اختبار مدى توافر المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول لنظام المعلومات المحاسبي في الشركات المساهمة العامة الفلسطينية

زهران "محمد علي" دراغمه[1]، وصهيب توفيق جرار[2]

[1]، [2] قسم المحاسبة، كلية العلوم الإدارية والمالية، الجامعة العربية الأمريكية–جنين

zahran.daraghma@aauj.edu[1], sjarrar@aauj.edu[2]

الملخص

يهدف هذا البحث إلى إختبار مدى توافر المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول المنطقي للنظام المحاسبي، وكذلك اختبار مدى توفر المقومات الرقابية التي تحد من تهديدات الوصول المادي للحواسيب ومعداتها في الشركات المساهمة العامة (الصناعية، والخدماتية، وقطاع البنوك، وشركات التأمين) المدرجة في بورصة فلسطين للأوراق المالية، ولتحقيق الأهداف السابقة تم استخدام استبانة صممت خصيصاً للإجابة عن تساؤلات الدراسة بحيث تم توزيع 280 استبانة استرد منها 211 استبانة وهي تشكل (75.4%) من عينة الدراسة المكونة من (المديرين الماليين، والمحاسبين، والمدققين الداخليين، وموظفي الحاسب، ومدققي الحسابات الخارجيين). ولأغراض تحليل البيانات تم استخدام عدد من الأساليب الإحصائية وهي: (اختبار كرونباخ ألفا Cronbach's Alpha، والإحصاءات الوصفية، واختبار One Sample T Test، واختبار Kruskal–Wallis)، ولقد توصلت الدراسة لعدد من النتائج وهي: أن قطاعي التأمين والبنوك في فلسطين تتوفر فيهما المقومات الرقابية اللازمة للحد من تهديدات الوصول المنطقي والمادي لنظام المعلومات المحاسبي، وأن قطاعي الخدمات والصناعة في فلسطين يعانيان من ضعف شديد في توفر المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول المنطقي والمادي لنظام المعلومات المحاسبي. وبناء على هذه النتائج تم تقديم عدد من التوصيات أهمها: ضرورة قيام بورصة فلسطين للأوراق المالية ومجالس إدارة الشركات المساهمة العامة بإعطاء المزيد من الأهمية لهذا الأمر والزام الشركات بتعزيز المقومات الرقابية المتعلقة للحد من تهديدات مخاطر الوصول المنطقي والمادي للنظام.

الكلمات الدالة: *نظام المعلومات المحاسبي، والوصول المادي، والوصول المنطقي، والرقابة الداخلية، وأمن المعلومات، والشركات المساهمة، وبورصة فلسطين.*

مقدمة البحث

هذا العصر مليء بالمخاطر التي تحيط بالمنظومة، وذلك اقتضى البحث عن طرق تقود إلى معالجة مواضع الخطر في حال وقوعها أو وجوب توفر إجراءات تحد من المخاطر المرتقبة أو تمنعها (أي الوقاية منها) من خلال استخدام أساليب محددة، وأن هذه المخاطر أحاطت بمختلف جوانب الحياة، ولعل منظومة الأعمال كانت الأكثر حظاً من التأثر بالمخاطر الناتجة عن وجود قصور في مقومات الرقابة الداخلية (Hildani and Alanan, 2010; Dhillon, 1999)، وتفاقمت هذه المشكلة نتيجة حدوث ثورة معلوماتية أطاحت بالأنظمة اليدوية وأحلت مكانها الأنظمة المحوسبة التي تستند إلى تكنولوجيا المعلومات والاتصالات (Romney and Steinbart, 2003)، وينبغي الإشارة إلى أن نظامي المعلومات الإداري والمحاسبي أصبحا متكاملين، ومستندين حاسوبياً، ومرتبطين بالبيئة الخارجية من خلال شبكة الانترنت ومتكاملين داخلياً من خلالها. ولقد بيّن (Abu-Musa, 2006) أن هذا أتاح مناخاً مناسباً لنمو المخاطر المرتبطة بنظامي المعلومات الإداري والمحاسبي في المنشأة، وفي هذا السياق أيضاً أشار (Ahmad, 2012; Romney and Steinbart, 2010; Sun, et al., 2006) إلى أحد أهم المخاطر التي تواجه نظام المعلومات المحاسبي، وهي المخاطر الناتجة عن المجتمع البشري من داخل المنشاة أو خارجها، وتنحصر هذه المخاطر في مخاطر الوصول المادي لمكونات النظام المحاسبي والوصول المنطقي إلى نماذج إدخال البيانات أو معالجتها أو تخزينها أو القدرة على إنتاج المعلومات، وإذا كان الأمر كذلك فإن حرية الوصول تكون متاحة، وهذا هو أفضل مناخ لنمو المخاطر التي تؤول بالمنشأة إلى الخسارة، وبالتالي فإنه من الضروري أن تتوفر مجموعة من المقومات الرقابية في أي نظام محاسبي للحد من هذه المخاطر وحصرها في دائرة بعيدة عن النظام المحاسبي، ولقد أشار (Abdallah, 2013; Konchitchki and O'Leary, 2011) إلى أن وجود نظام معلومات محاسبي محوسب يتمتع بدرجة عالية من الأمن والجودة يؤدي إلى زيادة القيمة السوقية للسهم نتيجة لدوره في تحسين الأرباح، وكذلك بيّن (Sakini and Awada, 2011; Mansour et al., 2009; Beneish et al., 2008) أن انخفاض مستوى المخاطر والتهديدات التي تحيط بنظام المعلومات المحاسبي يؤدي إلى زيادة كفاءة نظام المعلومات المحاسبي. وقد أشار (Bodnar and Hopwood, 2010, P 197) أنّه يمكن الحد من هذه التهديدات من خلال توافر مقومات للرقابة الداخلية تمنع من الوصول المنطقي والمادي للحاسب،

ولقد بيّن (Davis, 1997) أهمية أن يتمتع المحاسبون بقدرات عالية لفهم مخاطر الحاسب والقدرة على مواجهتها، والحد منها بأقصى درجة ممكنة وهذا من متطلبات التأهيل المحاسبي.

إن ما تم طرحه سابقاً من مخاطر لا ينحصر في إقليم جغرافي معيّن بل أصاب قطاع الأعمال في كل أنحاء المعمورة ولكن تتفاوت الشركات من حيث المقاومة والوقاية من هذه المخاطر، ولهذا يجب إعطاء هذا الموضوع نصيباً من الأهمية في قطاع الأعمال الفلسطيني وخاصة الشركات التي تمتلك نظم إدارية ومحاسبية مؤتمته الكترونياً، وعليه جاءت هذه الدراسة؛ لتقديم دليلاً من واقع قطاع الأعمال الفلسطيني حول مدى توافر مقومات الحد من مخاطر الوصول المادي والمنطقي غير المصرح به إلى نظام المعلومات المحاسبي، من خلال دراسة ميدانية تقوم على استقصاء آراء أصحاب القرار وتحليلها، وهم ينحصرون في المديرين الماليين، والمحاسبين، والمدققين الداخليين، وموظفي الحاسب، ومدققي الحسابات الخارجيين، ومن هنا يتوقع أن تقدم هذه الدراسة دليلاً علمياً حول ذلك من واقع البيئة الفلسطينية، وطرح عدد من التوصيات الكفيلة بتحسين جودة نظام المعلومات المحاسبي في قطاع الأعمال الفلسطيني.

مشكلة البحث

يستوعب عالم الأعمال تطور تكنولوجيا المعلومات والاتصالات، وفي الوقت نفسه يواجه مخاطرهما المتزايدة. وهذا يثير تساؤلاً حول توقيت الحلول، أو توافر المقومات الوقائية الكفيلة بالتخلص من تلك المخاطر، ومن هنا فإنّ الاقتصاديات المتقدمة استطاعت أن تعمل على تصميم نظم رقابية أسهمت في الحد من هذه المخاطر إلى أدنى مستوياتها، وعليه يجب طرح استفسار مهم، وهو إلى أي مدى استطاع قطاع الأعمال الفلسطيني الحد من المخاطر المحيطة بنظامي المعلومات الإداري والمحاسبي؟ وبالتالي يمكن التعبير عن مشكلة هذه الدراسة من خلال طرح التساؤلات الآتية:

أولاً: ما مدى توافر المقومات الرقابية التي تحد من تهديدات مخاطر الوصول المنطقي لنظام المعلومات المحاسبي في الشركات المساهمة العامة الفلسطينية؟

ثانياً: ما مدى توافر المقومات الرقابية التي تحد من تهديدات مخاطر الوصول المادي لنظام المعلومات المحاسبي في الشركات المساهمة العامة الفلسطينية؟

أهداف البحث

جاءت هذه الدراسة لتحقيق الأهداف الآتية:

أولاً: تقديم دليل علمي من واقع الشركات الفلسطينية حول كفاءة مقومات الأمان في نظام المعلومات المحاسبي فيما يتعلق بتهديدي الوصول المنطقي والمادي إليها.

ثانياً: حصر التهديدات والثغرات الرقابية حول الوصول المنطقي والمادي لنظام المعلومات المحاسبي، مما يساعد مديري هذه الشركات على الحد منها لاحقاً.

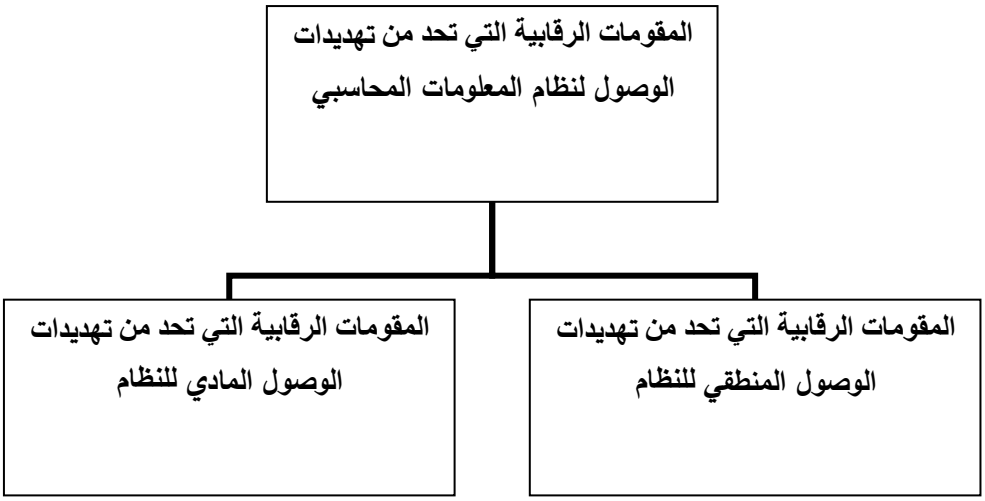
ولتحقيق الأهداف سابقة الذكر تم الاستناد إلى دراسة تطبيقية تقوم على استجواب آراء المديرين الماليين والمحاسبين والمدققين الداخليين وموظفي الحاسب ومدققي الحسابات الخارجيين.

أهمية البحث

إنّ أبرز ما يميّز هذه الدراسة أنها بحثت في مدى توافر المقومات الرقابية التي تحد من تهديدات مخاطر الوصول لنظام المعلومات المحاسبي للشركات المساهمة العامة الفلسطينية، وأيضاً فإنّ هذه الدراسة ذات طابع تطبيقي، إذ قد يستفاد من نتائجها لخدمة قطاع الأعمال الفلسطيني وتحديداً الشركات المساهمة العامة الفلسطينية، كما تبرز أهمية هذه الدراسة من خلال أهمية الموضوع الذي تتناوله بالبحث والتحليل، وخاصة أنه في حدود علم الباحثين لا يوجد دراسة طبقت على بيئة الأعمال الفلسطينية تناولت هذا الموضوع.

أنموذج البحث

الشكل رقم (1) يوضح أنموذج الدراسة الذي تم استقراؤه من الأدب النظري والدراسات السابقة، وقد تمّ الاعتماد عليه لصياغة فرضيات الدراسة.



الشكل (1): المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول المنطقي والمادي لنظام المعلومات المحاسبي.

المصدر: من تصميم الباحثين.

فرضيات البحث

بناءً على ما ورد في الأدب النظري والدراسات السابقة، وما تم عرضة في أنموذج البحث، تم صياغة الفرضيات الآتية:

الفرضية الأولى: لا تتوافر المقومات الرقابية التي تحد من تهديدات الوصول المنطقي لنظام المعلومات المحاسبي في الشركات المساهمة العامة الفلسطينية.

الفرضية الثانية: لا تتوافر المقومات الرقابية التي تحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي في الشركات المساهمة العامة الفلسطينية.

الفرضية الثالثة: لا توجد فروق ذات دلالة إحصائية في متوسط وجهة نظر المستجوبين حول مدى حجم تهديدات الوصول المنطقي لمكونات نموذج النظام المحاسبي في الشركات المساهمة العامة الفلسطينية تعزى للقطاع.

الفرضية الرابعة: لا توجد فروق ذات دلالة إحصائية في متوسط وجهة نظر المستجوبين حول حجم تهديدات الوصول المادي لمكونات النظام المحاسبي في الشركات المساهمة العامة الفلسطينية تعزى للقطاع.

