نموذج مقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية

A Proposal Model for Auditing Electronic Accounting Information System Security

دكتورة أماني هاشم السيد حسن هاشم(۞)

طبيعة المشكلة:

يلعب أمن المعلومات الأن دوراً هاماً لأسباب عديدة ، منها ما تتعرض له الشبكات من مخاطر ، فسواء تعامل البشر مع نظم المعلومات المحاسبية الإلكترونية والغش والتلاعب بمختلف أنواعهم ، وأعطال الشبكات ، وتلف الأجهزة والبرامج ووسائط التخزين ، والهجمات الناتجة عن الفيروسات والبرامج الضاره ، تمثل بعض هذه المخاطر ، وقد تعددت الدراسات والأبحاث التى تحدد دور المراجع فى هذا التوجه ،إلا أن الأمر بحاجة إلى تبنى متغير هام له الأثرالفعال ، وهو برنامج المراجعة والذى يلزم أن يضع أمن نظم المعلومات المحاسبية من بين أولوياته .

ومن المتفق عليه مهنياً وعملياً أن المراجع يؤدى دوره من خلال إطارعلمى وعملى من محدداته برنامج المراجعة ، والذى من أولوياته أن يتفق ومبادئ ومعاييرالمراجعة العامة المتفق عليها ، لذا فهو بحاجة إلى التطوير ليتفق ومستجدات بيئة أمن نظم المعلومات المحاسبية الإلكترونية .

وبناء على ما تقدم فإن هذا التوجه يحتاج إلى إطار من المحددات الواضحة التى تشكل إستراتيجية لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية ، تأخذ فى اعتبارها النقاط التالية :

(۞) مدرس المحاسبة كلية التجارة – جامعة الأزهر فرع بنات القاهرة.

١- إرساء الأمن الشامل للمنشأة، بما يواكب طبيعة واحتياجات بيئة الأعمال مع مراعاة المستجدات المستقبلية المتوقعة.

٢- توجهات المراجعة العادية والروتينية المتعلقة بإبداء الرأى فى البيانات الموضحة بالقوائم المالية، مع فحص لنظام المعلومات القائم على هذه البيانات والسياسات والمعايير المطبقة فى المنشأة مثل الموازنات التخطيطيه و نظام الرقابة الداخلية.

٣- مراعاة احتياجات برنامج المراجعة من مجالات جديدة مثل الخبرات الهندسية والإحصائية والفنية لتغطية مستجدات أمن بيئة التعامل الإلكترونى .

فالأمر بحاجة إلى الإجابة على السؤال التالى :

ما هو برنامج المراجعة الذى يناسب توجهات المنشآت الأمنية فى ظل المخاطر الحالية والمستجدة لأمن نظم المعلومات المحاسبية الإلكترونية؟

يتبنى السؤال السابق مجموعة من الأسئله الفرعية التالية :

- هل برنامج المراجعة الحالى يناسب التوجهات الأمنية؟
- ما هى المستجدات التى يمكن أن تطرأ على برنامج المراجعة ليفى باحتياجات الأمن الحالية والمستقبلية؟
- ما هو الإطار العام لبرنامج مراجعة يحقق الأمن الشامل للمنشأة فيما يتعلق بأمن نظم المعلومات المحاسبية الإلكترونية؟

تحاول الدراسة الإجابة على الأسئلة السابقة، وتلك هى مشكلتها .

أهمية الدراسة:

يعد موضوع الدراسة من أهم المواضيع للأسباب التالية :

١ . أمن الأفراد والمنشآت والأنظمة يدعمه أمن المعلومات .

٢ . يلزم أن تتبلور مراجعة أمن نظم العلومات المحاسبية الإلكترونية عبر نموذج ذات كفاءة وفعالية مرتفعة لمراجعتها .

وفى اعتقاد الباحثة أن هذا الموضوع لن يتقادم ، فكل يوم يطالعنا الجديد ، فى عالم المعرفة الذى لاسقف له ، ولذلك فنحن بحاجة إلى توجه جديد يدعم هذه الثوابت .

هدف الدراسة:

تسعى هذه الدراسة إلى تحقيق الأهداف التالية :

١ . التوجه الصادق والفعال نحو تدعيم أمن الأنظمة المحاسبية الإلكترونية .

٢ . تبنى نموذج جديد مقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية .

تساؤلات الدراسة:

حتى تتمكن الدراسة من تحقيق أهدافها فيلزم الإجابة على الأسئلة التالية :

١ . ما هى الدعائم التى يرتكز عليها النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية؟

٢ . ماهى الخطوات المقترحة لإرساء نموذج ذات كفاءة و فعالية مرتفعة ، لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية ؟

منهج الدراسة:

تتبع هذه الدراسة المنهج الاستقرائى للوقوف على آخر الأخطار التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية ، ومحاولة التصدى لها من قبل فريق المراجعة ،

وفى سبيل تحقيق ذلك، لجأت الباحثة إلى مجموعة من المراجع، منها الكتب والدوريات العربية والأجنبية وكذلك المؤتمرات والندوات المحلية و العربية والدولية، كما قامت باستقراء الكثير من المقالات والمؤتمرات والندوات على شبكة المعلومات التى تناولت هذا الموضوع بإسهاب شديد ، وخاصة الأجنبية منها .

خطة الدراسة:

تحقيقاً لأهداف الدراسة تم تقسيمها إلى أربع مباحث كما يلى :

المبحث الأول : تناول الدراسات المحاسبية السابقة المتصلة بالموضوع .

المبحث الثانى : تناول الاعتبارات التى تبناها النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية .

المبحث الثالث : تناول معايير المراجعة التى بنى عليها النموذج المقترح .

المبحث الرابع : تناول النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية .

المبحث الأول

الدراسات المحاسبية السابقة

وتعرض وفق ترتيب زمنى يبدأ من الأحدث لبعض الدراسات السابقة حول الموضوع :

Gary Swindon ,Study,2006 (١/١)

تهدف هذه الدراسة إلى تحقيق الإلتزام والمحاسبة بالنسبة لقواعد الأمن فى قانون التأمين الصحى الأمريكى ، فيمكن أن يقوم المراجعون الداخليون بدور فعال فى عملية الإلتزام بمساعدة المنشآت فى الحصول على كسب أكبر من خلال مراجعة الأمن بالقانون السابق.

فيلزم أن يرتكز الإلتزام فى قانون التأمين الصحى الأمريكى على ثلاث نقاط هى :

١- تحديد نموذج الحوكمه بالمنظمة.

٢- الإهتمام بجداول المراجعة، فى جميع مستويات الرقابة، مع تحديد البنود التى تثير الإنتباه فى مجال المراجعة.

٣- تحديد أهم القواعد ومتطلبات الأوضاع بواسطة التنظيمات المترتبة على طبيعة المنشأة (كمثال : خاصة، غير هادفة لتحقيق الربح، تجارية عامة) .

وقد توصلت الدراسة إلى أن التوافق الناتج عن الإلتزام بمتطلبات المراجعة من القواعد المختلفة، وتبنى المنظمات لنموذج الحوكمة يمكن أن يلقى الضوء على الإحتياجات الأساسية للتغييرات فى أسلوب المنشأة فى مواجهة مخاطر تكنولوجيا المعلومات واستعمالات مصادرها .

(٢/١) Requel Filipek, study, 2006 :

وتهدف هذه الدراسة إلى بيان خطورة botnets وأن عدد متزايد من المنظمات يقع ضحية لها دون معرفتهم، لذلك فلابد من عمل خطوات لحماية الشبكات والحاسبات المتعلقة بها، حتى يتم إحباط هذه الهجمات.

يجد لصوص الإنترنت طرق سرية لاقتحام الشبكات والمثال الحالى هو استعمال الـbots، برامج الربوت التى تغزو الكمبيوتر وتمكن المهاجم من السيطرة على الحاسب من بعد، حيث يعتبر العديد من خبراء أمن المعلومات أن الريبوتات تعد التخوف الأمنى الأول بسبب انتشارها العريض التطور والاستعمال المستمر للأنشطة الغير شرعية.

وقد خلصت الدراسة إلى طرق محاربة الـ Botnets وذلك بعمل استراتيجيات تسمح بإصلاح الكمبيوتر بأحدث الأنظمة ضد الفيروسات وغيرها، واستعمال الحوائط النارية ، وعزل الحاسبات التى كانت خارج المكتب ، وتغيير كل كلمات السر Password للشبكة المصابة وللمستخدمين، ثم إعادة توصيل الحاسب للشبكة بعد التأكد من أنه قد تم تنظيفه تماماً وخلوه من الفيروسات، وتطبيق سياسات لفرض عقوبات على المستخدمين لمن يقوم منهم بتشغيل برامج غير معروفة على الأجهزة.

(٣/١) J. Stephen McNally, 2005, Study: :

تهدف هذه الدراسة إلى تقييم مستويات الرقابة بالمنشأة، فيلزم تقييم فعالية تصميم وتنفيذ هذه الضوابط، بالإضافة إلى دراسة تفصيلية وعملية على الرقابة على المعاملات، وتحديد مستويات الرقابة بداخل المنشأة والتى لها أكبر الأثر على الإفصاح فى القوائم المالية، و توجد ستة خطوات يمكن إتباعها تتمثل فى متطلبات مستويات الرقابة، هذه الخطوات تحدد ما يلى :

- خطة المشروع وتحديد معالمه الرئيسية.
- بناء هيكل لتقييم مستويات الرقابة بالمنشأة.
- الحصول على مدخلات لتصميم مستويات الرقابة بالمنشأة.
- توثيق وتقييم مستويات الرقابة بالمنشأة.
- اختبار فعالية مستويات الرقابة بالمنشأة.
- الدمج بين تصحيح الأخطاء والتحسين المستمر .

