أثر مخاطر تكنولوجيا المعلومات على مكونات هيكل الرقابة الداخلية مسئولية مراجعي الحسابات عنها – دراسة ميدانية –

د. وليد سمير عبد العظيم الجبلى

معهد العبور العالي للإدارة والحاسبات ونظم المعلومات، مصر

Walidsamir7@gmail.com

Received: 07/07/2018 *Accepted: 04/06/2019*

ملخص:

تهدف الدراسة إلى معرفة أثر مخاطر تكنولوجيا المعلومات على المكونات الخمسة لنظام الرقابة الداخلية و مسئولية المراجع عن تلك المخاطر، وقد توصلت الدراسة الى مجموعة من النتائج أهمها ان للمخاطر تكنولوجيا المعلومات أثر بالغ على نظام وهيكل الرقابة الداخلية ،حيث سيتسع نطاق ومهام نظام الرقابة الداخلية ومن ثم تعرضه لمزيد من المخاطر تلك المخاطر جعلت مكونات وعناصر هيكل الرقابة الداخلية الخمس المتعارف عليها غير كافية لرقابة أنشطة تكنولوجيا المعلومات مما تطلب ضرورة تعديلها لتتلاءم مع أنشطة وخصائص تكنولوجيا المعلومات كإضافة عنصر الاستجابة للمخاطر .

الكلمات المفتاحية: مخاطر تكنولوجيا المعلومات، هيكل الرقابة الداخلية، مسئولية مراجعي الحسابات

Abstract:

The study aims at identifying the impact of information technology risk on the five components of the internal control system and the auditor's responsibility for these risks. The study reached a number of results, the most important of which is that the information technology risks have an impact on the internal control system and structure. Risk exposure The components and elements of the usual five internal control structure have not been sufficient to control IT activities and need to be adapted to the activities and characteristics of information technology, such as the addition of the risk response component.

keywords: *IT risk, internal control structure, auditor responsibility*

تمهيد:

رغم أن استخدام المنشآت لتكنولوجيا المعلومات حقق بعض المزايا خاصة تلك المتمثلة في زيادة بعض جوانب الرقابة الداخلية وزيادة الإنتاجية، إلا أن استخدامها عرض البيانات المحاسبية والمراجعين الذين يتعاملون مع هذه البيانات لمشاكل ومخاطر جديدة، تلك المشاكل والمخاطر كان لها أثرها على أساليب الرقابة المطبقة وأدوات وإجراءات الرقابة المستخدمة، حيث أكدت إحدى الدراسات (Debreceny Roger & G.L. Gray,2003,p36) "أنه من الممكن تغيير صياغة ملف كامل بمجرد أن يتاح للمستفيد الدخول إلى النظام التكنولوجي المستخدم التي يوجد عليها البيانات فإنه يستطيع بمهارة متواضعة تغير الملفات بدقة دون ترك أي أثر أو معرفة الفاعل أو الملف الذى أصابه التغيير"، وهناك من يؤكد على أن استخدام تكنولوجيا المعلومات قد غيرت من طريقة أداء الأعمال وأتاحت للمنشآت فرصة العمل في الأسواق الدولية والوصول إلى مستهلكين جدد وأصبح الاعتماد عليها من حقائق دنيا الأعمال بل وأصبحت من المقومات الأساسية لقدرة

المنشأة على المنافسة والاستمرار كما أصبحت أداة تساعد الإدارة على إدارة المنشأة واتخاذ القرارات (شريف سعيد البراد، 2000، ص 733) .

مشكلة البحث:

أن لتكنولوجيا المعلومات بالغ الأثر على نظام وهيكل الرقابة الداخلية، حيث سيتسع نطاق ومهام نظام الرقابة الداخلية ومن ثم تعرضه لمزيد من المخاطر أهمها :(فاروق جمعة ،2002، ص 277)

1- مخاطر تتعلق باختفاء الدليل المادي الملموس والتحول إلى استخدام الملفات الإلكترونية؛

2- مخاطر تتعلق بسند المراجع كعدم وجود دفاتر يومية؛

3- مخاطر تتعلق بارتكاب الغش وسهولة التلاعب؛

4- مخاطر اختراق النظام من قبل برامج أخرى (الفيروسات)؛

5- مخاطر الفصل غير الملائم بين المهام والوظائف؛

6- مخاطر الاعتماد الكلى على أنظمة الحاسب واعتماد بعض أساليب الرقابة اليدوية على نظم الرقابة الإلكترونية؛

7- مخاطر تركيز الوظائف والمعرفة في يد موظفين معينين، حيث أن هذا التركيز سوف يجعل الموظفين على علم بكيفية التشغيل وتوزيع المخرجات وعلى علم بنقاط الضعف في نظام الرقابة الداخلية ويكونوا في وضع يمكنهم من تغيير أو تعديل البيانات.

وعلى ذلك يمكن صياغة مشكلة الدراسة في السؤال التالي " هل هناك أثر للمخاطر التي أوجدتها تكنولوجيا المعلومات على المكونات الخمسة لنظام الرقابة الداخلية (بيئة الرقابة – تقييم المخاطر – أنشطة الرقابة – المعلومات والاتصال – المتابعة) وما هي حدود مسئولية المراجع عن تلك المخاطر "

هدف البحث:

الهدف الرئيسي للبحث هو: "تهدف الدراسة إلى معرفة أثر مخاطر تكنولوجيا المعلومات على المكونات الخمسة لنظام الرقابة الداخلية (بيئة الرقابة – تقييم المخاطر – أنشطة الرقابة – المعلومات والاتصال – المتابعة) ومسئولية المراجع عن تلك المخاطر "

فروض البحث:

تتأسس الدراسة في هذا البحث على فرض أساسي وهو تؤثر مخاطر تكنولوجيا المعلومات على تقييم المراجعين لنظام الرقابة الداخلية.

أهمية البحث:

تنبع أهمية البحث من الحاجة المتزايدة لمعرفة أثر المخاطر التي أوجدتها تكنولوجيا المعلومات على المكونات الخمسة لهيكل الرقابة الداخلية في ظل الاستخدام المتزايد لتكنولوجيا المعلومات من قبل المنشآت الهادفة وغير الهادفة للربح في عملياتها المختلفة، وبالتالي فإن البحث سوف يساهم في حل بعض المشاكل في مجال توجيه المراجعين نحو تقديرهم للمخاطر التي يجب أخذها في الاعتبار كمخاطر أمن وسلامة المعلومات، والعمل على توجيههم نحو زيادة الكفاءة والفاعلية وتحسين الأداء.

أسلوب البحث:

سوف يعتمد الباحث على أسلوب البحث المكتبي التحليلي الميداني من خلال استقراء أدبيات المراجعة الخاصة بتكنولوجيا المعلومات وأثرها على المكونات الخمس لنظم الرقابة الداخلية، مع الاهتمام بتحليل آراء ممارسي مهنة المراجعة في مصر من خلال قائمة الاستقصاء.

خطة البحث:

وعلى هذا سوف تتعرض الدراسة إلى ما يلي:

الفصل الاول: مخاطر تكنولوجيا المعلومات؛

الفصل الثاني: مزايا ومخاطر استخدام تكنولوجيا المعلومات في الرقابة الداخلية؛

الفصل الثالث: أدوات وإجراءات الرقابة الداخلية على أمن وسلامة المعلومات؛

الفصل الرابع: أثر استخدام تكنولوجيا المعلومات على مكونات هيكل الرقابة الداخلية؛

الفصل الخامس: الدراسة الميدانية.

الفصل الاول: مخاطر تكنولوجيا المعلومات.

يؤكد البعض على أن نظام المعلومات الإلكترونية يتعرض لكثير من المخاطر والتهديدات ومنها التلاعب في البيانات قصد تدميرها سواء بالحذف أو التغير أو الدمج غير الصحيح لبعضهما أو بخلطها ببيانات أخرى غير حقيقية أو تبويبها بشكل خاطئ تفقد معها مدلولها ومعناها (أحمد عبد القادر أحمد ، 2000، ص 60) وأن ذلك التلاعب يمكن أن يحدث في أجزاء مختلفة من نظام المعلومات المحاسبي المستخدم كحساب التكاليف – المخزون - النقدية 000 الخ، وقد يكون تدمير البيانات ناتجاً عن تغيير (تعديل) في البيانات (Modification) Data change بشكل لا يجعلها تعبر عن الحقائق التي نتجت عنها أصلاً مثل التلاعب في حسابات المدنيين والدائنين بقصد الغش، وقد يحدث هذا التلاعب في مراحل مختلفة عن النظام مثل المدخلات – التشغيل - التخزين أو المخرجات، ويمكن أن يكون تدمير البيانات جزئياً أو كلياً وفى الحالة الأخيرة قد يصعب تصحيح

البيانات أو استعارتها مما يشكل خسارة كبيرة لنظام المعلومات وما ينتجه من قرارات وقد يهدف التلاعب في النظام إلى الاطلاع على بيانات سرية Disclosure of Confidential Data مثل بيانات تخطيط الربحية أو بيانات الأفراد (الرواتب -الترقيات -العلاوات) ويمكن للمتلاعب في هذه الحالة ليس فقط الاطلاع على البيانات وإساءة استخدامها بل أيضاً سرقة بعضها أو كلها، ذلك كله قد ينتج عنه خسائر للمنشآت تكون كبيرة في بعض الحالات (أحمد عبد السلام أبو موسى ، 2000 ،ص 3)

وعلى هذا يمكن أن تعرف مخاطر تكنولوجيا المعلومات The Risk of IT بأنها: "إمكانية حدوث خسارة أو تدمير للبيانات أو استخدام البيانات أو البرامج بطريقة تضر بطرف آخر أو إمكانية حدوث أضرار بالأجهزة أو النظام سواء كانت تلك الخسارة ناتجة من الداخل أو الخارج بغرض تحقيق مصلحة شخصية أو بغرض اللعب أو العبث".

والجدير بالذكر أن هناك نوع من عدم التميز الواضح بين مخاطر أمن نظم المعلومات Security Threats وبين عدم كفاية الضوابط الرقابية لأمن تلك النظم Inadequacy of Security Controls فقد اعتبرت ضعف أو عدم كفاية بعض الأدوات والضوابط الرقابية المتعلقة بأمن نظم المعلومات على أنها تهديدات أو مخاطر لأمن تلك النظم على سبيل المثال : (Ryan S.D. Bardalai, 2005 , pp137-140)

1- ضعف الرقابة على وسائل الاتصال Media (الشرائط والأقراص المغنطة)؛

2- ضعف الرقابة على المناولة اليدوية لمدخلات ومخرجات الحاسب؛

3- عدم وجود نسخ إضافية من البيانات وعدم وجود رقابة على قراءة وتحديث وتعديل البيانات؛

4- عدم الفصل الجيد بين الوظائف المحاسبية وكذلك بين وظائف ومهام نظم المعلومات؛

5- عدم كفاية الرقابة على رسائل حفظ وتخزين المعلومات مع عدم وجود نظام جيد للمراجعة والفحص.

ثالثاً: تصنيف مخاطر تكنولوجيا المعلومات:

إن مخاطر تكنولوجيا المعلومات يمكن تصنيفها وتبويبها من وجهات نظر مختلفة كالآتي:

أولاً: وفقاً لمصدرها:

يمكن تبويب مخاطر أمن نظم المعلومات وفقاً لمصدرها إلى عنصرين أساسيين هما:

أ -مخاطر داخلية Internal Risk: ويمثل موظفي الشركة المصدر الرئيسي لتلك المخاطر.

ب -مخاطر خارجية External Risk: ويمثل المغامرون والقراصنة (Hackers) والكوارث الطبيعية Natural Disasters المصدر الرئيسي لتلك المخاطر.

ثانياً: وفقاً للمتسبب فيها The Perpetrator: يمكن تقسيمها الى: -

أ-**مخاطر ناتجة عن العنصر البشرى** :Human Threats -تحتل هذه النوعية من المخاطر المكانة الأولى نظراً لأنه بكفاءة وفعالية العنصر البشرى في ظل نظم متوسطة الكفاءة يمكن أن تنجح المنشأة وبالعكس تفشل أنجح الأنظمة مع إهمال وسوء أدائها وتنقسم إلى: (أماني هاشم السيد حسن، 2005، ص 171-173)

1 - سوء أداء الموارد البشرية Malfunctions: أي وقوع أخطار نتيجة لسوء الأداء الذي تقدمه الموارد البشرية والبرامج والأجهزة ويكون الإهمال أو القصور في الكفاية بصفة عامة سواء كان بحسن نية أو متعمداً فالنتيجة في النهاية واحدة، وبالتالي فإن خطأ العنصر البشرى البسيط قد يؤدى إلى خسائر كبيرة تفوق الخسائر التي يمكن أن تحققها المخاطر الأخرى مجتمعة.