الأدب النظري والدراسات السابقة

فيما يأتي عرض للأدب النظري والدراسات السابقة:

أولاً: الأدب النظري

يتناول هذا القسم من البحث أمن نظام المعلومات المحاسبي، وإمكانية الاعتماد على النظام، ومخاطر الوصول المنطقي للنظام، ومخاطر الوصول المادي للنظام، وفيما يأتي عرض ذلك:

أمن نظام المعلومات المحاسبي

بسبب التحول من النظام المحاسبي اليدوي إلى النظام المحاسبي المحوسب (وتحديداً التحول من الأنظمة المحاسبية المحوسبة المغلقة إلى الأنظمة المحاسبية المحوسبة المفتوحة داخلياً وخارجياً)، فقد ازدادت المخاطر التي تحيط بنظام المعلومات المحاسبي (البحيصي، والشريف، 2008)، وعليه فإن نظام المعلومات المحاسبي يواجه مجموعةً من التهديدات تتمثل في الكوارث الطبيعية، ومخاطر مرتبطة بالبرامج والمعدات الحاسوبية، ومخاطر بشرية مقصودة وغير مقصودة (Romney and Steinbart, 2010)، وبيّن (Fardinal, 2013; Curtis and Borthick, 1999) انه يمكن الحد من هذه المخاطر إذا توفر نظام أمن ورقابة فعّال يحدّ من التهديدات المحتملة وتحديداً المتعلقة بالوصول المادي والمنطقي لنظام المعلومات المحاسبي. ولقد ورد في التشريع الأمريكي Sarbanes-Oxley Act لعام 2002م أنه يجب على مديري الشركات تأسيس دائرة رقابية تعزز من وجود معايير صارمة للرقابة المالية الداخلية ورقابة تكنولوجيا المعلومات في الشركة. وقد أشار (Neogy, 2014) إلى أنّ وجود نظام أمن فعّال يحيط بنظام المعلومات المحاسبي يؤدي إلى إدخال ومعالجة البيانات بطريقة صحيحة، والحصول على معلومات مفيدة ضمن الصلاحيات الممنوحة. ولقد أشار (Arsenie-Samoil and Cuza, 2011) وكذلك (حمادة، 2010) إلى أنّ هناك مجموعه من العوامل تؤدي إلى زيادة مخاطر الهجمات الالكترونية لنظام المعلومات المحاسبي (الوصول المنطقي) وتتمثل في: (1) عدم القدرة على تعزيز أمن النظام. (2) وجود نقص في وعي وتدريب مستخدمي نظام المعلومات المحاسبي. (3) عدم اتباع الإجراءات المرسومة للحد من الوصول للنظام. (4) قدرة الأشخاص غير المصرّح لهم الوصول لنظام المعلومات المحاسبي.

إمكانية الاعتماد على النظام

يمتاز نظام المعلومات المحاسبي بخاصية الاعتمادية Reliability عندما يتصف بمجموعة من الخصائص (Amiri, 2013; Mndzebele, 2013; Hall, 2011; Romney and Steinbart, 2010; Krishnan et al., 2005)، وهي:- أولاً: أن يكون النظام متاحاً وقت الحاجة إليه. ثانياً: الأمن ضد الوصول المادي والمنطقي لنظام المعلومات المحاسبي. حيث أشار (Mathias and Ogundeji, 2013) إلى أهمية وجود مقومات فاعلة لحماية نظام المعلومات المحاسبي من التهديدات الداخلية والخارجية المحيطة به. ثالثاً: تكامل النظام، ما يعني أن المعالجة مكتملة ودقيقة، في الوقت المناسب وتعدّ من المصرح لهم القيام بذلك. وقد بيّن (Alzoubi, 2011; Romney and Steinbart, 2010) أنّ المعلومات التي يقدمها النظام المحاسبي يجب أن تتسق مع ما ورد في الإطار المفاهيمي للمحاسبة المالية الصادر عن مجلس معايير المحاسبة المالية وبين اتساق هذه الخصائص مع خاصية الاعتمادية على النظام. رابعاً: قابلية النظام للصيانة دون أن يؤثر ذلك على الخصائص الثلاث سابقة الذكر (احمرو، 2006). وقد بيّن كثير من الباحثين أن الخاصية الثانية (الأمن المادي والمنطقي) تعتبر من أهم خصائص إمكانية الاعتماد على نظام المعلومات المحاسبي (Bawaneh, 2014; Mathias and Ogundeji, 2013; Al Hanini, 2012; Beneish, Billings and Hodder, 2008)، وقد قسّم الباحثون المخاطر التي ترتبط بأمن النظام إلى قسمين هما: أ) مخاطر الوصول المادي لنظام المعلومات المحاسبي. ب) مخاطر الوصول المنطقي لنظام المعلومات المحاسبي. وفيما يلي عرض لهذه الأسس الأمنية.

مقومات الحدّ من تهديدات الوصول المنطقي للنظام

يقصد بالوصول المنطقي للحاسب القدرة على الوصول لبيانات الحاسب لشخص من داخل الشركة أو خارجها، غير مصرح له بذلك، وتمكّن هذا الشخص من القيام بعمليات الاطلاع على البيانات ونسخها والإضافة عليها وتعديلها، أو الحذف منها (Romney and Steinbart, 2003)، وهناك مجموعة من المقومات الرقابية التي تؤدي إلى الحدّ من الوصول المنطقي لبيانات النظام وهي: 1) وجود كلمة مرور واسم دخول لكل مستخدم لبرامج الشركة المالية والادارية، وهذا الأمر ضروري لمنع دخول الأشخاص غير المصرح لهم بإدخال البيانات الخاصة بالنظام المحاسبي أو معالجتها أو الاطلاع عليها (Campbell, 2003; Anderson, 2008; Hayale and Abu Khadra, 2008; Bawaneh, 2014) 2) أن يتم استخدام طرفيات

(لوحة مفاتيح وشاشة) دون وجود مجسم جهاز الكمبيوتر، ويستخدم هذا الإجراء للحد من الاستخدام غير المنطقي للحاسب (Davis, 1997; Anderson, 2008). 3) أن تكون بعض المهام معطلة في شاشات المستخدمين حسب صلاحياتهم؛ وذلك تبعاً للتفويض الممنوح، وهذا الإجراء للحدّ من الوصول المنطقي غير المبرر مما يحدّ من مخاطره (Mathias and Ogundeji, 2013; Al Hanini, 2012; Anderson, 2008). 4) أن يكون إدخال البيانات مصرحاً به لعدد محدد من الأشخاص ضمن الصلاحيات الممنوحة (هلدني، والغبان، 2010) و(Al Hanini, 2012). 5) أن تكون عملية معالجة البيانات مصرحاً بها لعدد محدد من الأشخاص ضمن الصلاحيات الممنوحة لهم (Mathias and Ogundeji, 2013; Al Hanini, 2012). 6) أن يكون الاطلاع على المخرجات مصرحاً به لعدد محدد من الأشخاص ضمن الصلاحيات الممنوحة لهم (Mathias and Ogundeji, 2013; Al Hanini, 2012). 7) أن تكون شبكة الانترنت الداخلية للشركة محمية بكلمات مرور (Davis, 1997). 8) أن تمتلك الشركة برامج مرخصة للحماية من الفيروسات والتهديدات المختلفة (Al Hanini, 2012; Samoil, Mihalache and Cuza, 2011). 9) أن تستخدم الشركة برامج حماية من الفيروسات وبرامج جدران نارية (Mathias and Ogundeji, 2013; Al Hanini, 2012). 10) أن تقوم الشركة بحجب مواقع الانترنت والبريد الالكتروني غير الرسمية (Bunke et al., 2012). 11) أن تكون البرامج المحاسبية والمالية محمية بكلمات مرور (Hayale and Abu Khadra, 2008; Bawaneh, 2014). 12) وجود شاشة Screen Saver محمية بكلمة مرور (Hayale and Abu Khadra, 2008). 13) الحد من إمكانية الوصول للأجهزة داخل الشركة من خلال الشبكة (Gul and Chia, 1994). 14) وجود برامج تجعل الجهاز يغلق عندما يحاول شخص ما الوصول للنظام (Burtescu, 2009; Bunke, Koschke and Sohr, 2012). 15) يتم حماية المجلدات الموجودة على الحاسب (الملفات) بكلمات مرور (Al Hanini, 2012). 16) أن تكون شاشات النظام الإداري والمحاسبي مختلفة من شخص لآخر حسب الصلاحيات الممنوحة (Hayale and Abu Khadra, 2008). 17) أن يتم إجراء نسخ احتياطي للبيانات باستخدام وسائل تخزين خارجية (Mathias and Ogundeji, 2013; Al Hanini, 2012; Anderson, 2008). 18) عند القيام بإدخال خاطئ لاسم المستخدم أو كلمة المرور ثلاث مرات يجب أن تتعطل شاشة الإدخال تلقائياً (Hayale and Abu Khadra, 2008).

مقومات الحدّ من تهديدات الوصول المادي للنظام

إن الوصول المادي لنظام المعلومات المحاسبي يعني القدرة على الوصول لمعدات الحاسب والشبكة الخاصة بالشركة، مما يؤدي إلى مخاطر مثل السرقة أو التدمير أو الاستخدام السيئ المتعمّد (Romney and Steinbart, 2003)، وهناك مجموعه من المقومات الرقابية التي تؤدي إلى الحد من الوصول المادي لمعدات النظام وهي: 1) وضع أجهزة الحاسب ومعداته في غرف مغلقة (Henage and Henage, 2013; Hayale and Abu Khadra, 2008). 2) عدم قدرة كل شخص الوصول للأجهزة والمعدات الحاسوبية (Kanai et al., 2014; Anderson, 2008). 3) وجود أجهزة إنذار للكشف عن دخول أشخاص غير مخولين بذلك (Henage and Henage, 2013). 4) وجود أقفال على أجهزة الحاسب أي إغلاق صناديقها باقفال (Henage and Henage, 2013). 5) أن يتم تعطيل مداخل USB (Anderson, 2008). 6) أن يتم تعطيل القرص المضغوط CD-ROM (Anderson, 2008). 7) وجود كاميرات تصوير مقابل أجهزة الحاسب والمعدات (Kanai et al., 2014). 8) يستطيع الأشخاص المخول لهم فقط الدخول إلى غرف الحاسب والمعدات المساندة (Bunke, Koschke and Sohr, 2012). 9) وجود حساسات دخان وحرائق في غرف أجهزة الحاسب (Kanai et al., 2014; Henage and Henage, 2013). 10) صعوبة فك جهاز الكمبيوتر والمعدات المرتبطة به (Romney and Steinbart, 2003). 11) وجود سجل يدون فيه أسماء الضيوف الذين يدخلون الشركة وأماكن العمل (Bunke, Koschke and Sohr, 2012). 12) عدم ظهور كوابل الانترنت للعيان (Burtescu, 2009). 13) عدم ترك الحاسب المحمول الخاص بالشركة في السيارة (CPA Australia, 2008). 14) أن تكون قطع الكمبيوتر مؤمّنة بغرف محكمة الإغلاق (Henage and Henage, 2013). 15) إتلاف أجهزة الكمبيوتر القديمة وتحديداً القرص الصلب (CPA Australia, 2008). 16) يتم تأمين وسائل التخزين المنقولة بكلمات سر (Campbell, 2003; Anderson, 2008; Hayale and Abu Khadra, 2008; Bawaneh, 2014). 17) عدم ظهور أسلاك الهاتف والانترنت، حيث تكون داخل الحائط أو تحت البلاط (Burtescu, 2009). 18) يتم حفظ النسخ الورقية من المعلومات المالية داخل خزائن مغلقة (Bunke et al., 2012).

ثانياً: الأدبيات السابقة

فيما يلي عرض لأهم الدراسات السابقة:

جاءت دراسة (Bawaneh, 2014) لاختبار مدى توافر ثلاثة مقومات لأمن المعلومات وإجراءات الرقابة في البنوك الأردنية في ظل استخدام أنظمة المعلومات المحاسبية المحوسبة، والمقومات الثلاث هي الرقابة العامة على مستوى البنك، والرقابة العامة على تكنولوجيا المعلومات، ورقابة التطبيقات الخاصة بمعالجة العمليات، وتم استخدام منهج دراسة الحالة لعدد من البنوك الأردنية، وتم جمع البيانات من خلال إجراء مقابلات مع الموظفين ذوي العلاقة بأمن المعلومات والمحاسبين في البنوك الأردنية. ولقد توصلت الدراسة إلى عدد من النتائج أهمها: (1) أن يتمكن البنك من حماية نفسه من غش الكمبيوتر من خلال تصميم إجراءات رقابية متعلقة برقابة المدخلات، ورقابة عمليات المعالجة، ورقابة المخرجات، ورقابة المكونات المادية. (2) أن تستطيع البنوك الحدّ من جرائم الحاسب، وإساءة استعماله، والغش من خلال دعم الإدارة العليا لخطط الأمن، وتدريب العاملين وزيادة وعيهم حول الأمن، وتقييم مقاييس الرقابة الوقائية ووجود كلمات سر للدخول. (3) وضعت الدراسة حلاّ لمشكلة امن الحاسب لمعظم البنوك الأردنية ويتمثل في تصميم أنظمة رقابية تتكون من إجراءات رقابية خاصة ببيئة الحاسب والانترنت للحد من جرائم الحاسب والغش. (4) توصلت الدراسة إلى عدم وجود محاسب جنائي في البنوك الأردنية Forensic Accountant يمتلك مهارات رفيعة للحد من مخاطر استخدام الحاسوب في بيئة أنظمة المعلومات المحاسبية. وأوصت الدراسة البنوك الأردنية بأهمية تعيين خبراء في مجال الأمن وخاصة المحاسب الجنائي، وكذلك أوصت بأهمية قيام البنوك بوضع إجراءات رقابية وقائية للحد من المخاطر.