وقد توصلت الدراسة إلى أن هذه الخطوات تناسب شركات القطاع العام ، ولا تناسب شركات القطاع الخاص والمنشآت غير الهادفة لتحقيق الربح ، وأيضا يمكن أن يحقق مزايا نتيجه لتشغيله والحصول على أفضل الممارسات والتى تؤدى إلى حوكمة رشيدة ونتائج ماليه طيبة.

(٤/١) دراسة م. إبراهيم محمد عبد المنعم -٢٠٠٤

وتهدف هذه الدراسه إلى ، إيضاح أهمية مراجعة نظم المعلومات مع عرض لمنهجيات بناء نظم المعلومات المختلفة، بالإضافة إلى إرساء للمفاهيم الأساسية لبناء النظم، مع تقييم لنظم المعلومات بطريقه سهلة تساعد على إستلام النظام من الجهة المنفذة له ،كما يهدف أيضا إلى تقسيم المستفيدين إلى ثلاث طوائف مختلفة متمثلة فى :

- جهات بناء النظم لتحديد مطالبها جيداً بناء على البنود المذكورة.
- الجهات المنفذة للتقيد بالمنهجيات التي تحدد مراحل بناء النظم.
- جهات مراجعة جودة بناء نظم المعلومات.

وقد توصلت الدراسة للنتائج التالية:

إمكانية تقييم الأنظمة وفقا لمجموعات مختلفة من المتغيرات منها :

- الاستفادة المحسوسة وتعرف بدرجة إعتقاد مستخدم النظام بأن النظام لا يحتاج إلى مجهود عند تطبيقه.
- اليسر ويعرف بدرجة التى يعتقد مستخدم النظام بأنه لا يصعب عليه تطبيقه.
- الاستعمال ويعرف بالزمن المستخدم لتطبيق النظام.

(٥/١) دراسة د.عبيد دياب العجيلى، ٢٠٠٤:

وتهدف هذه الدراسة إلى تحديد الأدوات و الوسائل التى يمكن الإعتماد عليها لتأمين صلاحية نظام المعلومات مع تصور شامل للمخاطر وأنواعها و سبل علاجها والفترات الزمنية المستغرقة فى ذلك، مع إيضاح لأنواع الخلل التى يمكن أن تصيب أنظمة المعلومات وأثر ذلك على موارد المنشأة المصابة مع عرض لمجموعة من الأدوات المرشدة للمراجعيين والمدققين فى تحديد نقاط الضعف بالنظام لعلاجها ، ومن هذه الأدوات مصفوفة المخاطر.

وقد توصلت الدراسة إلى ضرورة الإلتزام بإيجاد الضوابط المناسبة لضمان سلامة نظم المعلومات وإعتماد المراجعيين والمدققين ذوى الخبرات العالية فى نظم المعلومات للتأكد من صلاحية أنظمة الرقابة الداخلية وأن إعدادها وتصميمها وتنفيذها تم طبقا للمواصفات القياسية العالمية.

(٦/١) دراسة أ.د/ سمير أبو غابه، ٢٠٠٣:

تهدف هذه الدراسة إلى تحليل أساليب الرقابة المختلفة الخاصة بأمن الأنظمة الإلكترونية للمعلومات بدراسة العناصر التالية :

- المخاطر المنتظر أن تواجهها الأنظمة الإلكترونية للمعلومات.

- الأساليب المادية للرقابة لتحقيق أمن الأنظمة الإلكترونية للمعلومات.
- الأساليب الإجرائية للرقابة لتحقيق أمن الأنظمة الإلكترونية للمعلومات.

وقد توصلت الدراسة إلى ما يلى:

- ضرورة أن نضع فى اعتبارنا أن تطبيق أساليب الرقابة المختلفة الخاصة بأمن الأنظمة الإلكترونية سيقلل احتمال تعرض هذه الأنظمة لمخاطر مختلفة.
- ويجب أن نضع أيضاً فى الاعتبار صعوبة إرساء نظام تشغيل إلكترونى آمن بنسبة مائه فى المائه.
- ونود أن ننبه إلى أن مراجعى الأنظمة الإلكترونية يلزم أن يهتموا إهتماما بالغاً بأمن الأنظمة الإلكترونية وأساليب الرقابة المختلفة التى يمكن أن تحقق الأمن الشامل، هذا وعليهم التأكد بصفة دورية ومستمرة من مدى كفاية هذه الإساليب وفاعليتها.

وقد ركزت الدراسات السابقة على النقاط التالية:

١- دور نموذج الحوكمة بالمنظمة فى إحداث التغيير.

٢- تطبيق سياسات لفرض عقوبات على المستخدمين لمن يقوم منهم بتشغيل برامج غير معروفة على الأجهزة.

٣- النموذج المقترح يمكن أن يحقق مزايا نتيجة لتشغيله والحصول على أفضل الممارسات والتى تؤدى إلى حوكمة رشيدة ونتائج ماليه طيبة.

٤- إمكانية تقييم الأنظمة وفقاً لمجموعات مختلفة من المتغيرات.

٥- إعتماد المراجعيين ذوى الخبرات العالية فى نظم المعلومات للتأكد من صلاحية أنظمة الرقابة الداخلية، وأن إعدادها وتصميمها وتنفيذها تم طبقاً للمواصفات القياسية العالمية.

٦- أن مراجعى الأنظمة الإلكترونية يلزم أن يهتموا إهتماما بالغاً بأمن الأنظمة الإلكترونية وأساليب الرقابة المختلفة التى يمكن أن تحقق الأمن الشامل، هذا وعليهم التأكد بصفة دورية ومستمرة من مدى كفاية هذه الإساليب وفاعليتها.

بإستعراض الدراسات المحاسبية السابقة ، تستنتج الباحثة أن هذه الدراسات قد حققت الهدف الذى أعدت من أجله، إلا أنها لم تتناول موضوع الدراسة وهو إرساء نموذج مقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية هذا ما دعا الباحثة إلى تناوله بالبحث والدراسة.

المبحث الثانى

الاعتبارات التي يتبناها النموذج المقترح

بداية تشير الباحثة إلى أن تنفيذ النموذج المقترح يتطلب التنسيق بين مصممي النظام ومنفذيه والمستفيدين منه للتوصل الى مزاياه التي تم الإتفاق عليها بين الخبراء والمستفيدين.

فيلزم انجاز النموذج المقترح وفقا لما يلي:

١- تحقيق الاهداف التي يسعى النموذج إلى إرسائها .

٢- الإلتزام بالوقت المحدد للإنجاز.

٣- الأخذ فى الاعتبار أمن نظم المعلومات المحاسبية الإلكترونية، مع تطوير مايدعمها من الإجراءات والإستراتيجيات، طبقا لما هو مخطط .

وذلك لإرساء نموذج مقترح فعال لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية بما يتفق مع كافة الاعتبارات والإمكانيات بما يضمن استمرارية النظام من حيث التعديل والإضافة – كما سيرد في الخطوة السادسة في النموذج المقترح – بما يوفي متطلبات واحتياجات المستفيدين (د. أحمد مصطفى ناصف، ٢٠٠٤، ص٩ بتصرف).

وحتى يستمد النموذج فعالياته وكفاءته فلابد من توافر مجموعة من الاعتبارات المختلفة اللازم أخذها في الاعتبار قبل التقديم للنموذج المقترح تتمثل فيما يلي:

(١/٢) قيود بناء النظام ويمكن للباحثة تقديمها في النقاط التالية:

(١/١/٢) القيود الأخلاقية:

وهي القيود التي تفرضها القوانين الأخلاقية التي فرضتها الأديان وماتعارف عليه البشر من حيث الصدق والأمانة وتقدير جهود الآخرين.

(٢/١/٢) القيود السياسية والاجتماعية مثل منع بناء نظم تساعد على ارتكاب الجريمة أو نشر الرزيلة أو ترويج الممنوعات (أ.ابراهيم محمد عبد المنعم ،٢٠٠٤ ص٦).

(٣/١/٢) القيود الاقتصادية وهي ماقد تفرضها بعض الدول على مواطنيها تحت شعارات مختلفة مثل حماية المنتجات الوطنية وما شابه ذلك .

(٤/١/٢) قيود حماية الملكية الفكرية بمعنى إعادة النظر في جميع الدعاوى المتشددة والتي تؤدي لتقييد الملكية الفكرية ، مع ضرورة مراجعة القوانين الوطنية التي يتم اعدادها حاليا بما يلائم الملكية الفكرية والموقف الدولي الجديد ومن أهم سماته المرونة في التفسير (د . صلاح الدين فهمي محمود ،٢٠٠٢ ص٢١ بتصرف).

(٢/٢) يلزم أن تحدد جميع أنواع المخاطر التي يتعرض لها نظام المعلومات المحاسبية قبل تحقيق أهداف المنشأة ، كما يجب أن يفهم المراجع خطوات مراجعة برنامج نظم المعلومات الإدارية ، وتوضح الباحثة خطورة دورالخبرة والتدريب و المعرفة في كفاءة وفعالية فريق المراجعة، عند قيامه بمهامه .

(٣/٢) إن توثيق نظم المعلومات من أهم العناصر لضمان جودة واستمرارية النظام حيث ، يلزم توثيق جميع مراحل تحليل وتصميم وتنفيذ نظام المعلومات وهو يشمل (د . محمد عز الدين الشرقاوي، ٢٠٠٤ ، ص٣) :

(٢/٣/١) توثيق النظام المفاهيمي لقاعدة البيانات Conceptual Database Design وهو لا يشتمل توثيق تصميم قاعدة بيانات النظام القائم فحسب بل بالنسبة للنظام المقترح وتوثيق الفروق بين المفاهيم الموجودة في النظامين.

(٢/٣/٢) توثيق التصميم المنطقي لقاعدة البيانات Logical Database design وهي تشمل خطوات تحويل النظام المفاهيمي إلى نظام منطقي وتحديد الاعتمادية الدالية Functional dependencies .

