DOI: https://doi.org/ http://jadara.edu.jo

The impact of cybersecurity governance in reducing cloud accounting risks - An applied study in Jordanian public shareholding industrial companies

"Mohammad Saeed"Alzghoul - Inaam Muhsin Al-Zwaylif
Professor Doctor
Department of Accounting - Faculty of Finance & Business -
The World Islamic Sciences and Education University
Correspondence:
6200501022@std.wise.edu.jo
inaam.zwaylif@wise.edu.jo

Received: 27/1/2024 Accepted:16/4/2024

Abstract:
This study aimed to identify the impact of cybersecurity governance in reducing cloud accounting risks in Jordanian public shareholding industrial companies. To achieve the objectives of the study, the descriptive analytical approach was followed, by developing a questionnaire and distributing it to a sample of (239) male and female employees, and after conducting statistical analysis. Through the (SPSS) program and using the multiple regression equation, the study showed a set of results, the most notable of which are: the presence of a statistically significant effect at the significance level ($\alpha \leq 0.05$) of cybersecurity governance in reducing cloud accounting risks in Jordanian public shareholding industrial companies. The study recommended a group Among the recommendations, the most prominent of which are: Paying attention to supporting cloud accounting by developing a charter according to which it operates and defines the scope of its work and duties.

Keywords: cybersecurity governance, cloud accounting risks, Jordanian public shareholding industrial companies.

DOI: https://doi.org/ http://jadara.edu.jo

أثر حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية

الباحث"محمد سعيد" محمد الزغول **الباحثة إنعام محسن الزويلف**
أستاذ دكتور
المحاسبة – كلية المال والأعمال – جامعة العلوم الأسلامية
للمراسلة:
6200501022@std.wise.edu.jo inaam.zwaylif@wise.edu.jo

استلام البحث:27/1/2024 قبول البحث:16/4/2024

الملخّص

هدفت هذه الدراسة للتعرف على أثر حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، ولتحقيق أهداف الدراسة تم إتباع المنهج الوصفي التحليلي، من خلال تطوير استبانة وتوزيعها على عينة مكونة من (239) موظف وموظفة، وبعد إجراء التحليل الإحصائي من خلال برنامج (SPSS) وباستخدام معادلة الانحدار المتعدد أظهرت الدراسة مجموعة من النتائج من أبرزها: وجود أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لحوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، وأوصت الدراسة بمجموعة من التوصيات من أبرزها: الاهتمام بدعم المحاسبة السحابية من خلال وضع ميثاق يعمل بموجبه ويحدد نطاق عملها وواجباتها.

الكلمات المفتاحية: حوكمة الأمن السيبراني، مخاطر المحاسبة السحابية، الشركات الصناعية المساهمة العامة الأردنية.

المقدمة

يشهد العصر الحالي تطورا سريعا في مجال تكنولوجيا المعلومات والاتصالات مما جعل الشركات تقوم بممارسة أنشطة عديدة ترتبط بتكنولوجيا المعلومات والاتصالات. ومن بين ما افرزه هذا التطور هو ظهور الحوسبة السحابية واستخدام خدماتها في مجال المحاسبة. والحوسبة السحابية عبارة عن نموذج تقني لتمكين الوصول بشكل مناسب وعند الحاجة الى مجموعة مشتركة من موارد الحوسبة كالشبكات والخوادم والتطبيقات والخدمات والتخزين، والتي من الممكن توفيرها واصدارها بصورة سريعة مع وجود حد أدني من جهد الإدارة أو التفاعل مع مقدمي الخدمة (NIST, 2011).

تعتبر المحاسبة السحابية أحد أهم الإنجازات التي توصلت إليها تكنولوجيا برامج الحوسبة السحابية وتهدف الى معالجة البيانات المحاسبية وتوصيل المعلومات الى المستخدمين في الوقت الملائم وبسرعة عالية وبأقل التكاليف. وعلى الرغم من المزايا التي تحققها المحاسبة السحابية، إلا أنها تواجه مخاطر عديدة نتيجة اعتمادها على الفضاء السيبراني كمخاطر فقدان المعلومات ومخاطر الاختراق والهجمات السيبرانية مما يشكل تحديا كبيرا للمنشآت التي تعتمد المحاسبية السحابية. ونتيجة لمخاطر المحاسبة السحابية، برزت اهمية وجود ضمانات امنية في هذه البيئة تمثلت بالأمن السيبراني، مما يحتم وجود حوكمة للأمن السيبراني من اجل الحد من المخاطر المترتبة على استخدام المحاسبة السحابية.
ويعد التدقيق الداخلي أحد الأدوات الرقابية الهامة التي تعلب دورا بارزا في تحقيق اهداف المنشأة من خلال اعتماد أسلوب منهجي ومنظم لتقييم وتعزيز الحوكمة وإدارة المخاطر والرقابة. ولكي يتم الوصول لذلك، يجب ان يتسم التدقيق الداخلي بالجودة ليكفل حسن سير العمل ويحد من المخاطر خاصة في ظل التطور التقني المتزايد واستخدام المحاسبة السحابية وما ترتب عليه من تأثيرات في بيئة العمل. ومن هنا جاءت هذه الدراسة للبحث في الدور الوسيط لجودة التدقيق الداخلي في العلاقة بين حوكمة الأمن السيبراني والحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

مشكلة الدراسة

نظرا لاستخدام المحاسبة السحابية من قبل العديد من الشركات واعتماد الفضاء السيبراني لهذا الغرض، أصبح الامن السيبراني يشكل جانبا أساسيا من امن وسلامة النظام المحاسبي في هذه الشركات، الامر الذي يحتم وجود حوكمة للأمن السيبراني للحد من المخاطر المصاحبة لاستخدام المحاسبة السحابية كمخاطر فقدان المعلومات ومخاطر الاختراق والهجمات السيبرانية مما يقلل من ثقة المستثمرين في القوائم المالية ويحد من قدرة الشركات على النمو والاستمرار. ويحتم استخدام المحاسبة السحابية وما يرافقها من مخاطر على النظام المحاسبي، وجود تدقيق داخلي يتسم بالجودة للتأكد من وجود حوكمة فعالة وتطبيق سليم لنظام الرقابة الداخلية طبقا لما هو محدد، وبما يمكن من تحقيق أمن وسلامة البيانات المالية وتلافي نقاط الضعف التي قد تكون لها آثار غير مرغوبة ومخاطر محتملة. ومن هنا يمكن صياغة المشكلة في التساؤل الآتي: ما أثر حوكمة الأمن السيبراني بأبعادها (إستراتيجية الأمن السيبراني، وصلاحيات ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والتدقيق الدوري للأمن السيبراني، والتوعية والتدريب للأمن السيبراني) في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية؟

أهمية الدراسة

تستمد الدراسة أهميتها من أهمية وحداثة موضوعها وشحة الدراسات التي تناولتها –حسب علم الباحث–، حيث تطرقت الدراسة الحالية لدراسة أثر حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية ومن هنا من المؤمل ان تقدم هذه الدراسة إضافة جديدة الى المعرفة في مجالها. وتنبثق الأهمية العلمية للدراسة أيضا من مساهمة نتائجها في فهم العلاقة بين متغيرات الدراسة مما يثري المكتبة العربية ويفتح الآفاق للمزيد من الدراسات حول موضوع هذه الدراسة في البيئة الأردنية. وتتمثل الأهمية العملية للدراسة في إبراز أثر حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية والتي تعتبر أحد أهم الركائز لاستقرار وازدهار الاقتصاد الأردني، فضلا عن لفت نظر الشركات الصناعية المستخدمة للمحاسبة السحابية الى أهمية حوكمة الامن السيبراني في تقليل المخاطر المصاحبة لاستخدام المحاسبة السحابية.

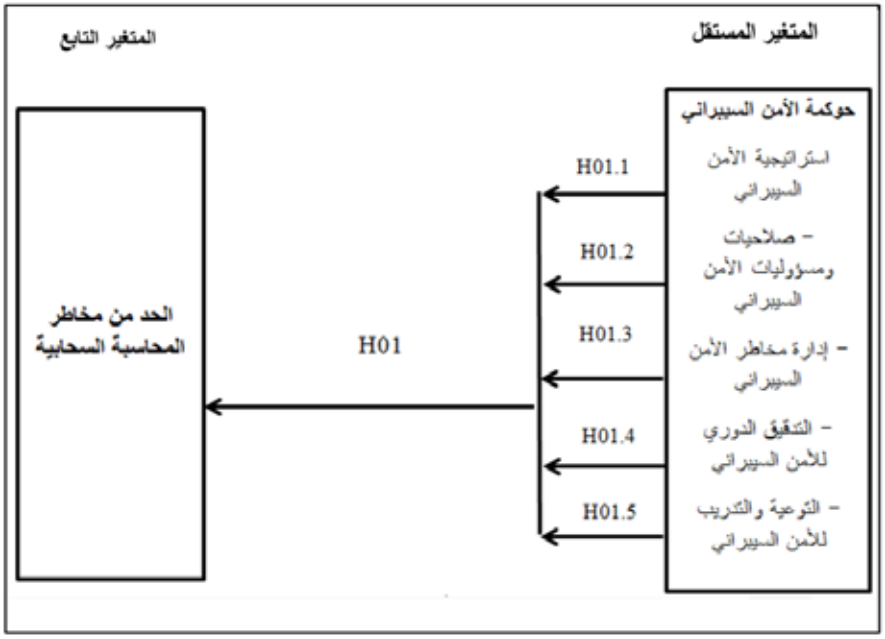
أهداف الدراسة

تسعى هذه الدراسة إلى للتعرف على بأثر حوكمة الأمن السيبراني بأبعادها (إستراتيجية الأمن السيبراني، وصلاحيات ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والتدقيق الدوري للأمن السيبراني، والتوعية والتدريب للأمن السيبراني) مجتمعة ومنفردة في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

أنموذج الدراسة

يظهر الشكل (1) أنموذج الدراسة والذي يبين وجود متغيرين، الأول هو المتغير المستقل والمتضمن حوكمة الأمن السيبراني، والثاني متغير المتغير التابع والمتمثل الحد من مخاطر المحاسبة السحابية ويتضمن تخيل للعلاقة بين تلك المتغيرات التي تناولتها الدارسة الحالية.