وجاءت دراسة (Financial Conduct Authority– London, 2013) لتقويم دور أنظمة الرقابة الداخلية في الحد من مخاطر الوصول المادي والمنطقي لنظام المعلومات المحاسبي في البنوك البريطانية، ولإتمام الدراسة تم اختيار عينة مكونة من 17 بنكاً بريطانياً وتم استقراء آراء المحاسبين، والمدققين الداخليين، وموظفي الرقابة خلال الفترة الممتدة من 2012 إلى 2013م، وتوصلت الدراسة لعدد من النتائج أهمها: 1) إن البنوك البريطانية لديها أنظمة رقابة داخلية تسهم في الحد من تهديدات ومخاطر الوصول المادي والمنطقي لنظام المعلومات المحاسبي. 2) إن فريق العمل في البنوك البريطانية لديه ثقافة رقابية عالية المستوى، مما يسهم في الحد من مخاطر الوصول المادي والمنطقي. 3) يوجد في البنوك البريطانية بعض الثغرات الرقابية المتعلقة ببطاقات الفيزا والعمليات المصرفية الالكترونية. وبناء على النتائج سابقة الذكر فإن الدراسة أوصت البنوك البريطانية بضرورة تصميم أنظمة رقابة وأمن للحد من التهديدات التي لم تعالج.

وهدفت دراسة (Mathias and Ogundeji, 2013) إلى تقويم مخاطر الأمن على نظام المعلومات المحاسبي المحوسب في نيجيريا في ظل انتشار تكنولوجيا المعلومات في بيئة الاعمال، وبشكل محدد جاءت هذه الدراسة للإجابة عن استفسارين هما: (1) – ما مدى وجود مخاطر تواجه نظام المعلومات المحاسبي المحوسب الخاص بالشركات الموجودة في نيجيريا. (2)– ما أنواع المخاطر الموجودة. ولتحقيق أهداف هذه الدراسة تم استخدام استبانة صممت خصيصاً للإجابة عن تساؤلات الدراسة موجّهة لمستخدمي نظام المعلومات المحاسبي المحوسب وهم (المدققون الداخليون، والمحاسبون، ومدققو نظم المعلومات، وموظفو التمويل، وموظفو تكنولوجيا المعلومات). حيث تم توزيع 200 استمارة استرد منها 158 استمارة. وتم استخدام عدد من الأساليب الإحصائية المتمثلة في (اختبار كرونباخ الفا، والإحصاءات الوصفية، وتحليل التباين، والانحدار اللوجستي Logistics Regression، وتوصلت الدراسة لعدد من النتائج تتمثل في أهم المخاطر التي تواجه نظام المعلومات المحاسبي وتتمثل فيما يأتي: 1 – قيام الموظفين بإدخال خاطئ للبيانات من غير قصد. 2– حذف المستخدمين جزءاً من بيانات النظام المحاسبي المحوسب من غير قصد. 3 – تبادل الملفات والوثائق بين العاملين بشكل غير مصرح به. 4 – الوصول غير المصرح به لنظام المعلومات بمستويات (المدخلات، والمعالجة، والمخرجات)، واسترجاع البيانات وقراءتها. 5 – انتشار الفيروسات داخل النظام لسوء الاستخدام. وكان من أهم التوصيات التي وضعتها الدراسة ضرورة أن تقوم الشركات الموجودة في نيجيريا بتعزيز نظم الرقابة الداخلية فيها للحد من المخاطر التي تحيط بالنظام.

وهدفت دراسة (Al Hanini, 2012) إلى تحديد مدى وجود مخاطر نظم المعلومات المحاسبية في البنوك الأردنية، وتحديد مسبباتها وطرق الوقاية منها. ولتحقيق ذلك تم تصميم استبانة وتوزيعها لعينة مكونة من 63 مستجوباً، وهم مساعدو المدراء العامين، ومديرو الدوائر، ومديرو الفروع ومساعدوهم، والموظفون في البنوك الأردنية. وتم استخدام مجموعه من الأساليب الإحصائية تتمثل في (اختبار كرونباخ ألفا، والإحصاءات الوصفية، واختبار T)، وتوصلت الدراسة إلى عدد من النتائج كان من أهمها: (أولاً) هناك مخاطر تهدد أمن نظام المعلومات المحاسبي في البنوك الأردنية تتعلق بـ: (أ) تعمّد قيام الموظفين بإدخال بيانات خاطئة للنظام. (ب) وجود مخاطر ناتجة عن دخول فيروسات للنظام. (ج) وجود مخاطر متعلقة بالرقابة الداخلية، حيث يستطيع الموظفون غير المصرح لهم الاطلاع على مخرجات النظام. (د) وجود مخاطر تهديدات مختلفة. (ثانياً) توصلت الدراسة إلى الأسباب التي تؤدي إلى حدوث هذه المخاطر وهي: (أ) نقص خبرات موظفي البنوك الأردنية في الحفاظ على أمن

المعلومات، ويعزى ذلك لكون هؤلاء الموظفين بحاجة إلى تدريب حول وسائل حماية أمن نظام المعلومات المحاسبي. (ب) عدم وجود سياسات في البنوك الأردنية تؤدي إلى وضع الشخص المناسب في المكان المناسب. وبناء على النتائج سابقة الذكر خرجت الدراسة بمجموعة من التوصيات حول اقتراح إجراءات يجب أن تتبعها البنوك الأردنية للحد من المخاطر ومن أهمها: (1) أن يقوم البنك بتحديث وسائل الحماية بشكل متوازٍ مع التطور التكنولوجي. (2) أن يتم أخذ نسخ احتياطية من البيانات وحفظها في مكان آمن بعيد. (3) إنشاء بنية تحتية في البنك للحد من تهديدات الوصول المادي والمنطقي للنظام.

وهدفت دراسة (Cheh et al., 2010) إلى تحديد المتغيرات المالية وغير المالية التي تعتبر بمثابة تهديدات تحدّ من قوة نظام الرقابة الداخلية حسب Sarbanes-Oxley Act للشركات المدرجة في الأسواق المالية الأمريكية وهي New York Stock Exchange، American Stock Exchange، NASDAQ، Regional U.S. Stock Exchange، Canadian Stock Exchange، Over-the-Counter Markets. وتكوّن مجتمع الدراسة من جميع الشركات المدرجة والمتاح وجود بياناتها في قاعدة البيانات Compustat Database والبالغ عددها 10000 شركة، وحصر الباحثون العوامل التي تضعف نظام الرقابة الداخلي بـ 35 متغيراً؛ وعلى أساس ذلك تم وضع شرط لاختيار عينة يتمثل في أن يتوفر عن الشركات معلومات عن المتغيرات قيد التحليل في قاعدة البيانات Compustat Database، وبعد تطبيق هذا الشرط تم اختيار عينة مكونة من 869 شركة مدرجة، ولأغراض التحليل تم استخدام أسلوب Decision Tree Method بهدف تحديد المتغيرات التي تضعف نظام الرقابة الداخلي، وتشير نتائج الدراسة انه تمّ الكشف عن 23 متغيراً تؤدي إلى ضعف نظام الرقابة الداخلي وضعف مقومات الأمن في نظام المعلومات المحاسبي، وعليه أوصت الدراسة أن يقوم مدققو الحسابات باستخدام برمجية مبنية على 23 متغيراً؛ لتقييم أنظمة الرقابة الداخلية للشركات المدرجة في الأسواق المالية الأمريكية.

وهدفت دراسة (هلدني، والغبان، 2010) إلى التعرف على مدى كفاءة وفعالية نظم الرقابة الداخلية وفعاليتها في تحقيق السلامة البنكية في ظل نظام المعلومات المحاسبي الالكتروني، ولتحقيق هذا الهدف قام الباحثون بإجراء دراسة ميدانية طبقت على 10 مصارف في العراق، حيث تم استخدام استمارة استبيان أعدت خصيصاً لتحقيق غرض الدراسة، ووزع 140 استبانة استرد منها 123 استبانة وتمّ استخدام عدد من الأساليب الإحصائية متمثلة في (التكرارات النسبية، والمتوسطات الحسابية والتحليل العاملي) لتحليل بيانات الدراسة، وخلصت الدراسة لعدد من النتائج أهمها: هناك ضعف في أنظمة الرقابة الداخلية التي تتماشى

ومتطلبات التطور في تكنولوجيا المعلومات. وهناك قصور في عملية تحديث نظم الرقابة وتطويرها في الشركات العراقية بشكل لا يفي بما يتطلبه استخدام تكنولوجيا المعلومات، وأيضاً هناك قصور في توافر أساليب الرقابة العامة والرقابة على التطبيقات اللازمة لتحقيق صحة ومصداقية المعلومات المعدة من البنوك، وبينت الدراسة أيضاً أن هناك ضعفاً في أنظمة الرقابة الداخلية التي تضمن عدم الوصول للبيانات والأجهزة، وقد أوصت الدراسة البنوك العراقية أن تأخذ بعين الاعتبار وجود مخاطر داخلية وخارجية، وأن تصمم أنظمة رقابية من شأنها الحد من هذه المخاطر.

وكذلك جاءت دراسة (Hayale and Abu Khadra, 2008) بهدف الاستقصاء والبحث عن التهديدات التي تواجه نظام المعلومات المحاسبي في البنوك الأردنية، ولتحقيق هذا الهدف استخدم الباحثان استمارة استبانة صممت خصيصاً لذلك، بحيث يتكون مجتمع الدراسة من جميع البنوك الأردنية والبالغ عددها 23 بنكاً تم استثناء 3 بنوك كونها حديثة التأسيس، بحيث تم توزيع 40 استمارة استبانة للمدققين الداخليين، ومديري دائرة الحاسب في هذه البنوك، وقد استرد منها 30 استبانة، وتم الاستعانة بنموذج الرائدين في هذا المجال Romney and Steinbart، وتوصلت الدراسة لعدد من النتائج أهمها: 1- تعاني البنوك الأردنية من وجود ثغرات في أنظمتها المحاسبية تمكن من تسهيل اختراقها. 2- يواجه نظام المعلومات المحاسبي مشاكل رقابية تتيح لمرتكبي الجرائم فرصة الوصول المادي والمنطقي لبيانات ومكونات النظام المالي في البنك. وقد أوصت الدراسة البنوك الأردنية أن تعزز من أنظمة الرقابة على نظم المعلومات المحوسبة للحدّ من التهديدات المحتملة.

أمّا دراسة (البحيصي، والشريف، 2008) فهدفت لتقييم المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في البنوك العاملة في قطاع غزة، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر. ولأغراض ذلك تم إعداد استبيان خاص تم توزيعه على البنوك العاملة في محافظات قطاع غزة، ومن ثم تم تحليل البيانات التي تم جمعها؛ وبناء على ذلك تم استخلاص بعض النتائج التي أسهمت في التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في البنوك العاملة في قطاع غزة، أهمها: 1) مخاطر نظم المعلومات المحاسبية المحوسبة موجودة بشكل لافت للنظر. 2) عدم وجود محاسبين لديهم الإلمام الكافي بأساليب الحدّ من مخاطر تكنولوجيا المعلومات في البنوك العاملة في قطاع غزة. 3) إن مخاطر نظم المعلومات المحاسبية الالكترونية ترجع إلى أسباب تتعلق بموظفي البنك، نتيجة قلة الخبرة، والوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة البنك؛ نتيجة لعدم وجود سياسات واضحة

ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى البنك، وعلى ضوء نتائج الدراسة تم التوصل إلى مجموعة من التوصيات أهمها: (1) من الضروري أن تدعم الإدارة العليا للبنوك أمن المعلومات لديها، وأن تعمل على إنشاء قسم خاص بتكنولوجيا المعلومات في كافة البنوك من أجل حماية أمن نظم المعلومات المحاسبية، وكذلك تطوير قدرات العاملين لديها في مجال أمن المعلومات وحمايتها. (2) ضرورة وضع إجراءات تضمن جاهزية نظم المعلومات للعمل في حالة الأزمات، وذلك من خلال استخدام تجهيزات منيعة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها. وكذلك العمل على تشفير المعلومات عند الحفظ والنقل والتخزين على مختلف الوسائط كي لا يتمكن أحد من اختراقها. (3) يجب وضع ضوابط أمن ورقابة للمعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم اتصالات سلكية ولاسلكية.

وكذلك هدفت دراسة (Abu-Musa, 2006) إلى استقصاء المخاطر التي تواجه نظام المعلومات المحاسبي في الشركات السعودية، ولأغراض تحقيق هذا الهدف استخدم الباحث استمارة استبانة صممت خصيصاً وتم توزيع 400 استمارة على الشركات في 7 مدن بالمملكة استرد منها 208 استمارة وبعد استثناء الاستمارات غير المكتملة تبقى 136 استمارة صالحة لإجراء التحليل اللازم، ولأغراض اختبار فرضيات الدراسة تم استخدام عدد من الأساليب الإحصائية وتم التوصل إلى عدد من النتائج أهمها: 1- أن أكثر من نصف المنشآت السعودية تعاني من خسائر مالية نتيجة لوجود ضعف في نظام الرقابة الداخلية وشُحّ مقوّمات الأمن المتعلق بالوصول المادي والمنطقي للنظام. 2- وبينت الدراسة أن هناك إدخال خاطئ للبيانات لنظام المعلومات المحاسبي بطريقة مقصودة أو غير مقصودة. 3- يقوم موظفو الشركات محل الدراسة بشكل مقصود بتدمير بيانات الشركة. 4- يتبادل العاملون "الباسورد Password" كل للآخر، مما يتيح لهم الدخول غير المصرح به لمكونات النظام. 5- إن نظام المعلومات المحاسبي والحاسب مليء بالفيروسات ولا تتوافر برامج حماية مرخصة. 6- يوجد ضعف في الرقابة على مخرجات النظام واستخدام وتوزيع خاطئ لغير المصرح لهم. 7- يمكن لأي شخص الاطلاع على بيانات ومعلومات النظام المحاسبي. 8- يمكن لأي موظف يعمل على النظام بطباعة المعلومات وتوزيعها على الأشخاص الذين ليس لهم حق (غير مصرح لهم) الاطلاع عليها نهائياً. 9- النظام المحاسبي الموجود في المنشآت السعودية يعاني من تهديدات الأمن والأمان من حيث الوصول المادي أو المنطقي للنظام. وخرجت الدراسة بعدد من التوصيات أهمها: يجب على الشركات السعودية أن تعزز

الإجراءات الرقابية على امن النظام للحد من التهديدات سابقة الذكر، وأنه يجب على الشركات السعودية أن تعمل على تحقيق الأمن وتحقيق حماية أفضل لنظام المعلومات المحاسبي.