(٢/٤) منهجية النظام Methodology System (م.ابراهيم محمد عبد المنعم، ٢٠٠٤، ص٦-٧):

وترى الباحثة أنها تعبر عن شرح دقيق لكل خطوة من خطوات تنفيذ النظام وكذلك تحديد المطلوب لكل مرحلة من مراحل بناء النظام المحاسبي، مع بيان لدور الأفراد والجماعات لتنفيذ المهام المحددة في كل مرحلة، مع الأخذ في الاعتبار المخرجات المحاسبية المطلوبة ودرجة جودتها ومعايير قياسها لكل مرحلة من مراحل النظام المحاسبي، مع عدم إغفال الوسائل المستخدمة لتطوير البناء وتنفيذ كل مهمة محاسبية ، مع العلاج السريع للأخطاء .

(٢/٥) تقييم النظام:

ويتم ذلك بمعرفة لجنة من المراجعين الداخليين بالمنشأة ، وتؤكد الباحثة في هذه المرحلة على أهمية التأهيل العلمي لفريق المراجعة من حيث درايته بمعلومات كافية عن وثائق التكويد وخطة بناء قواعد البيانات ووثائق تركيب الشبكات وكل مايتطلبه عمل فريق مراجعة أمن نظم المعلومات المحاسبية الإلكترونية، وذلك بموجب النموذج التالي(م.ابراهيم محمد ،٢٠٠٤،ص٣٣) :

نموذج اختبار وثائق النظام المتبع لمراجعة أمن نظم المعلومات المحاسبية

System Documents Test Model for Auditing Accounting Information System Security

مسلسل	ملاحظات	التقييم	الدرجة العظمى	المكون
١			٤٠	مراجعة وثائق التكويد
٢			٢٠	مراجعة وثيقة دليل المستخدم
٣			١٠	مراجعة وثيقة خطة التركيب
٤			١٠	مراجعة وثيقة خطة بناء قواعد البيانات
٥			١٠	مراجعة وثيقة تركيب الشبكات
٦			١٠	مراجعة وثيقة صيانة الأجهزة والمعدات
٧			٢٠	مراجعة وثيقة صيانة المباني المقام عليها العمل
			١٢٠	التقييم النهائي

رفض... قبول... إبداء الملاحظات.....

توقيع أعضاء لجنة المراجعة والاستلام ..... التاريخ / /

وتؤكد الباحثة أن هذا النموذج للتقييم سوف يفيد في الخطوة السادسة في النموذج المقترح من قبل الباحثة نظرا لأهمية الأول في التطوير بمعرفة مواطن الأخطاء وبالتالي العلاج السريع لها مع الأخذ في الاعتبار التطوير المستمر وتلك مضمون الخطوة السادسة من النموذج المقترح .

(٦/٢) وأخيرا تؤكد الباحثة على أهمية تلافي النموذج المقترح للأخطاء التالية (د.أمين السيد أحمد لطفي، ٢٠٠٤، ص٤٤٣و٤٤٤):

(١/٦/٢) أخطاء في تصميم نظام الرقابة الداخلية والتي قد تتمثل في تصميم غير كاف لنظام الرقابة الداخلية الشامل .

(٢/٦/٢) غياب الفصل بين الواجبات .

(٣/٦/٢) غياب الفحص الملائم والموافقة عن العمليات المالية والقيود المحاسبية.

(٤/٦/٢) إجراءات غير كافية لتقييم وتطبيق المبادىء المحاسبية .

(٥/٦/٢) احتياطيات غير كافية لحماية الأصول بجميع أنواعها .

(٦/٦/٢) غياب أساليب رقابية أخرى تتسق ونشاط العملية المالية .

هذا عن الضوابط التي يلزم توافرها في النظام قبل تصميمه ، وترى الباحثة أنه من الملائم الأخذ في الاعتبار معايير المراجعة الدولية والعربية والمصرية التي بنى عليها النظام ، وتلك موضوع المبحث القادم.

المبحث الثالث

معايير المراجعة التي بنى عليها النموذج المقترح

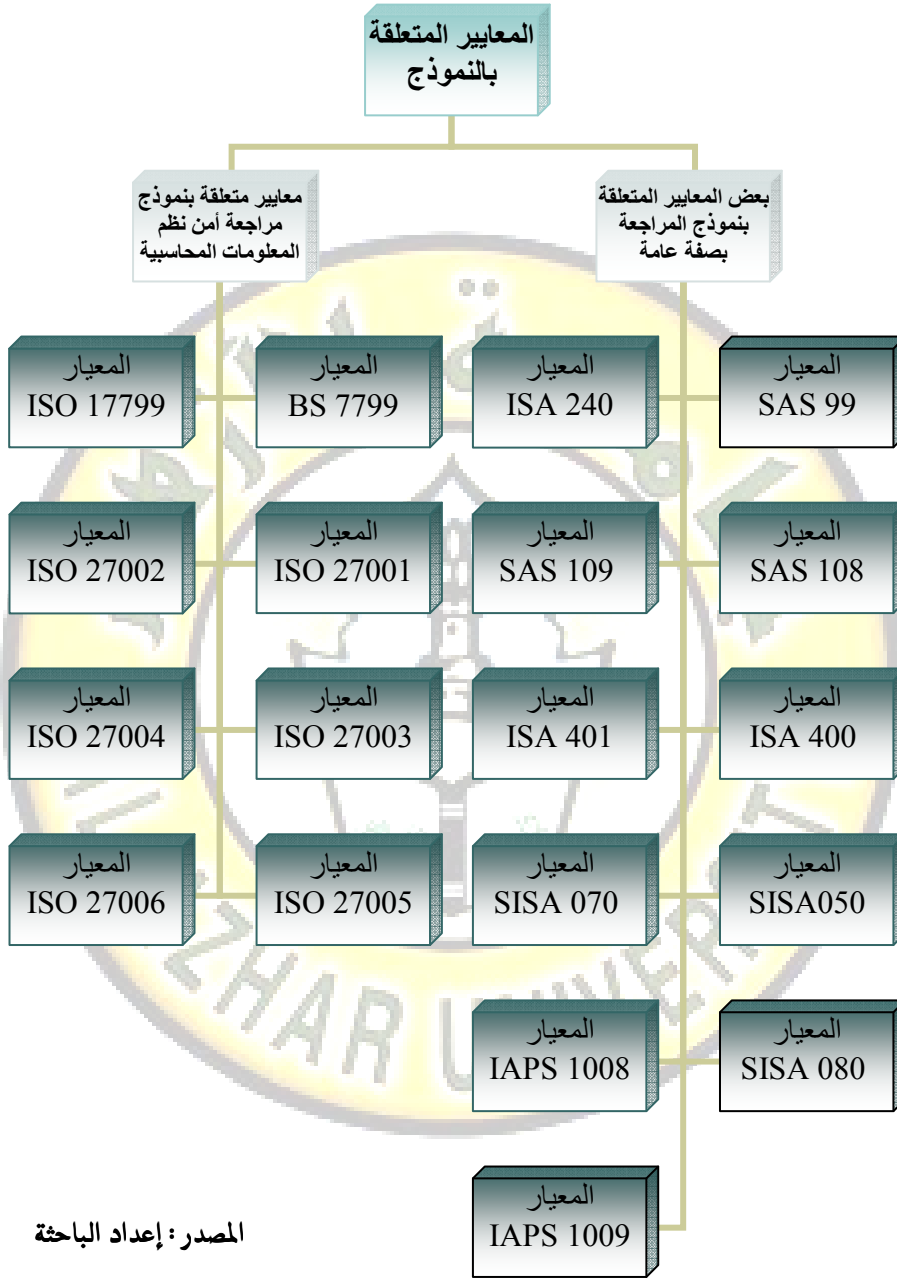
Auditing Standards For The Proposal Model

تم تصميم المعايير للحصول على نتائج أكثر فعالية لمراجعة النموذج المقترح كنتيجة للتقييم الأدق للمخاطر وتطوير التصميم وأداء إجراءات المراجعة للاستجابة للمخاطر ، وهذاسوف يجعل المراجعين أكثر قدرة على التركيز على تلك المناطق التي تكون فيها نسبة الخطر أعلى(John A. Fogarty, Lynford Grham, 2006,p.2)

رأت الباحثة أن المعايير المتصلة بنموذج مراجعة أمن نظم المعلومات المحاسبية الإلكترونية كثيرة ومتشعبة، لذلك اقتصر التقديم على المعايير المتعلقة بإعداد النموذج، وأمن المعلومات وأيضاً بيئة التشغيل الإلكتروني قدر الإمكان لخدمة أهداف الدراسة، وتضيف الباحثة أن حقل المعايير ثماره متجددة، فكل يوم يتم تعديل الإصدارات المتاحة أو استحداث إصدارات جديدة للحاجة إليها ، وفيما يلي إيضاح لبعض المعايير المتصلة بالنموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية :

١. بداية ستقدم الدراسة الشكل رقم (١/٣) وهو يوضح المعايير المتعلقة بالنموذج بشكل عام .

٢. يلى ذلك شرحه بالتعليق على كل إصدار سواء تم تطبيقه بالفعل، أو أنه معيار مرتقب له علاقة بموضوع أمن نظم المعلومات المحاسبية الإلكترونية.