2 - مخاطر ناتجة عن الغش الإلكتروني Electronic Fraud Risk: أي تعرض نظم المعلومات الإلكترونية لمخاطر الغش والتلاعب والاقتراب غير المصرح به عن طريق انتحال شخصية مستخدم حقيقي للنظام وتصميم أساليب للتلاعب وذلك بهدف الحصول على أحوال غير مشروعة أو أصول.

ب-**مخاطر ناتجة عن العنصر غير البشرى** Non Human :

وهي المخاطر التي ليس للإنسان دخل فيها والتي تكون نتيجة ظروف قهرية مثل: الزلازل والبراكين والأعاصير وغيرها من الكوارث الطبيعية.

ثالثاً. وفقاً لتعمدها Intention:

يمكن تبويب تلك المخاطر على أساس العمدية إلى مخاطر ناتجة عن: (Coe, Kathleen ,op cit , p4)

أ -تصرفات متعمدة أو مقصودة Intentional مثل الإدخال المتعمد لبيانات غير صحيحة أو التدمير المتعمد للبيانات ويجب أن نؤكد أن التصرفات المتعمدة عادة يكون بقصد ارتكاب بعض جرائم الحاسب وتدمير بعض أو كل الملفات الهامة أو بعض مكوناتها بهدف التربح من ورائها وعادة تأخذ تلك التصرفات شكل الإلغاء Deleting أو تعديل وتحريف Alternating أو خلق معلومات مضللة وغير صحيحة.

ب -تصرفات غير مقصودة أو غير متعمدة Accidental، مثل الإدخال أو التدمير غير المتعمد للبيانات نتيجة السهو أو الخطأ، وعلى الرغم من أن غالبية تلك التصرفات تكون مكلفة في بعض الأحيان إلا إنها يمكن تصحيحها Corrected أو تفاديها Avoided بمزيد من التدريب للموظفين وحسن الإشراف عليهم.

رابعاً: بناءً على الآثار الناتجة عنها Consequences :

يمكن تصنيف تلك المخاطر وفقاً للآثار الناتجة عنها إلى: (OECD, 1992 ,pp18-19)

أ -مخاطر ينتج عنها أضرار مادية Physical damage للنظام وأجهزة الحاسب الآلي أو التدمير المادي لوسائل تخزين البيانات مثل الشرائط والأقراص المغنطة والتي قد تنتج من بعض الظواهر الطبيعية كالفيضانات أو انقطاع التيار الكهربائي أو من سقوط النظم أو الشبكات لفترات طويلة.

ب -مخاطر فنية ومنطقية Technical or Logical والتي قد تصيب البيانات الموجودة بالحاسب أو على الشرائط المغنطة، وقد يكون ذلك بتحريف البرامج وإدخال جراثيم للكمبيوتر والتي قد تؤثر سلباً على إتاحة البيانات Availability عند الحاجة إليها، وذلك يحجبها عن الأشخاص المخول لهم الاطلاع عليها أو استخدامها Denial of Use أو الإفصاح عن البيانات السرية لأشخاص غير مخول لهم الاطلاع عليها Confidentiality والتي قد تؤثر على الموقف التنافسي للمنشأة أو التأثير على تكامل Integrity البيانات والبرامج داخل النظام.

خامساً: وفقاً لعلاقتها بمراحل النظام التكنولوجي المستخدم:

تصنف مخاطر أمن المعلومات على أساس علاقتها بمراحل النظام إلى: (محمد عبد الفتاح، 2003، ص209)

1- **مخاطر المدخلات** Input Risk **وتتمثل تلك المخاطر في:**

أ -**إدخال بيانات غير سليمة:** ويكون ذلك بخلق بيانات زائفة وغير صحيحة ولكن باستخدام نماذج ومستندات سليمة وإدخالها خلسة داخل رزم العمليات بدون أن يتم اكتشافها مثل إدخال أمر بيع مباشر مع قيود المبيعات.

ب-**تعديل أو تحريف في بيانات المدخلات:** ويكون ذلك بالتلاعب في المستندات والمدخلات الأصلية بعد اعتمادها من الشخص المسئول وقبل إدخالها إلى الحاسب وقد يحدث ذلك بزيادة رقم المصروف الفعلي الموجود بالمستندات أو تغير اسم أو عنوان مقدم طلب القرض أو تغير معدل الفائدة على بعض العمليات.

جـ-**حذف بعض المدخلات:** ويكون ذلك بحذف بعض المستندات كلية أو استبعاد بعض البيانات قبل إدخالها إلى الحاسب الآلي وذلك بحذف المستندات من رزمة السجلات أو حتى حذف الرزمة بالكامل.

د-**إدخال البيانات أكثر من مرة:** ويكون ذلك باختيار بعض المستندات وإدخال بياناتها أكثر من مرة إلى النظام مثل أوامر الدفع أو أوامر تسليم المخزون وذلك لتشغيلها أكثر من مرة لصالح القائم بعملية الاختلاس أو التلاعب.

2- **مخاطر تشغيل البيانات:**

وينصب تأثير تلك المخاطر بصفة أساسية على البيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتتمثل تلك المخاطر في:

1- تعديل وتحريف البرامج أو عمل نسخ غير قانونية منها.

2- استخدام البرامج بطريقة غير مصرح أو مرخص بها.

3- إدخال القنابل الموقوتة Logic Banks والجراثيم Viruses إلى أجهزة الحاسب الآلي.

4- تعديل وتحريف البرامج باستخدام حصان طروادة أو أسلوب سلامى أو غيرها من الأساليب التي تحتاج إلى خبرات متخصصة في الحاسب والبرمجة.

3 -مخاطر مخرجات الحاسب: إن مخاطر مخرجات الحاسب تتمثل في سرقة تلك المخرجات Stetting أو إساءة استخدامها Misuing أو توجيهها إلى أشخاص غير مصرح لهم باستلامها أو الاطلاع عليها نظراً لسريتها أو لأنهم غير مخول لهم صلاحيات الاطلاع عليها أو أن هؤلاء الأشخاص لا تتوافر فيهم المقومات الأمنية Non Security Cleared Personnel.

سادساً: مخاطر ناتجة من استخدام الشبكات NETWORK RISKS **وهي:**

أ -**مخاطر ناتجة عن استخدام البريد الإلكتروني** E-Mail **في التعاملات** (عيد حميدة، 2002، ص62)

نظراً لسرعة وسهولة إرسال الرسائل بواسطة البريد الإلكتروني جعل كثيراً من المنشآت يعتمد عليه في إنهاء بعض صفقاتها الأمر الذي قد يسهل حدوث بعض أنواع الاحتيال ... فقد تكون رسائل البريد الإلكتروني متضمنة مجموعة من الفيروسات تهدف إلى ضياع البيانات والمعلومات الموجودة داخل النظام، لذلك يجب الحذر من فتح الملفات الملحقة بالرسائل الإلكترونية لأنها أكثر وسائل الاختراق من قبل قراصنة ومحترفي شبكة الإنترنت. ولذلك فإنه يجب عدم فتح الملفات المرفقة إذا كانت من أحد الأنواع التي تنتهي بالاختصارات التالية:

1- EXE (Executable Files) يعنى وجود ملف تنفيذي، وهذا خطير جداً لأنه ينفذ الأمر المطلوب بنسبة دون إذن أحد.

2- BAT (Batch Files) يعنى وجود أمر معين موجه لأحد ملفات التشغيل في الجهاز.

3- APP (Application Files) يعنى وجود ملف به برنامج تطبيقي وهو خطير لأنه ممكن أن يكون به معلومات لا يجوز للغير الاطلاع عليها.

ب - **الخطر الأمني الناتج من الفيروسات:** الفيروس هو شفرة أو كود أو برنامج يقوم بنسخ وتكرار وإلحاق نفسه ضمن برنامج أو ملفات الحاسب عند التنفيذ ويعمل تلقائياً، محدثاً تأثيرات غير مرغوبة دون علم أو رغبة المستخدم الفعلي للحاسب، وتسبب تلك الفيروسات أمور غير متوقعة وأشياء غير مرغوبة وأن كثير من هذه الفيروسات تحاول الهرب من اكتشافها إما بطريقة ترميزها أو تغير من نفسها بعض الشيء في كل مرة تتزايد فيها، ويمكن تقسيم الفيروسات إلى ثلاثة أنواع رئيسية هي :(P. Raul Lin ,2006 ,p 4)

1- فيروسات ملفات التلويث File Infector viruses.

2- الفيروسات التي تصيب التشغيل System أو بدء العمل boot-record.

3- الفيروسات الصغيرة Macro Viruses.

جـ -مخاطر تعرض موقع المنشأة للغش والاحتيال: يحاول الدخلاء "Outsiders" إخفاء هويتهم والتخفي كشخص آخر ويطلق على ذلك الخداع spoofing ويعمل الخداع على إعادة توجيه اتصال الموقع إلى موقع مختلف من المستهدف، وعلى الرغم من أن هذه الطريقة لا تدمر الملفات إلا أنها تهدد سلامة الموقع وتهدد عمليات التوثيق ويجعل من الصعوبة التحقق من المرسل الحقيقي للرسالة، حيث يمكنهم سرقة بيانات بطاقات الائتمان وكلمات المرور للعملاء ومن هذه المعلومات يمكنهم انتحال هوية هؤلاء العملاء.

هـ-خطر تعطيل الشبكة: (آمنة ماجد الربيجات، 2005، ص 368) بمعنى أن تتوقف الشبكة عن العمل نتيجة عطل الأجهزة أو فقد البيانات أو البرامج بسبب حادث أو غيره وما يترتب على ذلك من تكاليف ومصاريف إضافية حيث أكدت نتائج إحدى الدراسات أن تهديدات ومخاطر الشبكات تحدث بصفة دورية وبمتوسط حسابي قدره 3.359 وهذا يشير إلى أن نوع الشبكات المستخدمة ومستوى جودة تكنولوجياتها هي الخطر الحقيقي لأمن الشبكات لذلك أوصت الدراسة بضرورة استخدام شبكات وأنظمة مساعدة للشبكات على مستوى عال من الجودة والتكنولوجيا.

و-خطر Botnets **(ربوت الشبكات)**: (Requel Filipek,2006,pp1-2)

هو نوع من مخاطر غزو الشبكات حيث يجد لصوص النت طريقة سرية لاقتحام الشبكات عن طريق استخدام Bots التي تمكن المهاجم (اللص) من السيطرة على الحاسب من بعد، حيث يتم توجيه أجهزة النظام من بعد بواسطة اختراق الشبكة من نقاط ضعيفة بها دون علم المشرق عليها (الخطر يكمن هنا)، يهدف سرقة كلمة السر، أو يعرفه أسماء المستثمرين أو أرقام الحسابات بالبنوك أو أرقام بطاقات الائتمان أو الحصول على أموال. حيث يعتبر العديد من خبراء أمن المعلومات أن Bots تعد التخوف الأمني الأول بسبب انتشارها استعمالها المستمر من جانب اللصوص وأن عدد متزايد من المنظمات يقع ضحية Bot nets دون معرفتهم، وأن أفضل طريقة لمحاربة Bot nets هي عمل استراتيجيات تسمح بإصلاح الحاسب بأحدث الأنظمة ضد الفيروسات واستعمال الحوائط النهارية وعزل الحاسبات التي كانت خارج المكتب وتغيير كلمة السر للشبكة المصابة وللمستخدمين وتطبيق سياسات لفرض عقوبات على المستخدمين لمن يقوم منهم بتشغيل برامج غير معروفة على الأجهزة.

الفصل الثاني: مزايا ومخاطر استخدام تكنولوجيا المعلومات في الرقابة الداخلية.

(أ) **المزايا:** هناك العديد من المنافع والامتيازات التي يطرحها استخدام تكنولوجيا المعلومات وذلك لتحقيق مزيداً من الفعالية والكفاءة للرقابة الداخلية لتوفير معلومات آمنة ودقيقة لمستخدمي القوائم المالية وأهمها: (عبد الوهاب نصر على، 2006، ص 248-249)

1- تحسين الوقتية. أي توفير المعلومات في الوقت المناسب وزيادة الدقة في المعلومات وتخفيض الخطر الذي يحيط بإجراءات الرقابة وتحسين إمكانية الفصل المناسب بين المهام Segregation.

2- القدرة على تحسين وتطوير أساليب الرقابة الداخلية عن طريق الاستفادة بالإمكانيات التي يتيحها الحاسب الآلى للرقابة الذاتية على عمليات التشغيل اليومية.

3- القدرة على تشغيل حجم كبير من العمليات المعقدة في وقت محدود وبتكلفة صغيرة علاوة على انعدام الأخطاء التشغيلية والحسابية تقريباً وانخفاض درجة الاعتماد على العنصر البشرى.