مميزات البحث

1 – إنه حَسب علم الباحثينَ يعتبر البحث الاول الذي فحص مدى توفر المقومات الرقابية التي تحد من تهديدات مخاطر الوصول لنظام المعلومات المحاسبي في الشركات المساهمة العامة الفلسطينية المدرجة في بورصة فلسطين.

2 – أن البحث الحالي ينبثق عنه أنموذج يبين نقاط القصور في أنظمة الرقابة الداخلية لمواجهة تهديدات مخاطر الوصول لنظام المعلومات المحاسبي في الشركات المساهمة العامة الفلسطينية المدرجة في بورصة فلسطين.

منهج البحث

تعتمد هذه الدراسة على المنهج الوصفي التحليلي بحيث تم تصميم أداة الدراسة (الاستبانة) من خلال الرجوع إلى الأدب المحاسبي، ونتائج الدراسات السابقة حول التهديدات الرقابية المتعلقة بالوصول المادي والمنطقي لنظام المعلومات المحاسبي، واستقرائها للخروج بمقياس قادر على الإجابة عن تساؤلات هذه الدراسة، والمتعلقة بمدى توفر المقومات الرقابية الكفيلة بالحد من مخاطر الوصول إلى نظام المعلومات المحاسبي، بحيث تم توزيع الاستبانة باليد على فئات المستجوبين وهم (المديرون الماليون، والمحاسبون، والمدققون الداخليون، وموظفو الحاسب، ومدققو الحسابات الخارجيون)، وقسمت الاستبيانة إلى ثلاثة أقسام وهي: القسم الأول: يتضمن أسئلة عامة، واستكشافية الهدف منها تحديد خصائص أفراد عينة الدراسة (معلومات شخصية خاصة بالمستجوب) وتم صياغتها في القسم الأول بند أ من الاستبانة وهي أربعة أسئلة (من 1 إلى 4 بالقسم الأول من الاستبانة)، أما القسم الأول بند ب فيتضمن أسئلة لجمع معلومات عن الشركة التي يعمل بها المستجوب، وتم صياغة ثمانية أسئلة وهي الأسئلة (من 5 إلى 12 في القسم الأول من الاستبانة). القسم الثاني: تضمن القسم الثاني من الاستبانة 18 فقرة صممت لقياس مدى توفر المقومات الرقابية التي تحد من تهديدات الوصول المنطقي لنظام المعلومات المحاسبي، وتم تصميم هذه الفقرات بناءً على استقراء الأدب النظري سابق الذكر. القسم الثالث: تضمن القسم الثالث من الاستبانة 18 فقرة صممت

لقياس مدى توفر المقومات الرقابية التي تحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي، وتم تصميم هذه الفقرات بناءً على استقراء الأدب النظري سابق الذكر. وأن هذه الدراسة لا تتضمن متغيرات مستقلة وتابعة لكونها دراسة استكشافية.

مجتمع البحث وعيّنته

يتكون مجتمع الدراسة من الشركات المساهمة العامة التي بلغ عددها حتى بداية عام 2015 ثمانياً وأربعيين شركة مدرجه في بورصة فلسطين للأوراق المالية، وتمثل الشركات القطاع الصناعي، والخدماتي، والمصرفي، وقطاع التامين. أما عينة الدراسة فقد تكونت من (40) شركة مساهمة عامة، تم استجواب عدة فئات فيها تتمثل في المديرين الماليين، والمحاسبين، والمدققين الداخليين، وموظفي الحاسوب، ومدققي الحسابات الخارجيين. والجدول رقم (1–أ) يوضح عدد الاستبانات الموزعة والمستردة حسب المستجوب؛ إذ بلغت نسبة الاستبانات المستردة 75.4% أي بواقع 211 استبانة من أصل 280 استبانة، ويبيّن الجدول (1–أ) أن العينة ممثلة لمجتمع الدراسة ويمكن الاعتماد عليها في تعزيز نتائج هذه الدراسة.

جدول (1–أ): توزيع عينة الدراسة، ونسبة المسترد من كل فئة حسب المستجوب

الفئة الفرعية	عدد الاستبانات الموزعة	عدد الاستبانات المستردة	نسبة الاستبانات المستردة %
المديرون الماليون	40	27	67.5
المحاسبون	120	93	77.5
المدققون الداخليون	40	34	85.0
مُوظفو الحاسب	40	31	77.5
مُدققو الحسابات الخارجيون	40	26	65.0
المجموع	**280**	**211**	**75.4**

جدول (1–ب): توزيع عينة الدراسة، ونسبة المسترد من كل فئة حسب القطاع

الفئة الفرعية	عدد الاستبانات الموزعة	عدد الاستبانات المستردة	نسبة الاستبانات المستردة %
القطاع الصناعي	80	61	76.3
القطاع الخدماتي	80	57	71.3
قطاع البنوك والخدمات المالية	60	52	86.8
قطاع التامين	60	41	68.3
المجموع	**280**	**211**	**75.4**

أما الجدول (1–ب) فيعرض عدد الاستبانات الموزعة والمستردة حسب القطاع، حيث بلغت نسبة الاستبانات المستردة 75.4%. ويتبين من الجدول (1–ب) أن العينة ممثلة لمجتمع الدراسة ويمكن الاعتماد عليها في تعزيز نتائج هذه الدراسة.

التحليل الإحصائي، ونتائج الدراسة

تم تحليل البيانات المجمعة من المستجوبين باستخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS)، وتم تنفيذ الاختبارات الإحصائية عند مستوى دلالة إحصائية 0.05، وفيما يتعلق بأسئلة الدراسة المتعلقة (بتوافر) المقومات المتعلقة بالأمن أو عدم توافرها فيما يخص امن الوصول المنطقي للبيانات، والمادي للمعدات، فقد اعتمد التبويب الثنائي، حيث إن الرقم 2 يرمز لتوافر المقوم والرقم 1 يرمز لعدم توافره، ولغايات تحليل الإجابات اعتمد الباحثان على أساليب الإحصاء الوصفي، واختبار كرونباخ الفا Cronbach's Alpha، واختبار T، واختبار Kruskal–Wallis؛ لتحديد مدى وجود فروق في مدى توافر المقومات الخاصة بأمن الوصول المنطقي للبيانات، وأمن الوصول المادي للمعدات.

صدق الأداة وثبات المقياس

تم عرض أداة الدراسة (الاستبانة) على عدد من المختصين في مجالات المحاسبة، والحاسوب لتقويم الصدق الظاهري لها واختباره، ولإخراجها بصورة تكون فيها صالحة لما يراد قياسه، وأجريت التعديلات الضرورية بناءً على وجهة نظر المقوّمين، وفيما يتعلق بثبات المقياس فتم استخدام معامل الثبات (كرونباخ ألفا) للأسئلة الخاصة بأبعاد الدراسة (الأسئلة الخاصة بتوفر مقومات الأمن للوصول المنطقي للبيانات، والأسئلة الخاصة بتوافر مقومات الأمن للوصول المادي للمعدات)، حيث كانت نسبته (95.4%) لكل الفقرات معاً، وما نسبته (95.1%) للفقرات المتعلقة بالمقومات الرقابية التي تحد من تهديدات الوصول المنطقي لنظام المعلومات المحاسبي، و(95.7%) للفقرات المتعلقة بالمقومات الرقابية التي تحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي، وتعتبر هذه المعاملات مرضية وجيدة (Sekaran and Bougie, 2013).

خصائص عينة البحث

يبين الجدول (2) أن ما نسبته 91.9% من المستجوبين هم من حملة البكالوريوس والماجستير، وهذا من شأنه أن يعزز من نتائج الدراسة؛ لكون معظم المستجوبين يحملون درجات علمية بكالوريوس فأعلى. أما فيما يتعلق بتخصص المستجوبين فيلاحظ

أن ما نسبته 41.7% تخصصهم في مجال المحاسبة، و46% منهم في حقول العلوم التجارية، وما نسبته 12.3% في مجال الحاسوب، وهذا يوضح أن المستجوبين هم من المتخصصين بموضوع الدراسة، أما فيما يتعلق بعدد سنوات خبرة المستجوبين فيلاحظ أن ما نسبته 32.7% لديهم خبرات خمس سنوات فما دون، و40.8% منهم لديهم خبرات من ست سنوات إلى عشر، و18.5% منهم لديهم خبرات تتراوح من إحدى عشرة سنة إلى خمس عشرة، و8.1% منهم لديهم خبرات 16 عاماً فأكثر. وبالتالي فان المستجوبين لديهم خبرات كافية من شانها أن تعزز إمكانية تعميم نتائج هذه الدراسة، وأخيراً فيما يتعلق بالوصف الوظيفي للمستجوب فيلاحظ أن ما نسبته 12.2% مديرون ماليون، و44.1% يعملون في مجالات المحاسبة، وما نسبته 16.1% مدققون داخليون، وما نسبته 14.7% موظفو حاسوب، وما نسبته 12.3% منهم مدققو حسابات خارجيون، وهذا يبين أن وظائفهم ضمن مجال هذه الدراسة.

جدول (2): ملخص يعرض الخصائص الخاصة بالمستجوب

أولاً: الدرجة العلمية للمستجوب	عدد المشاهدات (N)	النسبة المئوية (%)
دبلوم فما دون	17	8.1
بكالوريوس	157	74.4
ماجستير فاعلي	37	17.5
المجموع	*211*	*100.0%*
ثانياً: تخصص المستجوب	**(N)**	**(%)**
محاسبة	88	41.7
أحد تخصصات التجارة الأخرى	97	46
في مجال الحاسوب	26	12.3
المجموع	211	*100.0%*
ثالثاً: عدد سنوات الخبرة للمستجوب	**(N)**	**(%)**
5 سنوات فما دون	69	32.7
من ست إلى عشر سنوات	86	40.8
من 11 إلى 15 سنه	39	18.5
16 عاماً فأكثر	17	8.1
المجموع	211	*100.0%*
رابعاً: الوصف الوظيفي للمستجوب	**(N)**	**(%)**
المديرون الماليون	27	12.8
المحاسبون	93	44.1
المدققون الداخليون	34	16.1
موظفو الحاسب	31	14.7
مدققو الحسابات الخارجيون	26	12.3
المجموع	*211*	*100.0%*

جدول (3): ملخص يعرض معلومات تتعلق بالشركة التي تعمل بها المستجوب

أولاً: القطاع الذي تنتمي له شركتكم	عدد المشاهدات (N)	النسبة المئوية (%)
القطاع الصناعي	51	24.2
القطاع الخدماتي	59	28
القطاع المصرفي	59	28
قطاع التامين	42	19.9
المجموع	*211*	*100.0%*
ثانياً: عدد الموظفين في مكان عملك	**(N)**	**(%)**
اقل من 20 موظفاً	50	23.7
من 20 إلى 49 موظفاً	27	12.8
من 50 إلى 99 موظفاً	29	13.7
100 موظف فأكثر	105	49.8
المجموع	211	*100.0%*
ثالثاً: عدد المتخصصين بالحاسوب مكان عملك	**(N)**	**(%)**
لا يوجد	20	9.5
من 1 إلى 5 موظفين	31	14.7
من 6 إلى 10 موظفين	46	21.8
أكثر من 10 موظفين	114	54
المجموع	211	*100.0%*
رابعاً: برامج ويندوز وأوفيس مرخصة	**(N)**	**(%)**
نعم	179	84.8
لا	32	15.2
المجموع	*211*	*100.0%*

نتائج فرضيات الدراسة

فيما يأتي عرض لنتائج اختبار فرضيات الدراسة مقسم إلى جزأين:

الجزء الأول: نتائج اختبار الفرضية الأولى الخاصة بتهديدات مخاطر الوصول المنطقي، والفرضية الثانية الخاصة بتهديدات مخاطر الوصول المادي لنظام المعلومات المحاسبي حسب القطاع. وفيما يأتي عرض لنتائج التحليل:

أولاً: اختبار مدى توفر المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول (المنطقي والمادي) لنظام المعلومات المحاسبي في الشركات المساهمة الفلسطينية الصناعية.