المصدر : إعداد الباحثة

الشكل رقم (١/٣) شكل يوضح المعايير المتعلقة بالنموذج

(١/٣) بعض المعايير المراجعة المتعلقة بالنموذج بصفة عامة:

(١/١/٣) معيار المراجعة الدولي رقم (ISA 240) وأهم ما يتعلق بهذا المعيار بالنسبة لموضوع مراجعة أمن المعلومات وترى الباحثة ضرورة إلتزام فريق المراجعة بممارسة الشك المهني الجماعي Brain Storming في وجود تلاعب عند وضع خطة المراجعة(د . عبد الوهاب نصر، ٢٠٠٥ ، ص١٨)، ويتفق معيار المراجعة الامريكي رقم (٩٩) SAS مع المعيار السابق في ذلك ، إلا أنه يختلف عنه في رؤيته ضرورة توافر ثلاثة محددات للتلاعب هى :

- توافر دافع للتلاعب.
- وجود ضعف فى الرقابة الداخلية لتحويل الدافع لواقع.
- وجود التبرير لإرتكاب التصرف.

ويتم تكثيف الإستفسارات للإدارة لتحديد مخاطر التلاعب، مع الأخذ فى الاعتبار تبريرات الأفراد كشرط لحدوث التلاعب، وتوفير إرشادات أوضح لتقدير المخاطر الناجمة عن التحريفات الجوهرية، عدم سلامة الإعتراف بالإيراد ، وأخيراً وضع ضوابط متى تكون الإدارة معوقة للرقابة الداخلية (د . عبد الوهاب نصر، ٢٠٠٥، ص٢١).

من العرض السابق يتضح إهتمام المعيار SAS.99 والمعيار ISA.240 بالتفكير الجماعى الخلاق، ومما يؤكد ذلك الإتجاه، تبنى لجنة مراجعة التقارير المالية بمجمع المحاسبين والمراجعيين القانونيين الأمركيين AICPA[1] له، حيث أوضحت أن أعضاء لجنة المراجعة عليهم أن يزيدوا من فعالية تعاملهم مع الإدارة بالنسبة للرقابة الداخلية وأن يتبادل الأعضاء فيما بينهم أفكار Brainstorming فيما يختص بكيف وأين يمكن أن تقع الإدارة فى الغش، وترى الباحثة أن ماسبق إيضاحه من

(1) http://www.w3j.com/5/53.instone.html

محددات وردت بالمعيارين السابقين. يلزم أخذهما فى الاعتبار لتخطيط المراجعة فى النموذج المقترح.

(٣/١/٢) المعيار الدولى للمراجعة ISA.400 بعنوان «تقدير المخاطر والرقابة الداخلية» ، من متطلبات هذا المعيار مايلى :

- أن يقوم المراجع بعمل تقدير للمخاطر الملازمة ولمخاطر الرقابة لتوكيدات القوائم المالية الرئيسية (د . طارق عبد العال حماد ، ٢٠٠٤ ، ص٢٠١).
- مراعاة بيئة أنظمة المعلومات التى تستخدم الحاسب الآلى عند تصميم إجراءات المراجعة لتقليل مخاطرها لأدنى حد (د .طارق عبد العال حماد ، ٢٠٠٤ ، ص٢٠٣).

(٣/١/٣) المعيار الدولى للمراجعة ISA.401 بعنوان «بيئة التشغيل الإلكترونى للمعلومات لأغراض معايير المراجعة الدولية» ، ومن أهم ما تناول هذا المعيار فى الفقرات من ٤ ـ ٦ما يلى :

- مستوى المهارة والكفاءة التى يلزم أن تتوافر للمراجع عند تنفيذ عملية المراجعة فى بيئة التشغيل الإلكترونى للمعلومات.
- الإرشادات بشأن تفويض العمل للمساعدين ممن تتوافر لديهم هذه المهارات (د . محمد عبد الدايم، ٢٠٠٤ ، ص٣).

وقد إنبثق هذا المعيار من معيار المراجعة رقم (٣) الذى أصدره مجمع المحاسبين القانونيين الأمريكيين عام ١٩٧٤ والذى تناول أساليب الرقابة على النحو التالى :

The Meaning and Purposes of Application Controls تختص أساليب الرقابة على التطبيقات بوظائف خاصة يقوم بأدائها قسم معالجة البيانات إلكترونيا وتهدف إلى توفير درجة تأكيد معقولة Reasonable Assurance عن سلامة عمليات تسجيل ومعالجة البيانات وإعداد التقارير، وتنقسم غالبا أساليب

الرقابة على التطبيقات إلى ثلاث مجموعات ، وهي أساليب الرقابة على المدخلات وأساليب الرقابة على معالجة البيانات وأساليب الرقابة على المخرجات (د .أحمد حجاج وآخرون، ٢٠٠٢ ، ص٣٥٣) .

(٤/١/٣) SISA050 Planning :

من متطلبات هذا المعيار أن يقوم مراجع نظم المعلومات بتخطيط عملية المراجعة مع فريق المراجعة الذي يقوم بعملية التخطيط (David C.Yang Liming Guan,2004,pp.552).

(٥/١/٣) SISA 070 Reporting :

من متطلبات هذا المعيار عند إعداد تقرير المراجعة فعلى مراجع نظم المعلومات أن يحدد المجال والأهداف والفترة التي تتم فيها المراجعة وكيفية أداء عملية المراجعة، وأن يعرف المنشأة ويحدد النتائج والتوصيات التي يلزم على المراجع أخذها في الاعتبار(David C.Yang Liming Guan,2004,pp.553).

(٦/١/٣) SISA 080 Follow-up activities :

من متطلبات هذا المعيار أن يقوم المراجع بمتابعة الأنشطة ويسأل ويقيم النتائج والتوصيات والملخصات في التقرير السابق وماهو الموقف المتخذ حيالها والوقت والطريقة التي تم التصرف بها(David C.Yang Liming Guan,2004,pp.553).

(٢/٣) معايير متعلقه بنموذج مراجعة أمن نظم المعلومات المحاسبية:

(١/٢/٣) IAPS.1008

Risk Assessments and Internal Control Characteristics and Considerations

خصائص واعتبارات تقدير المخاطر والرقابة الداخلية لنظم المعلومات الإلكترونية.

(٢/٢/٣) IAPS. 1009

Computer Audit Techniques Assisted الأساليب الفنية للمراجعة المدعومة بالحاسب الآلي (د .أمين السيد لطفي، ٢٠٠٤، ص٤٦٠).

(٣/٢/٣) SAS. 108

Planning and Supervision وهو يتناول التخطيط والإشراف في الخطوة الأولى في النموذج وقد تم تداول هذا المعيار ليتم التأكد من الإدارة المكلفة بالحوكمة والمراجعين وافقو أن تتضمن المراجعة المعيار 108 SAS للتخطيط والإشراف اللذان من متطلباتهما أن يحصل المراجعون على توضيحات مكتوبة من العميل تحترم مدة التعاقد **(Tohn A.Fogarty, Lynford Graham, 2006, p.3)**

(٤/٢/٣) SAS. 109

Understanding The Entity and Its Environment and Assessing The Risks of Material Misstatement

الفهم التام لكينونة البيئة وتقييم المخاطر المحيطة ، فإجراءات تقييم المخاطر فحسب لا تكفي كأساس لتكوين رأي المراجع بل يجب أن يقترن بها التفكير الجماعي لإيجاد حالة Brainstorming وهو ماورد في المعيار SAS 99السابق ذكره وأيضا تناول المعيار SISA 050 ومن متطلبات هذا المعيار أن يقوم مراجع نظم

المعلومات بتخطيط عملية المراجعة وذلك بوصف الأهداف مع مراعاة الاقتران في معايير المراجعة .(Tohn A. Fogarty, Lynford Graham, 2006, p.3)

(٥/٢/٣) ISO. 17799

تتناول الدراسة أهم معايير أمن المعلومات، وهو المعيار الذي تبناه قانون أمن المعلومات الأمريكي Sarbanes-Oxley Act 2002، و المعيارالأول فى الولايات المتحدة الأمريكيه الذى تناول أمن المعلومات، أسوة بالمعيار البريطانى BS. 7799 ، وقد تم تطبيق المعيار ISO. 17799 كبداية عام ٢٠٠٠ و تم تحديثه[٢] فى ١٥يونيو ٢٠٠٥، و تم تصميمه لتلبية إحتياجات الشركات التي ترغب فيما يلى :

١. تطوير فعالية إدارة أمن المعلومات وتعزيز الممارسات والجهود الأمنية .

٢. ويد المعيار كبار المديرين بمعلومات قيمة تتصل بموضوعات الأمن والتي يمكن أن تطبق قبل تقييم، المخاطر، وتشمل أيضا أفضل الممارسات بشأن تحديد الأصول الهامة.

٣. كما يمد بمعلومات عن دور الهياكل التنظيمية كجزء من جهود أمن المعلومات، مثل الأنواع المختلفة من الرقابة المطبقة لتخفيف المخاطر الإدارية والتقنين والرقابة المادية، فعلى سبيل المثال إجراء.

٤. فحوص الأداء لأقسام الموارد البشرية تعتبر إحدى أنواع الرقابة الإدارية المتنوعة المطبقة لتخفيف المخاطر (MARKT. EDMEAD, June 10, 2006, P.1)

(2) http://www.w3j.com/5/53.instone.html

(٦/٢/٣) سلسلة ISO 27000 [٣] :

ومن الجدير بالذكر أن سلسلة ISO 27000 هى مجموعة من المعاييرتحدد قضايا ومواضيع هامة خاصة لدعم أمن المعلومات ، والتالى فكرة موجزه عنها بالترتيب :

١- ISO.27001 بعنوان «أمن المعلومات الإدارية مع تحديد أدلة الإثبات» ، وقد تم تطبيق هذا المعيار فى أكتوبر ٢٠٠٥.

٢- ISO.27002 بعنوان «أمن المعلومات الموحدة» ومن المتوقع أن يحل محل المعيار ISO.17799 في أواخر عام ٢٠٠٧.

٣- المعيار ISO.27003 بعنوان «أمن المعلومات ونظم إدارة تنفيذ العمليات» ومن المتوقع أن يتم تطبيقه في ٢٠٠٧- ٢٠٠٨ .