4- الاستفادة من الإمكانيات الضخمة لتخزين المعلومات في صورة ملفات إلكترونية وسرعة استرجاعها.

5- ارتفاع جودة قرارات الإدارة العليا كنتيجة طبيعية لارتفاع جودة المعلومات التي يقدمها النظام المستخدم بعد تشغيلها بصورة دقيقة.

(**ب**) **المخاطر**: هناك العديد من المخاطر الناتجة من استخدام تكنولوجيا المعلومات في الرقابة الداخلية وهى ما أوضحها معيار المراجعة الأمريكي رقم SAS 94 لسنة 2001 تحت عنوان "تأثير تكنولوجيا المعلومات على اعتبارات المراجع عن نظام الرقابة الداخلية عند مراجعة القوائم المالية"، حيث جاء في الفقرة رقم (19) أن استخدام تكنولوجيا المعلومات يجعل الرقابة الداخلية أمام العديد من المخاطر وهى: (AICPA، SAS No 94 , Parag 19.)

1- الاعتماد على نظم أو برامج تقوم بمعالجة البيانات بشكل غير دقيق أو تعالج ببيانات غير دقيقة أو الاثنين معاً.

2- دخول أشخاص غير مصرح لهم، لتدمير البيانات أو تغيرها أو تسجيل معاملات غير موجودة أو غير دقيقة أو غير مصرح بها.

3- تغير في البيانات الرئيسية لغير المصرح لهم، وتغير في النظام أو البرامج لغير المصرح لهم.

4- الفشل في إجراء تغيرات جوهرية في النظام أو البرامج، والفقد المحتمل للبيانات.

وعلى هذا يمكن تصنيف مخاطر استخدام تكنولوجيا المعلومات في الرقابة الداخلية إلى:

أ - مخاطر تسجيل وتشغيل العمليات الإلكترونية:

وتتمثل تلك المخاطر في المشاكل التي تواجه هيكل الرقابة الداخلية نتيجة التشغيل الإلكتروني للبيانات (EDP) وهي: (محمد مصطفى أحمد الحبالى ،2003، ص 275-277)

1- مخاطر تتعلق باختفاء الدليل المادي الملموس والتحول إلى استخدام الملفات الإلكترونية ففي ظل استخدام IT أصبحت البيانات المحاسبية غير مرئية وغير قابلة للقراءة ويصاحب ذلك مخاطر تتمثل فى سهولة ارتكاب الغش والتلاعب بل وصعوبة اكتشافها.

2- مخاطر تتعلق بسند المراجعة Audit Trail Risk: سند المراجعة هو الذي يمكننا من تتبع العملية من مصدرها حتى نتائجها النهائية وتشتمل تلك المخاطر على:

- عدم وجود دفاتر يومية حيث يتم الإدخال مباشرة لدفاتر الأستاذ.
- عدم وجود المستندات الأصلية بعد الإدخال المبدئي حيث يتم التخلص منها.
- لا يمكن ملاحظة التتابع والتشغيل حيث أنه يتم داخل الحاسب.

3 - مخاطر تتعلق بارتكاب الغش وسهولة التلاعب: حيث أن التلاعب والغش في ظل IT أصبح يتسم بخصائص تختلف عن تلك المتعارف عليها في ظل النظم اليدوية وهذا ما يجب أن يراعيه المراجع بدقة.

4- مخاطر متعلقة بالعاملين بنظم المعلومات القائمة على استخدام الحاسبات الإلكترونية. حيث أن زيادة خبرة ودراية العاملين في النظام بمرور الوقت يساعد قدرتهم على تخطى نقاط الرقابة الموضوعة للنظام مما يسهل عملية الغش وسهولة التلاعب.

5- مخاطر الفصل غير الملائم بين المهام والوظائف Improper Segregation Of duties: حيث أن ما يقرب من نصف عمليات الغش والاحتيال في أنظمة التشغيل الإلكتروني للبيانات (EDP) ترجع إلى عدم وجود فصل ملائم بين المهام كما أن الفصل الملائم بين المهام يعتبر من العناصر المكونة لنظام الرقابة الداخلية الجيد، ويأخذ الأهمية الثانية بعد ضرورة وجود سياسات محكمة للتصريح بنشأة العمليات والموافقة عليها -من بين 48 عنصر من العناصر المكونة لنظام الرقابة الداخلية.

6- تعقيد وصعوبة فهم أنشطة الحسابات الإلكترونية لغير المتخصصين وشدة إغراء العائد من الغش باستخدام الحاسب للمتخصصين وصعوبة اكتشافه وتتبعه.

(ب) مخاطر مرتبطة بتطبيق إجراءات الرقابة الداخلية:

هناك مجموعة من المخاطر التي يجب أخذها في الاعتبار عند اختيار وتطبيق إجراءات الرقابة الداخلية على تنفيذ العمليات الإلكترونية والتي تتعين تدنيتها وتتمثل أهم تلك المخاطر في: (د/ السيد عبد المقصود دبيان، د/ وليد السيد كشك، 2002، ص513-514)

1- **الاعتماد الكلى على أنظمة الحاسب**: نظراً للسرعة الكبيرة التي تتم بها عملية تشغيل ونقل وتداول البيانات واعتمادها على الحاسب الإلكتروني مما يترتب عليه انخفاض فرصة التصحيح والترشيد لأخطاء الإدخال والتشغيل ومن ثم تزداد الحاجة إلى استخدام أنظمة الرقابة الآلية التي تركز على أنظمة الرقابة المانعة وانخفاض الاعتماد على أنظمة الرقابة الاكتشافية التي تتم بعد الحدث.

2- **مخاطر الاختراق المتعمد**: والتقاط أرقام بطاقات الائتمان للعملاء المتعاملين ونهب أموالهم وحصول أطراف خارجية ليس لها علاقة بعمليات المنشأة على البيانات الموجودة بالنظام المحاسبي وإطلاع المنافسين عليها.

3- **مخاطر فشل الإرسال**: حيث أن عملية نقل وتداول البيانات الإلكترونية تتم عبر شبكة Net تمر بمراحل عديدة (إرسال -ترجمة -تخزين -استلام) فقد تتعرض تلك المعاملات خلال تلك المراحل إلى بعض المخاطر مثل فقدان بعض البيانات أو التحريف أو التعديل أو عدم إرسال الرسالة من الأصل.

4- **مخاطر فقدان التوثيق** Authentication Risks: تنشأ نتيجة فقدان الدليل المادي الذي يمكن من خلاله إثبات الحقوق والالتزامات (المستندات الورقية) والاعتماد على التبادل الإلكتروني وعدم وضوح هوية المتعاملين في التجارة الإلكترونية ويترتب على فقدان التوثيق ظهور نوع جديد من المخاطر يسمى مخاطر إنكار الالتزامات Republication Risk كإنكار استلام البضاعة أو إنكار استلام النقدية المحمولة إلكترونياً أو إنكار استلام أمر التوريد.

5- **مخاطر تركيز الرقابة**: حيث أن التبادل الإلكتروني أصبح يعتمد على الرقابة الإلكترونية وتربية الأعمال البشرية بقدر الإمكان ودورة العمل الإلكتروني وضغوطه مما يترتب عليه أن أصبحت أعمال الرقابة في أيدي أفراد قلائل وأصبح تجميع عدد من المهام تحت مسئولية شخص واحد مثل مشغل الحاسب مما يزيد من مخاطر سهولة ارتكاب الغش والأخطاء.

الفصل الثالث: أدوات وإجراءات الرقابة الداخلية على أمن وسلامة المعلومات.

تتطلب عملية تصميم نظام لأمن المعلومات ضرورة تحديد مفهوم الوقاية من المخاطر والتهديدات، حيث أن الوقاية الكاملة من المخاطر والتهديدات يصعب تنفيذها في الواقع العملي لأنها تتطلب مجهود وتكاليف واحتياجات يصعب توفيرها في ظل تحليل المنافع والتكاليف حيث أن أي نظام لابد وأن يكون منافعه أكثر من تكاليفه، ولكن يمكن تصميم نظام يساعد على تخفيض احتمالات حدوث تهديدات أو أخطار لنظم المعلومات إلى أدنى حد ممكن. ويجب أن يتصف تصميم نظام لأمن وسلامة المعلومات بالقدرة على (Leuhlfing, M.E , 2000 ,p 2)

1- معرفة كل محاولات الدخول الفاشلة للنظام والكشف عن أسبابها ومصادرها أي الحماية ضد الدخول غير المسرح به.

2- اتخاذ كافة الإجراءات اللازمة لسرعة استعادة أي أجزاء مفقودة منه من خلال استخدام النسخ الاحتياطية.

3- اكتشاف نقاط الضعف فيه وتصحيحها بصفة مستمرة.

4- أن يتصف بالمرونة بمعنى أنه عند فشل إجراءات الأمن في القضاء على تهديد معين فإنه يجب إعادة تصميم إجراءات أمنية جديدة تمنع مثل هذا التهديد.

5- يجب أن يتضمن نظام الأمن على القدرة فى تحقيق الأمن للمكونات المادية الرئيسية الملموسة للحاسب الآلي والتي تتكون من Secondary Memory CPU, Primary, Memory والمعدات الأخرى الملحقة بالحاسب وحمايتها من التخريب المتعمد أو الكوارث أو الحرائق.

لقد افترضت إحدى الدراسات أربعة خطوات رئيسية لتصميم النظام الجيد لأمن وسلامة المعلومات وتتمثل تلك الخطوات فيما يلى: (International Audit Services, 2004,)

- عدم الانتظار والبدء فوراً في تصميم نظام لأمن المعلومات.
- إشراك مستخدمي النظام وتوعيتهم للحصول على تأييدهم وموافقتهم على أهمية تصميم نظام الأمن.
- التعرف على نقاط الضعف في النظام ومصادر اختراقه وكيفية مواجهتها.
- التعرف على الثغرات التي تهدد أمن وسلامة النظام والعمل على معالجتها.

وقد حددت بعض الدراسات أسواء ثماني ممارسات متعلقة بإدارة نظم تكنولوجيا المعلومات في الشركات متوسطة وصغيرة الحجم وذلك حتى يمكن للشركات الأخرى الاستفادة من تلك الممارسات والتعلم منها وتتمثل تلك الممارسات في: (Lanz J , 2002,pp 4-51)

1- عدم إعداد نسخ احتياطية للبيانات Back Ups أو إعداد نسخ احتياطية وتخزينها فى أماكن غير ملائمة Off-Sit.

2- عدم الاختيار الدوري لخطة استمرارية الأعمال Business Continuity Plan وهي الخطة التي يتم من خلالها استعادة أو استرجاع Recovery نظام المعلومات إلى وضعه الأصلي وذلك عند فقد أو تدمير أي بيانات نتيجة اختراقه.

3- عدم استخدام أو تحميل التعديلات الأمنية Security Patches والتي يتم إعدادها بواسطة منتجو البرامج (Microsoft) وذلك لمعالجة الثغرات الأمنية التي تظهر في البرامج التي ينتجونها.

4- عدم متابعة الدوريات والمواقع الخاصة بأمن وسلامة المعلومات والتي تعرض الثغرات الأمنية التي تتعرض لها الشركات الأخرى مثل (WWW. Computer World. Com).

5- منح الموظفين employees صلاحيات أكثر من اللازم فيما يتعلق بالوصول إلى البيانات والمعلومات، حيث يجب قصر هذه الصلاحيات على ما يحتاجه كل موظف لأداء أعماله وفقاً لمسئولياته.

6- عدم الاختيار المناسب والملائم لبرامج وأنشطة التشغيل وعدم اختبارها قبل تشغيلها مما قد ينتج عنه أخطاء في التشغيل والتي يصعب إصلاحها بعد ذلك.

- الضوابط والإجراءات اللازمة لتحقيق الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات:

هناك مجموعة من الأبعاد والجوانب المتعلقة بأمن المعلومات والموجودة داخل المعيار 17799 الصادر عن منظمة المعايير الدولية عام 2000 والمأخوذ عن المعيار البريطاني 7799 الذي صدر عام 1995 -والذي يتضمن إرشادات وتوصيات تتعلق بالممارسات الجيدة في مجال إدارة أمن المعلومات وهي مستمدة من أفضل ممارسات وإجراءات الرقابة الداخلية على أمن وسلامة المعلومات في العديد من الشركات العالمية وهي: (Elsff. M. M and Salms-SH, 2000, pp 243- 256)

1- وجود سياسة واضحة لأمن وسلامة المعلومات Security Policy تؤكد على دعم الإدارة والتزامها بتحقيق أمن وسلامة المعلومات.