الشكل رقم (1) أنموذج الدراسة



المصدر من إعداد الباحث بالاعتماد على المراجع الآتية:

متغيرات الدراسة	المراجع
المتغير المستقل: حوكمة الأمن السيبراني	(البنك المركزي الأردني، 2018)، (المركز الوطني للأمن السيبراني، 2019)، (Ali et al., 2020)، (زمورة وبن عيسى، (2022)، (Tawfiq et al., 2021)،
المتغير التابع: الحد من مخاطر المحاسبة السحابية	(دمدوم وآخرون، 2020)، (Musyaffi & Arinal, 2021))

فرضيات الدراسة

الفرضية الرئيسية H01: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لحوكمة الأمن السيبراني بأبعادها (إستراتيجية الأمن السيبراني، وصلاحيات ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والتدقيق الدوري للأمن السيبراني، والتوعية والتدريب للأمن السيبراني) في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

وتتفرع من هذه الفرضية الفرضيات الفرعية الآتية:

الفرضية الفرعية الأولى H01.1: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لاستراتيجية الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الثانية H01.2: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لصلاحيات ومسؤوليات الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الثالثة H01.3: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لإدارة مخاطر الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الرابعة H01.5: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) للتدقيق الدوري للأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الخامسة H01.6: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) للتوعية والتدريب للأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

التعريفات المفاهيمية والإجرائية

حوكمة الأمن السيبراني: هي النظام المكون من الاستراتيجيات والعمليات والإجراءات والصلاحيات والمسؤوليات التي تساعد الشركات على اكتشاف الهجمات السيبرانية، وتحديد كيفية الاستجابة لها، ومنع حدوثها (البنك المركزي الاردني، 2018).

وتم قياس حوكمة الأمن السيبراني من خلال الأبعاد التالية (المركز الوطني للأمن السيبراني، 2019):
– إستراتيجية الأمن السيبراني: وتعني ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل الجهة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.
– صلاحيات ومسؤوليات الأمن السيبراني: وتتمثل بتحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الامن السيبراني في الجهة المعنية.
– إدارة مخاطر الأمن السيبراني: وبقصد بها حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
– التدقيق الدوري للأمن السيبراني: وهو ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على الجهة.
– التوعية والتدريب بالأمن السيبراني: ويعني توعية العاملين بالجهة وإلمامهم بمسؤولياتهم في الأمن السيبراني، وضمان تزويدهم بالمهارات والمؤهلات والتدريبات اللازمة في هذا المجال لحماية الأصول المعلوماتية والتقنية للجهة، وتأدية مسؤولياتهم في مجال الأمن السيبراني بكفاءة عالية.

الحوسبة السحابية: هي عبارة عن نموذج تقني لتمكين الوصول بشكل مناسب وعند الحاجة الى مجموعة مشتركة من موارد الحوسبة كالشبكات والخوادم والتطبيقات والخدمات والتخزين، والتي من الممكن توفيرها واصدارها بصورة سريعة مع وجود حد أدني من جهد الإدارة أو التفاعل مع مقدمي الخدمة (NIST,2011).
المحاسبة السحابية: هي استخدام برامج محاسبية مستضافة على سيرفرات لطرف ثالث على الانترنت مما يسهل على الشركات اعداد حساباتها من خلال شركات محاسبة متخصصة، مما أدى إلى تخفيض تكاليف إعداد القوائم المالية وامتثال أكثر للأنظمة والقوانين المعمول بها (Dimitriu and Matei 2014,).
مخاطر المحاسبة السحابية: هي التهديدات التي تواجه المؤسسة أثناء تنفيذ وتطبيق المحاسبة السحابية مثل انقطاع الاتصال بالإنترنت وعدم الموثوقية وضياع وتلف المعلومات والاختراق والهجمات السيبرانية (لغريبي وآخرون، 2020).

حدود الدراسة

الحدود المكانية: تم إجراء هذه الدراسة على الشركات الصناعية المساهمة العامة الأردنية.
الحدود الزمانية: تم إجراء هذه الدراسة على الشركات الصناعية المساهمة العامة الأردنية لعام 2023.
الحدود العلمية: اقتصرت الدراسة على قياس أثر حوكمة الأمن السيبراني بأبعادها (دون التطرق الى الجوانب الفنية أو التقنية ذات الصلة): إستراتيجية الأمن السيبراني، وصلاحيات ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والتدقيق الدوري للأمن السيبراني، والتوعية والتدريب للأمن السيبراني، في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.
الحدود البشرية: تم إجراء هذه الدراسة على عينة من مدراء الإدارات ونوابهم ورؤساء الأقسام والموظفين العاملين في الدائرة المالية وتكنولوجيا المعلومات في الشركات الصناعية المساهمة العامة الأردنية.

الإطار النظري والدراسات السابقة

الإطار النظري

حوكمة الأمن السيبراني

في عالم يعتمد بشكل كبير على التكنولوجيا والإنترنت، تزداد المخاوف تزداد بشأن الأعمال والمشاريع التي تعتمد عليها، فكل ما يمثل تهديدات للأنظمة والمعدات والأجهزة الإلكترونية عبر الإنترنت يمثل مخاطر سيبرانية وتهديدات حقيقية تؤثر في الأمن والخصوصيات (Qasaimeh & Jaradeh, 2022). ويمكن تعريف المخاطر السيبرانية على أنها التهديدات الناشئة من عمليات القرصنة الإلكترونية والاختراق والاستغلال غير المشروع للأنظمة والبيانات الإلكترونية التي تمتلكها الشركة، ويتعلق حجم المخاطر السيبرانية بتقدير احتمال حدوث حدث معين فيما يتعلق بأصول المعلومات للشركة، وتقييم الأثر المحتمل لذلك الحدث على عمليات الشركة بشكل عام (البنك المركزي الأردني، 2018).

ووصفت المخاطر السيبرانية أيضا بأنها كل ما يمثل تهديدا للأنظمة الإلكترونية أو البيانات المتداولة عبر الإنترنت وتشمل أنواعا متعددة كالإختراقات الإلكترونية والبرمجيات الخبيثة والفيروسات والإحتيالات الإلكترونية وبالتالي فإنها تؤثر على الأعمال التجارية والصناعات والمؤسسات الحكومية والخاصة (المنيع، 2022؛ Rehman, 2015).

ويرى الباحث أن مفهوم المخاطر السيبرانية يتجلى في إحتمالية وقوع الضرر أو الخسارة نتيجة الهجوم السيبراني والذي يؤثر على الأفراد والمنظمات بشكل عام سواء في القطاع العام أو الخاص، بالإضافة إلى أنها تمثل تحديا كبيرا للأمن السيبراني من خلال تقليل المخاطر وإتخاذ التدابير الأمنية المناسبة والمساهمة في تعزيز الثقة في البيئة الرقمية.

تتضمن المخاطر السيبرانية أنواعا متعددة، منها الاختراقات الإلكترونية كالهجمات على الشبكات، والبرمجيات الخبيثة كالفيروسات والديدان وأحصنة طروادة، البرمجيات الضارة، والاحتيال الإلكتروني عبر الإنترنت. ويمكن أن تؤثر المخاطر السيبرانية بشكل كبير على العديد من القطاعات، بما في ذلك الأعمال التجارية والصناعات والمؤسسات الحكومية وغيرها (Cebula & Young, 2010). وقد أشار عبد الحافظ (2023) إلى أن التكلفة العالمية للجرائم السيبرانية قد وصلت إلى ما يقرب من 8.4 تريليون دولار في عام 2022، ومن الواضح أن هذا الرقم يمثل تكلفة كبيرة تؤثر بشكل سلبي على إقتصاد الدول، ومن المتوقع أن تزداد هذه التكلفة خلال العام الحالي، حيث يتوقع أن تتجاوز (11) تريليون دولار.