٤- المعيار ISO.27004 هذا المعيار يتتبع إيجاد معايير لقياس فاعلية التطبيقات الأمنية وتشمل قضايا مثل ماذا نقيس؟ كيف نقيس؟ ، ومن المتوقع تطبيقه ٢٠٠٧- ٢٠٠٨ .

٥- المعيار ISO .27005 يغطي هذا المعيار المقبل أمن المعلومات وإدارة المخاطر .

٦- المعيار ISO. 27006 ويغطي هذا المعيار المقبل تطبيق وتنفيذ متطلبات خطة تغطية الكوارث Disaster Recovery Plan .

من العرض السابق للمعايير وكما سبق تقسيمها إلى نوعيين معايير مراجعة متصلة بنماذج المراجعة بصفة عامة، وأخرى متعلقة بأمن المعلومات، أصبح من اللائق التقديم للنموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية، وفقاً لمجموعة من الخطوات كما سيرد إيضاحها فى المبحث القادم.

(3) http://www.w3j.com/5/53.instone.html

المبحث الرابع

النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية
The Electronic Accounting Information System Security Proposal Model

نظراً لأن الهدف الأساسى للنموذج هو إرساء الأمن الشامل، فيلزم أن يعمل على منع الهجمات والتهديدات من النجاح في اخترق النظام وتحقيق أهدافها سواء بالحذف الكلي والجزئي أو السرقة للبيانات والمعلومات ، ومن المعروف أن هذه الأنظمة تهددها الكثير من المخاطر مثل الفيروسات viruses و warms وهي الشهيرة بالديدان وكذلك Botnets وهي عبارة عن هجمات على الشبكات من المناطق الضعيفة فيها للسيطرة على الشبكة دون معرفة القائمين عليها (Raquel Filipek ,2006 ,P.1)، لذلك كان لا بد من التحديث كما نوضح ذلك في الخطوة السادسة .

وقد تم تحديد ستة مراحل للنموذج المقترح كما يوضحها الشكل ١/٣ ، ويلي ذلك إيضاح لكل خطوة .

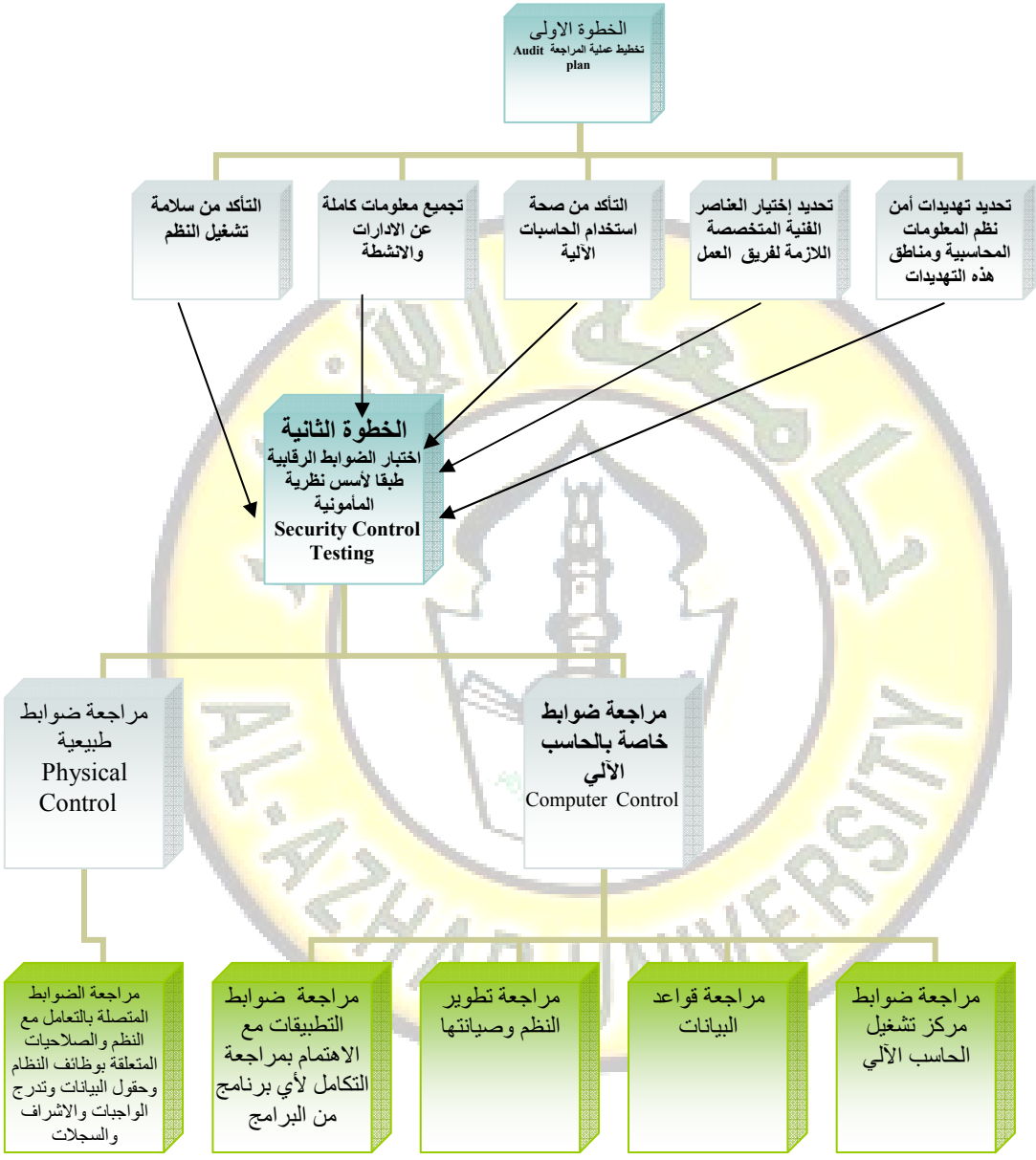
ثانياً : مراحل النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية :

Accounting Information System Security Proposal steps:

يوضح الشكل رقم (١/٤) مراحل النموذج التي تتمثل في ستة خطوات يتم تقديمها بالصورة التالية :

١ . بداية ستقدم الدراسة الشكل رقم (١/٤) وهو يوضح الخطوات المتعلقة بالنموذج بشكل عام .

٢ . يلى ذلك شرحه بالتعليق على كل خطوة من خطوات النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية .



الخطوة الثالثة

تابع الشكل رقم (١/٤)

تابع الشكل (١/٤)

المصدر : إعداد الباحثة

الشكل رقم (١/٤)

(٢/٤) خطوات النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية

(٤/٢/١) الخطوة الأولى : مرحلة تخطيط عملية المراجعة **Audit Plan** :

وتمثل الخطوة الأولى حجر الزاوية بالنسبة لعملية المراجعة ، حيث يهتم المراجع بتجميع معلومات كاملة عن الإدارات والأنشطة محل عملية المراجعة ، آخذا في الاعتبار كل التفاصيل والإجراءات ودورات العمل بها (د .أحمد عز الدين زيدان ، ٢٠٠٤ ، ص١٤) ، فيكون الاهتمام في هذه المرحلة بكفاءة وفاعلية العنصر البشري الفني المتخصص واللازم لفريق العمل ، والذي يقوم بدوره بتحديد مناطق الخطر المحتوية على تهديدات لأمن نظم المعلومات المحاسبية تحقيقاً للهدف العام لخطة المراجعة ، لذلك يتم تصميمه بما يتناسب مع احتياجات أمن المعلومات لذا فيلزم أن يتصف بالمرونة الكافية وهو يتطلب تكاليف ضخمة لتطبيقه كما يحتاج إلى فترة زمنية طويلة نسبياً لوضعه موضع التنفيذ (د .علي إبراهيم طلبة ، ٢٠٠٥ ، ص٣٢-٣٣) .

هذا وتتفق الباحثة مع رأى د . سمير أبو غابة في أن مراجعي أمن نظم المعلومات المحاسبية عليهم الاهتمام بأمن هذه الأنظمة وأساليب الرقابة المختلفة التي توفر أقصى درجات الأمن والتأكد بصفة مستمرة من كفاءة هذه الأساليب وفعاليتها ، وتضيف الباحثة ضرورة الأخذ في الحسبان مقارنة التكلفة بالعائد كما سبق وأن أوضحنا ، حيث يتم التنازل عن هذه الأنظمة للأمن في حالة ما إذا كانت الخسائر الناتجة عن حدوث المخاطر أقل من تكلفة تصميم الأنظمة لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية إلى أنظمة أقل منها تكلفة (طاهر الكري ، ٢٠٠٥ ، ص٢) .

تؤكد الباحثة أن الهدف من الخطوه الأولى هو التخطيط لعملية المراجعة، أخذاً فى الاعتبار تقييم الرقابة على الأمن، حيث يمكن أن يتم ذلك فى المنشآت الصغيرة والمتوسطة بعمل جداول أو مصفوفات للأمن تشمل عناصر الرقابة التالية:

- الرقابة على المنشأة بأكملها.
- الرقابة على الأجهزة.
- الرقابة على البرامج .
- الرقابة على المعلومات وتكاملها.

أما بالنسبة للمنشآت الكبيرة فيمكنها أن تطبق نظام الجداول كقاعدة ولكن بتفاصيل أكثر مع تطويرها بما يواكب حجم المنشأة (Ahmad A.Abo-Musa-2004-P.276)

(٢/٢/٤) الخطوة الثانية: مرحلة اختبار الضوابط الرقابية

Security Control Testing

تتناول هذه الخطوة اختبار الضوابط الرقابية، حيث تنقسم أنواع الضوابط إلى ما يلى:

- ضوابط وقائية .
- ضوابط كاشفة .
- ضوابط مصححة.