الجدول (4)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المنطقي لنظام المعلومات المحاسبي: قطاع الصناعة*

اسم المتغير	المقوم		المتوسطات الحسابية	قيمة ت المحسوبة	المعنوية الإحصائية	القرار
	يتوفر	لا يتوفر				
يوجد كلمة مرور واسم دخول لبرامج الشركة لكل موظف.	23 45.1%	28 54.9%	1.45	−0.697	0.489	لا يتوفر
يتم استخدام طرفيات (لوحة مفاتيح وشاشة) بدون وجود جهاز الكمبيوتر، بمعنى وجود جهاز حاسوب مركزي (Server).	20 39.2%	31 60.8%	1.39	−1.562	0.125	لا يتوفر
عند دخولك لحسابك كمستخدم للبرامج فان بعض المهام معطلة حسب صلاحياتك.	20 39.2%	31 60.8%	1.39	−1.562	0.125	لا يتوفر
إدخال البيانات مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	7 13.7%	44 86.3%	1.14	−7.454	0.000	لا يتوفر
معالجة البيانات مصرح بها لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	9 17.6%	42 82.4%	1.18	−6.001	0.000	لا يتوفر
الاطلاع على المخرجات مثل التقارير المالية أو الإدارية مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة للمستخدم.	11 21.6%	40 78.4%	1.22	−4.888	0.000	لا يتوفر
شبكة الانترانت الداخلية للشركة محمية بكلمات مرور.	11 21.6%	40 78.4%	1.22	−4.888	0.000	لا يتوفر
يوجد برامج مرخصة للحماية من الفيروسات والتهديدات المختلفة.	17 33.3%	34 66.7%	1.33	−2.500	0.016	لا يتوفر
يوجد برامج حماية من الفيروسات وبرامج جدران نارية.	13 25.5%	38 74.5%	1.25	−3.977	0.000	لا يتوفر
يتم حجب مواقع الانترنت والبريد الالكتروني غير الرسمية.	12 23.5%	39 76.5%	1.24	−4.413	0.000	لا يتوفر
البرامج المحاسبية والمالية محمية بكلمات مرور.	13 25.5%	38 74.5%	1.25	−3.977	0.000	لا يتوفر
يوجد شاشة Screen Saver محمية بكلمة مرور.	7 13.7%	44 86.3%	1.14	−7.454	0.000	لا يتوفر
عدم الوصول للأجهزة داخل الشركة من خلال الشبكة.	14 27.5%	37 72.5%	1.27	−3.573	0.001	لا يتوفر
وجود برامج تجعل الجهاز يغلق عندما يحاول أحد غير مصرح له الدخول للنظام.	14 27.5%	37 72.5%	1.27	−3.573	0.001	لا يتوفر
يتم حماية المجلدات الموجودة على الحاسوب (الملفات) بكلمات مرور.	2 03.9%	49 96.1%	1.04	−16.78	0.000	لا يتوفر
شاشات النظام الإداري والمحاسبي تختلف من شخص لأخر حسب الصلاحيات.	7 13.7%	44 86.3%	1.14	−7.454	0.000	لا يتوفر
القيام بإعداد نسخ احتياطية من البيانات والمخرجات باستخدام وسائل تخزين خارجية.	2 03.9%	49 96.1%	1.04	−16.78	0.000	لا يتوفر
عند إدخال اسم مستخدم أو كلمة مرور خاطئة ثلاث مرات تتعطل شاشة الإدخال.	7 13.7%	44 86.3%	1.14	−7.454	0.000	لا يتوفر
متغير الوصول المنطقي للنظام	**12 23.5%**	**39 76.5%**	**1.23**	**−7.311**	**0.000**	**لا يتوفر**

*تم استخدام قيمة اختبار (Test Value) تساوي 1.5 ((1+2) /2)، ومن الأهمية بمكان الإشارة إلى أن الفرضية الخاصة باختبار T هي كما يلي: ***الفرضية الصفرية:*** المتوسط الحسابي = 1.5، أما ***الفرضية البديلة:*** المتوسط الحسابي ≠ 1.5، وإحصائياً إذا كانت قيمة المعنوية الإحصائية أكبر من 0.05 فإننا نقبل الفرضية الصفرية التي تنص على عدم توفر المقوم، أما إذا كانت قيمة المعنوية الإحصائية يساوي أو اقل من 0.05 *فإننا نقول إن المقوم متوفر إذا كانت قيمة T المحسوبة موجبة.*

الجدول (5)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي: قطاع الصناعة

اسم المتغير	المقوم		المتوسطات	قيمة ت	المعنوية	القرار
	يتوفر	لا يتوفر	الحسابية	المحسوبة	الإحصائية	
يتم وضع أجهزة الحاسوب ومعداته في غرف مغلقة.	7 13.7%	44 86.3%	1.14	-7.454	0.000	لا يتوفر
عدم قدرة أي شخص غير مخول له للوصول للأجهزة والمعدات الحاسوبية.	7 13.7%	44 86.3%	1.14	-7.454	0.000	لا يتوفر
وجود أجهزة إنذار للكشف عن دخول الأشخاص غير المخول لهم.	13 25.5%	38 74.5%	1.25	-3.977	0.000	لا يتوفر
يوجد أقفال على أجهزة الحاسوب (قفل الصندوق بقفل).	14 27.5%	37 72.5%	1.27	-3.573	0.001	لا يتوفر
تم تعطيل مداخل USB.	2 03.9%	49 96.1%	1.04	-16.78	0.000	لا يتوفر
تم تعطيل القرص المضغوط CD-ROM.	2 03.9%	49 96.1%	1.04	-16.78	0.000	لا يتوفر
يوجد كاميرات تصوير مقابل أجهزة الحاسوب والمعدات.	7 13.7%	44 86.3%	1.14	-7.454	0.000	لا يتوفر
فقط الأشخاص المخولون يمكنهم الدخول لغرفة الحاسوب والمعدات المساندة.	8 15.7%	43 84.3%	1.16	-6.672	0.000	لا يتوفر
يوجد حساسات دخان وحرائق في غرف أجهزة الحاسوب.	7 13.7%	44 86.3%	1.14	-7.454	0.000	لا يتوفر
من الصعب فك جهاز الكمبيوتر والمعدات المرتبطة به.	7 13.7%	44 86.3%	1.14	-7.454	0.000	لا يتوفر
يوجد سجل يدون فيه أسماء الضيوف الذين يدخلون لاماكن العمل.	2 03.9%	49 96.1%	1.04	-16.78	0.000	لا يتوفر
عدم ظهور كوابل الانترنت للعيان.	8 11.8%	45 88.2%	1.12	-8.391	0.000	لا يتوفر
لا يتم ترك الحاسوب المحمول الخاص بالشركة بالسيارة.	14 31.4%	35 68.6%	1.31	-2.839	0.007	لا يتوفر
قطع الكمبيوتر مؤمنه بغرف محكمة الإغلاق.	22 43.1%	29 56.9%	1.43	-0.980	0.332	لا يتوفر
أجهزة الكمبيوتر القديمة يتم إتلافها وتحديداً القرص الصلب.	12 23.5%	39 76.5%	1.24	-4.413	0.000	لا يتوفر
وسائل التخزين المنقولة يتم تأمينها بكلمات سر.	16 31.4%	35 68.6%	1.31	-2.839	0.007	لا يتوفر
عدم ظهور أسلاك الهاتف والانترنت (تكون داخل الحائط او تحت البلاط).	16 31.4%	35 68.6%	1.31	-2.839	0.007	لا يتوفر
يتم حفظ النسخ الورقية من المعلومات المالية بداخل خزائن مغلقة.	13 25.5%	38 74.5%	1.25	-3.977	0.000	لا يتوفر
متغير الوصول المادي للنظام	**10 19.6%**	**41 80.4%**	**1.20**	**-9.304**	**0.000**	**لا يتوفر**

يتضح من الجدول رقم 4 أن نظام المعلومات المحاسبي في الشركات المساهمة العامة الصناعية يعاني من قصور عام في توفر أدنى مستوى لمقومات الحد من الوصول المنطقي لنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المنطقي 7.311- عند مستوى أهمية إحصائية 0.00 وهذا يقود لنتيجة مفادها وجود ضعف عام في نظام الرقابة الداخلي للشركة الصناعية والمتخصص بالحد من تهديدات مخاطر الوصول المنطقي للبيانات والمعالجة ومخرجات النظام. ويبيّن الجدول رقم 5 أن نظام المعلومات المحاسبي في الشركات المساهمة العامة الصناعية يعاني من قصور عام في توفر أدنى مستوى لمقومات الحد من الوصول المادي لنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المادي 7.311- عند مستوى أهمية إحصائية 0.00 وهذا يقود لنتيجة مفادها وجود ضعف عام في نظام الرقابة الداخلي للشركة الصناعية والمتخصص بالحد من تهديدات مخاطر الوصول المادي لأجهزة الحاسب ومعداته.

ثانياً: اختبار مدى توافر المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول (المنطقي والمادي) لنظام المعلومات المحاسبي في الشركات المساهمة الفلسطينية الخدمية.

يتضح من الجدول 6 أن هناك بعض المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول المنطقي للنظام المحاسبي متوفرة في الشركات الخدماتية وهي: أنه يوجد كلمة مرور واسم دخول لبرامج الشركة لكل موظف، وأيضاً فان شبكة الإنترانت الداخلية للشركة تكون محمية بكلمات مرور، وكذلك أنه يوجد برامج مرخصة للحماية من الفيروسات والتهديدات المختلفة، ويتبين أيضاً وجود برامج حماية من الفيروسات وبرامج جدران نارية، وأن البرامج المحاسبية والمالية محمية بكلمات مرور.

ويبين الجدول رقم 6 أن نظام المعلومات المحاسبي في الشركات المساهمة العامة الخدمية يعاني من قصور في كثير من النواحي كما وضح سابقاً في توافر مستوى مقبول من المقومات اللازمة للحد من الوصول المنطقي لنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المنطقي 0.615- عند مستوى أهمية إحصائية 0.541، وهذا يقود لنتيجة مفادها وجود ضعف عام في نظام الرقابة الداخلي للشركة والمتخصص بالحد من تهديدات مخاطر الوصول المنطقي للبيانات والمعالجة ومخرجات النظام في الشركات الخدماتية.

الجدول (6)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المنطقي لنظام المعلومات المحاسبي: قطاع الخدمات

اسم المتغير	المقوم		المتوسطات الحسابية	قيمة ت المحسوبة	المعنوية الإحصائية	القرار
	يتوفر	لا يتوفر				
يوجد كلمة مرور واسم دخول لبرامج الشركة لكل موظف.	39 66.1%	20 33.9%	1.66	2.591	0.012	يتوفر
يتم استخدام طرفيات (لوحة مفاتيح وشاشة) بدون وجود جهاز الكمبيوتر، بمعنى وجود جهاز حاسوب مركزي (Server).	27 45.8%	32 54.2%	1.46	−0.648	0.520	لا يتوفر
عند دخولك لحسابك كمستخدم للبرامج فان بعض المهام معطلة حسب صلاحياتك.	22 37.3%	37 62.7%	1.37	−2.002	0.050	لا يتوفر
إدخال البيانات مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	35 59.3%	24 40.7%	1.59	1.445	0.154	لا يتوفر
معالجة البيانات مصرح بها لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	29 49.2%	30 50.8%	1.49	−0.129	.0.898	لا يتوفر
الاطلاع على المخرجات مثل التقارير المالية أو الإدارية مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة للمستخدم.	29 49.2%	30 50.8%	1.49	−0.129	.0.898	لا يتوفر
شبكة الإنترانت الداخلية للشركة محمية بكلمات مرور.	39 66.1%	20 33.9%	1.66	2.591	0.012	يتوفر
يوجد برامج مرخصة للحماية من الفيروسات والتهديدات المختلفة.	41 69.5%	18 30.5%	1.69	3.224	0.002	يتوفر
يوجد برامج حماية من الفيروسات وبرامج جدران نارية.	39 66.1%	20 33.9%	1.66	2.591	0.012	يتوفر
يتم حجب مواقع الأنترنت والبريد الالكتروني غير الرسمية.	9 15.3%	50 84.7%	1.15	−7.360	0.000	لا يتوفر
البرامج المحاسبية والمالية محمية بكلمات مرور.	40 67.8%	19 32.2%	1.68	2.901	0.050	يتوفر
يوجد شاشة Screen Saver محمية بكلمة مرور.	19 32.2%	40 67.8%	1.32	−2.901	0.005	لا يتوفر
عدم الوصول للأجهزة داخل الشركة من خلال الشبكة.	28 47.5%	31 52.5%	1.47	−0.388	0.700	لا يتوفر
وجود برامج تجعل الجهاز يغلق عندما يحاول أحد غير مصرح له الدخول للنظام.	24 40.7%	35 59.3%	1.41	−1.445	0.154	لا يتوفر
يتم حماية المجلدات الموجودة على الحاسوب (الملفات) بكلمات مرور.	17 28.8%	42 71.2%	1.29	−3.563	0.001	لا يتوفر
شاشات النظام الإداري والمحاسبي تختلف من شخص لأخر حسب الصلاحيات.	25 42.4%	34 57.6%	1.42	−1.175	.0.245	لا يتوفر
القيام بإعداد نسخ احتياطية من البيانات والمخرجات باستخدام وسائل تخزين خارجية.	29 49.2%	30 50.8%	1.49	−.129	0.892	لا يتوفر
عند إدخال اسم مستخدم أو كلمة مرور خاطئة ثلاث مرات تتعطل شاشة الإدخال.	13 22.0%	46 78.0%	1.22	−5.139	0.000	لا يتوفر
متغير الوصول المنطقي للنظام	**28 47.5%**	**31 52.5%**	**1.48**	**−0.615**	**0.541**	**لا يتوفر**