وتشمل أنواع المخاطر السيبرانية التي تواجه المنظمات والأفراد على ما يلي:

أولا: مخاطر التهديدات الإلكترونية وتشكل التهديدات الإلكترونية مخاطر جدية على الأفراد والمنظمات التي تستخدم الإنترنت، ومن أهم هذه المخاطر ما يلي (المركز الوطني للأمن السيبراني، 2019؛ Kure et al., 2018): الفيروسات وهي برامج خبيثة تستهدف التكنولوجيا الحاسوبية وتعمل على تكاثرها وتلحق الضرر بالنظام والملفات. والبرمجيات الخبيثة وتشمل برامج التجسس والأدوار الخلفية، وهي تستخدم للتجسس على المستخدمين وسرقة معلوماتهم الحساسة. والقرصنة الإلكترونية وتهدف لاختراق الأنظمة والشبكات وسرقة البيانات أو تعطيل الخدمات. والتصيد الإلكتروني ويستخدم هذا النوع من الهجمات رسائل مزيفة أو مواقع وهمية لخداع الأفراد والحصول على معلومات شخصية حساسة. والتصيد الاجتماعي ويعتمد على التلاعب النفسي لإقناع الأفراد بالكشف عن معلومات سرية أو تنفيذ أفعال غير مرغوب فيها.

ثانيا: مخاطر إدارة الأمن السيبراني حيث هناك العديد من المخاطر والتحديات التي تحيط بإدارة الأمن السيبراني، ومن المخاطر الرئيسية (يعقوب وآخرون، 2022) كضعف التنظيم والسياسات وتعني عدم وجود إجراءات أمنية صارمة أو عدم تطبيقها بشكل صحيح مما يجعل المؤسسة عرضة للهجمات السيبرانية. كقلة التدريب والتوعية: وتعني نقص الوعي الأمني لدى الموظفين مما يؤدي إلى زيادة فرص الوقوع ضحية للهجمات الاجتماعية والتصيد الإلكتروني. وقلة الاستعداد للهجمات الإلكترونية وتعني عدم وجود خطط أمنية فعالة لمواجهة الهجمات السيبرانية مما يعرض المؤسسة للخطر.

ثالثا: مخاطر إدارة البيانات والمعلومات وتشمل مخاطر إدارة البيانات والمعلومات العديد من التحديات والمشاكل التي يمكن أن تؤثر في أمن وسلامة البيانات والمعلومات في المؤسسات، منها ما يلي (الحيدري، 2023) كعدم تأمين البيانات بشكل صحيح الأمر الذي يتسبب في تسرب أو سرقة البيانات الحساسة، ويمكن أن يتسبب أيضا في فقدان الثقة لدى العملاء والمستخدمين. والتسرب العرضي والأخطاء البشرية مما يسبب تسرب البيانات عن طريق الخطأ من قبل الموظفين الأمر الذي قد يكون له تأثيرا واضحا على الأمن السيبراني. وسوء الاستخدام وذلك من خلال إستخدام غير آمن للتطبيقات والتقنيات غير المعتمدة مما قد يؤدي إلى ضعف أمن النظام.

رابعا: مخاطر الأمن المادي وتتعلق مخاطر الأمن المادي بحماية المنظمات من التهديدات التي يمكن أن تواجهها في الواقع الفعلي، وتشمل ما يلي (المركز الوطني للأمن السيبراني، 2019) كسرقة الأجهزة الحاسوبية أو السرقة من المكاتب والمرافق. والحرائق والكوارث الطبيعية مثل الفيضانات والزلازل التي قد تؤدي إلى تعطيل الأنظمة وفقدان البيانات.

خامسا: مخاطر الأمن السيبراني العالمية وتشكل مخاطر الأمن السيبراني العالمية تحديا كبيرا للدول والمؤسسات على مستوى العالم، وتشمل هذه المخاطر بالآتي (غريب، 2018) كالهجمات السيبرانية المتطورة وتزداد تهديدات الهجمات السيبرانية في التطور والتعقيد، مما يصعب اكتشافها ومواجهتها. وتستهدف هذه الهجمات الأنظمة الحكومية والبنية التحتية الحيوية والشركات الكبيرة. والفدية الرقمية حيث يتم هنا تشفير البيانات ثم طلب فدية مالية مقابل فك تشفيرها مما يؤدي إلى خسائر مالية كبيرة للشركات والأفراد. ومن المتوقع إزدياد وإستمرار تهديدات الأمن السيبراني خلال العام 2024 من خلال إستخدامات وطرق جديدة كمنصات الألعاب الإلكترونية وعالم الواقع الإفتراضي، وإستخدام الذكاء الإصطناعي الذي سيسرع من هجمات التصيد الإحتيالي (الصليبي، 2024).

ويرى الباحث أن المخاطر المذكورة سابقا تمثل تحديات كبيرة تواجه الأفراد والمنظمات سواء في القطاع العام أو الخاص في عصرنا الرقمي المتسارع. ولذلك، يجب أن يكون الأمن السيبراني أحد الأولويات الرئيسة للحماية من هذه المخاطر والتهديدات وضمان سلامة وحماية الأنظمة والبيانات.

تعددت المفاهيم التي تناولت مصطلح الأمن السيبراني، حيث يفهمه وينظر إليه كل فرد من وجهة نظره الخاصة. ومع ذلك، فإن جميع المفاهيم تشترك في مضمون وقالب متقارب في المعنى، وهو حماية المواقع الإلكترونية من المخاطر والتهديدات الناجمة عن وسائل إلكترونية أخرى (يونس، 2018). ويمثل الأمن السيبراني مجموعة من الأنشطة والعمليات التي تؤدي إلى تأمين الحماية للموارد البشرية والمالية المتعلقة بتقنيات الإتصال وتضمن الحد من حدوث الأضرار والخسائر المترتبة في حال تحقق المخاطر والتهديدات، بالإضافة إلى إعادة الأوضاع إلى ما كانت عليه بوقت قياسي دون توقف العجلة الإنتاجية (الجبور، 2019).

ويرى الباحث من خلال ما تقدم من تعريفات أن الأمن السيبراني هو مجموعة القوانين والتعليمات والإجراءات والعمليات المستخدمة لحماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج في الفضاء السيبراني والأنظمة التي تدعم الفضاء السيبراني من التهديدات الرقمية والأحداث التي لا تتوافق مع أحكام القانون.

وتكمن أهمية حوكمة الأمن السيبراني فيما يلي (عبد الرضا والمعموري، 2020؛ Maleh et al., 2018):

– الحفاظ على البيانات والمعلومات الحساسة: تعد البيانات والمعلومات الحساسة أصولا حيوية للشركات والحكومات مما يتطلب تطبيق سياسات وإجراءات فعالة للحفاظ على هذه البيانات ومنع وصول الأفراد غير المصرح لهم.

– الحماية من التهديدات السيبرانية: تساهم حوكمة الأمن السيبراني في تقديم استراتيجيات وحلول للوقاية من هذه التهديدات ومكافحتها.

– الحفاظ على الاستقرار الاقتصادي والاجتماعي: تساعد حوكمة الأمن السيبراني العديد من القطاعات الحكومية والاقتصادية على إستمرار أعمالها بكفاءة من خلال منع والحد من وقوع الهجمات سيبرانية التي قد تتعرض لها هذه الإقتطاعات.

– الامتثال للتشريعات والقوانين: تفرض الحكومات والجهات التنظيمية متطلبات صارمة للأمن السيبراني من أجل حماية المستهلكين وضمان الامتثال للقوانين، وتلعب حوكمة الأمن السيبراني دورا مهما في ضمان التزام المؤسسات بالقوانين واللوائح السارية.

– الحفاظ على سمعة المنظمات: تؤثر الهجمات السيبرانية الناجحة على سمعة المنظمات وتؤدي إلى فقدان ثقة العملاء والشركاء، ومن خلال تطبيق إجراءات الأمن السيبراني، يمكن للمؤسسات الحفاظ على سمعتها وبناء علاقات قوية مع الأطراف المعنية.

– ضمان إستمرارية العمليات الإنتاجية: يمكن أن تساعد حوكمة الأمن السيبراني في ضمان استمرارية العمليات في حالة وقوع هجوم إلكتروني، وذلك من خلال وضع تدابير وقائية للحماية من الهجمات الإلكترونية، وتحديد الإجراءات التي يجب اتخاذها في حالة وقوع هجوم إلكتروني.

– حماية الأصول الرقمية للمنظمة: يمكن أن تساعد حوكمة الأمن السيبراني في حماية الأصول الرقمية للمنظمات، وذلك من خلال وضع سياسات وإجراءات لتنظيم الوصول إلى البيانات، وحماية البيانات من الوصول غير المصرح به.

– تعزيز الثقة والمصداقية بين المنظمة وعملائها وشركائها: يمكن أن تساعد حوكمة الأمن السيبراني في تعزيز الثقة والمصداقية بين المنظمة وعملائها وشركائها، وذلك من خلال إظهار أن الشركة تأخذ سلامة بياناتها على محمل الجد وتوليها الاهتمام الكافي.

– توفير بيئة عمل آمنة للعاملين: يمكن أن تساعد حوكمة الأمن السيبراني في توفير بيئة عمل آمنة للعاملين، وذلك من خلال وضع سياسات وإجراءات للحماية من التهديدات الإلكترونية، وتوفير التدريب للعاملين على كيفية حماية أنفسهم من الهجمات الإلكترونية.

– تلبية متطلبات ومعايير الأمن السيبراني: يمكن أن تساعد حوكمة الأمن السيبراني في تلبية متطلبات ومعايير الأمن السيبراني والقوانين واللوائح المحلية والدولية، وذلك من خلال وضع سياسات وإجراءات تتوافق مع هذه المتطلبات والمعايير، مما يمكن المنظمات من حماية أنظمتها وبياناتها من التهديدات الإلكترونية، وتحقيق العديد من الفوائد الأخرى.