وقد أثبتت إحدى الدراسات (د . الهتيمي ود . آمنه ربيحات ، ٢٠٠٥) أن درجة فعالية الضوابط الوقائية ٧٧٪، والكاشفة ٧,٦٪، والمصححة ١٠٠٪.

هذا مع الأخذ في الاعتبار أنه يمكن تقسيم هذه الضوابط بطريقة أكثر فاعلية كما قسمها د . أحمد عز الدين زيدان (د .أحمد عز الدين زيدان، ٢٠٠٤ ص ١٢-١٣بتصرف) إلى نوعين:

الأول : ضوابط خاصة بالحاسب الآلي Computer Control :

وتخص ضوابط مركز التشغيل وقواعد البيانات وتطوير النظم وصيانتها وضوابط التطبيقات وتهتم بالتكامل الآلي لأي برنامج من البرامج .

النوع الثاني وهى ضوابط طبيعية Physical control :

تتصل هذه الضوابط بالتكامل مع النظم والصلاحيات الخاصة بوظائف النظام وحقول البيانات وتدرج الواجبات والإشراف والسجلات .

وترى الباحثة أن فريق مراجعة أمن نظم المعلومات المحاسبية عليه مراجعة الضوابط السابقة بإختلاف أنواعها ومسمياتها مع الأخذ في الاعتبار كفاءة وفاعلية نظام المراجعة ذلك كما أوضحه الشكل رقم (١/٤) بتطبيق نظرية المأمونية Reliability Theory والتي تقدم قياسا لدرجة إمكانية الإعتماد على نظام الرقابة عن طريق تقدير احتمال نجاح النظام في أداء مهمته (د .محمد محمود عبد المجيد ، ٢٠٠١ ، ص٤٤٥و٤٤٦) مع الأخذ في الاعتبار أنه لا بد من تحليل المخاطر Risk Analysis وهو يعنى المقارنة بين تكلفة التهديدات وتكلفة مقاومتها بتطبيق أدوات أمنية بتكلفة أقل من تكلفة أضرار التهديدات، وإحصاء التهديدات Enumerating Threats وفيها يتم تحديد كل التهديدات التى تواجه الشركة ثم تحليل خطورتها Threat Security Analysis حيث يتم تقدير تكلفة التهديدات واحتمال حدوثها ويتم ذلك بموجب المعادلة التالية :

خطورة التهديدات = تكلفة التهديد فى حالة نجاحه × احتمال نجاحه

(د . محمد عبد الدايم، ٢٠٠٤ ، ص٦) .

وتنبه الباحثة إلى أن أهمية هذه الخطوة تكمن فى التحديد الدقيق والواضح للتهديدات وتكاليفها ، مع تطبيق أحدث الأساليب الإحصائية فى حساب نسب حدوثها .

(٤/٢/٣) الخطوة الثالثة : الفحص والاختبار التفصيلي للعمليات

Detailed Testing Phase

وتتضمن هذه الخطوة إهتمام فريق مراجعة أمن نظم المعلومات المحاسبية ببعض العمليات بصورة تفصيلية من خلال مجموعة من الأدوات بعضها يعتمد على برنامج كومبيوتر (CAAT) Computer Assisted Audit Tools فيتم تركيب برنامج خاص للتعامل مع بعض العمليات الهامة ومتابعتها وتقييم ماتم بالنسبة لها (د .أحمد عز الدين زيدان ، ٢٠٠٤ ،ص١٣) طبقا لشروط المحددة مسبقا للوقوف على مدى ماتحققه من نتائج ، مع الأخذ في الاعتبار معايير أمن المعلومات وحمايتها وتكاملها (Stanly Weiner 1995,p.1) .

وتشير الباحثة إلى أن البرامج المستخدمة في عملية المراجعة يتم تطويرها من فترة لأخرى وأنه يلزم مراجعتها من فترة لأخرى وفقاً لحالتين (د .أحمد عز الدين زيدان ، ٢٠٠٥ ، ص١١) :

الأولى : أن يتم مراجعة التطوير بالجهود والموارد الذاتية وذلك يتطلب فريق مدرب من المراجعين الداخليين والخارجيين والذين يتحلو بالأخلاق في التعامل مع الموظفين والعملاء والمستهلكين والأطراف الأخرى (J.STEPHEN MCNALLY, 2005,p.2) ، وأن يتم التأكد من بيئة الأمن وتحديد فعالية الرقابة الداخلية ، ومدى الإلتزام بسياسات و إجراءات تكنولوجيا المعلومات مع الفهم التام لتعقيدات شبكات المعلومات وعدم الإنتظار إلى أن يحين إكتشاف نقاط الضعف .

بالشبكات والفهم التام لنظم التشغيل والبرمجيات والأجهزة والبرامج (Lakshmana rao Vmuri,2006, p.1)

الثانية : أن يتم مراجعة التطوير من خلال جهة خارجية متخصصة وموثوق في كفاءتها وخبرتها ، وتؤكد الباحثة على أهمية الأخلاق في هذا المجال إتفاقا مع الرأي السابق .

والهدف من هذه الخطوة اختبار فعلي لبعض العمليات اليومية Daily Transactions للإطمئنان على سلامة ودقة البيانات المتداولة في النظام (د .أحمد عز الدين زيدان ، ٢٠٠٤ ،ص١٣) .

وترى الباحثة أن هذه الخطوة هامة وتستند إلى مايتحلى به فريق مراجعة أمن نظم المعلومات المحاسبية من أخلاق و حياد واستقلال وأمانة وتدريب وخبرة عالية ، كما ترى الباحثة الاستعانة بمراجعين من المنشأة مع التحفظ على ماسبق ذكره من تدريب عالي وخبرة وكفاءة وأخلاق لأن ذلك يحقق هدفين :

الأول : السرية وهى حجر الزاوية بالنسبة لأمن المعلومات .

الثاني : الاكتفاء الذاتي وضغط التكاليف .

(٤/٢/٤) الخطوة الرابعة : اختبار الأرصدة Balances Tests

وتتضمن هذه الخطوة أن يقوم فريق مراجعة أمن نظم المعلومات بما يلى :

- تقييم نهائي ، لمدى صحة وسلامة ودقة كشوف الحسابات والقوائم المالية .
- هل توجد فروق ناتجة عن أخطاء في تنفيذ بعض نظم المعلومات المحاسبية ، والمثال على ذلك طرق حساب اهلاك الأصول وكذلك حساب المخصصات .
- التحقق من دقة البيانات المالية الأخرى (د .أحمد عز الدين زيدان ،٢٠٠٤ص١٤)

وتـرى الباحثـة ضـرورة أن يـتم في هـذه الخطـوة مايسـمى بمعاينـة الحمايـة Protective Sampling وبموجبهـا يقـوم فريـق مراجعـة أمـن نظـم المعلومـات المحاسبية بتطبيق أساليب الاختبار العشوائي للحصول على أكبر تغطية للقيم المالية للمجتمع، بحيث يضمن أن العناصر ذات القيمة المالية الكبيرة والتي يمكن أن تؤدي إلى أخطاء مالية كبيرة لم تهمل هذا إلى جوار الأساليب الأخرى (C.William Thomas , Emerson , 1986,p.368)

(٤/٢/٥) الخطوة الخامسة: إعداد التقرير: Preparing The Report of Audit

وتود الباحثة أن تنبه إلى أن التقرير النهائي لعملية المراجعة يجب أن يشـتمل علـى أهـداف المراجعـة ونطـاق عمليـة المراجعـة، والأسـاليب المتبعـة فيهـا، وأهـم الملاحظات والنتائج التي تم التوصل إليها، مؤيدة بالمستندات وذلك فضلا عن التوصيات النهائية (د .أحمد عز الدين زيدان،٢٠٠٤ص١٤)، ولقد أثبتت Barbara Arel أنه توجد علاقة مباشرة بين حوكمة المنظمات (لجنة المراجعة) وجودة تقاريرها المالية (Barbara Arel ,2005).

وتؤيد الباحثة رأي د .أحمد عز الدين زيدان، في ضرورة توافر اعتبارات معنية في التقرير النهائي لعملية المراجعة منها التأكيد على مسئولية الإدارة العليا فى إعتماد الضوابط الرقابية وهو ما يصفه Sarbanes-Oxley Act , 2002 بأنه إبداء الرأي فيما تعده الإدارة العليا من إجراءات رئيسية معتمدة وصادرة بشأن كفاءة وفاعلية المراجعة الداخلية.

و تقدم لجنة مراجعة أمن نظم المعلومات المحاسبية التقرير النهائي لعملية المراجعة (د .أحمد عز الدين زيدان، ٢٠٠٤، ص١٥ بتصرف)، وضمن ما يحدده (Sarbanes-Oxley act, 2002) مسئوليات لجنة المراجعة في شركات القطاع

العام التجارية بأمريكا إستقلالية كل عضو من أعضاء اللجنة كما يحدد عمله متطلبات أخرى (Ganesh M.Pandit-2006,p.42).

وتود أن تنبه الباحثة إلى ضرورة توافر مجموعة من الاعتبارات العامة الأخرى اللازم مراعاتها فى التقرير النهائى لعملية المراجعة، ومن أهمـــــها مايلى: (د .أحمد عز الدين زيدان، ٢٠٠٤، ص١٤-١٥)

١- تعريف و تحديد الإجراءات الرئيسية المعتمدة أو الصادرة من الإدارة العليا بشأن المراجعة الداخلية والتعليق على مدى كفاءتها وفعاليتها .

٢- توضيح أي اختلاف أو عدم توافق Non-Compliance مع المعايير المتعارف عليها في أمن المعلومات (وقد سبق إيضاحها فى المبحث الثالث).

٣- التعليق على مستوى المعرفة والتخصص والخبرة لدى العاملين بإدارة النظم وتكنولوجيا المعلومات ومدى إعدادهم وتأهيلهم لمواجهة المخاطر في مجال نظم المعلومات.