الجدول (7)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي: قطاع الخدمات

اسم المتغير	المقوم		المتوسطات	قيمة ت	المعنوية	القرار
	يتوفر	لا يتوفر	الحسابية	المحسوبة	الإحصائية	
يتم وضع أجهزة الحاسوب ومعداته في غرف مغلقة.	19 32.3%	40 67.8%	1.32	-2.901	0.005	لا يتوفر
عدم قدرة أي شخص غير مخول له للوصول للأجهزة والمعدات الحاسوبية.	31 52.5%	28 47.5%	1.53	0.388	0.700	لا يتوفر
وجود أجهزة إنذار للكشف عن دخول الأشخاص غير المخول لهم.	18 30.5%	41 69.5%	1.31	-3.224	0.002	لا يتوفر
يوجد أقفال على أجهزة الحاسوب (قفل الصندوق بقفل).	15 25.4%	44 74.6%	1.25	-4.298	0.000	لا يتوفر
تم تعطيل مداخل USB.	3 5.1%	56 94.9%	1.05	-15.571	0.000	لا يتوفر
تم تعطيل القرص المضغوط CD-ROM.	4 6.8%	55 93.2%	1.07	-13.093	0.000	لا يتوفر
يوجد كاميرات تصوير مقابل أجهزة الحاسوب والمعدات.	13 22%	46 78%	1.22	-5.139	0.000	لا يتوفر
فقط الأشخاص المخولون يمكنهم الدخول لغرفة الحاسوب والمعدات المساندة.	36 61%	23 39%	1.61	1.720	0.091	لا يتوفر
يوجد حساسات دخان وحرائق في غرف أجهزة الحاسوب.	13 22%	46 78%	1.22	-5.139	0.000	لا يتوفر
من الصعب فك جهاز الكمبيوتر والمعدات المرتبطة به.	13 22%	46 78%	1.22	-5.139	0.000	لا يتوفر
يوجد سجل يدون فيه أسماء الضيوف الذين يدخلون لاماكن العمل.	11 18.6%	48 81.4%	1.19	-6.132	0.000	لا يتوفر
عدم ظهور كوابل الانترنت للعيان.	33 55.9%	26 44.1%	1.56	0.910	0.367	لا يتوفر
لا يتم ترك الحاسوب المحمول الخاص بالشركة بالسيارة.	40 67.8%	19 32.2%	1.68	2.901	0.005	يتوفر
قطع الكمبيوتر مؤمنه بغرف محكمة الإغلاق.	24 40.7%	35 59.3%	1.41	-1.445	0.154	لا يتوفر
أجهزة الكمبيوتر القديمة يتم إتلافها وتحديداً القرص الصلب.	29 49.2%	30 50.8%	1.49	-0.129	0.898	لا يتوفر
وسائل التخزين المنقولة يتم تأمينها بكلمات سر.	36 61%	23 39%	1.61	1.720	0.091	لا يتوفر
عدم ظهور أسلاك الهاتف والانترنت (تكون داخل الحائط او تحت البلاط).	30 50.8%	29 49.2%	1.51	0.129	0.898	لا يتوفر
يتم حفظ النسخ الورقية من المعلومات المالية بداخل خزائن مغلقة.	37 62.7%	22 37.3%	1.63	2.002	0.050	يتوفر
متغير الوصول المادي للنظام	**22 37.3%**	**37 62.7%**	**1.38**	**-3.185**	**0.002**	**لا يتوفر**

ويتضح من الجدول رقم 7 أن نظام المعلومات المحاسبي في الشركات الخدماتية المساهمة العامة يعاني من قصور في كثير من النواحي كما ذكر سابقاً في توافر مستوى مقبول من المقومات اللازمة للحد من الوصول المادي لأجهزة الحاسب والمعدات المتعلقة بنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المادي 3.185- عند مستوى أهمية إحصائية 0.002، وهذا يقود لنتيجة مفادها وجود تدنٍ في مستوى نظام الرقابة الداخلي للشركة الخدمية والمتخصص بالحد من تهديدات مخاطر الوصول المادي لأجهزة الحاسوب والمعدات المرتبطة به.

ثالثاً: تقويم مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول (المنطقي والمادي) لنظام المعلومات المحاسبي في الشركات المساهمة الفلسطينية المصرفية.

يتضح من الجدول رقم 8 أن هناك قصوراً ضئيلاً يتمثل في جانبين متعلقين بأمن الوصول المنطقي لنظام المعلومات المحاسبي في البنوك وهما: أنه يمكن الوصول لأجهزة الحاسب في البنك من خلال الشبكة، وكذلك فإنه لا تتم حماية المجلدات الموجودة على الحاسوب (الملفات) بكلمات مرور. ويبين الجدول رقم 8 أن نظام المعلومات المحاسبي في البنوك الفلسطينية يتمتع بمستوى عالٍ من الأمن الخاص بالحد من تهديدات مخاطر الوصول المنطقي حيث يتوافر مستوى متميز من المقومات اللازمة للحد من الوصول المنطقي لنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المنطقي 19.61 عند مستوى أهمية إحصائية 0.00 وهذا يقود لنتيجة مفادها وجود نظام رقابة داخلي قوي في البنك يعمل على الحد من تهديدات مخاطر الوصول المنطقي للبيانات المعالجة ومخرجات النظام.

أما الجدول رقم 9 فيعرض مدى توافر المقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول المادي (لمعدات النظام: الحاسب والمعدات المرتبطة به) لنظام المعلومات المحاسبي في البنوك الفلسطينية، ويلاحظ توافر هذه المقومات الرقابية بشكل مميز، وتتمثل فيما يلي: أنه يتم وضع أجهزة الحاسوب ومعداته في غرف مغلقة، وأيضاً لا يستطيع أي موظف غير مخول الوصول للأجهزة والمعدات الحاسوبية، ويوجد في البنوك الفلسطينية أجهزة إنذار للكشف عن دخول هؤلاء الأشخاص، كما يوجد كاميرات تصوير مقابل أجهزة الحاسوب والمعدات، والأشخاص المخولون فقط يتمكنون من الدخول الى غرفة الحاسوب

والمعدات المساندة، كما يوجد حساسات دخان وحرائق في غرف أجهزة الحاسوب، وكذلك من الصعب فك جهاز الكمبيوتر والمعدات المرتبطة به، ويتوافر في البنوك الفلسطينية سجل تدون فيه أسماء الضيوف الذين يدخلون لأماكن العمل، وأن كوابل الإنترنت والهاتف لا تظهر للعيان، وأنه لا يتم ترك الحاسوب المحمول الخاص بالبنك بالسيارة، وأن قطع الكمبيوتر مؤمنة بغرف محكمة الإغلاق، وأيضاً فإن أجهزة الكمبيوتر القديمة يتم إتلافها وتحديداً القرص الصلب، وأن وسائل التخزين المنقولة يتم تأمينها بكلمات سر، وأيضاً يتم حفظ النسخ الورقية من المعلومات المالية داخل خزائن مغلقة. وأيضاً يتضح من الجدول رقم 9 أن هناك قصوراً ضئيلاً يتمثل في ثلاثة جوانب متعلقة بأمن الوصول المادي لنظام المعلومات المحاسبي في البنوك وهي: عدم وجود أقفال على أجهزة الحاسوب، وأنه لا يتم تعطيل مداخل USB والقرص المضغوط CD-ROM في البنوك الفلسطينية. ويبين الجدول رقم 9 أن نظام المعلومات المحاسبي في البنوك الفلسطينية يتمتع بمستوى عالٍ من الأمن الخاص بالحد من تهديدات مخاطر الوصول المادي كما وضح سابقاً، حيث يتوافر مستوى متميز من المقومات اللازمة للحد من الوصول المادي لنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المادي 14.68 عند مستوى أهمية إحصائية 0.00 وهذا يقود لنتيجة مفادها وجود نظام رقابة داخلي بمستوى عالٍ من الكفاءة في البنك يعمل على الحد من تهديدات مخاطر الوصول المادي لأجهزة الحاسوب والمعدات المتعلقة به.

رابعاً: تقويم مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول (المنطقي والمادي) لنظام المعلومات المحاسبي في شركات التامين المساهمة العامة الفلسطينية.

يبين الجدول رقم 10 أن نظام المعلومات المحاسبي في شركات التامين الفلسطينية يتمتع بمستوى عالٍ من الأمن الخاص بالحد من تهديدات مخاطر الوصول المنطقي كما وضح سابقاً، حيث يتوافر مستوى متميز من المقومات اللازمة للحد من الوصول المنطقي لنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المنطقي 16.08 عند مستوى أهمية إحصائية 0.00 وهذا يقود لنتيجة مفادها وجود نظام رقابة داخلي قوي في شركات التامين الفلسطينية يعمل على الحد من تهديدات مخاطر الوصول المنطقي للبيانات والمعالجة ومخرجات النظام.

الجدول (8)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المنطقي لنظام المعلومات المحاسبي: قطاع البنوك

اسم المتغير	المقوم		المتوسطات الحسابية	قيمة ت المحسوبة	المعنوية الإحصائية	القرار
	يتوفر	لا يتوفر				
يوجد كلمة مرور واسم دخول لبرامج الشركة لكل موظف.	59 100%	0 00.0%	2.00	7.36	0.000	يتوفر
يتم استخدام طرفيات (لوحة مفاتيح وشاشة) بدون وجود جهاز الكمبيوتر، بمعنى وجود جهاز حاسوب مركزي (Server).	50 84.7%	9 15.3%	1.85	19.61	0.000	يتوفر
عند دخولك لحسابك كمستخدم للبرامج فان بعض المهام معطلة حسب صلاحياتك.	57 96.6%	2 03.4%	1.97	10.03	0.000	يتوفر
إدخال البيانات مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	53 89.8%	6 10.2%	1.90	10.03	0.000	يتوفر
معالجة البيانات مصرح بها لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	53 89.8%	6 10.2%	1.90	10.03	0.000	يتوفر
الاطلاع على المخرجات مثل التقارير المالية أو الإدارية مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة للمستخدم.	53 89.8%	6 10.2%	1.90	8.98	0.000	يتوفر
شبكة الإنترانت الداخلية للشركة محمية بكلمات مرور.	52 88.1%	7 11.9%	1.88	5.61	0.000	يتوفر
يوجد برامج مرخصة للحماية من الفيروسات والتهديدات المختلفة.	47 79.7%	12 20.3%	1.80	6.13	0.000	يتوفر
يوجد برامج حماية من الفيروسات وبرامج جدران نارية.	48 81.4%	11 18.6%	1.81	13.09	0.000	يتوفر
يتم حجب مواقع الأنترنت والبريد الالكتروني غير الرسمية.	55 93.2%	4 06.8%	1.93	8.10	0.000	يتوفر
البرامج المحاسبية والمالية محمية بكلمات مرور.	59 100%	0 00.0%	2.00	7.36	0.000	يتوفر
يوجد شاشة Screen Saver محمية بكلمة مرور.	51 86.4%	8 13.6%	1.86	19.61	0.000	يتوفر
عدم الوصول للأجهزة داخل الشركة من خلال الشبكة.	29 49.2%	30 50.8%	1.49	0.129	0.898	لا يتوفر
وجود برامج تجعل الجهاز يغلق عندما يحاول أحد غير مصرح له الدخول للنظام.	57 96.6%	2 03.4%	1.97	10.03	0.000	يتوفر
يتم حماية المجلدات الموجودة على الحاسوب (الملفات) بكلمات مرور.	30 50.8%	29 49.2%	1.51	−0.648	0.520	لا يتوفر
شاشات النظام الإداري والمحاسبي تختلف من شخص لأخر حسب الصلاحيات.	53 89.8%	6 10.2%	1.90	10.03	0.000	يتوفر
القيام بإعداد نسخ احتياطية من البيانات والمخرجات باستخدام وسائل تخزين خارجية.	27 45.8%	32 54.2%	1.46	15.63	0.000	يتوفر
عند إدخال اسم مستخدم أو كلمة مرور خاطئة ثلاث مرات تتعطل شاشة الإدخال.	53 89.8%	6 10.2%	1.90	7.36	0.000	يتوفر
متغير الوصول المنطقي للنظام	**49 83%**	**10 17%**	**1.83**	**19.61**	**0.000**	**يتوفر**

الجدول (9)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي: قطاع البنوك

اسم المتغير	المقوم		المتوسطات الحسابية	قيمة ت المحسوبة	المعنوية الإحصائية	القرار
	يتوفر	لا يتوفر				
يتم وضع أجهزة الحاسوب ومعداته في غرف مغلقة.	50 84.7%	9 15.3%	1.85	7.360	0.000	يتوفر
عدم قدرة أي شخص غير مخول له للوصول للأجهزة والمعدات الحاسوبية.	51 86.4%	8 13.6%	1.86	8.106	0.000	يتوفر
وجود أجهزة إنذار للكشف عن دخول الأشخاص غير المخول لهم.	57 96.6%	2 03.4%	1.97	19.61	0.000	يتوفر
يوجد أقفال على أجهزة الحاسوب (قفل الصندوق بقفل).	30 50.8%	29 49.2%	1.51	0.129	0.898	لا يتوفر
تم تعطيل مداخل USB.	26 44.1%	33 55.9%	1.44	0.910	0.367	لا يتوفر
تم تعطيل القرص المضغوط CD-ROM.	27 45.8%	32 54.2%	1.46	-0.648	0.520	لا يتوفر
يوجد كاميرات تصوير مقابل أجهزة الحاسوب والمعدات.	52 88.1%	7 11.9%	1.88	8.981	0.000	يتوفر
فقط الأشخاص المخولون يمكنهم الدخول لغرفة الحاسوب والمعدات المساندة.	49 83.1%	10 16.9%	1.83	6.709	0.000	يتوفر
يوجد حساسات دخان وحرائق في غرف أجهزة الحاسوب.	48 81.4%	11 18.6%	1.81	6.132	0.000	يتوفر
من الصعب فك جهاز الكمبيوتر والمعدات المرتبطة به.	53 89.8%	6 10.2%	1.90	10.04	0.000	يتوفر
يوجد سجل يدون فيه أسماء الضيوف الذين يدخلون لاماكن العمل.	43 72.9%	16 27.1%	1.73	3.920	0.000	يتوفر
عدم ظهور كوابل الانترنت للعيان.	46 78%	13 22%	1.78	5.139	0.000	يتوفر
لا يتم ترك الحاسوب المحمول الخاص بالشركة بالسيارة.	46 78%	13 22%	1.78	5.139	0.000	يتوفر
قطع الكمبيوتر مؤمنه بغرف محكمة الإغلاق.	53 89.8%	6 10.2%	1.90	10.04	0.000	يتوفر
أجهزة الكمبيوتر القديمة يتم إتلافها وتحديداً القرص الصلب.	40 67.8%	19 32.2%	1.68	2.901	0.005	يتوفر
وسائل التخزين المنقولة يتم تأمينها بكلمات سر.	51 86.4%	8 13.6%	1.86	8.106	0.000	يتوفر
عدم ظهور أسلاك الهاتف والانترنت (تكون داخل الحائط او تحت البلاط).	43 72.9%	16 27.1%	1.73	3.920	0.000	يتوفر
يتم حفظ النسخ الورقية من المعلومات المالية بداخل خزائن مغلقة.	50 84.7%	9 15.3%	1.85	7.360	0.000	يتوفر
متغير الوصول المادي للنظام	**45 76.3%**	**14 23.7%**	**1.77**	**14.68**	**0.000**	**يتوفر**

