة المعروضة بين يديك الكريمتين جزءً من متطلبات استكمال البحث الموسوم:

الامن السيبراني في ظل الالتزام بمتطلبات COBIT

أملي أن أحظى بمعرفتكم وخبرتكم في التأشير بعلامة (√) داخل المربع المناسب المقابل للأسئلة المرافقة، ويحدوني الأمل في الحصول على أكبر قدر ممكن من العناية والدعم من فيض الخبرة التي تمتلكونها، لما لذلك من تأثير على الاستنتاجات التي سيتوصل إليها الباحثان ونتائج البحث بشكل عام.

مع فائق التقدير والاحترام

الأستاذ المساعد الدكتور عادل صبحي الباشا

الجامعة العراقية كلية الادارة والاقتصاد، قسم المحاسبة

Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. Special Issue, Part (1): 374-393
Doi: www.doi.org/10.25130/tjaes.19.SP3.1.22

المحور الاول: الالتزام بمتطلبات COBIT						
ت	الأسئلة	اتفق نماما	اتفق	الى حد ما	لا اتفق	لا اتفق تماماً
.1	يمثل نظام COBIT أداة بيد الوحدة الاقتصادية لإدارة وحوكمة تقنية المعلومات وبما يضمن اضافة قيمة للوحدة الاقتصادية.					
.2	يُستخدم نظام COBIT لتحسين أداء الأعمال بإطار متوازن لخلق قيمة لتقنية المعلومات وخفض المخاطر المحتملة منها وبالتالي الارتقاء بمستوى اداء الوحدة.					
.3	يساعد نظام COBIT في إدارة وإيجاد حلول للمخاطر المتعلقة بتقنية المعلومات وبما يضمن تحقيق اهداف الوحدة الاقتصادية.					
.4	يحرص نظام COBIT على التأكيد بأن على الوحدة الاقتصادية ان تُدرك قيمة استثمارها في مجال تكنولوجيا الأعمال والعمل على تطوير هذه الاستثمارات.					
.5	يُستخدم نظام COBIT لزيادة الشفافية وتعظيم الرؤية في مستقبل الوحدات الاقتصادية وبما يضمن ثقة اصحاب المصلحة.					
.6	يحرص نظام COBIT على توفير اعلى مستويات الامان في الوحدات الاقتصادية مما ينعكس على توفير نظرة مستقبلية ثاقبة.					
.7	لبناء نظام إدارة وحوكمة تقنية المعلومات فاعل وكفوء على نظام COBIT ان يوفر خمسة مكونات اساسية لا يمكن الاستغناء عنها (الاطار، التعريف واوصاف العمليات، اهداف الرقابة، ارشادات الادارة ونماذج النضج).					
.8	يساعد نظام COBIT على تلبية احتياجات أصحاب المصلحة المختلفة.					
.9	يمتلك نظام COBIT القدرة على التوافق أو الاندماج مع أحدث الأُطر والمعايير ذات الصلة مما يساعد على التوافق وعلى جميع المستويات.					
.10	يعمل نظام COBIT على التمييز الواضح بين الحوكمة والإدارة حيث إن كل قسم مطلوب منه أنواع مختلفة من الأنشطة تتطلب هياكل تنظيمية مختلفة تخدم أغراض مختلفة.					
.11	أصبحت تقنية المعلومات شيء أساسي يجب توافره في الوحدات بغض النظر عن حجمها ونشاطها، سواء كانت تجارية أو غير ربحية أو من القطاع العام، لتعزيز كفاءتها وجودة منتجاتها/ خدماتها.					
.12	يعمل نظامCOBIT على تحديد إمكانات التطور التدريجي لمعالجة ما تشهده تكنولوجيا المعلومات من تقلبات مستمرة وبالتالي المحافظة على قدرة مواجهة التقلبات.					

Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. Special Issue, Part (1): 374-393
Doi: www.doi.org/10.25130/tjaes.19.SP3.1.22

المحور الاول: الالتزام بمتطلبات COBIT						
ت	الأسئلة	اتفق نماما	اتفق	الى حد ما	لا اتفق	لا اتفق تماماً
.13	يستخدم نظام COBIT نموذجًا مفتوح المصدر يسمح بجمع التعليقات من المجتمع العالمي لمتخصصي إدارة وإدارة تكنولوجيا المعلومات لتحسين المنهجية وبالتالي القدرة على التكيف مع الفرص الجديدة في المستقبل.					
.14	يحدد نظام COBIT عوامل التصميم التي يجب أن تأخذها الوحدة الاقتصادية في الاعتبار لبناء أفضل نظام حوكمة مناسب لجميع احتياجات اصحاب المصلحة.					