2- تنظيم الأمن Security Organization. أي توفير المناخ الإداري الملائم الذي يضمن تطبيق سياسات وإجراءات تحقيق الأمن وتحديد الأفراد المسموح لهم بالاطلاع عن البيانات.

3- تبويب ورقابة الأصول Asset Classification and Control أي توفير حماية ملائمة لأصول نظم المعلومات بمختلف مكوناتها وتحديد المسئولين عنها والعمل على تبويب المعلومات حسب أهميتها ودرجة حساسيتها ودرجة سريتها والاعتماد عليها.

4- أمن الأفراد Personal Security ويهدف إلى تخفيض الأخطار المرتبطة بالخطأ البشرى، وإعداد برامج مستمرة لتوعية الموظفين وتعريفهم بالتهديدات والأخطار المختلفة.

5- الأمن المادي والبيئي Physical and Environmental Security ويشمل ذلك تأمين مكان نظام المعلومات وتأمين مصادر الطاقة والحماية من انقطاع الكهرباء وتحديد من لهم حق الوصول إليه.

6- التحكم في الوصول إلى النظام System Access Control ووجود رقابة على الدخول إلى معلومات النظام بحيث يتم تحديد المعلومات التي يصرح لكل مستخدم الوصول إليها حسب الأنشطة المكلف بأدائها والأعمال المكلف بإنجازها دون الوصول إلى المعلومات الأخرى التي لا تخص عمله.

7- تطوير وصيانة النظام System Development and Maintenance بصفة مستمرة حيث يلزم عند تطوير النظام تحديد متطلبات الأعمال ومنها يتم التوصل إلى متطلبات الأمن الواجب توافرها في هذا النظام والتي على أساسها يتم تحديد ضوابط وإجراءات أمن المعلومات التي يجب الاستعانة بها لضمان الاستمرار الكفء للنظام بعد تطويره وصيانته.

8- الالتزام Compliance أي الالتزام بالمتطلبات والقيود القانونية والتنظيمية والتعاقدية بهدف تجنب خرق المنشأة لأي متطلبات ناتجة عن أي من القيود السابقة مع مراعاة تشريعات وقوانين الدول المختلفة عند تبادل البيانات.

الوسائل التي تستخدم لتحقيق الرقابة الداخلية على أمن وسلامة المعلومات: -

هناك العديد من الوسائل والإجراءات التي يمكن استخدامها لتحقيق الرقابة على أمن وسلامة المعلومات في ظل بيئة تكنولوجية المعلومات منها: (Lin, L ,2001,pp1-3 / Mahadevan,c. ,2001, pp2: 5)

1- **التشفير** Encryption: يمثل التشفير أهم الطرق المستخدمة للحفاظ على سرية وسلامة البيانات التي يتم تداولها بين الأطراف المختلفة، وذلك لضمان عدم إطلاع أطراف غير مصرح لها على تلك البيانات، وفيها يتم تحويل البيانات من الصيغة العادية المفهومة إلى صيغة مشفرة لا يمكن قراءتها أو فهمها ثم يتم إرسالها إلى المرسل إليه الذي يستخدم مفتاح لفك الشفرة Decryption لإعادة البيانات من الصيغة المشفرة إلى صيغتها العادية مرة أخرى ويمكن استخدام إحدى الطرق التالية في عملية التشفير.

أ -التشفير باستخدام المفتاح المتماثل Symmetric Key Cryptography.

ب -التشفير باستخدام المفتاح غير المتماثل Symmetric Key Encryption.

2- الحماية من الفيروسات Virus Protection : أشهر طرق الوقاية من الفيروسات هي استخدام البرامج المضادة للفيروسات Untie Virus والتي تقوم بعمل فحص دوري للنظام التكنولوجي المستخدم بحثاً عن أشهر أنواع الفيروسات باستخدام ما يعرف بتوقيع الفيروس Virus Signature أو عن طريق مراقبة السلوك غير المألوف للبرامج Virus Behavior Uncommon علاوة على عدم فتح أي ملف إلى بعد التأكد من مصدرة وتقليل الدخول إلى Net ونقل الملفات File Transfer واستخدام البريد الإلكتروني E. Mail واستخدام برنامج Avast 4Home الذى يقوم بوظيفة مفيدة تسمى Virus chest التي يقوم من جلالها بإنشاء مساحة آمنة على الحاسب لتخزين الملفات المهمة فيها دون خوف لتعرضها لأى فيروس.

3- إعداد نسخ احتياطية Bock Ups: وفيها يتم إعداد نسخ احتياطية من البيانات أو البرامج لمواجهة فقد أو ضياع أو تحريف البيانات أو البرامج نتيجة أخطاء التشغيل أو تدمير نظام المعلومات عن طريق الاختراق الخارجي.

هذا وقد سبق أن أوضحنا أن عدم إعداد نسخ احتياطية للبيانات يعد من أسواء 8 ممارسات متعلقة بإدارة أمن نظم المعلومات في الشركات متوسطة وصغيرة الحجم.

4- الحوائط النارية Fire Walls: هي أدوات تقع على طرف شبكة Net الخاصة بالشركة هدفها تأمين الإدخال للشركة وتنقية وفلترة البيانات الداخلة والخارجة طبقاً لقواعد ومعايير معدة سلفاً وتعريف المستخدمين والتحقق من هويتهم وتحديد البيانات التي يمكن لكل مستخدم الوصول إليها وفقاً لطبيعة عمله ومسئولياته داخل الشركة وتوجد عدة أنواع من الجدران النارية منها:

- جدران الحماية بالفلترة Ket Filtering Fire Walls.
- جدران الحماية للتطبيقات الاستخدامات Application Fire Walls.

- جدران الحماية التي تقوم بالفحص State full Packet Inspection Fire Walls.
- الشبكات الافتراضية المخصوصة Virtual Private net Worke.

أي أن الجدران النارية تقوم بالمهام الآتية:

- تأمين الإدخال إلى الشبكة والرقابة على كل الروابط والتدفقات من وإلى الشبكة.
- تنقية وفلترة البيانات الداخلة والخارجة طبقاً لقواعد معدة من قبل.
- تعريف المستخدم والتحقق من هويته ومراقبة أنشطة الشبكة وإبلاغ المسئولين عند حدوث أى أحداث طارئة وغير مرغوبة والتأكد من التطبيقات التي يحملها محتوى الرسائل المتبادلة هو استخدام مسموح به.

5- استخدام وسائل تعريف المستخدم User Authentication:

ويتم استخدام وسائل تعريف المستخدم لحماية النظام من أخطار التدخل غير الشرعي بانتحال صفة شخص مصرح له باستخدام النظام Impersonation وتستخدم للحماية من هذه الأخطار وسائل متعددة منها:

أ -**كلمة السر** Pass Words: إن استخدام كلمة المرور ما زالت أكثر الطرق انتشاراً واستخداماً في أنظمة المعلومات للشركات على الرغم من وجود طرق حديثه للتعرف على هوية مستخدمي المعلومات مثل طريقة بصمات الصوت الأصابع لذلك عادة تستخدم الشركات إجراءات رقابية هدفها تأمين كلمات المرور الخاصة بالمستخدمين ومنع القراصنة من الاستيلاء عليها مثل إجبار المستخدم على تغير كلمة المرور الخاصة به بصورة دورية (كل شهر مثلاً) وتوعية المستخدم بضرورة الاحتفاظ بكلمة المرور الخاصة به وعدم إطلاع أي شخص عليها أو كتابتها في مكان يمكن الوصول إليه ومنع المستخدم من تكرار كلمة ... إلخ....

ب- التعريف باستخدام الخصائص البيولوجية Biometrics Authentication:

وذلك بالاعتماد على الصفات البيولوجية لشخص المستخدم مثل الطول –بصمة الإصبع -بصمة الصوت وتعتبر هذه الوسيلة من الوسائل الجيدة للتعريف لأن هناك استحالة في قهرها وهناك طريقتان للتعريف:

1 -طريقة التعريف مرة واحدة One Time Authentication.

2 -طريقة التعريف رسالة مع استخدام التوقيعات الرقمية Message By Message Authentication With Digital Signatures.

جـ-التوقيعات الرقمية والإلكترونية Digital and Electronic Signatures:

تستخدم التوقيعات الرقمية الإلكترونية مفاتيح الشفرة Encryption Keys لعمل توقيعات سرية لا يمكن إنكارها وقد أصدر الكونجرس الأمريكي عام 2000 قانون التوقيعات الإلكترونية الذي يعطى هذه التوقيعات نفس الموقع القانوني للتوقيعات العادية.

6- مراجعة الأمن Security Audit : من الأدوات الهامة في تحقيق أمن المعلومات القيام بمراجعة دورية لنظم الرقابة الداخلية على أمن المعلومات التي تطبقه الشركة بغرض الكشف عن نقاط القوة والضعف والعمل على تلافى الأخير وعلاجه، وغالباً ما تتضمن تلك المراجعة قيام فرق من الخبراء بمحاولة اختراق الشبكات الخاصة بالشركة عن طريق محاكاة القراصنة وهو ما يعرف بالقرصنة الأخلاقية Ethical Hacking وتتم هذه المراجعة وفقاً لخطة محددة مسبقاً ومصممة خصيصاً للشركة محل المراجعة، وهذه المراجعة قد يقوم بها أفراد من إدارة المراجعة الداخلية بالشركة أو مراجعون مهنيون من خارجها ممن لديهم خبرة في مجال أمن معلومات شبكات الحاسب. وبعد انتهاء المراجعة يجب أن يقدم فريق المراجعة تقريراً فنياً مفصلاً عن حالة نظام الأمن الخاص بالشركة.

الفصل الرابع: أثر استخدام تكنولوجيا المعلومات على مكونات هيكل الرقابة الداخلية:

يرى البعض "أن التطور الحادث في نظام تكنولوجيا المعلومات والاتصالات وانتشار تطبيقاتها بشكل مكثف قد أحدث تطوراً هائلاً في المفاهيم والإجراءات الأساسية عند تقييم هيكل الرقابة الداخلية، وقد أدى هذا التطور بدوره إلى اتساع نطاق تطبيق أساليب المراجعة، وبالتالي إضافة أعباءً جديدة على المراجع المكلف بتقييم هيكل الرقابة الداخلية (سعاد حسن خضر وآخرون، 1996، ص229).

كما يرى البعض أن "التعريف الذي وضعته لجنة Coso للرقابة الداخلية يعد هو الأنسب للمشروعات التي تستخدم تكنولوجيا المعلومات في إتمام معاملاتها التجارية، حيث عرفت لجنة Coso الرقابة الداخلية بأنها عملية Process وبالتالي فهي تعتبر ديناميكية Dynamic أي مستمرة الأمر الذي يتناسب مع طبيعة البيئة التي تمارس من خلالها تلك المشروعات أنشطتها" (أمل عبد الفضيل، ص 109).

كما أن الهدف الأساسي للمراجعة لن يتغير في ظل بيئة تكنولوجيا المعلومات ولكن إجراءات المراجعة هي التي تتغير بسبب اختفاء مسار المراجعة (عبيد سعد المطيري، ص 46) ويرى آخر أن أهداف الرقابة الداخلية في ظل بيئة IT لا تختلف عن الأهداف التقليدية لأنظمة الرقابة الداخلية. إلا أنه إزاء المخاطر التي يتعرض لها النظام في ظل بيئة IT، خاصة في ممارسة التجارة التي تتم عبر شبكة الإنترنت فإن هناك هدف إضافي ينبغي أن تعمل أنظمة الرقابة الداخلية على تحقيقه وهو توفير الثقة للمتعاملين في مزاولة أنشطة التجارة الإلكترونية وأيضاً الثقة في الموقع الذي يتم من خلاله مزاولة تلك التجارة".

هذا ويرى البعض أن تكنولوجيا المعلومات تتطلب ضرورة تحقيق مجموعة من الأهداف الفرعية وذلك كما يلي: (أماني حسين كامل، مرجع سابق، ص 99)

- الهدف الأول للرقابة الداخلية هو كفاءة وفعالية العمليات.

- الهدف الثاني للرقابة الداخلية هو "إمكانية الثقة في التقارير المالية".

ومن أجل أن تتحقق تلك الأهداف يجب أن تتحقق أولاً الأهداف الفرعية التالية:

- أمن المعلومات (سواء المرسلة أو المخزنة أو المنشورة على الموقع).
- أمن المعاملات عبر الإنترنت "متضمنا التوثيق والتصريح وعدم الإنكار وإمكانية المساءلة والسرية والنزاهة والإتاحية.
- أمن الخصوصية "أي أمن المعلومات الخاصة بالعملاء المتعاملين مع المنشأة.