(٦/٢/٤) الخطوة السادسة: علاج الأخطاء والتحسين المستمر Engage in Gab Remediation and Continuous Improvement

تم في الخطوة الأولى التخطيط لعملية المراجعة وذلك بتجميع معلومات عن الإدارات والأنشطه وإجراءات أخرى ، وترى الباحثة أن تبدأ جهود العلاج بسرعة شديدة كلما أمكن ذلك، مع جعل مستويات الرقابة أكثر فاعلية وكفاءة ، فعلى سبيل المثال بالرغم من أن فريق المراجعة الداخلية يقوم بعملية تقييم شامل للمخاطر لتطوير خطة المراجعة السنوية، فسوف يكون قادراً على تحسين العمل بتطبيق إستقصاءات ذات تفاصيل أكبر عن عوامل المخاطر الخادعة، وعند السؤال عن متطلبات الإدارة لتقييم المراجعة الداخلية ، فالمقابلات الشخصية سوف تكون الأفضل (J.STEPHEN McNALLY, 2005, p.5) وذلك بالإضافة إلى نموذج

اختبار وثائق النظام المتبع لمراجعة أمن نظم المعلومات المحاسبية، وقد تم إيضاحه فى المبحث الثانى ، كما أن هذه المتطلبات سوف تزيد من معلومات ومفاهيم الادارة عن جودة هيكل الرقابة الداخلية ، لذلك فعلى الإدارة أن تأخذ ذلك في اعتبارها بصفة جدية.

هذا وترى الباحثة أنه بالنسبة للخطوة السادسة فيلزم مايلي :

١- يتم علاج الأخطاء عن طريق التغذية المرتدة Feed Back وذلك بمراجعة أخطاء النموذج بعد الإنتهاء من تشغيله ومعرفة طرق علاجها وذلك من خلال خبرة العاملين فى تطبيق النظام ، كما ترى الباحثة الاتصال بالمنشآت الأخرى التي تطبق النموذج مع تجميع الأخطاء واقتراح الحلول وتطبيقها كلما أمكن ذلك .

٢- أما بالنسبة للتطوير المستمر فإن الأمر هنا يختلف عن علاج الأخطاء حيث ترى الباحثة أن يكلف بعملية التطوير المستمر قسم البحوث والتطوير بالمنشأة الذي يقوم بإتصالاته لمعرفة الجديد في مجال مراجعة أمن نظم المعلومات وعمل الأبحاث في ذلك المجال مع الأخذ في الاعتبار ألا تزيد تكلفة البحوث عن تكلفة الخسائر الناجمة عن حدوث الأخطار المحيطة بالمنشأة.

٣- استخلاص نموذج جديد يربط بين علاج الأخطاء والتحسين المستمر يتبناه فريق المراجعة مستضيئاً بخبرته وممارسته لعملية مراجعة أمن نظم المعلومات المحاسبية وبذلك نصل إلى نوع جديد من المراجعين ، ليس مراجع نظم المعلومات المحاسبية الإلكترونية فحسب بل مراجع أمن نظم

المعلومات المحاسبية وهو التخصص الأكثر دقة والذي يحمي المنشأة من التهديدات الداخلية والخارجية.

و تنبه الباحثه إلى التحفظين التاليين:

١. أن نجاح النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية مرهون بتكاملة مع النماذج الأخرى المرتبطة بأهداف المنشأة، والتى يلزم أن يتم تنسيقها معا لتحقيق الهدف العام.

٢. الخطوات السابق الإشارة إليها تمثل الخطوات العامة اللازم إتباعها، بينما يجب أن يتم التعريف الواضح لمتطلبات بيئة الأعمال التى سيتم تطبيق النموذج فيها لتحديد ملامحه الخاصة به، ومن وجهة نظر الباحثة يتمثل أهمها فيما يلى:

- تعريف ومراجعة للمخاطر الحالية والمستجدة التى تواجه المنشأة اليوم وغدا.
- تحديد لنسب حدوث هذه المخاطر بتطبيق أحدث وأدق الأساليب الإحصائية والمتسقة مع نوع الأخطار محل الدراسة.
- حصر لتكاليف الأخطار المتوقعة.

وتضيف الباحثة أخيراً أن الأمن بيد الله سبحانه وتعالى. وبإنتهاء المبحث الرابع تكون الدراسة، قد توصلت إلى ملامح عامة للنموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية، وتمت الإجابه على تساؤل الدراسة الثانى.

وآخر دعوانا إن الحمد لله رب العالمين

الخلاصة :

تناولت الدراسة فى المبحث الأول الدراسات المحاسبية السابقة، بترتيب زمنى يبدأ من الأحدث فالأقدم .

وفى المبحث الثانى تناولت الاعتبارات التى تبناها النموذج المقترح متمثلة فى القيود التى بنى عليها النموذج وهى عباره عن قيود أخلاقية وسياسية واقتصادية اجتماعية وحماية الملكية الفكرية، يتم تحديد جميع أنواع المخاطر التى يتعرض لها نظام المعلومات المحاسبية الإلكترونية قبل تحديد أهداف المنشأة، يلزم تحليل وتصميم وتنفيذ نظام المعلومات، يلى ذلك تقييم النظام و أخيراً تؤكد الباحثة على أهمية تلافى النموذج المقترح للأخطاء التالية : أخطاء فى تصميم نظام الرقابة الداخلية، غياب الفصل بين الواجبات، غياب الفحص الملائم والموافقة عن العمليات المالية والقيود المحاسبية، احتياطات غير كافيه لحماية الأصول بجميع أنواعها، غياب أساليب رقابية أخرى تتسق ونشاط العملية المالية.

وفى المبحث الثالث تناولت الدراسة معايير المراجعة التى بنى عليها النموذج المقترح، وقسمتها الدراسة إلى مجموعتين هما :

الأولى : بعض المعايير المتعلقة بنموذج المراجعة بصفة عامه وقدأوضحتها الدراسة : معيار المراجعة الدولي رقم (ISA 240) ، معيار المراجعة الأمريكى SAS.99 ، المعيار الدولى للمراجعة ISA.400، المعيار الدولى للمراجعة ISA.401، SISA 080 Follow-up ، SISA 070 Reporting، SISA050 Planning SAS. 108, SAS. 109، I APS 1009, IAPS.1008، activities

الثانية : معايير متعلقة بنموذج مراجعة أمن نظم المعلومات المحاسبية وقد أوضحتها الدراسة أيضاً : ISO 17799 ، ISO 27001 ISO 27004, ISO 27003, ISO27002, ISO27005 , ISO 27006

وفى المبحث الرابع تناولت الدراسة النموذج المقترح من خلال ستة خطوات، أوضحها الشكل رقم (٤/١) ثم تناولتها الدراسة بالشرح فى الخطوات التالية :

الخطوة الأولى : مرحلة تخطيط عملية المراجعة Audit Plan .

الخطوة الثانية : مرحلة اختبار الضوابط الرقابية Security Control Testing .

الخطوة الثالثة : الفحص والاختبار التفصيلي للعمليات Detailed Testing Phase .

الخطوة الرابعة : اختبار الأرصدة Balances Tests .

الخطوة الخامسة : إعداد التقرير Preparing The Report of Audit .

الخطوة السادسة : علاج الأخطاء والتحسين المستمر Engage in Gab Remediation and Continuous Improvement .

وتنبه الباحثة إلى أن نجاح النموذج المقترح لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية مرهون بتكامله مع النماذج الأخرى المرتبطة بأهداف المنشأة، والتى يلزم أن يتم تنسيقها معا لتحقيق الهدف العام .

النتائج والتوصيات

توصلت الدراسة للنتائج التالية:

- لابد من توافر مجموعة من الاعتبارات تلزم لإرساء نموذج فعال لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية .
- توجد مجموعات من الإصدارات الدولية لإرساء نموذج فعال لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية، أهمها المعيار ISO 17799 وسلسلة ISO 27000 وهى مجموعة من المعايير تتناول أمن المعلومات.
- لبناء نموذج فعال لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية، لابد من توافر مجموعة من الخطوات تتلخص فيما يلى:

الخطوة الأولى: مرحلة تخطيط عملية المراجعة Audit Plan .

الخطوة الثانية: مرحلة اختبار الضوابط الرقابية Security Control Testing .

الخطوة الثالثة: الفحص والاختبار التفصيلي للعمليات Detailed Testing Phase .

الخطوة الرابعة: اختبار الأرصدة Balances Tests .

الخطوة الخامسة: إعداد التقرير Preparing The Report of Audit .

الخطوة السادسة: علاج الأخطاء والتحسين المستمر Engage in Gab Remediation and Continuous Improvement .

كما توصى الدراسة بالتوصيات التالية :

- إصدار معيار مراجعة مصرى، لمراجعة أمن نظم المعلومات المحاسبية الإلكترونية يتبنى أهداف ومتطلبات من شأنها النهوض بنماذج المراجعة، فى ضوء المعايير ISO 17799. وأيضا سلسلة المعايير ISO 27000 .
- التوسع فى تدريس مراجعة أمن نظم المعلومات المحاسبية الإلكتروتية فى كليات التجارة، لتوفير دارسيين متخصصين فى هذا الفرع من المراجعة وبذلك نصل إلى نوع جديد من المراجعين ، ليس مراجع نظم المعلومات المحاسبية فحسب بل مراجع أمن نظم المعلومات المحاسبية الإلكترونية وهو التخصص الأكثر دقة والذي يحمي الإجراءات بالمنشأة من التهديدات الداخلية والخارجية.
- الحاجة إلى إستحداث إدارة للمراجعة، مستقلة تماما عن مجلس الإدارة، تكون مسئولة عن المراجعة والرقابة الداخلية، تمارس عمليات المراجعة الداخلية لنظم المعلومات المحاسبية الإلكترونية بصفة مستمرة.
- تبنى سياسة تدعو إلى الدمج والتكامل بين برامج المراجعة بالمنشأة مما يؤدى إلى تحقيق أهدافها الرئيسية ومن أهمها إرساء الأمن الشامل لأهميته القصوى للمنشأة والبيئة.

