دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

العنوان:	الغش المالي من خلال أنظمة المحاسبة الإلكترونية : حتمية تطوير أساليب المراجعة والرقابة الداخلية
المصدر:	مجلة التجارة والتمويل
الناشر:	جامعة طنطا - كلية التجارة
المؤلف الرئيسي:	الجزار، سمير محمد مصطفى
المجلد/العدد:	ع 2
محكمة:	نعم
التاريخ الميلادي:	1988
الصفحات:	145 - 173
رقم MD:	328827
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	EcoLink
مواضيع:	المراجعة الخارجية ، النظم المحاسبية ، مراجعة الحسابات ، الرقابة المالية ، نظم المعلومات الإلكترونية ، المراجعة الداخلية ، الفساد المالي ، الجريمة والمجرمون ، أمن المعلومات ، الاختلاسات ، الحاسبات الإلكترونية
رابط:	http://search.mandumah.com/Record/328827

© 2020 دار المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو دار المنظومة.

بسم الله الرحمن الرحيم

الغش المالى من خلال أنظمة المحاسبة الالكترونية :
حتمية تطوير أساليب المراجعة والرقابة الداخلية

Fraud in Electronic Accounting Systems :
The Need For Tight Audit and Internal Control Procedures

دكتور

سمير محمد مصطفى الجزار

كلية التجارة - جامعة طنطا

"This boat That we just built is just Fine ... And don't you try to tell us it's not the sides and the back are divine .. It's the bottom I guess we Forgot .. "

- Sel Silverstein -

مقدمـة

عندما تم ادخال واستخدام نظم المعلومات الالكترونية كبديل لنظم المحاسبة اليدوية كان الاعتقاد أن نظم المعلومات الالكترونية تقدم نظاما محاسبيا خال من الغش المالى (Fraud - Proof) وذلك لان الكمبيوتر ليس لديه أى رغبة فى الغش المالى أو ارتكاب أية جرائم أو مخالفات مالية.

ولكن الملاحظ منذ استخدام أنظمة المعلومات الالكتونية، وعلى مدار العقدين الماضيين هو ازدياد ظاهرة الغش المالى، والاختلاسات، والتلاعب بأصول الوحدات الاقتصادية[1]. والملاحظة الاكثر أهمية هى أنه لم يتم اكتشاف أى من حالات الغش المالى عن طريق أساليب المراجعة الداخلية أو الخارجية، وانما تم اكتشاف هذه الحالات من واقع ظروف عشوائية. وأهم هذه الظروف تشمل الوفاة أو النقل المفاجئ للموظف المسئول، اختلاف بين الاشخاص المشتركين فى حالة الغش أو الاختلاس، أو شكوى من أحد الاطراف المتعاملين مع الوحدة الاقتصادية مثل بعض الموردين أو العملاء أو بنك الشركة.

ويهدف هذا البحث الى تحديد الخصائص المميزة لنظام المعلومات الالكترونية، وتحليل بعض حالات الغش المالى المصاحبة لاستخدام نظم المعلومات الالكترونية لتحديد الثغرات التى يستخدمها مرتكبى جرائم الغش المالى، وأخيرا اقتراح بعض أساليب تطوير نظم الرقابة الداخلية والمراجعة الخارجية لتضيق نطاق الغش المالى.

١-١ أهمية المشكلة :

يعتبر استخدام نظم المعلومات الالكترونية فى الوحدات الاقتصادية نتيجة حتمية لعاملين متلازمين. العامل الاول هو كبر حجم الوحدات الاقتصادية وتعدد أنشطتها واتساع

(1) United States of America, Chamber of Commerce, "A HandBook on White Collar Crime ", 1979.

نطاق عملياتها جغرافيا. وهذا بدوره أدى الى ضخامة حجم البيانات وتعدد مستويات تحليل المعلومات للاستعمال الداخلى على مختلف المستويات الادارية للوحدة الاقتصادية، وكذلك اعداد التقارير المالية للجهات الخارجية. والعامل الثانى هو تطور تكنولوجيا المعلومات . وهذا بدوره يرفع من كفاءة وكفاية نظام المعلومات بالوحدة الاقتصادية. فاستخدام الكمبيوتر وأدوات تحليل وتخزين المعلومات الالكترونية يعظم من طاقة نظام المعلومات ويزيد من سرعة مناولة وتحليل البيانات .

الا أن الجانب الآخر والمصاحب لاستخدام نظم المعلومات الالكترونية هو ارتفاع الخطر فى المعلومات (Information Risk) أى أن بعض الخصائص التشغيلية لنظام المعلومات الالكترونى تجعل الامر أكثر سهولة للتلاعب بالمعلومات (أى الغش المالى) ، ومن ثم تكون درجة صدق المعلومات والاعتماد عليها غير مؤكدة. وتشير حالات الغش المالى التى تم الافصاح عنها عن ضخامة هذا الخطر، وما ينتج عنه من خسائر للوحدات الاقتصادية والاضرار بمصالح مستخدمى المعلومات من خارج الوحدة الاقتصادية.