الأثر على بيئة الرقابة:

تؤكد إحدى الدراسات (عبد الوهاب نصر، مرجع سابق، ص 218) "أنه في ظل الاستخدام المتزايد لتكنولوجيا المعلومات في إتمام المعاملات المالية سيظل انتهاك الإدارة لنظم الرقابة الداخلية من المشاكل الهامة التي تواجه نظم الرقابة الداخلية كما أكدت أيضاً أن معدلات حدوث التلاعب في البيانات Fraud سوف تكون أقل من معدلات حدوث الأخطاء Errors إلا أنها سترتبط غالباً بانتهاك الإدارة لنظم الرقابة المعمول بها وكذلك بسبب سوء تطبيق الفصل بين الواجبات وعدم تدريب العاملين على أساليب تكنولوجيا المعلومات والاتصالات وعدم وجود تفويض سليم للسلطات" .

كما أن موظفي المنشأة قد يشكلون مصدر تهديد كبير على المنشأة سواء عن طريق الإهمال أو التصرف المتعمد الذي قد يصل إلى حد تحقيق مكاسب مادية من وراء بيع معلومات المنشأة مما يتطلب إعطاء أهمية كبيرة لعناصر بيئة الرقابة كما يلي: -

1- وجود إجراءات رقابية لحسن اختيار الموظفين من حيث الكفاءة الأخلاقية والمهنية.
2- وجود سياسات لأمن وخصوصية المعلومات وإتباعها من كل موظفي المنشأة وعلى كل المستويات.
3- وجود برامج تعليم وتوعية وتدريب مستمرة على أمن المعلومات وتنمية روح المشاركة بين الموظفين لتحسين ثقافتهم وسلوكهم وجعلهم خط دفاع حقيقي عن أمن معلومات ومعاملات المنشأة.

كما أن بيئة الرقابة في ظل تكنولوجيا المعلومات يجب أن تتكون من إطار أشمل بكثير من العناصر المتفرقة التي طرحها المفهوم التقليدي للرقابة الداخلية بالإضافة إلى أن هذه العناصر يجب أن يحملها إطار شامل متناسق يشتمل على مجموعة من العناصر التالية التي يمكن وضعها في ثلاثة مجموعات رئيسية وهي: (خديجة محمد عيد رمضان، 2005، ص 142-144)

1- أساليب تكنولوجيا المعلومات Information Technology Practices: وهي مستوى التكنولوجيا التي تستخدمه المنشأة في إدارة نشاطها.

2- أساليب إدارة المعلومات Information Management Practices: وتتعلق بكيفية إدارة تدفق المعلومات داخل النظام التكنولوجي المستخدم ويشمل -القدرة على إدارة المعلومات -استشعار المعلومات -جمع المعلومات -تنظيم المعلومات -التشغيل -الاحتفاظ بالمعلومات وصياغتها.

3- سلوكيات وقيم المعلومات Information Behaviors and Values: وتعبر عن السلوك والقيم المرغوبة في إدارة تكنولوجيا المعلومات وتشمل القدرة -النزاهة -الشفافية -التطلع للمستقبل -الاستخدام المشترك للمعلومات. وعلى هذا فإن تكنولوجيا المعلومات قد أوردت عناصر جديدة، لها أثر هام على بيئة الرقابة أهمها التأكيد على أهمية المعايير والقيم الأخلاقية الواجب توافرها في بيئة تكنولوجيا المعلومات.

- **الأثر على تقييم المخاطر:**

يرى البعض بأن الفرض القائل (عارف عبد الله، مرجع سابق، ص 60) "أن التشغيل الإلكتروني للبيانات سوف يؤدى إلى تخفيض أخطار الرقابة لأنه سيقضى على أي محاولة لسرقة الأصول من جانب العاملين، كما أنه سيؤدى إلى تحسين الدقة والكفاية في نظم الرقابة بما يوفره من تغذية عكسية مرتدة فورية غير صحيح، حيث لازالت مسألة نزاهة ودقة البيانات المحاسبية تمثل تحدياً هاماً أمام نظم التشغيل الإلكتروني للبيانات تزداد حدتها وبالتالي تزداد مخاطر الرقابة المترتبة عليها كلما زادت درجة التقدم التكنولوجي في تشغيل البيانات "

كما أن تقدير الخطر من قبل إدارة المشروع يعد أمراً أكثر أهمية في المشروعات التي تمارس الأنشطة الإلكترونية في إتمام معاملاتها المالية نظراً للأساليب غير التقليدية التي تعتمد عليها في إتمام صفقاتها ونظراً للمخاطر العديدة الكامنة من جراء إتمام تلك الصفقات سواء من جانب الدخلاء أو قراصنة الكمبيوتر "، لذلك يجب على المراجع التأكد من قيام إدارة المنشأة بتلك الوظيفة الهامة واتخاذها لكافة الوسائل الهامة اللازمة لمواجهة تلك المخاطر لتحقيق أهداف المنشأة والسيطرة على مخاطرها.

هذا ويرى البعض ضرورة إضافة مكون الاستجابة للمخاطر إلى مكونات الرقابة الداخلية فى ظل استخدام تكنولوجيا المعلومات لإتمام المعاملات التجارية حيث أن مخاطرها المتعددة تتطلب ضرورة الاهتمام بعمل تقييم لمستويات الخطر التي تتعرض لها الأصول والمعلومات المختلفة حيث بدون تقييم الخطر لا يمكن وضع طرق لسرعة منعه أو الحد من هذه المخاطر وهو ما يطلق عليه الاستجابة مع ضرورة تبنى المنشأة لاستراتيجيات تمكن من سرعة الاستجابة للمخاطر.

وهذا ويتفق الباحث على ضرورة إضافة مكون الاستجابة للمخاطر إلى مكونات الرقابة الداخلية وهو ما أكدته أيضا دراسة Coso الجديدة بعنوان "Enterprise Risk Management Frame Work" عام 2003 والتي حددت استجابات المخاطر في أربع مجموعات وهى: (Coso ,2003 ,pp1-3)

1- التجنب Avoidance: وهو التصرف الذي يتخذ لاستبعاد الأنشطة التي تسبب المخاطر فتجنب المخاطر قد يتطلب إيقاف خط إنتاج أو إلغاء التوسع في السوق.

2- التخفيض Reduction: وهو التصرف المتخذ لتخفيض احتمال التعرض للخطر أو لتخفيض تأثيره أو الاثنين معاً.

3- المشاركة Sharing: وهو التصرف المتخذ لتخفيض احتمال التعرض للمخاطر أو تأثيرها بالتحويل أو مشاركة المخاطر المألوفة منها عن طريق التأمين.

4- القبول Acceptance: أي عدم عمل أي تصرف للتخفيض من احتمالية أو تأثير المخاطر بمعنى القبول بالأمر الواقع.

الاثر على أنشطة الرقابة: (شحاته السيد ، مرجع سابق، ص22 / Thomas & Panl Munter ,2002 ,p2)

أنشطة الرقابة هي الأنشطة التي يتم أدائها لإلغاء المخاطر أو تخفيضها إلى مستوى مقبول، ولكن في ظل استخدام تكنولوجيا المعلومات سوف تزداد أهمية أنشطة الرقابة بنوعيها (الرقابة المناعة -الكاشفة) وسوف تهتم أكثر بالرقابة الآلية واستخدام برامج التقييم الذاتي للرقابة. "لأن العديد من نظم الرقابة المحاسبية والمالية التي يعتمد عليها المراجع يجب أن يتضمنها برنامج الحاسب فإن المراجع في ظل استخدام تكنولوجيا المعلومات يجب أن يهتم كثيراً بالمراحل المبكرة لتصميم النظام حيث غالباً ما يتم تشغيل قسم الحاسب بواسطة موظفين ذوى معرفة متخصصة مما حتم على المراجع أن يكون كفئاً وفعالاً في مراجعة عمليات تشغيل البيانات التي يقوم بها هؤلاء المتخصصون كما أن الصعوبات والمشاكل التي يواجهها المراجع في ظل التشغيل الإلكتروني للبيانات غالباً ما تتناسب عكسياً مع حجم الحاسب المستخدم، لأنه من الصعب تحقيق الفصل بين المهام في ظل الحاسبات الصغيرة بسبب نقص الأفراد المتخصصين " .

ونظراً لأهمية فحص ودراسة أنشطة الرقابة المتبعة في المشروعات التي تستخدم تكنولوجيا المعلومات في إتمام معاملاتها التجارية فقد أوجب قانون Sarbanes- Oxley الصادر في USA عام 2002 على المراجع أن يقوم بفحص أنشطة وأساليب الرقابة المتبعة في المشروعات وإظهار نتيجة فحصه في تقرير المراجعة، حيث يجب أن يحتوى التقرير على ما إذا كانت الأساليب والأنشطة المتبعة تحقق المحافظة على السجلات التي تعكس بعدالة ودقة صفقات المشروع وتأكيد معقول بأن الصفقات يتم تسجيلها وفقاً لمعايير المحاسبة التعارف عليها GAAP، كما يجب أن يحتوى التقرير على وصف لأى أوجه ضعف أو عدم اكتمال جوهرية في الأنشطة والأساليب الرقابية.(Alain. Valiquette , 2006,p 1-12)

هناك من يرى أن أنشطة الرقابة الداخلية المتعارف عليها والموجودة في تقرير لجنة Coso لم تعد كافية وملائمة لخصائص نظم تكنولوجيا المعلومات وما تتعرض له من مخاطر متعددة مما يتطلب تصميم أنشطة رقابة داخلية تتلاءم مع أنشطة تكنولوجيا المعلومات ولضمان توثيق ونزاهة معلومات ومعاملات التبادل الإلكتروني للبيانات EDP نظراً للأسباب التالية: (أماني حسين، مرجع سابق، ص 101-102)

1- يمكن أن تتعرض هذه النظم المفتوحة لوصول العملاء أو القراصنة أو غيرهم.

2- الاعتماد الكبير على الإجراءات الأتوماتيكية في التسجيل والمعالجة والتقرير عن المعلومات وما يترتب عليه من عدم وجود مستندات ورقية مما يتطلب الاعتماد على الرقابة الأتوماتيكية مثل التصريح بالوصول والمعاملات، ودقة إدخال البيانات وسرعة اكتشاف الأخطاء وتصحيحها.

3- إتاحة موقع المنشآت ونظامها في أداء العمل على مدار 24 ساعة لإنجاز المعاملات الإلكترونية وعدم توقفها، يتطلب أهمية وجود إجراءات رقابية للاحتفاظ بخطط لاستمرارية نظم وموقع المنشأة.

4- وجود إجراءات رقابية للفصل المادي بين مهام المسئولين عن إعداد وتشغيل وصيانة نظم وموقع المنشأة بالإضافة إلى الحماية المادية للأجهزة والبرامج وكوابل الاتصالات الخارجية.

5- تشكل تكنولوجيا التجارة الإلكترونية خطراً كبيراً على المعلومات وخاصة السرية والخصوصية مما يستدعى توفير طرق لرقابة وتأمين قواعد البيانات وحماية المعلومات المتنقلة عبر الشبكات.

- **الاثر على المعلومات والاتصالات:** (جورج دانيال غالى، ص343)

يعد نظام المعلومات من أهم العناصر المكونة للهيكل المتكامل للرقابة الداخلية. بما يوفره من معلومات مفيدة لأطراف عديدة عن طريق قنوات مفتوحة للاتصال تسمح بتدفق تلك المعلومات وإعداد التقارير.

"وتعتمد نظم المعلومات للمشروعات التي تستخدم تكنولوجيا المعلومات في إدارة معاملاتها التجارية على نظم تكنولوجية عالية الأوتوماتيكية حيث تستخدم الإجراءات الأوتوماتيكية لإنشاء وتسجيل ومعالجة والتقرير عن المعاملات في تقارير إلكترونية، كما يتولد عن الإجراءات الأوتوماتيكية مسار مراجعة إلكتروني والاعتماد بدرجة كبيرة على الرقابة الأوتوماتيكية المبرمجة المبنية داخل النظم والتي تطبق على كل المعاملات ". وتتطلب معاملات التجارة الإلكترونية ضرورة وجود قنوات اتصال بين المنشأة وموظفيها لإعلامهم بسياسة الأمن ونزاهة معالجة المعاملات وتذكيرهم بمسئوليتهم.

ويرى الباحث أن نظام الاتصال في ظل المعاملات التجارية الإلكترونية يجب أن يتسم بالتغذية العكسية وتوصيل المشاكل واختراقات الأمن للإدارة ومسئولي إدارة الأمن كما يجب نشر السياسات الأمنية على موقع المنشأة لإعلام العملاء بكيفية التعامل مع المنشأة فيما يتعلق بمعاملات التجارة الإلكترونية.

ويتميز نظام المعلومات في المشروعات التي تستخدم تكنولوجيا المعلومات في معاملاتها بـ:

1- توفير المعلومات بشكل فورى مستمر من خلال التشغيل الفوري للبيانات.