ومن وجهة نظر الباحث تلعب حوكمة الأمن السيبراني دورا هاما في تحقيق الثقة والشفافية في البيئة الرقمية من خلال ضمان حماية بيانات الأفراد والمؤسسات من أي تهديدات أو مخاطر سيبرانية.

أبعاد حوكمة الأمن السيبراني

يتطلب تطبيق أبعاد حوكمة الأمن السيبراني رؤية استراتيجية دقيقة، حيث لا تقتصر هذه الأبعاد على مجرد مجموعة من الخطوات التقنية، بل هي منهجية شاملة تقوم على التخطيط الاستراتيجي وتنسيق وترتيب الجهود بشكل فعال، مع الشراكة والتعاون المستدام. ويمكن للمنظمات من خلال تطبيق هذه الأبعاد بشكل متكامل تحقيق مستويات عالية من الأمن السيبراني وضمان استمرارية العمليات في عالمنا المترابط والمتطور. وتتمثل أبعاد حوكمة الأمن السيبراني بالآتي (ISO, 2022؛ المركز الوطني للأمن السيبراني، 2019؛ تعليمات البنك المركزي، 2018):

أولا: إستراتيجية الأمن السيبراني

وهي الجهود المبنية والمنسقة لضمان تحقيق متطلبات الأمن السيبراني في داخل المنظمة وتتضمن هذه الاستراتيجية وضع خطط عمل وأهداف ومبادرات ومشاريع تعزز الامتثال للتشريعات والقوانين ذات الصلة في مجال الأمن السيبراني، حيث تسعى الاستراتيجية الأمنية السيبرانية لتوفير إطار شامل للحماية من التهديدات السيبرانية والاستجابة للحوادث والمخاطر الأمنية بطريقة فعالة وفي الوقت المناسب.

ثانيا: الصلاحيات والمسؤوليات

وتهدف صلاحيات ومسؤوليات الأمن السيبراني إلى توضيح وتحديد الأدوار والمسؤوليات الواضحة لجميع الأطراف المشاركة في تطبيق وتنفيذ ضوابط الأمن السيبراني داخل الجهة. ويتم ذلك من خلال تعيين مسؤوليات محددة لكل فرد أو فريق يشترك في جهود الأمن السيبراني وضمان توزيع الصلاحيات الملائمة لتنفيذ تلك المسؤوليات بشكل فعال ومنسق، وتحقق هذه الصلاحيات والمسؤوليات تنظيم وتنسيق الجهود الفردية وتحقيق أهداف الأمن السيبراني بشكل فعال.

ثالثا: إدارة مخاطر الأمن السيبراني

وتعنى إدارة مخاطر الأمن السيبراني بتنفيذ عملية ممنهجة لتقييم وتحليل وتخفيض المخاطر المتعلقة بالأمن السيبراني في الجهة، وتهدف هذه العملية إلى حماية الأصول المعلوماتية والتقنية وذلك من خلال اتباع السياسات والإجراءات التنظيمية المحددة للجهة ومتطلبات التشريعات واللوائح ذات الصلة وتشمل إدارة مخاطر الأمن السيبراني تحديد المخاطر المحتملة وتقييم تأثيرها واحتمالية حدوثها وتنفيذ التدابير الوقائية والتصحيحية للحد من هذه المخاطر والتعامل معها بفعالية.

رابعا: التدقيق الدوري

ويهدف التدقيق الدوري إلى ضمان تحقيق الامتثال والفعالية لضوابط الأمن السيبراني في الجهة، ويتم ذلك من خلال التأكد من تطبيق وفعالية ضوابط الأمن السيبراني وفقا للسياسات والإجراءات التنظيمية المحددة للجهة ومتطلبات التشريعات واللوائح المحلية ذات الصلة، بالإضافة إلى المتطلبات الدولية المعترف بها للجهة ويشمل التدقيق الدوري تقييم فعالية تنفيذ الضوابط وتحديد الثغرات أو الاختلالات المحتملة والتوصية بتحسين العمليات وتصحيح أي نقص أو خلل يتم اكتشافه لضمان استمرارية وتحسين أمن الأنظمة والمعلومات السيبرانية.

خامسا: التوعية والتدريب بالأمن السيبراني

ويهدف هذا البعد إلى ضمان توعية العاملين بالجهة وإلمامهم بمسؤولياتهم في الأمن السيبراني، وضمان تزويدهم بالمهارات والمؤهلات والتدريبات اللازمة في هذا المجال لحماية الأصول المعلوماتية والتقنية للجهة، وتأدية مسؤولياتهم في مجال الأمن السيبراني بكفاءة عالية.

ومن وجهة نظر الباحث تمثل هذه الأبعاد عمقا إستراتيجيا للمنشآت بشكل عام في حماية الممتلكات والأصول الرقمية والبيانات الحساسة وضمان إستدامة عملها، بالإضافة إلى أنها تمثل مجموعة من الأسس والقواعد الأساسية والتي يجب أن تكون متكاملة كإستراتيجية عامة لحوكمة الأمن السيبراني في المنشآت.

الحد من مخاطر المحاسبة السحابية

مع تقدم التكنولوجيا وشبكات الإتصال، إتجهت العديد من المنظمات نحو إستخدام التطبيقات ذات العلاقة بأعمالها عبر السحب. وتعد الحوسبة السحابية أنموذجا جديدا يقوم على أنموذج الدفع بقدر الإستخدام للوصول بمرونة إلى موارد الأجهزة والبرمجيات من خلال شبكة الإنترنت والسماح للشركات والمؤسسات بخفض التكاليف وزيادة الأداء (الحسين والصميدعي، 2012). وتمثل الحوسبة السحابية تكنولوجيا تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالحاسوب إلى ما يسمى السحابة وهي جهاز خادم يتم الوصول إليه عن طريق الأنترنت، وبهذا تتحول برامج تكنولوجيا المعلومات من منتجات إلى خدمات، وتعتمد البنية التحتية للحوسبة السحابية على مراكز البيانات المتطورة والتي تقدم مساحات تخزين كبيرة للمستخدمين، كما أنها توفر بعض البرامج كخدمات للمستخدمين وتستند في ذلك على الإمكانيات التي توفرها تقنيات الشبكة العنكبوتية العالمية – الويب – (رزق، 2013). وتعني الحوسبة السحابية التحول عند إستخدام التطبيقات والبرامج الإلكترونية عبر أجهزة الحواسيب وإتصالها بشبكات داخلية إلى المتصفح عبر الإنترنت من أي مكان في العالم (الغول، 2014).

ويرى الباحث أن الحوسبة السحابية نقلة نوعية في عالم تكنولوجيا المعلومات، حيث مكنت من الإنتقال من إستخدام البرامج والتطبيقات المثبتة على الأجهزة الحاسوبية الشخصية الثابتة إلى إستخدام البرامج والتطبيقات على السحابة، مما يقلل في التكاليف ويحسن الأداء.

الدراسات السابقة

هدفت دراسة دمدوم وآخرون (2020) هذه الدراسة إلى التعرف إلى الإطار المفاهيمي للمحاسبة السحابية والممارسات العملية ضمن البيئة الجزائرية. وتم استخدام التحليل المالي للوقوف على العقبات التي تواجه التحول نحو ممارسات المحاسبة السحابية. وتوصلت الدراسة إلى أن بيئة الأعمال الجزائرية على درجة متوسطة من الوعي بمفهوم المحاسبة السحابية وندرة الشركات المعتمدة على المحاسبة السحابية. وأوصت الدراسة بتوفير الوعي بأهمية تبني المحاسبة السحابية في بيئة الأعمال الجزائرية كافة لما لها من أهمية مستقبلية للمؤسسات الجزائرية.

هدفت دراسة (Ali et al.,2020) إلى تحديد أثر الحوكمة السيبرانية في تقليل مخاطر المحاسبة السحابية في البنوك التجارية الأردنية. ولتحقيق هدف الدراسة تم تصميم استبانة وتوزيعها على عينة عشوائية ضمت (213) مدقق حسابات من المحاسبين القانونيين الذين يمارسون مهنة التدقيق في الأردن. واستخدمت الدراسة الانحدار الخطي المتعدد والانحدار التدريجي لاختبار الفرضيات. وتوصلت الدراسة إلى وجود تأثير ذي دلالة إحصائية لحوكمة الأمن السيبراني (متطلبات حوكمة الأمن السيبراني، وبرنامج

الأمن السيبراني، وسياسة الأمن السيبراني، وإدارة المعلومات السيبرانية، وتقييم وإدارة المخاطر السيبرانية) في الحد من مخاطر المحاسبة السحابية.

هدفت دراسة (Musyaffi & Arinal 2021) إلى التعرف إلى عوامل قبول المحاسبة السحابية والتركيز على مستخدمي المحاسبة السحابية من المحاسبين. ولتحقيق أهداف الدارسة تم توزيع إستبيان على الطلاب الذين لا يزالون في مرحلة البكالوريوس بإجمالي (123) مشاركا عبر نموذج (Google) ثم تحليله بإستخدام اسلوب معالجة البيانات من خلال (SmartPLS). وتوصلت الدراسة إلى أن سهولة الاستخدام والأمان الملحوظة يمكن أن تؤثر في نية استخدام المحاسبة السحابية. وإن الفائدة المتصورة غير قادرة على التحكم في اختيار استخدام المحاسبة السحابية، وذلك لأن المحاسبين المحتملين لا يزالون يعتبرون المحاسبة السحابية كوسيلة تعليمية فقط.