الجدول (10)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المنطقي لنظام المعلومات المحاسبي: قطاع التامين

اسم المتغير	المقوم		المتوسطات	قيمة ت	المعنوية	القرار
	يتوفر	لا يتوفر	الحسابية	المحسوبة	الإحصائية	
يوجد كلمة مرور واسم دخول لبرامج الشركة لكل موظف.	41 97.6%	1 %2.4	1.98	20.00	0.000	يتوفر
يتم استخدام طرفيات (لوحة مفاتيح وشاشة) بدون وجود جهاز الكمبيوتر، بمعنى وجود جهاز حاسوب مركزي (Server).	39 96.6%	3 7.1%	1.93	10.65	0.000	يتوفر
عند دخولك لحسابك كمستخدم للبرامج فان بعض المهام معطلة حسب صلاحياتك.	39 96.6%	3 7.1%	1.76	3.937	0.000	يتوفر
إدخال البيانات مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	32 76.2%	10 23.8%	1.98	20.00	0.000	يتوفر
معالجة البيانات مصرح بها لعدد محدد من الأشخاص ضمن الصلاحيات المخولة.	41 97.6%	1 %2.4	1.98	20.00	0.000	يتوفر
الاطلاع على المخرجات مثل التقارير المالية أو الإدارية مصرح به لعدد محدد من الأشخاص ضمن الصلاحيات المخولة للمستخدم.	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
شبكة الإنترانت الداخلية للشركة محمية بكلمات مرور.	37 88.1%	5 %11.9	1.88	7.53	0.000	يتوفر
يوجد برامج مرخصة للحماية من الفيروسات والتهديدات المختلفة.	33 78.6%	9 21.4%	1.79	4.45	0.000	يتوفر
يوجد برامج حماية من الفيروسات وبرامج جدران نارية.	35 83.3%	7 %16.7	1.83	5.72	0.000	يتوفر
يتم حجب مواقع الأنترنت والبريد الالكتروني غير الرسمية.	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
البرامج المحاسبية والمالية محمية بكلمات مرور.	41 97.6%	1 %2.4	1.98	20.00	0.000	يتوفر
يوجد شاشة Screen Saver محمية بكلمة مرور.	37 88.1%	5 %11.9	1.88	7.53	0.000	يتوفر
عدم الوصول للأجهزة داخل الشركة من خلال الشبكة.	33 78.6%	9 21.4%	1.79	4.45	0.000	لا يتوفر
وجود برامج تجعل الجهاز يغلق عندما يحاول أحد غير مصرح له الدخول للنظام.	38 90.5%	4 9.5%	1.90	8.82	0.000	يتوفر
يتم حماية المجلدات الموجودة على الحاسوب (الملفات) بكلمات مرور.	24 57.1%	18 42.9%	1.57	0.924	0.361	لا يتوفر
شاشات النظام الإداري والمحاسبي تختلف من شخص لأخر حسب الصلاحيات.	41 97.6%	1 %2.4	1.98	20.00	0.000	يتوفر
القيام بإعداد نسخ احتياطية من البيانات والمخرجات باستخدام وسائل تخزين خارجية.	37 88.1%	5 11.9%	1.88	7.53	0.000	يتوفر
عند إدخال اسم مستخدم أو كلمة مرور خاطئة ثلاث مرات تتعطل شاشة الإدخال.	34 81%	8 19%	1.81	5.04	0.000	يتوفر
متغير الوصول المنطقي للنظام	**36 85.7%**	**6 12.5%**	**1.87**	**16.08**	**0.000**	**يتوفر**

الجدول (11)

مدى توافر الأسس الرقابية اللازمة للحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي: قطاع التامين

اسم المتغير	المقوم		المتوسطات الحسابية	قيمة ت المحسوبة	المعنوية الإحصائية	القرار
	يتوفر	لا يتوفر				
يتم وضع أجهزة الحاسوب ومعداته في غرف مغلقة.	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
عدم قدرة أي شخص غير مخول له للوصول للأجهزة والمعدات الحاسوبية.	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
وجود أجهزة إنذار للكشف عن دخول الأشخاص غير المخول لهم.	39 96.6%	3 7.1%	1.93	10.65	0.000	يتوفر
يوجد أقفال على أجهزة الحاسوب (قفل الصندوق بقفل).	37 88.1%	5 11.9%	1.88	7.53	0.000	يتوفر
تم تعطيل مداخل USB.	33 78.6%	9 21.4%	1.79	4.45	0.000	يتوفر
تم تعطيل القرص المضغوط CD-ROM.	38 90.5%	4 9.5%	1.90	8.82	0.000	يتوفر
يوجد كاميرات تصوير مقابل أجهزة الحاسوب والمعدات.	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
فقط الأشخاص المخولون يمكنهم الدخول لغرفة الحاسوب والمعدات المساندة.	41 97.6%	1 %2.4	1.98	20.00	0.000	يتوفر
يوجد حساسات دخان وحرائق في غرف أجهزة الحاسوب.	41 97.6%	1 %2.4	1.98	20.00	0.000	يتوفر
صعوبة فك جهاز الكمبيوتر والمعدات المرتبطة به.	39 96.6%	3 7.1%	1.93	10.65	0.000	يتوفر
يوجد سجل يدون فيه أسماء الضيوف الذين يدخلون لاماكن العمل.	37 88.1%	5 11.9%	1.88	7.53	0.000	يتوفر
عدم ظهور كوابل الانترنت للعيان.	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
لا يتم ترك الحاسوب المحمول الخاص بالشركة في السيارة.	18 42.9%	24 57.1%	1.43	-0.920	0.361	لا يتوفر
قطع الكمبيوتر مؤمنه بغرف محكمة الإغلاق.	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
أجهزة الكمبيوتر القديمة يتم إتلافها وتحديداً القرص الصلب.	39 96.6%	3 7.1%	1.93	10.65	0.000	يتوفر
وسائل التخزين المنقولة يتم تأمينها بكلمات سر.	35 83.3%	7 16.7%	1.83	5.720	0.000	يتوفر
عدم ظهور أسلاك الهاتف والانترنت (تكون داخل الحائط أو تحت البلاط).	40 95.2%	2 4.8%	1.95	13.60	0.000	يتوفر
يتم حفظ النسخ الورقية من المعلومات المالية بداخل خزائن مغلقة.	38 90.5%	4 9.5%	1.90	8.82	0.000	يتوفر
متغير الوصول المادي للنظام	**37 88.1%**	**5 11.9%**	**1.89**	**14.92**	**0.000**	**يتوفر**

ويبيّن الجدول رقم 11 أن نظام المعلومات المحاسبي في شركات التامين الفلسطينية يتمتع بمستوى عالٍ من الأمن الخاص يحد من تهديدات مخاطر الوصول المادي كما وضح سابقاً حيث يتوافر مستوى متميز من المقومات اللازمة للحد من الوصول المادي لنظام المعلومات المحاسبي، وتم استخدام اختبار One Sample T Test عند نقطة اختبار 1.5، حيث بلغت قيمة T المحسوبة لمتغير الحد من الوصول المادي 14.92 عند مستوى أهمية إحصائية 0.00 وهذا يقود لنتيجة مفادها وجود نظام رقابة داخلي بمستوى عالٍ من الكفاءة في شركة التامين يعمل على الحدّ من تهديدات مخاطر الوصول المادي لأجهزة الحاسوب والمعدات المتعلقة به.

الجزء الثاني: نتائج اختبار الفرضية الثالثة والرابعة

يعرض هذا الجزء من الدراسة نتائج اختبار فرضيات الدراسة الثالثة والرابعة آخذين بعين الاعتبار المسلمات الآتية:

أولاً: تحديد مدى وجود فروق ذات دلالة إحصائية في متوسط وجهة نظر المستجوبين حول مدى حجم تهديدات الوصول المنطقي لمكونات نموذج النظام المحاسبي في الشركات الفلسطينية تعزى للقطاع.

ثانياً: تحديد مدى وجود فروق ذات دلالة إحصائية في متوسط وجهة نظر المستجوبين حول حجم تهديدات الوصول المادي لمكونات النظام المحاسبي في الشركات الفلسطينية تعزى للقطاع.

ولاختبار الفرضية الثالثة (الموضحة بأولاً أعلاه)، وفرضية الدراسة الرابعة (الموضحة بثانياً أعلاه) تم استخدام اختبار غير معلمي وهو اختبار Kruskal–Wallis الذي يقوم بترتيب القطاعات حسب كفاءة تصميم نظام رقابي للحد من تهديدات مخاطر الوصول المنطقي والمادي لنظام المعلومات المحاسبي.

وفيما يلي عرض لنتائج التحليل:

يتضح من الجدول رقم 12 أن هناك فروقاً ذات دلالة إحصائية في متوسط وجهة نظر المستجوبين حول مدى حجم تهديدات الوصول المنطقي لمكونات نموذج النظام المحاسبي في الشركات الفلسطينية تعزى للقطاع، حيث بلغت قيمة Chi–Square 111.722 عند مستوى معنوية إحصائية 0.000، ويتضح من الجدول أن قطاع التامين يحتل المرتبة الأولى في توفيره للمقومات الرقابية اللازمة للحد من تهديدات مخاطر الوصول المنطقي لنظام المعلومات المحاسبي، ويليه قطاع البنوك، ثم القطاع الخدماتي، وأخيراً قطاع الصناعة.

الجدول (12)

رتب توافر نظام أمن للحد من تهديدات الوصول المنطقي للنظام حسب القطاع باستخدام إحصائية Kruskal–Wallis

القطاع	متوسط الرتب Mean Rank	ترتيب القطاعات حسب كفاءة نظام الأمن للحد من تهديدات الوصول المنطقي
قطاع التامين	156.83	الأول: مستوى عال من كفاءة نظام الأمن للحد من تهديدات الوصول المنطقي.
قطاع البنوك	145.25	الثاني: مستوى عال من كفاءة نظام الأمن للحد من تهديدات الوصول المنطقي.
قطاع الخدمات	81.53	الثالث: عدم وجود نظام أمن للحد من تهديدات الوصول المنطقي.
قطاع الصناعة	47.05	الرابع: عدم وجود نظام امن للحد من تهديدات الوصول المنطقي.
قيمة Chi–Square تساوي 111.722، وقيمة درجات الحرية DF تساوي 3، وقيمة المعنوية الإحصائية تساوي 0.000.		
ملاحظة: عندما تكون قيمة المعنوية الإحصائية تساوي أو اقل من 0.05 يتم قبول الفرضية البديلة أي يوجد فروق، أما إذا كانت قيمة المعنوية الإحصائية أكبر من 0.05 فانة لا يوجد فروق (أي يتم قبول الفرضية الصفرية).		

ويتبين من الجدول رقم 13 أن هناك فروقاً ذات دلالة إحصائية في متوسط وجهة نظر المستجوبين حول مدى حجم تهديدات الوصول المادي لمكونات نموذج النظام المحاسبي في الشركات الفلسطينية تعزى للقطاع، حيث بلغت قيمة Chi–Square 124.722 عند مستوى معنوية إحصائية 0.000، ويتضح من الجدول رقم 13 أن قطاع التأمين يحتل المرتبة الأولى في توفيره للمقومات الرقابية اللازمة للحد من تهديدات الوصول المادي لنظام المعلومات المحاسبي، ويليه قطاع البنوك، ثم القطاع الخدماتي، وأخيراً قطاع الصناعة.

الجدول (13)

رتب توافر نظام أمن للحد من تهديدات الوصول المادي للنظام حسب القطاع باستخدام إحصائية Kruskal–Wallis

القطاع	متوسط الرتب Mean Rank	ترتيب القطاعات حسب كفاءة نظام الأمن للحد من تهديدات الوصول المنطقي
قطاع التامين	170.44	الأول: مستوى عال من كفاءة نظام الأمن للحد من تهديدات الوصول المادي
قطاع البنوك	139.32	الثاني: مستوى عال من كفاءة نظام الأمن للحد من تهديدات الوصول المادي
قطاع الخدمات	76.51	الثالث: عدم وجود نظام أمن للحد من تهديدات الوصول المادي
قطاع الصناعة	48.50	الرابع: عدم وجود نظام امن للحد من تهديدات الوصول المادي
قيمة Chi–Square تساوي 124.722، وقيمة درجات الحرية DF تساوي 3، وقيمة المعنوية الإحصائية تساوي 0.000		
ملاحظة: عندما تكون قيمة المعنوية الإحصائية تساوي أو اقل من 0.05 يتم قبول الفرضية البديلة أي يوجد فروق، أما إذا كانت قيمة المعنوية الإحصائية أكبر من 0.05 فانة لا يوجد فروق (أي يتم قبول الفرضية الصفرية).		