المراجـــــع

المراجع باللغة العربية:

أولا الكتب:

- د . عبد الوهاب نصر علي و د . شحاته السيد شحاته، «مراجعة الحسابات في بيئة الخصخصة وأسواق المال»، الدار الجامعية بالإسكندرية ، ٢٠٠٤ .
- د . علي إبراهيم طلبة، «مراجعة النظم الإلكترونية»، البيان للطباعة والنشر، ٢٠٠٦ .
- د . أمين السيد لطفي، «موسوعة د .أمين لطفي في المراجعة ، المراجعة في عالم متغير الكتاب الأول»، المؤسسة الفنية للطباعة والنشر، ص٤٤٣- ٤٤٤، ٢٠٠٤ .
- د . طارق عبد العال حماد، «موسوعة معايير المراجعة، شرح معايير المراجعة الدولية والأمريكية والعربية، الجزء الثاني، الرقابة الداخلية – أدلة الإثبات»، الدارالجامعية، ٢٠٠٤، ص٢٠١ .
- د . محمد توفيق محمد، «معايير و إرشادات المراجعة الإطار العلمي والتطبيق العملي»، بدون ناشر ، ٢٠٠٥ .

ثانيا الدوريات:

- د .عبد الوهاب نصر علي، «أثر محددات التلاعب في القوائم المالية على تخطيط إجراءات المراجعة وأثر ذلك على تقرير مراجع الحسابات عن القوائم المالية»، مجلة كلية التجارة للبحوث العلمية جامعة الاسكندرية العدد الأول مارس ٢٠٠٥ .

- د .سعاد خضر، «دراسة ميدانية عن العلاقة بين خبرة المراجع والتقييم المبدئي لمخاطر الرقابة الداخلية في ظل النظام الإلكتروني للبيانات»، المجلة العلمية للاقتصاد والتجارة ،كلية التجارة جامعة عين شمس العدد الأول، ٢٠٠٤ .
- د . صلاح الدين الهتيمى، د . آمنة ماجد الربيحات، «أثر التهديدات الأمنية فى ضوء تطبيق الحكومة الالكترونية - دراسة ميدانية فى عدد من الوزارات الأردنية وأمانة عمان الكبرى»، مجلة المحاسبة والإدارة والتأمين، كلية التجارة، جامعة القاهرة، ٢٠٠٥م.

ثالثا ندوات ومؤتمرات:

- د .أحمد عز الدين زيدان، «سياسة المراجعة و الرقابة على نظم المعلومات في البنوك»، ندوة مراجعة وتدقيق نظم المعلومات ، القاهرة ،٢٠٠٤ .
- أ.إ براهيم محمد عبد المنعم ، «أسلوب مقترح لمراجعة نظم المعلومات»، ندوة مراجعة وتدقيق نظم المعلومات ، المنظمة العربية للتنمية الادارية ، ٢٠٠٤ .
- د . محمد عبد الدايم، «أمن الشيكات الخاصة»، ندوة مراجعة وتدقيق نظم المعلومات، المنظمة العربية للتنمية الإدارية ، ٢٠٠٤ .
- د . صلاح الدين فهمي محمود، «الآثار الاقتصادية لاتفاقية حماية الملكية الفكرية بالتطبيق على صناعة الدواء في مصر» ، ندوة حول : الملكية الفكرية الحماية الشرعية والقانونية ، مركز صالح عبد الله كامل للاقتصاد الإسلامى ، جامعة الأزهر ، مايو ٢٠٠٢ .
- محمد عز الدين الشرقاوي، «تدقيق ومراجعة قواعد البيانات»، ندوة مراجعة وتدقيق نظم المعلومات ، المنظمة العربية للتنمية الإدارية، ٢٠٠٤ .

- د . عبيد دياب العجيلي ، «الأساليب الحديثة في تدقيق ومراجعة نظم المعلومات» ، ندوة مراجعة وتدقيق نظم المعلومات ، المنظمة العربية للتنمية الإدارية ، القاهرة ، إبريل ٢٠٠٤ .

رابعا شبكة المعلومات العالمية :

- «معيار الرقابة الداخلية لغرض مراجعة القوائم المالية»

http://www.scopa.org.sa/Au/Au11/index.htm

- د .طاهر الكري ، «تكلفة الاستثمار في أنظمة المعلومات وعلاقتها بأداء المنظمات – دراسة تطبيقية على البنوك التجارية بالأردن» ، مجلةالجندول ، السنة الثالثة ، العدد (٢٤)سبتمبر ٢٠٠٥م http://www.uluminsania.net

- د .سمير أبو غابة ، «أساليب الرقابة المختلفة الخاصة بأمن الأنظمة الإلكترونية للمعلومات» ، مجلة الرقابة الشاملة الجهاز المركزي للمحاسبات العددان ١٥٣ ، ١٥٤ يونيو نسخة إلكترونية ٢٠٠٣ . http://www.cao.gov.eg

المراجع باللغة الإنجليزية :

Books:

- **William Thomas and Emerson O. Honk, "Auditing Theory and practice", 1986.**

ترجمة د .أحمد حجاج و د .كمال الدين سعيد ، دار المريخ لنشر الرياض ، المملكة العربية السعودية ، ١٩٨٩ .

Periodicals:

David C. Yang, Liming Guan , "The Evolution of It Auditing and Internal Control Standards in Financial Statement Audits , The Case of The United States", Managerial Auditing Journal, Vol.19 N.4 2004.

- **Mark T. Emead, "Are You Familiar With Most Recent ISO/IEC 17799 changes?" IT Audit, The Institute of Internal Auditor ,U.S.A Vol.9, June10,2006.**
- **Raquel S.Filipek,"Security the IT Infrastructure Reduces Data Theft" IT Audit, The Institute of Internal Auditor,U.S.A, Vol.1, Nov 15 .2005.**
- **John A.Fogarty, Lynford Graham and Darrel R.Schubert, "Financial Statement Audit", Journal of Accountancy, Vol.202, No.1, July 2006.**
- **Lakshmana Raovemuri, "preparing for The Security Audit Recommendations for Biginner ,IT Auditors" , , The Institute of Internal Auditor U.S.A Vol.9 , June 10 2006.**
- **Raquel Filipek, "Botnets Could Invading Your, Network", IT Audit, The Institute of Internal Auditors, U.S.A. , Vol.9, January 10, 2006 .**
- **Ahmad A.Abu-Musa , "Investigating The Security Controls of CAIS in an Emerging Economy , An Empirical Study on The Egyption Banking Industry" , Managerial Auditing Journal, Research paper , Vol .No.19 , Issue 2, 2004.**
- **Dwight A.Haworth and Leah R.Pietron , "Sarbanes-Oxley: Achieving Compliance By Starting With ISO 17799", Information System Security Journal , Vol.No.23 , feb., 2006.**
- **Gary Swindon," Enhancing HIPAA Security Rule Compliance Efforts " IT Audit, , The Institute of Internal Auditors, U.S.A. Vol. 9, August 10, 2006 .**

Net Work:

- **John O`Leary "How to create and Sustain a Quality Security Awareness Program".**

  http://www.gocsi.com/training/erc/hcsgap=jsessionid
- **"Standards for Information Systems Control Professionals" http://www.isaca.org/printertemplate.cfm...**
- **Stanley Weiner "Auditing Business Risk Internal Control And Audit Implication of EDI", The CPA Journal, November 1995.**

  http://www.nysspa.org./cpajornal/1995/nov/aud1195.htm.

- **Ganesh M.Pandit , Vijaya Subraha manyam and Grace M.Conway , "Audit Committee Reports Before and After Sarbanes-Oxley" , The CPA Journal , October 2005 , P.42 http://www.nysscpa.org/printversion/cpaj/2005/1005/p42.htm**
- **Barbara Arel , Richard G.Brody and kurt pany , "Audit Firm Rotation and Audit Quality" , The CPA Journal , January 2005 , P.36**

  http://www.nysscpa.org/printversion/cpaj/2005/105/p36.htm .
- **J.Stephen Mc Nally , "Assessing Company Level Controls " , Journal of Accountancy . June 2005**

  http://www.aicpa.org/pubs/jofa/june2005/menally.htm .
- **Harvey Coustan , Lindam-Leinicke , W.Max Rexroad and Joceaostrosky ," Sarbanes-Oxley : What It Means to The Market Place" , Journal of Accountancy , feb 2004. http://www.aircpa.org/pubs/jofa/feb2004/cousta.htm .**
- **The Audit Committee and Oversight of Financial Reporting, "MANAGEMENT OVERRIDE OF INTERNAL CONTROLS, The Achilles , Heel of Fraud Prevention" , The audit Committee and Oversight of Financial Reporting AICPA http://www.aicpa.org/audcommctr/spotlight/achillesheel.(PDF)**
- **Dan Swanson, "SECURE STRATEGIES", Information Security Magazine , Oct.2000.**

  http://infosecuritymag.techarget.com/ar
- **"STATEMENT ON AUDITING STANDARDS NO.104-NO.111. RISK ASSEMENT STANDARDS"**

  http://www.aicpa.org/download/members/div/auditstd/ras-summary-for-for-website.pdf-microsoft1nt...
- **" The ISO 17799 Code of Practice"**

  http://www.w3j.com/5/53.instone.html
- **"INFORMATION SECURITY MANAGEMENT STANDARDS - THE ISO 27000 SERIES"**

  http://www.w3j.com/5/53.instone.html