2- التركيز على وجود نسخ احتياطية بديلة للملفات والبرامج.

3- توفير الأمن للمعلومات المنتجة من خلاله.

4- التوصيل الجيد للمعلومات لكافة أطراف المستويات الإدارية.

- **الاثر على المتابعة**: (Teresa. Wingfield, 2006, p1)

يتطلب أمن المعلومات Information Security ومعاملات تكنولوجيا المعلومات متابعة وفحص وتقييم مستمر لكل من سياسات الأمن وأداء الأفراد وأداء التشغيل حيث تتميز هذه الأنظمة بالتتابع المستمر في عملياتها والتشغيل الفوري لبياناتها الأمر الذي يتطلب ضرورة وجود نظام للمراقبة والمتابعة المستمرة داخل المشروع يتم من خلاله " التقييم المستمر Continuous Evaluation لأنشطة المنشأة واتخاذ الإجراءات المصححة في الوقت المناسب، الاكتشاف المبكر لأي تلاعب أو غش أو تحريف في الحسابات أو العمليات ".

وحيث أن اختراقات وحوادث الأمن والأخطاء المختلفة من الممكن أن تؤدى إلى انهيار وتوقف النظام التكنولوجي المستخدم مما يتطلب ضرورة وجود متابعة مستمرة لفحص كفاءة وفعالية الأنشطة الرقابية وضرورة وجود متابعة مستمرة لسياسات أمن المعلومات ولوائحها المنظمة لذلك يرى الباحث أن المتابعة المستمرة والتقييم مكون جوهري للرقابة الداخلية لأنشطة تكنولوجيا المعلومات،

ويرى الباحث ضرورة أن تنقسم عملية المتابعة لرقابة نظم تكنولوجيا المعلومات إلى: -

1. **متابعة الالتزام**: ويقصد بها متابعة الالتزام بسياسات أمن المعلومات وتوافقها مع ما يستجد من متطلبات وقوانين مع ضرورة تعديلها وتحديثها بما يتلاءم مع التهديدات والتغيرات الجديدة بالإضافة إلى متابعة عقود واتفاقيات مقدمي الخدمة بالإضافة إلى متابعة أفراد المنشأة بالحفاظ على متطلبات الأمن وربط ذلك ببرنامج الحوافز والجزاءات للمساعدة على تحسين التزامهم ويقوم بهذه المهام المستشار القانوني لفريق متابعة الالتزام ومسئولي الأمن ومسئولي الموارد البشرية.

2. **متابعة الرقابة**: ويقصد بها متابعة وتقييم الرقابات والعمليات بحيث يمكن عمل تحديد فورى للمشكلات واحتواءها والإسراع بالتغطية لتخفيض حجم الخسارة والتدمير وإعداد تقارير عن المشكلات المرتبطة بالأمن ووضع اقتراحات للحلول ويقوم بذلك مسئولي الأمن ومتخصص تكنولوجيا المعلومات.

مسئولية المراجع عن سلامة أمن المعلومات من التهديدات والمخاطر السابقة: تعتبر إدارة المشروع هي المسئولة عن أنظمتها التكنولوجية وسلامة أمن معلوماتها ومحتوياتها من المعلومات المالية وغير المالية ويعتبر المراجع مسئولاً عن تقييم

نظام الرقابة الداخلية والتي يتطلب منه بالضرورة تطوير أساليب المراجعة للتأكد من أن أنظمة الرقابة الداخلية كافية لمنع واكتشاف حالات الغش المالي وإبراء رأيه في نظم الرقابة الداخلية التي تتبعها المنشأة وكذلك توجيه النصح للإدارة في المشاكل التي تتعلق بالأمن والرقابة بشكل ديناميكي مستمر. ويجب أن يتحقق المراجع من كفاية سياسات ووسائل الحماية المطبقة بالشركة مثل جدران الحماية ..... الخ ونظم التشغيل ووسائل الحماية الأخرى الملائمة.

ويعتبر المراجع غير مسئول في حالة تأسيس مواقع مزيفة بغرض الغش التجاري الإلكتروني وفى حالة اختراق موقع الشركة للعبث بمحتوياته وتخريبه وفى حالة تشويه عرض القوائم المالية استخدام الوسائط المتعددة التي يوفرها الإنترنت وفى حالة نشر معلومات جزئية لم يتم مراجعتها عن الأداء المالي والتشغيل للشركة' والمراجع لا يعد مسئولاً عن الفيروسات التي تصيب الحاسبات الموجودة بالمنشأة التي يراجع حساباتها إلا أنه يجب عليه التأكد من: (عادل عبد الرحمن ، 2003، ص 145-146)

1- أن إدارة الحاسب بالمنشأة تراعى بدقة إتباع الوسائل الكفيلة بتجنب الإصابة بفيروسات الحاسب.
2- أن إدارة الحاسب بالمنشأة تراعى استخدام نسخ أصلية من البرامج والتطبيقات.
3- أن إدارة الحاسب بالمنشأة تراعى استخدام برامج مقاومة الفيروسات وتواظب على تجدديها بصفة مستمرة.
4- الحصول على تأكيد مكتوب من الإدارة يفيد بأنها اتخذت الإجراءات والوسائل الكفيلة لتجنب أضرار الفيروسات.
5- إضافة فقرة إضافية توضيحية في تقرير المراجعة، إذا ما تضمنت الإفصاحات التي تقدمها عن البيانات المحاسبية والقوائم المالية للمنشأة على درجة مؤثرة من عدم التأكد نحو القدرة على مواجهة آثار تلك الفيروسات.

يرى الباحث إن التحدي الرئيسي في مراجعة أنشطة تكنولوجيا المعلومات هو الطبيعة الإلكترونية لدليل المراجعة، حيث تحول من دليل ورقى مرئي إلى دليل إلكتروني لذا يجب على المراجع التحقق من أن الرقابة المبنية والمستخدمة لحماية إنشاء وتحويل وتسجيل والاحتفاظ بالمعلومات الإلكترونية كافية لتحقيق الثقة في المعلومات الإلكترونية المطلوب استخدامها كدليل مراجعة، في الوقت الذى تعتمد أنشطة تكنولوجيا المعلومات على نظم المعالجة الفورية التي تستلم مدخلات من مصادر متعددة (خارج - داخل المنشأة) وفرض الرقابة على هذه المصادر أمر يصعب تحقيقه مما يتطلب ضرورة استمرار وتقييم أنشطة الرقابة بصفة مستمرة.

كما أن اختفاء الدليل المادي الملموس للإثبات قد أثر على الأداء المهني للمراجع وعدم مقدرته على تقديم معلومات دقيقة عن نظم الرقابة الداخلية لتحديد مدى إمكانية الاعتماد عليها في المراجعة، "ففي ظل استخدام

تكنولوجيا المعلومات أصبح بالإمكان بث برامج محكمة الإعداد ذات أهداف معينة يتم بواسطتها اختراق نظام الرقابة الداخلية لتحقيق أهداف غير مشروعة مما أدى إلى أن المراجع أصبح يعمل في ظل ظروف عدم التأكد، وليس لديه ما يؤكد بالدليل أو القرينة أنها ذات التعليمات التي يتم تنفيذها فعلاً خلال الفترة المحاسبية وبالتالي افتقار القوائم المالية إلى المصداقية (ليلى عبد الحميد لطفى، 1997، ص 77) ، وعلى هذا يرى الباحث أنه من أجل تقييم نظام الرقابة الداخلية في ظل تكنولوجيا المعلومات يجب على المراجع أن يكون ملماً بالأمور التالية:

1- معرفة سياسات أمن المعلومات ومفهوم دورة حياة النظام والأساليب الرقابية على إعداد برنامج التطبيق.

2- معرفة أساليب التصريح والوصول وطرق المعالجة الآمنة وأساليب حماية البيانات.

كما يجب أن يكون لديه مهارة القدرة على تحليل وتقييم سياسات الأمن وإجراءاته وتقييم وسائل حماية البيانات كالتشفير والحماية من الفيروسات والقدرة على إجراء المتابعة المستمرة.

الفصل الخامس الدراسة الميدانية

أولا هدف الدراسة: -

في ضوء ما انتهى إلية الباحث في الدراسة التحليلية تستهدف الدراسة التطبيقية اختبار صحة فرض البحث والمتمثل في تؤثر مخاطر تكنولوجيا المعلومات على تقييم المراجعين لنظام الرقابة الداخلية.

ثانيا منهج الدراسة: -

إن المنهج الذي سيتبعه الباحث لتحقيق أهداف الدراسة هو تحديد أهم المشاكل المتعلقة بتقييم المراجعين لنظام الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات وقياس أهم الأساليب المقترحة لاكتشافها.

ثالثا أدوات الدراسة: -

قام الباحث باستخدام قائمة الاستقصاء كأحد أهم الأدوات البحثية لتحليل رأى عينة من المراجعين الخارجيين وبعض أساتذة الجامعات، كما أستخدم أسلوب المقابلات الشخصية لتدعيم استخدام الأسلوب السابق.

1/3مجتمع وعينة الدراسة: -

قياسا على الكثير من الدراسات السابقة يعتبر المراجعين الخارجيين وأساتذة الجامعات مجتمعا مناسبا لأجراء مثل هذه الدراسة، وقد شملت الدراسة بعض المكاتب الكبيرة والمتوسطة والصغيرة، والتي تم اختيارها عشوائيا ، وتم توزيع قائمة الاستقصاء عليهم وكان حجم العينة 75 مفردة

2/3 إدارة قائمة الاستقصاء:

قام الباحث بتوزيع قائمة الاستقصاء على أفراد العينة بنفسه حيث دعم الباحث أسلوب الاستقصاء بأسلوب المقابلات الشخصية، وترك الباحث لهم فرصة للرد وقد بلغت القوائم التي تم توزيعها كالتالي: -

القوائم	الموزعة	غير المستلمة	المستلمة	المستبعدة	المستخدمة
عدد	75	14	61	8	53
نسبة	100	18.6	81.4	13.1	86.9

4/3 التحليل الإحصائي للردود: -

لقد تم تحويل بيانات قائمة الاستقصاء الى أرقام كما يلي: -

1. نوع المؤهل بكالوريوس التجارة وما يعادله رقم (1) – ودبلومه المحاسبة والمراجعة رقم (2) -ماجستير في المحاسبة رقم (3) -والدكتوراه رقم (4).
2. سنوات الخبرة تم إدخالها كما هي بدون تغيير.
3. الأسئلة التي تتكون أحابتها من نعم تأخذ رقم (2) – ولا تأخذ رقم (1).
4. الأسئلة الترتيبية والتي بها 5 اختيارات إلى حد كبير جداً -إلى حد كبير -إلى حد متوسط إلى حد قليل -إلى حد قليل جداً – فقد تم أعطائها الأوزان التالية بالترتيب الآتي 5-4-3-2-1.

وقد تم إدخال البيانات السابقة في برنامج SPSS ويوضح الملحق (ب) النتائج الإحصائية الناتجة من استخدام البيانات والبرنامج المستخدم.

اختبار صحة فرض الدراسة

تؤثر مخاطر تكنولوجيا المعلومات على تقييم المراجعين لنظام الرقابة الداخلية يتم تحليل هذا الفرض من خلال الأبعاد الرئيسية التالية:

1- جودة الأساليب الحالية في اكتشاف مشاكل الرقابة في ظل تكنولوجيا المعلومات

2- مشاكل تطبيق الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات

3- العوامل المؤثرة على مكونات هيكل الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات

أولاً: -يمكن تحليل وجهة نظر المبحوثين في استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية ومدى مساعدته على اكتشاف مشاكل الرقابة في ظل بيئة تكنولوجيا المعلومات

جدول (1)

الاستجابة	التكرار	النسبة
نعم	5	%9.4
لا	48	%90.6

نلاحظ من الجدول السابق أن عدد من يرون أن استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية يساعد على اكتشاف مشاكل الرقابة في ظل بيئة تكنولوجيا المعلومات هو خمس مبحوثين فقط بنسبة 9.4% من إجمالي العينة أما باقي المبحوثين وعددهم 48 مفردة بنسبة 90.6% من عينة الدراسة يرون أن استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية لا يساعد على اكتشاف مشاكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات ومن ثم نتجه إلى تحليل المشاكل التي قد تكون سبباً في هذه المشكلة من وجهة نظر الباحث.