المحور الثاني: الامن السيبراني						
ت	الأسئلة	اتفق نماما	اتفق	الى حد ما	لا اتفق	لا اتفق تماماً
.1	يمكن أن تكون كل الأدوار جزءًا من عملك في مجال الأمن السيبراني المثير والمتغير باستمرار والمطلوب بشدة.					
.2	أصبحت شبكة المعلومات الإلكترونية المتصلة جزءًا لا يتجزأ من حياة الوحدة الاقتصادية من خلال جمع كميات هائلة من المعلومات الرقمية ومعالجتها وتخزينها ومشاركتها					
.3	مع قضاء العاملين في الوحدة الاقتصادية المزيد من الوقت على الإنترنت، يمكن أن تؤثر هويتهم، سواء عبر الإنترنت أو في وضع عدم الاتصال، على امن الوحدة الاقتصادية لذلك يجب توخي الحذر.					
.4	تتضمن بيانات الشركة معلومات مختلفة عن الموظفين والملكية الفكرية والقوائم المالية ويمكن اعتبار هذه الملكية الفكرية سرًا تجاريًا؛ ويمكن أن يكون فقدان هذه المعلومات كارثيًا على مستقبل الوحدة					
.5	مع ظهور إنترنت الأشياء (IoT)، هناك الكثير من البيانات التي يجب على الوحدة الاقتصادية إدارتها وتأمينها					
.6	مع السرعة والحجم وتنوع البيانات التي تم إنشاؤها بواسطة إنترنت الأشياء والعمليات اليومية للأعمال، أصبحت سرية هذه البيانات وسلامتها وتوفرها حيوية لبقاء الوحدة الاقتصادية.					
.7	تعد السرية والنزاهة والتوافر، والمعروفة باسم ثالوث CIA، بمثابة دليل لأمن المعلومات للوحدة الاقتصادية حيث تضمن السرية خصوصية البيانات عن طريق تقييد الوصول من خلال تشفير المصادقة وتضمن النزاهة أن المعلومات دقيقة وجديرة بالثقة ويضمن التوافر أن المعلومات في متناول الأشخاص المصرح لهم					

المحور الثاني: الامن السيبراني						
ت	الأسئلة	اتفق نماما	اتفق	الى حد ما	لا اتفق	لا اتفق تماماً
.8	يجب أن تقيد سياسات الوحدة الاقتصادية الوصول إلى المعلومات للأفراد المصرح لهم وأن تضمن عدم عرض هذه البيانات إلا للأشخاص المصرح لهم من خلال تقسيم البيانات وفقًا لمستوى الأمان أو الحساسية للمعلومات.					
.9	يجب عدم تغيير البيانات أثناء النقل وعدم تغييرها من قبل الوحدات غير المصرح لها.					
.10	إن حماية وحدة اقتصادية ما من كل هجوم إلكتروني محتمل غير ممكن، وذلك لعدة منها ان الخبرة اللازمة لإنشاء شبكة آمنة وصيانتها قد تكون باهظة الثمن					
.11	سيستمر المهاجمون دائمًا في إيجاد طرق جديدة لاستهداف الشبكات وفي النهاية سينجح الهجوم الإلكتروني المتقدم والمستهدف لذلك ستكون الأولوية بعد ذلك هي مدى سرعة استجابة فريق الأمان للهجوم لتقليل فقدان البيانات ووقت التعطل والإيرادات.					
.12	قد يقوم المتسلل (أو مجموعة القرصنة) بتخريب موقع الوحدة الاقتصادية على الويب من خلال نشر معلومات غير صحيحة وإفساد سمعتها التي استغرق بناؤها سنوات لذلك فقد تبدو الشركة غير موثوقة وربما تفقد مصداقيتها.					
.13	إذا تم اختراق موقع الوحدة الاقتصادية أو الشبكة، فقد يؤدي ذلك إلى تسريب مستندات سرية وكشف أسرار تجارية وملكية فكرية مما يؤدي فقدان كل هذه المعلومات إلى إعاقة نمو الشركة وتوسعها.					
.14	التكلفة المالية للخرق أعلى بكثير من مجرد استبدال أي أجهزة مفقودة أو مسروقة لذلك هناك حاجة ماسة للاستثمار في الأمان الحالي وتعزيز الأمن المادي لمبنى ومعدات ومعلومات الوحدة الاقتصادية.					