هدفت دراسة (Tawfiq et al.2021) إلى معرفة التأثير الفكري لحوكمة الأمن السيبراني في التطبيق الصحيح للمحاسبة السحابية في البنوك التجارية الأردنية. ولجمع البيانات اللازمة للدراسة تم تصميم استبانة وتوزيعها على عينة من المدققين الخارجيين العاملين في مهنة المراجعة في الأردن بلغ عددهم (213) مدقق. وتم استخدام تحليل الانحدار الخطي المتعدد المتدرج لإختبار الفرضيات الدراسية. توصلت الدراسة إلى وجود تأثير فكري لحوكمة الأمن السيبراني في التطبيق الصحيح للمحاسبة السحابية.

هدفت دراسة زمورة وبن عيسى (2022) إلى التعرف إلى أهمية حوكمة الأمن السيبراني من خلال سياسة وطنية لإدارة مخاطر الأمن السيبراني وأمن المعلومات مع ضمان دعمها من خلال توفير الوسائل التقنية والبشرية والقانونية والتشريعية، بالإضافة الى مواجهة التهديدات والمخاطر الأكثر فعالية والتي تمس مختلف القطاعات الحكومية والصناعية والتجارية. وتوصلت الدراسة إلى أن الإحصائيات والمعلومات للهيئات والمنظمات الدولية تشير إلى هشاشة الأمن السيبراني في الجزائر وإختلالات ملحوظة في مجال الإجراءات التنظيمية والتقنية مقارنة مع المعايير الدولية.

ما يميز هذه الدراسة عن الدراسات السابقة

تسعى هذه الدراسة إلى اختبار أثر حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية. وبالنظر إلى الدراسات السابقة سواء العربية منها أو الاجنبية التي تمكن الباحث من الاطلاع عليها، نجد أن الدراسة الحالية قد تميزت بكونها تناولت متغيرات وأبعاد لم تتناولها الدراسات السابقة بصورة مجتمعة –بحسب علم الباحث–، مما يساهم في تقديم إضافة علمية جديدة للأدبيات ذات العلاقة بموضوع الدراسة خاصة في ظل شح الدراسات في البيئة الأردنية والعربية في هذا السياق.

وتميزت الدراسة الحالية كذلك بتطبيقها على القطاع الصناعي والذي يمثل أحد القطاعات الاقتصادية الحيوية المكونة للاقتصاد الأردني وركيزة لتحقيق الاهداف التنموية والاقتصادية.

منهجية الدراسة

اعتمدت الدراسة في إجرائها على المنهج الوصفي والذي يهتم بمجموعة من الأساليب المعنية بجمع البيانات وتلخيصها وتنظيميها وعرضها بطريقة واضحة على صورة جداول وأشكال بيانية، وحساب المقاييس الإحصائية المختلفة لها مثل مقاييس النزعة المركزية، وقياس قوة الارتباط واعتمدت الدراسة أيضاً في إجراءاتها على المنهج الاستدلالي (التحليلي) ويعتمد هذا المنهج على استقراء ما تعنيه الأرقام ومعرفة دالتها الإحصائية وتفسيرها ووصفها بشكل أوسع من المنهج الوصفي وتأتي هذه الخطوة بعد

تبويب واختبار آراء العينة للوصول إلى نتائج أكبر وأوسع بشكل عامّ من المجتمع (قنديلجي، 2013).
مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من جميع الشركات الصناعية المساهمة العامة وعددها (53) شركة (مركز إيداع الأوراق المالية، 2023). وجاء إختيار الشركات الصناعية كمجتمع دراسة نظرا لأهمية دور القطاع الصناعي في المملكة الأردنية الهاشمية في تحقيق التنمية الإقتصادية. حيث تم تطبيق هذه الدراسة على الشركات الصناعية التي تعمل على نظام المحاسبة السحابية والتي. وقد تكونت عينة الدراسة على العاملين في الأقسام المالية والأقسام المحاسبية والأقسام الرقابية والأقسام البرمجية.

قام الباحث بتحديد عينة الدراسة بطريقة عشوائية؛ إذ قام الباحث بتوزيع (250) استبانة على الموظفين المستهدفين استرجعت منها (242) استبانة وبعد مراجعة الاستبانات تبين أن هناك (3) استبانات غير صالحة للتحليل الإحصائي؛ بناء على ما سبق فأن عينة الدراسة تكونت من (239) موظف وموظفة، ويوضح الجدول رقم (1) توزيع أفراد عينة الدراسة تبعاً لمتغيرات الشخصية.

الجدول رقم (1)

توزيع أفراد عينة الدراسة تبعاً للمتغيرات الشخصية

المتغير	المستوى	العدد	النسبة المئوية(%)
المؤهل العلمي	بكالوريوس	186	77.8
	ماجستير	31	13.0
	دكتوراه	7	2.9
	أخرى	15	6.3
	المجموع	239	100.0
عدد سنوات الخبرة في العمل	أقل من 5 سنوات	14	5.9
	5- أقل من10 سنوات	94	39.3
	10- أقل من15 سنة	70	29.3
	15 سنة فأكثر	61	25.5
	المجموع	239	100.0
المسمى الوظيفي	مدير	20	8.4
	نائب مدير	21	8.8
	رئيس قسم	38	15.9
	موظف	160	66.9
	المجموع	339	100.0
التخصص	محاسبة	30	12.6
	إدارة أعمال	53	22.2
	علوم مالية ومصرفية	81	33.9
	أخرى	75	31.4
	المجموع	239	100.0

مصادر جمع البيانات

إعتمدت الدراسة على:

– المصادر الثانوية: تمثلت المصادر الثانوية بمطالعة كتب ودراسات حول موضوع الدراسة، وتم الا– ستعانة ببعض المواقع الالكترونية التي خدمت موضوع الدراسة.

– المصادر الأولية: تمثلت المصادر الأولية في استبانة تم بناؤها وتطويرها لكي تتناسب مع طبيعة الدراسة وتم صياغة أسئلتها للتعبير عن كل بعد من أبعاد الدراسة للتمكن من قياسها معتمدة على ما تم طرحه في الدراسات السابقة.

أداة الدراسة:

قام الباحث بتطوير وبناء أداة الدراسة (الإستبانة)، بعد الاطلاع على الأدب النظري والدراسات السابقة، وتمت الاستعانة في تطوير فقرات الاستبانة على الاستبانات في دراسات سابقة تناولت موضوعات قريبة من موضوع الدراسة التي صممت الإستبانة لمعرفة أثر حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، حيث تم تطوير الاستبانة لتتناسب مع أهداف الدراسة الحالية. تكونت أداة الدراسة (الإستبانة) في صورتها من الأقسام الآتية:

– القسم الأول: الخصائص الديمغرافية يهدف للتعرف على الخصائص الديمغرافية لأفراد عينة لدراسة، وتتضمن (المؤهل العلمي، عدد سنوات الخبرة في العمل، المسمى الوظيفي، التخصص).

– القسم الثاني: المتغير المستقل (حوكمة الأمن السيبراني) يتكون من (30) فقرة موزعة على خمس مجالات على النحو الآتي:(استراتيجية الأمن السيبراني، صلاحيات ومسؤوليات الأمن السيبراني، إدارة مخاطر الأمن السيبراني، التدقيق الدوري للأمن السيبراني، التوعية والتدريب للأمن السيبراني).

– القسم الثالث: المتغير التابع (مخاطر المحاسبة السحابية) يتكون من (20) فقرة.

ولتحليل البيانات تم الاعتماد على مقياس ليكرت الخماسي (بدرجة كبيرة جداً، بدرجة كبيرة، بدرجة متوسطة، بدرجة قليلة، بدرجة قليلة جداً)، أما فيما يتعلق بالحدود التي اعتمدتها هذه الدراسة عند التعليق على المتوسط الحسابي للمتغيرات الواردة في نموذج الدراسة فهي ولتحديد درجة الموافقة فقد حددت الباحثة ثلاثة مستويات هي (مرتفع، متوسط، منخفض) بناءًا على المعادلة الآتية (الشريفين والكيلاني، 2007):

طول الفترة= (الحد الأعلى للبديل– الحد الأدني للبديل) / عدد المستويات

(5–1) /3 = 4/3 =1.33

– تدل المتوسطات الحسابية المتراوحة ما بين (–1.00 أقل من 2.33) على مستوى منخفض.

– تدل المتوسطات الحسابية المتراوحة ما بين (–2.33 أقل من 3.66) على مستوى متوسط.

– تدل المتوسطات الحسابية المتراوحة ما بين (–3.66 5.00) على مستوى مرتفع.

ثبات أداة الدّراسة

تم التحقق من ثبات أداة الدراسة تم استخراج معامل كرونباخ ألفا (Cronbac Alpha Coefficient) حيث تكون النّتيجة مقبولة إحصائيًّا إذ كانت قيمته أكبر من (0.70) (Sekaran & Bougie,2020)، ويوضح الجدول رقم (2) ذلك.