ثانياً: المشاكل التي تؤدى إلى عدم فعالية الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية

جدول (2)

العبارة	نعم		لا		الإجمالي	
	عدد	نسبة	عدد	نسبة	عدد	نسبة
الاختراق الخارجي من قبل برامج أخرى (الفيروسات)	43	%81.1	5	%9.4	48	%100
الاختراق الداخلي من قبل العاملين بالمنشأة	43	81.1	5	9.4	48	%100
اختفاء الدليل المادي الملموس وسند المراجعة	46	%86.8	2	%13.2	48	%100
الفصل غير الملائم بين المهام والوظائف	39	%73.6	9	%16.4	48	%100
كل المشاكل السابقة	38	%71.7	10	%18.9	48	%100

من الجدول السابق يتضح لنا ما يلي: -

أ -القائلين بأن الاختراق الخارجي من قبل برامج أخرى (الفيروسات) من المشاكل التي تؤثر على استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية هو 43 عينة من المبحوثين بنسبة 81.1%

ب -عدد المبحوثين القائلين بأن الاختراق الداخلى من قبل العاملين بالمنشأة من المشاكل التي تؤثر على استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية هو 43 مفردة بنسبة 81.1% .

جـ -عدد المبحوثين القائلين بأن اختفاء الدليل المادى الملموس وسند المراجعة من المشاكل التي تؤثر على استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية هو 46 مفردة بنسبة 86.8%

د -عدد المبحوثين القائلين بأن الفصل غير الملائم بين المهام والوظائف من المشاكل التي تؤثر على استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية هو 39 مفردة بنسبة 73.6%

هـ -عدد المبحوثين القائلين بأن جميع المشاكل السابقة هي المشاكل التي تؤثر على استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية هو 38 مفردة بنسبة 71.7%

ومما سبق يمكن القول بأن المشاكل السابقة هي من أهم المشاكل التي تعوق استخدام الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية عن اكتشاف مشاكل الرقابة في ظل بيئة تكنولوجيا المعلومات.

❖❖ ويمكن معرفة الأهمية النسبية للعبارات السابقة عن طريق تحليل الأهمية النسبية بواسطة اختبار فريدمان (Friedman Test) للمشاكل التي تؤدى إلى عدم فعالية الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية

جدول (3): الأهمية النسبية لمشاكل الرقابة فى ظل بيئة تكنولوجيا المعلومات

العبارات	متوسط الرتب	كا2	المعنوية
الاختراق الخارجي من قبل برامج أخرى	3.00	167.578	0.00
الاختراق الداخلي من قبل العاملين بالمنشأة	3.00		
اختفاء الدليل المادي الملموس وسند المراجعة	2.81		
الفصل غير الملائم بين المهام والوظائف	3.25		
كل المشاكل السابقة	3.31		

كما هو موضح في الجدول السابق يلاحظ أن مستوى المعنوية أقل من 5% وهذا يدل على وجود اختلاف فى الأهمية النسبية للمشكلات السابقة من وجهة نظر عينة الدراسة.

كما يلاحظ أن أعلى متوسط رتب هو للعنصر القائل كل المشاكل السابقة =3.31 وأقل متوسط رتب هو للعنصر القائل اختفاء الدليل المادي الملموس وسند المراجعة = 2.81.

فمن الملاحظ أن جميع المشاكل السابقة هي من مشكلات الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات والتي بسببها يصعب اكتشاف الغش والتلاعب أما عن اختفاء الدليل المادي الملموس وسند المراجعة فيأتي في المرتبة الأخيرة من حيث الأهمية النسبية من وجهة نظر عينة الدراسة ونخلص من ذلك أن المشكلات التي وضعها الباحث هي من أهم مشكلات الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

ثانياً-العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية (بيئة الرقابة – تقييم المخاطر – أنشطة الرقابة – المعلومات والاتصالات – المتابعة) في ظل استخدام تكنولوجيا المعلومات.

جدول (4)

العبارات	إلى حد كبير جداً		إلى حد كبير		إلى حد متوسط		إلى حد قليل		إلى حد قليل جداً		الإجمالي	
انتهاك الإدارة لنظم الرقابة الداخلية	2	%3.8	30	%56.6	12	%22.6	8	%15.1	1	%1.9	53	%100
تهديدات مرتبطة بسلوك موظفي المنشأة	3	%5.7	25	%47.2	16	%30.2	7	%13.2	2	%3.8	53	%100
عدم تدريب العاملين على	2	41.5	20	%37.7	1	1.9	6	11.3	4	%7.5	53	%100

أساليب تكنولوجيا المعلومات	2	%											
عدم وجود تفويض سليم للسلطات	3	%5.7	29	%54.7	11	%20.8	8	%15.1	2	3.8	53	%100
عدم تعرض نظم تكنولوجيا المعلومات للتعديل والتحريف من قبل الغير	16	30.2 %	24	%45.3	3	%5.7	7	%13.2	3	%5.7	53	%100
عدم وجود دليل مستندي مما يتطلب الاعتماد علي الرقابة الاتوماتيكية	18	%34	20	%37.7	5	%9.4	6	%11.3	4	%7.5	53	%100
عدم المحافظة على سرية وامن وخصوصية المعلومات المنتقلة عبر الشبكات	9	%17	32	%60.4	2	%3.8	6	%11.3	4	%7.5	53	%100
عدم وجود نسخ احتياطية للمعلومات والملفات والبرامج	6	11.3 %	19	%35.8	18	%34	6	%11.3	4	%7.5	53	%100
ضعف التوصيل الجيد للمعلومات لكافة المستويات الإدارية	1	%1.9	23	%43.4	17	%32.1	6	%11.3	6	11.3 %	53	%100
عدم وجود أساليب جيدة لمتابعة إجراءات الالتزام بالسياسات الرقابية	1	%1.9	26	%49.1	15	%28.3	7	%13.2	4	%7.5	53	%100

من الجدول السابق يتضح لنا الآتي:

أ -عدد المبحوثين القائلين بأن انتهاك الإدارة لنظم الرقابة الداخلية من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية إلى حد كبير جدا هم عدد 2 مفردة من العينة والقائلين إن لها تأثير كبير هم 30 مفردة بنسبة 56.6% من العينة وهذا يدل على اقتناع المبحوثين بأن انتهاك الإدارة لنظم الرقابة الداخلية من أهم العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

ب -أما عدد المبحوثين القائلين بأن هناك تهديدات مرتبطة بسلوك موظفي المنشأة إلى حد كبير جداً هم 3 مفردات من العينة بنسبة 5.7% من العينة أما الذين قالوا بأن لها تأثير إلى حد كبير هم 25 مفردة من مفردات الدراسة بنسبة 47.2% وها يدل أيضا على أن عامل التهديدات المرتبطة بسلوك موظفي المنشأة من العوامل المؤثر على مكونات هيكل الرقابة الداخلية فى ظل بيئة تكنولوجيا المعلومات.

جـ -وبالنسبة لعدد المبحوثين القائلين بأن عدم تدريب العاملين على أساليب تكنولوجيا المعلومات من العوامل الهامة المؤثرة على مكونات هيكل الرقابة الداخلية هم 42 مفردة بنسبة 79.2% من عينة الدراسة وهذا يدل على أن عدم تدريب العاملين على أساليب تكنولوجيا المعلومات من أهم العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

د -عدد المبحوثين القائلين بأن عدم وجود تفويض سليم للسلطات من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية إلى حد كبير جدا هم عدد ثلاث مفردات بنسبة 5.7% من العينة والقائلين أن لها تأثير كبير هم 29 مفردة بنسبة 54.7% من العينة وهذا يدل على اقتناع المبحوثين بأن عدم وجود تفويض سليم للسلطات من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

هـ -عدد المبحوثين القائلين بأن عدم تعرض نظم تكنولوجيا المعلومات للتعديل والتحريف من قبل الغير من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية إلى حد كبير جدا هم عدد 16 مفرده بنسبة 30.2% من العينة والقائلين أن لها تأثير كبير هم 24 مفردة بنسبة 45.3% من العينة وهذا يدل على اقتناع المبحوثين بأن عدم تعرض نظم تكنولوجيا المعلومات للتعديل والتحريف من قبل الغير من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

و -عدد المبحوثين القائلين بأن عدم وجود دليل مستندي مما يتطلب الاعتماد على الرقابة الأتوماتيكية من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية إلى حد كبير جدا هم عدد 18 مفرده بنسبة 34% من العينة والقائلين إن لها تأثير كبير هم 20 مفردة بنسبة 37.7% من العينة وهذا يدل على اقتناع المبحوثين بأن عدم وجود دليل مستندي مما يتطلب الاعتماد على الرقابة الأتوماتيكية من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

ز -عدد المبحوثين القائلين بأن عدم المحافظة على سرية وامن وخصوصية المعلومات المنتقلة عبر الشبكات من العوامل التى تؤثر على مكونات هيكل الرقابة الداخلية إلى حد كبير جدا هم عدد 9 مفرده بنسبة 17% من العينة والقائلين أن لها تأثير كبير هم 32 مفردة بنسبة 60.4% من العينة وهذا يدل على اقتناع المبحوثين بأن عدم المحافظة على سرية وامن وخصوصية المعلومات المنتقلة عبر الشبكات من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات،

ح -عدد المبحوثين القائلين بأن عدم وجود نسخ احتياطية للمعلومات والملفات والبرامج من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية إلى حد كبير جدا هم عدد 6 مفرده بنسبة 11.3% من العينة والقائلين أن لها تأثير كبير هم 19 مفردة بنسبة 35.8% من العينة وهذا يدل على اقتناع المبحوثين بأن عدم وجود نسخ احتياطية

للمعلومات والملفات والبرامج من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

ط -عدد المبحوثين القائلين بأن ضعف التوصيل الجيد للمعلومات لكافة المستويات الإدارية من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية إلى حد كبير جدا هم عدد 1 مفرده بنسبة 1.9% من العينة والقائلين إن لها تأثير كبير هم 23 مفردة بنسبة 43.4% من العينة وهذا يدل على اقتناع المبحوثين بأن عدم ضعف التوصيل الجيد للمعلومات لكافة المستويات الإدارية من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات

ومما سبق يتضح لنا أن العوامل السابقة هي العوامل الرئيسية التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل الاستخدام المتزايد لتكنولوجيا المعلومات

ويمكن معرفة الأهمية النسبية للعبارات المكونة للبعد السابق عن طريق تحليل الأهمية النسبية للعوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات

جدول (5) الأهمية النسبية للعوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات

العبارات	متوسط الرتب	كا2	المعنوية
انتهاك الإدارة لنظم الرقابة الداخلية	6.11	174.70	0.00
تهديدات مرتبطة بسلوك موظفي المنشأة	5.85		
عدم تدريب العاملين على أساليب تكنولوجيا المعلومات	8.01		
عدم وجود تفويض سليم للسلطات	6.05		
تعرض نظم تكنولوجي المعلومات للتعديل والتحريف من قبل الغير	7.53		
عدم وجود دليل مستندي مما يتطلب الاعتماد على الرقابة الأتوماتيكية	7.40		
عدم المحافظة على سرية وأمن خصوصية المعلومات المنتقلة عبر الشيكات	7.12		
عدم وجود نسخ احتياطية للمعلومات والملفات والبرامج	5.45		
ضعف التوصيل الجيد للمعلومات لكافة المستويات الإدارية	4.92		
عدم وجود أساليب جيدة لمتابعة إجراءات الالتزام بالسياسات الرقابية	5.28		
عوامل أخرى	2.27		

كما هو موضح في الجدول السابق يلاحظ أن مستوى المعنوية أقل من 5% وهذا يدل على وجود اختلاف في الأهمية النسبية للعوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات.

كما يلاحظ أن أعلى متوسط رتب هو للعنصر القائل عدم تدريب العاملين على أساليب تكنولوجيا المعلومات =8.01 وأقل متوسط رتب هو للعنصر القائل للعوامل الأخرى = 2.27.

فمن الملاحظ أن عدم تدريب العاملين على أساليب تكنولوجيا المعلومات هو أهم عامل من العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية وظل بيئة تكنولوجيا المعلومات أما عن العوامل الأخرى فتأتى في المرتبة الأخيرة من حيث الأهمية النسبية من وجهة نظر عينة الدراسة حيث أنه لم يذكر أي عامل جديد من وجهة نظر المبحوثين وهذا يدل على اتفاق المبحوثين على أن العوامل السابقة هي العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات.

ثالثاً: قياس معامل الارتباط بين العوامل المؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات (متغير تابع) ومشاكل تطبيق الأساليب الحالية للمساعدة على اكتشاف مشاكل الرقابة في ظل بيئة تكنولوجيا المعلومات (متغير مستقل).