نتائج البحث

توصلت الدراسة لعدد من النتائج هي:

أولاً: يحتل قطاع التأمين الفلسطيني المرتبة الأولى في قدرته على إنشاء بيئة رقابية عالية المستوى، تعمل على الحد من تهديدات الوصول المنطقي لبيانات النظام المحاسبي وعمليات معالجة البيانات والاطلاع على مخرجات النظام. ويحتل القطاع

المصرفي الفلسطيني المرتبة الثانية من حيث امتلاكه لبيئة رقابية عالية الجودة، تعمل على الحد من تهديدات مخاطر الوصول المنطقي لبيانات النظام المحاسبي وعمليات معالجة البيانات والاطلاع على مخرجات النظام، وهذه النتائج تتفق مع نتائج دراسة (Bawaneh, 2014)، ودراسة (Financial Conduct Authority– London, 2013)، ودراسة (Al Hanini, 2012)، ودراسة (هلدني، والغبان، 2010)، ودراسة (Hayale and Abu Khadra, 2008)، ودراسة (البحيصي، والشريف، 2008).

ثانياً: إن قطاع الخدمات الفلسطيني يعاني من مشكلة حقيقية فيما يتعلق بتوافر المقومات اللازمة؛ للحد من مخاطر الوصول المنطقي لبيانات النظام المحاسبي وعمليات معالجة البيانات والاطلاع على مخرجات النظام. وهذه النتائج تتفق مع نتائج دراسة (Mathias and Ogundeji, 2013).

ثالثاً: إن قطاع الصناعة الفلسطيني كان الأكثر ضعفاً من حيث قدرته على صياغة الحد الأدنى من المقومات الرقابية اللازمة للحد من الوصول المنطقي والمادي لنظام المعلومات المحاسبي؛ وهذه النتائج تتفق مع نتائج دراسة (Cheh et al., 2010).

التوصيات

بناء على النتائج السابقة، فإن هذه الدراسة جاءت بعدد من التوصيات هي:

1- توصي الدراسة قطاعي الصناعة والخدمات بإعادة تصميم نظام رقابي يعمل على الحد من تهديدات الوصول المنطقي والمادي لنظام المعلومات المحاسبي، وذلك بسبب ما تعانيه هذه القطاعات من افتقار شديد لتوفر المقومات الرقابية اللازمة للحد من هذه التهديدات.

2- من الضروري أن يقوم مجلس إدارة الشركة المساهمة العامة الفلسطينية بإلزام وحدة الرقابة الداخلية للقيام بتصميم أنموذج رقابي يعمل على الحد من تهديدات مخاطر الوصول المنطقي والمادي لنظام المعلومات المحاسبي، ويمكن الاستفادة من هذه الدراسة في الاسترشاد بالمطلوب لتعزيز ذلك.

3- ضرورة قيام هيئة سوق رأس المال الفلسطينية وإدارة سوق فلسطين للأوراق المالية بوضع أنظمة وتعليمات تلزم الشركات المساهمة العامة الفلسطينية المدرجة في بورصة فلسطين بتطبيق أنموذج للحد من تهديدات مخاطر الوصول المنطقي والمادي لنظام المعلومات المحاسبي؛ بسبب أهمية ذلك في حماية حقوق المساهمين وذوي العلاقة ومصالحهم.

4 – من الضروري أن يتم تعديل أنظمة الرقابة الداخلية بشكل مستمر لمواكبة التحديات المستجدة.

المراجع

أولاً: المراجع العربية

1. إسماعيل حسين احمرو، (2006)، أسباب ضعف الإجراءات الرقابية في نظم المعلومات المحاسبية: دراسة تحليليه، تنميه الرافدين، 82(28)، ص 21–42.
2. آلان عجيب هلدني، وثائر صبري الغبان، (2010)، دور الرقابة الداخلية في ظل نظام المعلومات المحاسبي الالكتروني دراسة تطبيقية على عينة من المصارف في إقليم كردستان العراق، مجلة علوم إنسانية، 45 (7)، ص 1 – 39.
3. رشا حمادة، (2010)، اثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية في زيادة موثوقية المعلومات المحاسبية: دراسة ميدانية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، 1 (26)، ص 305 – 334.
4. عصام محمد البحيصي، وحرية شعبان الشريف، (2008)، مخاطر نظم المعلومات المحاسبية الالكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة، مجلة الجامعة الإسلامية: سلسلة الدراسات الإنسانية، 2 (16)، ص 895 – 923.

ثانياً: المراجع الأجنبية

5. Abdallah, A. (2013). The Impact of Using Accounting Information Systems on the Quality of Financial Statements Submitted to the Income and Sales Tax Department in Jordan. European Scientific Journal. Vol. 1. PP 41-48.
6. Abu-Musa, A. (2006). Exploring Perceived Threats of CAIS in Developing Countries: the Case of Saudi Arabia. Managerial Auditing Journal. Vol. 21, issue 4. PP 387 – 407.
7. Ahmad, M. (2012). Problems and Internal Control Issues in AIS from the View Point of Jordanian Certified Public Accountants. Journal of Emerging Trends in Computing and Information Sciences. Vol. 3, no. 12. PP 1622-1625.
8. Al Hanini, E. (2012). The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks; their Reasons and Ways of Prevention. European Journal of Business and Management. Vol. (4), issue (20). PP 53 – 63.

9. Alzoubi, A. (2011). The Effectiveness of the Accounting Information System under the Enterprise Resources Planning (ERP). Research Journal of Finance and Accounting. Vol 2, no 11. PP 10 -18
10. Amiri, A. (2014). Effect of Accounting Information System (AIS) on Software Qualitative. International Journal of Business and Management Invention. Volume 2, issue 4. PP 6-11.
11. Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Second Edition. John Wiley and Sons, Inc.
12. Arsenie-Samoil, M., and Cuza, M. (2011). Security of the Accounting Information System Infrastructure. Journal Ovidius University Annals, Economic Sciences Series. Volume XI, issue 1. PP 1339-1345.
13. Bawaneh, S. (2014). Information Security for Organizations and Accounting Information Systems: A Jordan Banking Sector Case. International. Review of Management and Business Research. Vol. 3, issue 2. PP 1174-1188.
14. Beneish, M., Billings M., and Hodder L. (2008). Internal Control Weaknesses and Information Uncertainty. The Accounting Review. Vol. 83, no. 3. PP 665-703.
15. Bodnar, G. and Hopwood W. (2010). Accounting Information Systems. Tenth Edition. Prentice Hall.
16. Bunke, M., Koschke, R., and Sohr, K. (2012). Organizing Security Patterns Related to Security and Pattern Recognition Requirement. International Journal on Advances in Security. Vol 5, no 1 & 2. PP 46-67.
17. Burtescu, E. (2009). Database Security-Attacks and Control Methods. Journal of Applied Quantitative Methods. Volume 4, issue 4. PP 449-454.
18. Campbell, K., Gordon, L., Loeb, M., and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. Journal of Computer Security. Volume 11, number 3. PP 431-448.
19. Cheh, J., Lee, J. and Kim, I. (2010). Determinants of Internal Control Weaknesses. Contemporary Management Research. Vol. 6, No. 2. PP 159-176.
20. CPA Australia. (2008). Internal Controls for Small Business. Copyright CPA Australia Ltd. Website: www.cpaaustralia.com.
21. Curtis M., and Borthick A. (1999). Evaluation of Internal Control from a Control Objective Narrative. Journal of Information Systems. Vol. 13, no. 1. PP 63-81.

22. Davis, E. (1997). An Assessment of Accounting Information Security. The CPA Journal. Vol. 67, no. 3. March.
23. Dhillon, G. (1999). Managing and Controlling Computer Misuse. Information Management & Computer Security. Vol. 7, number 4. PP. 171-175.
24. Fardinal, D. (2013). The Quality of Accounting Information and the Quality of Accounting Information Systems through the Internal Control System. Research Journal of Finance and Accounting. Vol 4, no 6. PP 156-161.
25. Financial Conduct Authority- London. (2013). Banks' Control of Financial Crime Risks in Trade Finance. Financial Conduct Authority :Thematic Review/ Financial Conduct Authority. PP 1-49.
26. Gul, F., and Chia, Y. (1994). The Effects of Management Accounting Systems, Perceived Environmental Uncertainty and Decentralization on Managerial Performance: A Test of Three-Way Interaction. Accounting, Organizations and Society. Volume 19, issues 4–5. PP 413–426.
27. Hall, J. (2011). Accounting Information System. 7th ed, South-Western Publishing Co.
28. Hayale, T. and Abu Khadra, H. (2008). Investigating Perceived Security Threats of Computerized Accounting Information Systems: An Empirical Research applied on Jordanian banking sector. Journal of Economic & Administrative Sciences. Vol. 24, no. 1, PP 41 – 67.
29. Henage, R. and Henage, D. (2013). Physical Security: The Weak Link in Internal Control Design?. American International Journal of Contemporary Research. Vol. 3, no. 10. PP 83-86.
30. Hildani, A. and A'anan, T. (2010). The Role of the Internal Control in Light of the Electronic Accounting Information Systems. The Journal of Humanities Sciences. Issue 45, PP 1-39.
31. Kanai, S., Nakamoto, K., Takemoto, A., and Furuya, M. (2014). Physical Security for Companies that Maintain Social Infrastructure. Hitachi Review. Vol. 63, no. 5. PP 40-44.
32. Konchitchki, Y. and O'Leary D. (2011). Event Study Methodologies in Information Systems Research. International Journal of Accounting Information Systems. Vol. (12), issue (2). PP 99 – 115.

33. Krishnan, R., Peters J., Padman R., and Kaplan D. (2005). On Data Reliability Assessment in Accounting Information Systems. Information Systems Research. Volume 16, issue 3. PP 307 – 326.
34. Mansour, E., Mohammad, A., Missi, F. and Hamdan A. (2009). Examining the Existence of (SYSTRUST) Model and its Impact on Jordanian Commercial Banks Performance. European and Mediterranean Conference on Information Systems (EMCIS2009). July 13-14. Crowne Plaza Hotel. Izmir.
35. Mndzebele, N. (2013). The Usage of Accounting Information Systems for Effective Internal Controls in the Hotels. International Journal of Advanced Computer Technology (IJACT). Vol 2, no 5. PP 156-161.
36. Muhrtala, T. and Ogundeji, M. (2013). Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case. Universal Journal of Accounting and Finance. Vol. (1), issue (1). PP 9 – 18.
37. Neogy, T. (2014). Evaluation of Efficiency of Accounting Information Systems: A Study on Mobile Telecommunication Companies in Bangladesh. Global Disclosure of Economics and Business. Volume 3, no 1. PP 40-55.
38. Romney, M. and Steinbart, P. (2003). Accounting Information System. Ninth Edition. Prentice Hall International Edition.
39. Sakni, S. and Awawda, H. (2011). The Risks of Using Information Technology and their Impact on the Performance of the Computerized Information Systems. Journal of Information Studies. Vol 11. PP 240-319.
40. Sarbanes-Oxley Act. (2002). The United States.
41. Sekaran U. and Bougie R. (2013). Research Methods for Business - A Skill-building Approach. 6th Edition. John Wiley & Sons, Inc.
42. Sun, L., Srivastava, R. and Mock T. (2006). An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions. Journal of Management Information Systems. Vol. 22, no. 4. PP 109-142.

Examining the Availability of the Required Controlling Procedures that Obstruct the Logical and Physical Access to AIS: the Case of the Listed Companies in the PEX

Zahran "Mohammad Ali" Daraghma[1], Suhaib Tawfiq Jarrar[2]
[1], [2]Accounting Department, Faculty of Administrative and Financial Sciences, Arab American University- Jenin
zahran.daraghma@aauj.edu[1], sjarrar@aauj.edu[2]

Abstract

This paper comes to examine the availability of the required controlling procedures that obstruct the logical and physical access threats that face the accounting information system (AIS) of the listed corporations in the Palestine Exchange; PEX: (industrial, service, banking and insurance sectors). Indeed, this study goes together with a specially designed questionnaire, used to answer the study questions. 280 questionnaires were distributed to the respondents (financial managers, accountants, internal auditors, computer employees and external auditors). 211 questionnaires, which statistically constitute (75.4%) of the study sample, were taken back. To achieve the previous objectives, a number of statistical methods have been used (Cronbach's Alpha, Descriptive Statistics, One Sample T Test, and Kruskal–Wallis). The findings show that both the banking and insurance sectors in Palestine possess the required controlling fundamentals that prevent the logical and physical access threats to the AIS. Another finding of this study states that the service and the industrial sectors in Palestine are highly under threat as they suffer from the lack and weakness of the availability of the fundamentals of controlling needed to prevent the logical access and the physical access threats to the AIS. However, the findings of this paper came up with the following recommendations: Firstly, PEX and board of directors of the listed corporations should obligate the companies to work on enhancing the controlling fundamentals that prevent the logical and physical access. Secondly, the industrial and the service sectors should take into account the importance of designing the logical and physical access landscapes to minimize the current threats that face the AIS.

Keywords: *Accounting information system, logical access, physical access, internal control, information security, corporations, Palestine Exchange.*