الجدول رقم (2)
معامل الثبات بطريقة كرونباخ ألفا لمجالات الدراسة وأبعادها

المجال	البُعد	معدل الثبات بطريقة كرونباخ ألفا
حوكمة الأمن السيبراني	استراتيجية الأمن السيبراني	0.845
	صلاحيات ومسؤوليات الأمن السيبراني	0.866
	إدارة مخاطر الأمن السيبراني	0.863
	التدقيق الدوري للأمن السيبراني	0.846
	التوعية والتدريب للأمن السيبراني	0.867
	حوكمة الأمن السيبراني ككل	0.849
مخاطر المحاسبة السحابية ككل		0.860

يظهر من جدول رقم (2) أن معاملات الثبات بطريقة كرونباخ ألفا لمجالات الدراسة وأبعادها تراوحت ما بين (0.846–0.949) وجميعها أكبر من (0.70) مما يدل على أن أداة الدراسة تتمتع بثبات مقبول إحصائياً.

اختبار التوزيع الطبيعي

يظهر الجدول رقم (3) نتائج اختبار التّوزيع الطّبيعيّ لإجابات المشاركين للتّأكّد إذا ما كانت البيانات موزعة طبيعيًّا أم لا، إذ تمّ احتساب قيمة اختبار الإلتواء (Skewness) وتشير القيمة الّتي تقع خارج نطاق (±1) إلى أنّ التّوزيع منحرف إلى حدّ كبير، وتمّ استخراج قيمة اختبار التّفرطح (Kurtosis) ويكون التّوزيع طبيعيًّا إذا لم تتجاوز قيمته (±1.96).

الجدول رقم (3)
نتائج اختبار (Skewness & Kurtosis)

المجال	البُعد	Kurtosis	Skewness
حوكمة الأمن السيبراني	استراتيجية الأمن السيبراني	−0.486	0.257
	صلاحيات ومسؤوليات الأمن السيبراني	−0.644	0.544
	إدارة مخاطر الأمن السيبراني	−0.203	0.209
	التدقيق الدوري للأمن السيبراني	−0.205	−0.608
	التوعية والتدريب للأمن السيبراني	−0.427	0.069
مخاطر المحاسبة السحابية ككل		−0.333	0.020

بناءَ على بيانات الاختبار والمشار إليها في الجدول رقم (3) يتّضح أنّ توزيع البيانات كان طبيعيًّا إذ لم تقع قيم (Skewness) خارج نطاق (±1) ولم تتجاوز قيمة (±1.96) (Kurtosis) عند مستوى (0.05).

اختبار الازدواج الخطي

تم استخدام معامل تضخم التباين (Variance Inflation Factor (VIF وقيم التباين المسموح به (Tolerance) بهدف التأكد من خلو البيانات من مشكلة الازدواج الخطي بين المتغيرات الدراسة، وهي المشكلة التي يعني وجودها أن يكون متغيراً مستقلاً دالاً لمتغير مستقل آخر، أي يرتفع بارتفاعه وينخفض بانخفاضه. وتظهر النتائج في الجدول (4).

الجدول (4)
نتائج اختبار الازدواج الخطي بين متغيرات الدراسة

البُعد	التباين المسموح به	معامل تضخم التباين
استراتيجية الأمن السيبراني	0.305	3.283
صلاحيات ومسؤوليات الأمن السيبراني	0.498	2.009
إدارة مخاطر الأمن السيبراني	0.361	2.773
التدقيق الدوري للأمن السيبراني	0.419	2.385
التوعية والتدريب للأمن السيبراني	0.396	2.528

يتضح من النتائج في الجدول (4) أن نموذج الدراسة يخلو من مشكلة الازدواج الخطي بين المتغيرات إذ جاءت قيم معامل تضخم التباين بشكل ملائم من حيث أنها أقل من (10) وكذلك قيم التباين المسموح به التي حققت معيار القبول وهو أن تكون قيمتها أكبر من (0.1).

أساليب المعالجة الإحصائية

لتحقيق أهداف الدراسة وتحليل البيانات التي تم تجميعها، قام الباحث بترميز البيانات وإدخالها إلى الحاسب الآلي باستخدام الحزم الإحصائية للعلوم الاجتماعية (SPSS)، وتم باستخدام العديد من الأساليب الإحصائية المناسبة والموجودة في هذا البرنامج.

عرض نتائج التحليل الإحصائي

يشتمل هذا الجزء على عرض وتحليل للبيانات التي تجمعت لدى الباحث من خلال الاستبانة التي تم توزيعها على الأفراد المبحوثين، حيث تم تحليل إجابات هؤلاء الأفراد على فقرات الاستبانة المتعلقة بكل مجال من مجالات الدراسة في محاولة للتعرف على أثر حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، بالإضافة إلى اختبار مدى صحة الفرضيات التي ورت في هذه الدراسة، **وفيما يلي عرض النتائج:**

أولاً: النتائج الوصفية الخاصة بحوكمة الأمن السيبراني في الشركات الصناعية.

تم استخراج المتوسطات الحسابية لإجابات أفراد عينة الدراسة عن أبعاد مجال حوكمة الأمن السيبراني بأبعاده (استراتيجية الأمن السيبراني، صلاحيات ومسؤوليات الأمن السيبراني، إدارة مخاطر الأمن السيبراني، التدقيق الدوري للأمن السيبراني، التوعية والتدريب للأمن السيبراني)، كما هو مُبين بالجدول رقم (5).

جدول (5)
المتوسطات الحسابية لإجابات أفراد عينة الدراسة عن أبعاد مجال حوكمة الأمن السيبراني مرتبة تنازليا وفقاً للمتوسط الحسابي

الرتبة	الرقم	البُعد	المتوسط الحسابي	الانحراف المعياري	مستوى التقييم
1	2	استراتيجية الأمن السيبراني	3.76	0.81	مرتفع
2	1	صلاحيات ومسؤوليات الأمن السيبراني	3.59	0.72	متوسط
3	3	إدارة مخاطر الأمن السيبراني	3.52	0.69	متوسط
4	4	التدقيق الدوري للأمن السيبراني	3.51	0.85	متوسط
5	5	التوعية والتدريب للأمن السيبراني	3.49	0.85	متوسط
		مخاطر المحاسبة السحابية ككل	3.57	0.65	متوسط

يتضح من الجدول رقم (5) أن المتوسط الحسابي العام لمجال حوكمة الأمن السيبراني ككل بلغ (3.57) بمستوى تقييم متوسط، وأن المتوسطات الحسابية لإجابات أفراد العينة عن أبعاد مجال حوكمة الأمن السيبراني تراوحت بين (3.76–3.49)، حيث جاء في المرتبة الأولى بُعد " صلاحيات ومسؤوليات الأمن السيبراني " بمتوسط حسابي (3.76) ومستوى تقييم مرتفع، وفي المرتبة الثانية جاء بُعد " استراتيجية الأمن السيبراني " بمتوسط حسابي (3.59) ومستوى تقييم متوسطة، واحتل المرتبة الثالثة بُعد " إدارة مخاطر الأمن السيبراني " بمتوسط حسابي (3.52) ومستوى تقييم متوسط، وجاء بالمرتبة الرابعة بُعد" التدقيق الدوري للأمن السيبراني" بمتوسط حسابي (3.51) ومستوى تقييم متوسط، وأخيراً جاء بالمرتبة الخامسة بُعد" التوعية والتدريب للأمن السيبراني" بمتوسط حسابي (3.49) ومستوى تقييم متوسط، ويمكن تفسير هذه النتيجة بأن حوكمة الأمن السيبراني تمنح الشركة القدرة على استثمار الأعمال بفعالية في حالة الإدارة الجيدة وإطار حوكمة الأمن السيبراني لتزويد الشركات بفرص مهمة من أجل خلق قيمة جديدة لها؛ إذ تواجه الشركات مجموعة متنوعة من التحديات والمخاطر من أهمها المخاطر السيبرانية؛ إذ أن الشركات تعتبر بيئة خصبة وجذابة للتعرض للمشاكل السيبرانية والتهديدات والمخاطر الموجهة إليها، وتعاني من هذه المخاطر وتبعياتها، وتهتم الشركات الصناعية بالإفصاح عن المخاطر السيبرانية في تقاريرهم السنوية مما يدل على تعرضهم لهذه المخاطر الأمر الذي يحتم على هذه الشركات الاستثمار في الأمن السيبراني وآلياته.

ثانياَ: النتائج الوصفية الخاصة بمخاطر المحاسبة السحابية في الشركات الصناعية

تم استخراج المتوسطات الحسابية لإجابات أفراد عينة الدراسة عن فقرات مجال الحد من مخاطر المحاسبة السحابية، كما هو مُبين بالجدول رقم (6).