جدول (6)

المتغير المستقل	معامل ارتباط بيرسون	المعنوية
مشاكل تطبيق الأساليب الحالية للمساعدة على اكتشاف مشاكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات	0.447	0.001

من خلال الجدول السابق نستطيع استنتاج ما يلي: -

- وجود علاقة ارتباط بين المتغير المستقل (مشاكل تطبيق الأساليب الحالية للمساعدة على اكتشاف مشاكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات) والمتغير التابع (العوامل المؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات) حيث أن معامل الارتباط هو 0.447 كما أن مستوى المعنوية (الدلالة) 0.001 وهو أقل من 5% وهذا أيضاً يدل على وجود علاقة ارتباط بين المتغير التابع والمتغير المستقل.

رابعاً: قياس معامل الانحدار بين العوامل المؤثر على مكونات هيكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات (متغير تابع) ومشاكل تطبيق الأساليب الحالية للمساعدة على اكتشاف مشاكل الرقابة في ظل بيئة تكنولوجيا المعلومات (متغير مستقل).

جدول (7)

المتغير المستقل	قيمة معامل الانحدار	الثابت	قيمة T	الدلالة Sig.	معامل التحديد R2
مشاكل تطبيق الأساليب الحالية للمساعدة على اكتشاف مشاكل الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات	0.0065	5.23	3.571	0.001	0.46

يتضح من الجدول السابق ما يلي: -

- إشارة معامل الانحدار موجبة للمتغير المستقل، فإن ذلك يعنى أن العلاقة بين المتغير المستقل والمتغير التابع علاقة طردية، بمعنى أن الزيادة في المتغير المستقل تؤدى إلى الزيادة في المتغير التابع.

- إن زيادة المتغير المستقل بمقدار وحدة واحدة يؤدى إلى تغير طردي في المتغير التابع بمقدار 0.0065 وحدة تقريباً.
- أن مستوي الدلالة لاختبار T- test للمتغير المستقل مع المتغير التابع هي 0.001 وهى أقل من مستوي معنوية 5% و هذا يدعم صحة الفرض بوجود علاقة معنوية ذات دلالة إحصائية بين تأثير استخدام تكنولوجيا المعلومات على تقييم المراجعين لنظام الرقابة الداخلية.
- يوضح معامل التحديد R^2 النسبة المئوية للتفسيرات التي يستطيع تفسيرها المتغير المستقل للتغيرات التي تطرأ على المتغير التابع حيث أن قيمة معامل التحديد R^2 هي 0.46
- يمكن صياغة نموذج الانحدار البسيط للمتغير المستقل على المتغير التابع: -

❖ المتغير المستقل (م): مشاكل تطبيق الأساليب الحالية لفحص وتقييم نظام الرقابة الداخلية في ظل بيئة تكنولوجيا المعلومات

❖ المتغير التابع (ص) العوامل التي تؤثر على مكونات هيكل الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات

ص= 5.23 + 0.0065م

ومن التحليلات السابقة يمكن أن نخلص إلى صحة الفرض القائل " تؤثر مخاطر تكنولوجيا المعلومات على تقييم المراجعين لنظام الرقابة الداخلية.

الخاتمة (نتائج الدراسة)

خلص الباحث الى مجموعة من النتائج أهمها ما يلي: -

1- ان لمخاطر تكنولوجيا المعلومات أثر بالغ على نظام وهيكل الرقابة الداخلية ،حيث سيتسع نطاق ومهام نظام الرقابة الداخلية ومن ثم تعرضه لمزيد من المخاطر (كمخاطر تتعلق باختفاء الدليل المادي الملموس ،مخاطر تتعلق بسند المراجعة وسهولة التلاعب والغش، مخاطر الفيروسات ..... أخ) تلك المخاطر جعلت مكونات وعناصر هيكل الرقابة الداخلية الخمس المتعارف عليها غير كافية لرقابة أنشطة تكنولوجيا المعلومات مما تطلب ضرورة تعديلها لتتلاءم مع أنشطة وخصائص تكنولوجيا المعلومات كإضافة عنصر الاستجابة للمخاطر وعنصر التوافق والتكامل بين النواحي الإدارية –ا لتكنولوجية – القانونية مع موقع المنشأة على net .

2- ظهور العديد من المخاطر والمشاكل التي تعيق عمل المراجع التقليدي عند تنفيذ مهام عملية المراجعة في ظل بيئة تكنولوجيا المعلومات، ومن ثم التأثير السلبي على رأيه الفني المحايد ومن أهم هذه المشاكل ما يلي: -

- مشاكل متعلقة بنظام الرقابة الداخلية.
- مشاكل خاصة بجمع أدلة الإثبات الالكترونية.

3- بالرغم من الاهتمام المتزايد بتكنولوجيا المعلومات على كافة المستويات ومن كافة المؤسسات الهادفة وغير الهادفة للربح، إلا أنها لم تحظى بالاهتمام الكافي من قبل المراجعين، على الرغم من الحاجة الشديدة للدور الذي يمكن أن يلعبه المراجع في هذا المجال من أجل بث مزيد من الثقة والاطمئنان والأمان للأطراف المتعاملة من خلالها مما يساهم في تقليل فجوة التوقعات بشكل كبير

4- يمكن مراجعة تكنولوجيا المعلومات وأساليبها بأحد الأسلوبين التاليين: -

- أن يتم مراجعتها في إطار المراجعة المالية لحسابات المشروع ككل باعتبارها جزءا من الأنشطة التي يمارسها المشروع بصفة عامة.
- ان يقوم المراجع بتصميم إجراءات توضع خصيصا لمراجعتها مع استحداث أساليب المراجعة التي تناسبها.

ويفضل الباحث الأسلوب الثاني نظرا للطبيعة المتميزة لأنشطة تكنولوجيا المعلومات، حيث تتصف بالديناميكية والاستمرارية والمسار غير المرئي لمراجعتها، كما أن الأدلة تكون الكترونية وليست ورقية.

قائمة المراجع:

أولا العربية:

1- د/ أحمد عبد السلام أبو موسى: أهمية مخاطر نظم المعلومات المحاسبية الالكترونية، دراسة تطبيقية على المنشآت السعودية، مجلة التجارة والتمويل، كلية التجارة، طنطا، العدد الثاني، 2004.

2- د/ أحمد عبد القادر أحمد، مجالات استخدام منشآت الأعمال لتكنولوجيا الإنترنت وانعكاسات ذلك على مهنة المراجعة، مجلة الدراسات والبحوث التجارية، كلية التجارة -جامعة بنها، العدد الثاني، 2003.

3- د/ السيد عبد المقصود دبيان، د/ وليد السيد كشك، الاتجاهات الحديثة في الرقابة الداخلية على أمن نظم المعلومات في ظل التجارة الإلكترونية ودور المعايير الدولية، مؤتمر التجارة الإلكترونية: الأفاق والتحديات، كلية التجارة -جامعة الإسكندرية، يوليو 2002 (25 -27).

4- د/ سعاد حسن خضر وآخرون، المراجعة وتقييم الرقابة الداخلية في ظل تشغيل البيانات الموزعة، المجلة العلمية للاقتصاد والتجارة، كلية التجارة -عين شمس، العدد الأول، 1996.

5- د/ شريف سعيد البراد، الثقة في نظم المعلومات مقارنة بين الواقع المصري والأمريكي – دراسة ميدانية تطبيقية، مجلة الاقتصاد والتجارة، كلية التجارة، عين شمس، العدد الرابع، اكتوبر 2000.

6- د/ صلاح الدين الهتيمى -د/ آمنة ماجد الربيجات، أثر التهديدات الأمنية في ضوء تطبيق الحكومة الإلكترونية، دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمان الكبرى، مجلة المحاسبة والتأمين والإدارة، كلية التجارة -جامعة القاهرة، 2005.

7- د/ عادل عبد الرحمن أحمد، دراسة تحليلية لأثر النشر الإلكتروني للبيانات والتجارة الإلكترونية على طبيعة عملية المراجعة ومسئولية المراجع مع دراسة اختبارية للنشر الإلكتروني للبيانات في السعودية، مجلة البحوث التجارية، كلية التجارة ببنها، العدد الثاني، 2003.

8- د/ عبد الوهاب نصر على -د/ شحاته السيد، الرقابة والمراجعة الحديثة في بيئة تكنولوجيا المعلومات وعولمة أسواق المال (الواقع والمستقبل)، الدار الجامعية، 2006.

9- د/ عبيد سعد المطيرى، مستقبل مهنة المحاسبة والمراجعة تحديات وقضايا معاصرة، دار المريخ، 2004.

10- د/ ليلى عبد الحميد لطفي، أثر استخدام النظم الإلكترونية في المراجعة على كفاءة الأداء المهني للمراجع، المجلة العلمية لكلية التجارة، جامعة الأزهر، العدد الثالث عشر، يونية 1997.

11- د/ محمد عبد الفتاح محمد، إطار مقترح لمراجعة نظم معلومات التجارة الإلكترونية، مجلة الفكر المحاسبي، العدد الأول، السنة السابعة، 2003.

12- د/ محمد مصطفى أحمد الحبالى، الاتجاهات الحديثة في المراجعة في ظل المتغيرات التكنولوجية في نظم المعلومات المحاسبية، مجلة الاقتصاد والتجارة، كلية التجارة -عين شمس، العدد الأول، يناير 2003.

13- د/ منير محمد الجنيهى، د/ ممدوح محمد، الشركات الإلكترونية، دار الفكر الجامعي، 2005.

14- د/فاروق جمعة عبد العال، دور المعلومات المحاسبية في زيادة المنفعة من منظومة التجارة الإلكترونية، مجلة الدراسات والبحوث التجارية، كلية التجارة ببنها، العدد الأول، 2003.

15- أ/ أماني حسين كامل خليل، إطار مقترح لتقييم الرقابة الداخلية لأنشطة التجارة الإلكترونية، رسالة دكتوراه -غير منشورة، كلية التجارة -جامعة حلوان، 2006.

16- أ/ أمل عبد الفضيل عطية: إطار مقترح لمراجعة التجارة الإلكترونية، رسالة دكتوراه غير منشورة، كلية التجارة، جامعة بنها، 2006.

ثانيا الاجنبية:

1- Debreceny Roger & G.L. Gray, "Financial Reporting on Internet and The External Audit", The CPA Journal, April 2003. (Www. Nysscpa. Org/cpa Journal/ 2003/)

2- - Ryan S.D. Bardalai, "Evaluating Security Threats in Mainframe and Client / Server Environments", The CPA Journal, Vol. 30, 2005. (www .nyss cpa /cpajournal/1997)

3- - Coe, Kathleen, "Employees: The First Line of Defense", It Audit, the Institute of Internal Auditors, USA, Vol. 6, Jan 2003. (Www. Theiia.org/it audit)

4- OECD, (Organization for Economic Co-operation and Development), "Guidelines for the Security of Information systems", The Council of the OECD, 26 November, 1992. (On line, www. The OECD. Org).

5- P. Raul Lin, "System Security Threats and Control", The CPA Journal, July 2006, Issue. (www .nyssCPA..Org/ CPA Journal/ 2006/ 706/Essentilas/ P.58.htm).

6- Requel Filipek, "Botnets could invading Your Net Work", It Audit, Vol. 19, Jan 2006.

7- AICPA, SAS No 94, "The Effect of Information Technology on the Auditor's Consideration of Internal Control in Financial Statement Audit", May 2001 (www. Aicpa. Com) Au. Section 319. Parag 19.

8- Teresa. Wingfield, "Effective It Controls: Why Continuous Mounting Requires Automation", It Audit, Vol 9. Nov 10, 2006. (Www. Theiia. Org/ It Audit/ Index. Cfm? Iid = 502 & Catid = 218 aid = 2421).

9- The Committee Of Sponsoring Organizations Of The Tread Way Commission (Coso), "Enterprise Risk Management Frame Work", 2003. (On Line : www. Erm. Coso. Org).

10- Alain. Valiquette, "Introducing New It Systems Into Sarbanes- Oxley Compliant Environment", It Audit, Vol 9, Nov 10, 2006. (www. Theiia. Org/ It Audit/ Index. Cfm? Catid = 218 IId = 502).

11- Leuhlfing, M.E. "Defending The Security Of The Accounting System", The CPA Journal, October 2000 . (www. Nysscpa. Org/ cpa Journal/ 2000/…).

12- Lanz J. "Worst Information Technology Practices In Small to Mid- Size Organization" The CPA Journal, April 2002.

13- International Audit Services, 2004, "Arisk Management Approach to Audit and Implementing Internal Controls", Internal Audit Management.(www. Clydesdale. Com, Audit- Management.htm).

14- -Elsff. M. M and Salms- SH, "Information Security Management, Apierarchical From work For Varialls Approaches", Computer & Security, Vol 19, 2000.

15- Mahadevan,c. "E- Commerce Security- Components Which make it safe", Information Systems Control Journal, 2001 . (www. Is aca. Org/ art 20. Htm).

16- Lin, L, "Internet Security", information Systems Control Journal, 2001.