جدول (6)
المتوسطات الحسابية والانحرافات المعياري لإجابات أفراد عينة الدراسة عن فقرات مجال الحد من مخاطر المحاسبة السحابية مرتبة تنازليا وفقاً للمتوسط الحسابي

الرتبة	الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	مستوى التقييم
1	8	تتسم مرحلة التحليل بفهم واضح لطبيعة المخاطر المتوقعة.	4.05	0.96	مرتفع
2	2	توفر خطة تضمن استمرارية العمل وتشتمل على إجراءات إعادة تشغيل عمليات الشركة بعد توقفها خلال فترة زمنية محددة.	3.88	0.86	مرتفع
3	6	يتم فهم الأسباب التي أدت إلى المشكلة أو المخاطر بشكل أفضل.	3.87	0.87	مرتفع
4	5	يتم استخدام الأساليب الإحصائية لتحليل بيانات المخاطر.	3.80	0.94	مرتفع
5	1	هنالك تحديد واضح لجهات ذات القدرة على النفاذ إلى المعلومات واستخدام تكنولوجيا المعلومات بشكل دقيق.	3.78	0.91	مرتفع
6	10	يتم التخلص من الأنشطة غير المهمة والتي تؤدي إلى حدوث المخاطر.	3.77	1.16	مرتفع
7	3	يتم بناء الإجراءات الاحترازية الهادفة للحد من الاختراق غير المشروع للمعلومات وقت حدوثها,	3.75	0.82	مرتفع
8	16	يتم تعديل وتطوير وتنفيذ عملية التقييم بشكل متوافق مع مستوى الخطر.	3.72	0.96	مرتفع
9	18	تقوم إدارة الشركة بمراقبة المعاملات والأنشطة والفعاليات المرتبطة بالأحداث ومقارنتها بمعايير محددة مسبقاً.	3.69	0.98	مرتفع
10	4	يتم اتخاذ الاجراءات التصحيحية اللازمة لضبط المخاطر السيبرانية والتقليل من أثارها.	3.68	0.89	مرتفع
11	9	يتم صياغة الإجراءات ووضع القواعد من أجل عملية التحسين.	3.67	1.17	مرتفع
12	7	يتم توضيح العلاقات السببية بين متغيرات المخاطر.	3.65	0.94	متوسط
13	17	تقوم إدارة الشركة بالتأكد من واقعية أهداف الأداء وقابليتها للتحقق.	3.64	0.97	متوسط
14	14	يتم التعامل مع أنشطة الرقابة الداخلية في الشركة كجزء من الواجبات اليومية.	3.63	1.04	متوسط
15	13	تساهم تقارير الأداء المقدمة لإدارة الشركة بمعالجة جوانب القصور وتطوير العمل فيما يتعلق بالمخاطر السيبرانية.	3.62	1.04	متوسط
16	11	يتم الاستجابة للتغيرات والتحسينات لفائدتها المرجوة.	3.61	1.02	متوسط
17	20	تقوم إدارة الشركة بتحديد أهداف كل مستوى إداري والمخاطر المرتبطة به.	3.58	0.98	متوسط
18	15	يتم اختبار وتطوير وتنفيذ عملية التقييم المستمرة لمكونات الرقابة الداخلية في الشركة.	3.56	1.06	متوسط
19	19	يتم تحديد المخاطر والفرص بعد إجراء دراسات ميدانية باستخدام تقنيات حديثة.	3.52	0.95	متوسط
20	12	يتم التحقق من أن السبب الرئيسي للمخاطر تم السيطرة عليه.	3.36	1.13	متوسط
مجال الحد من مخاطر المحاسبة السحابية ككل			3.69	0.52	مرتفع

يتضح من الجدول رقم (6) أن المتوسط الحسابي العام لمجال الحد من مخاطر المحاسبة السحابية ككل بلغ (3.69) بمستوى تقييم مرتفع، وأن المتوسطات الحسابية لإجابات أفراد العينة عن فقرات مجال الحد من مخاطر المحاسبة السحابية تراوحت بين (3.36–4.05)، حيث جاء في المرتبة الأولى الفقرة رقم (8) ونصها: تتسم مرحلة التحليل بفهم واضح لطبيعة المخاطر المتوقعة، بمتوسط حسابي (4.05) ومستوى تقييم مرتفع، وجاء بالمرتبة الأخيرة الفقرة رقم (12) ونصها: يتم التحقق من أن السبب الرئيسي للمخاطر تم السيطرة عليه، بمتوسط حسابي (3.36) ومستوى تقييم متوسط، ويمكن تفسير هذه النتيجة بأن استخدام المحاسبية السحابية يساهم في تحسين قدرة الشركة على مواكبة التطورات في بيئة تقنيات المعلومات، ومحاولة الاستفادة منها، بما يساهم في تحقيق كفاءة وفاعلية نظم المعلومات المحاسبية.

ويمكن تفسير هذه النتيجة بأن الشركات الصناعية تحاول توفير خطط لضمان التعامل مع المخاطر السيبرانية بالشكل السليم وذلك نظرا لتزايد الاهتمام بالتطبيقات الالكترونية والتعاملات الرقمية التي ساهمت في زيادة احتمالية حدوث المخاطر السيبرانية؛ إذ تضمن هذه الخطط للشركات الصناعية استمرارية العمل في ظل كثرة التحديات السيبرانية التي قد تواجه الشركات الصناعية في العصر الحالي، كما أن الشركات الصناعية تهتم ببناء الإجراءات الاحترازية الهادفة للحد من الاختراق غير المشروع للمعلومات وقت حدوثه.

ويمكن تفسير هذه النتيجة أيضاً بأن إدارة الشركات الصناعية تهتم بالتأكد من وجود خطة طوارئ لضمان سير العمل وتقليل احتمالات تعطل الأنظمة الالكترونية، كما أنها تهتم بالتأكد من توافر وعي كاف لدى مستخدمي أنظمة المعلومات الالكترونية، وذلك لضمان فهم الأسباب التي أدت إلى المشاكل أو المخاطر بشكل أفضل، فضلاً عن الاهتمام بالتخلص من الأنشطة غير المهمة والتي تؤدي إلى حدوث المخاطر.

ثالثاً: النتائج المتعلقة باختبار الفرضيات

الفرضية الرئيسية الأولى H01: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لحوكمة الأمن السيبراني بأبعادها (إستراتيجية الأمن السيبراني، وصلاحيات ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والتدقيق الدوري للأمن السيبراني، والتوعية والتدريب للأمن السيبراني) في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية. وتتفرع من هذه الفرضية الفرضيات الفرعية الآتية:

الفرضية الفرعية الأولى H01.1: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لاستراتيجية الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الثانية H01.2: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لصلاحيات ومسؤوليات الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الثالثة H01.3: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لإدارة مخاطر الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الرابعة H01.4: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) للتدقيق الدوري للأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

الفرضية الفرعية الخامسة H01.5: لا يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) للتوعية والتدريب للأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

للتحقق من صحة الفرضية الرئيسية والفرضيات الفرعية المنبثقة عنها تم تطبيق معادلة الانحدار المتعدد (Multiple Regression) لدراسة أثر أبعاد حوكمة الأمن السيبراني (إستراتيجية الأمن السيبراني، وصلاحيات ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والتدقيق الدوري للأمن السيبراني، والتوعية والتدريب للأمن السيبراني) في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، الجدول رقم (7) يوضح ذلك.

جدول (7)

معادلة الانحدار المتعدد (Multiple Regression) لدراسة أثر أبعاد حوكمة الأمن السيبراني في الحد من مخاطر المحاسبة السحابية

المتغير	معاملات غير قياسية		معاملات موحدة			R	R^2	المعدل R^2	F	الدلالة الإحصائية
	B	الخطأ المعياري	ß	T	الدلالة الإحصائية					
ثابت الانحدار	1.208	0.095		12.776	0.000	0.871	0.759	0.753	146.454	0.000
استراتيجية الأمن السيبراني	0.148	0.042	0.205	3.517	0.001					
صلاحيات ومسؤوليات الأمن السيبراني	0.113	0.029	0.177	3.870	0.000					
إدارة مخاطر الأمن السيبراني	0.207	0.040	0.274	5.121	0.000					
التدقيق الدوري للأمن السيبراني	0.110	0.030	0.182	3.656	0.000					
التوعية والتدريب للأمن السيبراني	0.119	0.031	0.196	3.832	0.000					

بالتالي ترفض الفرضية الرئيسية بالصيغة الصفرية لتصبح: يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لحوكمة الأمن السيبراني بأبعادها (إستراتيجية الأمن السيبراني، وصلاحيات ومسؤوليات الأمن السيبراني، وإدارة مخاطر الأمن السيبراني، والتدقيق الدوري للأمن السيبراني، والتوعية والتدريب للأمن السيبراني) في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

وفيما إختبار الفرضيات الفرعية فقد أظهرت النتائج ما يلي:

يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لاستراتيجية الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، حيث بلغت قيم (ß، 0.205، 3.517) (T) على التوالي وهي قيم دالة إحصائياً عند مستوى الدلالة ($\alpha \leq 0.05$)، وبالتالي تقبل الفرضية الفرعية الأولى بالصيغة البديلة.

- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لصلاحيات ومسؤوليات الأمن السيبراني

في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، حيث بلغت قيم (3.870، 0.177) (T، ß) على التوالي وهي قيم دالة إحصائياً عند مستوى الدلالة (α≤0.05)، وبالتالي تقبل الفرضية الفرعية الثانية بالصيغة البديلة.

– يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة (α≤0.05) لإدارة مخاطر الأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، حيث بلغت قيم (ß، 5.121، 0.274) (T) على التوالي وهي قيم دالة إحصائياً عند مستوى الدلالة (α≤0.05)، وبالتالي تقبل الفرضية الفرعية الثالثة بالصيغة البديلة.

– يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة (α≤0.05) للتدقيق الدوري للأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، حيث بلغت قيم (ß، 3.656، 0.182) (T) على التوالي وهي قيم دالة إحصائياً عند مستوى الدلالة (α≤0.05)، وبالتالي تقبل الفرضية الفرعية الرابعة بالصيغة البديلة.

– يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة (α≤0.05) للتوعية والتدريب للأمن السيبراني في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية، حيث بلغت قيم (ß، 3.832، 0.196) (T) على التوالي وهي قيم دالة إحصائياً عند مستوى الدلالة (α≤0.05)، وبالتالي تقبل الفرضية الفرعية الخامسة بالصيغة البديلة.

ويمكن تفسير هذه النتيجة بأن حوكمة الأمن السيبراني تساعد على فحص المعلومات المالية والادارية والتشغيلية، ومراجعة اعتماديتها وموثوقيتها والوسائل المستخدمة لتحديد وقياس وتصنيف وكتابة التقرير بمثل هذه المعلومات، كما يمكن تفسير هذه النتيجة إلى أن لحوكمة الأمن السيبراني تساهم في تحسين أساليب مواجهة مخاطر المحاسبة السحابية من خلال التطبيقات الخاصة بالوظائف التي يقوم بأدائها قسم معالجة البيانات إلكترونياً مما يساهم في توفير درجة معقولة من التأكد من سلامة عمليات تسجيل ومعالجة البيانات وإعداد التقارير، واتفقت هذه النتيجة مع دراسة (Ali et al., 2020) ودراسة Tawfiq et al. 2021)) ودراسة (زمورة وبن عيسى، 2022).

النتائج

– مستوى حوكمة الامن السيبراني في الشركات الصناعية المساهمة العامة الأردنية جاء متوسطا.

– مستوى مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية جاء متوسطا.

– يوجد أثر لحوكمة الامن السيبراني بأبعادها (إستراتيجية الأمن السيبراني، صلاحيات ومسؤوليات الأمن السيبراني، إدارة المخاطر، التدقيق الدوري للأمن السيبراني، التوعية والتدريب) في الحد من مخاطر المحاسبة السحابية في الشركات الصناعية المساهمة العامة الأردنية.

التوصيات

في ضوء ما سبق من نتائج فإن الدراسة توصي بما يلي:

– الاهتمام بدعم المحاسبة السحابية من خلال وضع ميثاق يعمل بموجبه ويحدد نطاق عملها وواجباتها.

– تعزيز دراية المحاسبة السحابية بطبيعة النظام المحاسبي المطبق من حيث تكامله وفاعليته وكفاءته والتزامه بالقيم المعيارية.

– زيادة الاهتمام من قبل إدارات الشركات الصناعية بتعزيز خطة المحاسبة السحابية، فيما يتعلق بتغطية جميع جوانب المخاطر المحتملة والمتعلقة بالمهام التي يتم تدقيقها.

– ضرورة أن تهتم الشركات الصناعية بتحديد جهات ذات القدرة على النفاذ إلى المعلومات واستخدام تكنولوجيا المعلومات بشكل دقيق.

المصادر والمراجع

أولا: المراجع باللغة العربية

إبراهيم، ليث سعد الله حسين، والصميدعي، عبد الله عبد الحق خميس (2012). تطبيقات الحوسبة السحابية العامة في المنظمات: أنموذج مقترح للمنظمات التعليمية العراقية. مجلة تنمية الرافدين، 34(110)، 141-156.

البنك المركزي الاردني (2018). تعليمات التكيف مع الهجمات السيبرانية، عمان، الأردن. https:// www.cbj.gov.jo/DetailsPage/CBJAR/NewsDetails.aspx?ID=213

الجبور، منى (2019). السيبرانية هاجس العصر. مجلة المكتبات والمعلومات والتوثيق في العالم العربي، 262-262، جامعة الدول العربية، مصر

الحيدري، زينب (2023). الأمن السيبراني المخاطر التحديات المواجهة. دار الشرق، ط1، الدوحة، قطر.

دمدوم، زكريا، مرغني، وليد وصدراوي، طارق (2020). تحديات إعتماد المحاسبة السحابية في بيئة الأعمال الجزائرية. مجلة العلوم الإقتصادية والتسيير والعلوم التجارية، 13(3)، 490-475.

الرفادي، بسمة يونس (2018). الحروب السيبرانية وأثرها في التنظيم الدولي. مجلة العلوم والدراسات الإنسانية، 49(4)، 14-1، جامعة بنغازي، ليبيا

رزق، مروة (2013). الحوسبة السحابية والتقنيات المتحركة: أبرز الاستراتيجيات الامنية في 2013. مصرس. https://www.masress.com/moheet/551449

زمورة، جمال، وبن عيسى، جمالي (2022). أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية في الجزائر. مجلة البحوث الإقتصادية المتقدمة، 7 (2)، 424-414.

الشريفين، نضال كمال، والكيلاني، عبد الله زيد (2007). مدخل إلى البحث في العلوم التربوية والإجتماعية. ط2، دار المسيرة، عمان، الأردن.

الصليبي، نايلة (2024). أبرز تهديدات الأمن السيبراني وأمن المعلومات المتوقعة عام 2024. مونت كارلو الدولية. https://www.mc-doualiya.com//20240109

عبد الحافظ، أحمد (2023، مايو). مؤتمر ومعرض مصر للأمن السيبراني وأنظمة إستخبارات المعلومات. 18-16 مايو، مركز مصر الدولي للمعارض، القاهرة، مصر.

عبد الرضا، عبد أسعد، والمعموري، علي إبراهيم (2020). الأمن السيبراني ودورة في إنتشار ظاهرة الإرهاب في العراق بعد العام 2003، مركز الدراسات الدولية، 2020(80)، 190-149، جامعة بغداد، العراق.

غريب، حكيم (2018). الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة. المجلة الجزائرية للدراسات السياسية، 5(2)، 119-104.

الغول، ريهام (2014). بيئات التعلم الإلكتروني في ضوء التكامل بين تكنولوجيا الحوسبة السحابية وخدمات الجيل الثاني للويب: رؤية مقترحة، تكنولوجيا التربية. دراسات وبحوث المؤتمر العلمي العاشر، عدد خاص، 422-397، مصر.

قنديلجي، عامر إبراهيم (2013). منهجية البحث العلمي. دار اليازوري العلمية للنشر والتوزيع. عمان، الأردن.

لغريبي، نور الهدى، وبن راية، نور الهدى، بلعريبي، إنتصار (2020). مساهمة المحاسبة السحابية في تخفيض تكلفة العمل المحاسبي دراسة ميدانية.] رسالة ماجستير غير منشورة [، جامعة الشهيد حمه لخضر، الوادي، الجزائر.

مركز إيداع الأوراق المالية (2023). الشركات المساهمة العامة – قطاع الصناعة.
https://www.sdc.com.jo/arabic/index.php?option=com_public&member_cat=900&member_sub_cat=4
المركز الوطني للأمن السيبراني الأردني (2019). قانون الأمن السيبراني رقم (16) لسنة 2019، الجريدة الرسمية، 5143https://ncsc.jo/AR/5143
المنيع، الجوهرة بنت عبد الرحمن (2022). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030. مجلة كلية التربية، 38(1)، 155-194 جامعة أسيوط، مصر.
يعقوب، إبتهاج، وهاب، أسعد، الفرطوسي، علي (2022). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة إختبارية. مجلة الدراسات المالية والمحاسبية والإدارية، 9(1)، 1404-1430.

ثانيا: المراجع باللغة الإنجليزية

Ali, O. A. M., Matarneh, A. J., Almalkawi, A., & Mohamed, H. (2020). The impact of cyber governance in reducing the risk of cloud accounting in Jordanian commercial banks-from the perspective of Jordanian auditing firms. Modern Applied Science, 14(3), 75-89.
Cebula, DD, & Young, L.R. (2010). Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI -2010- TN- 028, Software Engineering Institute, Carnegie Mellon University.
Dimitriu, Otilia, & Matei ،Marian. (2014). A new paradigm for accounting through cloud computing. Procedia economics and finance, 15(14), 840-846.
International Organization for Standardization -ISO- (2022) 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
https://www.iso.org/standard/27001
Kure, Halima Ibrahim, Islam, Shareeful, & Razzaque, Mohammad Abdur (2018). An Integrated Cyber Security Risk Management Approach for a Cyber Security-Physical System, Applied Sciences, 8(6), 889.
Maleh, Yassine, Sahid, Abdelkebir, & Belaissaoui, M. (2018). A capability maturity framework for IT security governance in organizations. Advances in Intelligent Systems and Computing, 735(1), 221-233.
Musyaffi, Ayatulloh Michael, & Arinal, Muna (2021). Critical factors of cloud accounting acceptance and security for prospective accountants: TAM extension, Jurnal Riset Akuntansi kontemporer, 13(1), 1-6.
National Institute of Standards and Technology-NIST (2011). The NIST Definition of Cloud, Computing. Online Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Qasaimeh, Ghazi, & Jaradeh, Hussam (2022). International Journal of Technology, Innovation and Management (IJTIM), 2(1), 68-86.

Rehman, Huma, Masood, Ashraf & Cheema, Ahmad (2015). Information Security Management in Academic Institutes of Pakistan. 2nd National Conference of Information Assurance (NCIA), 2, 47-51.

Sekaran, Uma, & Bougie, Roger (2020). Research Methods for Business: A Skill-building Approach, 8th Edition, Wiley.

Tawfik, Omar Iqbal, Al-Tahat, Saqer, Jasim, Abdulridha, & Abd Almonem, Osama (2021). Intellectual Impact of Cyber Governance in The Correct Application of Cloud Accounting in Jordanian Commercial Banks from The Point of View of Jordanian, Journal of Management Information and Decision Sciences, 24(5), 1-14.