وتفيد احصاءات وزارة العدل الامريكية (سجلات محكمة الجنايات في عام ١٩٧٩)، أن متوسط الاختلاسات المالية من خلال أنظمة الكمبيوتر هو ١,٣ مليون دولار للحالة الواحدة[٢]. وتفيد احصائيات غرفة التجارة بالولايات المتحدة الامريكية لعام ١٩٧٩ أن خسائر حالات الغش من خلال الكمبيوتر فى قطاع البنوك وحده قد بلغت بليون دولار فى عام ١٩٧٤ و ١,٧ بليون فى عام ١٩٧٩[٣]. كما يفيد تحليل حالات الغش المالى أنها تشمل اختلاسات من خلال المصروفات والمخزون بالإضافة الى استخدام الادارات العليا لملفات الكمبيوتر والارقام السرية للسجلات لتغطية الاختلاسات أو النتائج الاقتصادية غير المرغوب فيها (Vasarhelyi and Lin, 1988) .

(2) U.S. Department of Justice, Criminal Court Records, 1979.
(3) U.S. Chamber of Commerce " A Handbook on White Collar Crime", 1979.

وأمام هذه المشاهدات يرجع أصحاب المشروعات والباحثين أسباب ارتكاب الغش المالى الى عدم قدرة أنظمة المراجعة والرقابة الداخلية على مسايرة التطور المستمر فى أنظمة المعلومات الالكترونية، ومن ثم عدم القدرة على سد الثغرات فى نقط الرقابة ضد الغش المالى .

(Perry and Warner, 1978; and Davis and Weber, 1986)

ومن هنا يجب على الشركات التى تستخدم نظم المعلومات الالكترونية أن تعيد النظر فى أنظمة الرقابة الداخلية وتطويرها لتضيق نطاق وثغرات الغش المالى . أما من ناحية المراقب الخارجى، فانه وان كان غير مسؤل مباشرة عن اكتشاف حالات الغش المالى في الوحدة التى يراجعها، فإن مسؤليته عن تقييم نظام الرقابة الداخلية تقضى بضرورة تطوير أساليب المراجعة للتأكد من أن نظام الرقابة الداخلية كاف لمنع واكتشاف حالات الغش المالى .

١ - ٢ هدف البحث :

يهدف هذا البحث الى تحديد الثغرات فى نظم الرقابة الداخلية، والتى تسهل عملية ارتكاب الغش المالى ، ثم اقتراح أساليب رقابية أخرى لمنع أو اكتشاف الغش المالى المصاحب لنظم المعلومات الالكترونية.

ولتحقيق هذا الهدف فإن الباحث سوف يتناول الجوانب الآتية :

أولا : تحديد الخصائص التشغيلية لنظام المعلومات الالكترونى والتى لها آثارها السلبية على نظام الرقابة الداخلية.

ثانيا : تحليل بعض حالات عملية عن الغش المالى لتحديد الثغرات التى استخدمها مرتكبى جرائم الغش المالى .

ثالثا : اقتراح بعض أساليب الرقابة الداخلية والمراجعة الخارجية التى تساعد على

منع أو اكتشاف الغش المالى ، أى تضيق نطاق الغش المالى المصاحب لاستخدام أنظمة المعلومات الالكترونية.

١ - ٣ تعاريف ومصطلحات :

أ - الغش من خلال الكمبيوتر : Computer Fraud

ويقصد به التزوير فى البيانات المحاسبية بقصد تغطية اختلاسات أو اخفاء حقائق اقتصادية غير مرغوب فيها، والتى تلعب المعرفة بأسرار تشغيل / أو تصميم الكمبيوتر دورا أساسيا فيها .

ب - مراجعة أمن المعلومات : Information Security Audit

ويقصد بها اجراء المراجعة (أو الرقابة الداخلية) للتأكد من كفاية الاحتياطات لمنع تحوير (أو تضليل) البيانات المحاسبية سواء كان عن طريق القصد أو الجهل بتشغيل نظم المعلومات الالكترونية .

جـ - الخطر فى المعلومات : Information Risk

ويقصد به درجة عدم التأكد فى دلالة المعلومات عن الحقائق الاقتصادية فى المشروع ويأتى ذلك نتيجة عوامل كثيرة : منها دقة وضبط خطوات تشغيل النظام (المدخلات / التسويات .. الخ)، مدى فعالية نقط الرقابة للكشف عن الغش المالى، درجة تعقيد النظام، أمن المعلومات، وأخيرا التدريب الجيد والمستمر للقائمين على التشغيل .

د - الرفض غير المرئى : Counter Implementation

ويقصد به الاجراءات (الاتفاقات) السلوكية بين بعض الخلايا فى المشروع ضد هدف معين أو ضد خطة ادارية معينة، أو ضد ادخال أى نظام جديد قد يعرض مراكزهم أو منافعهم للخطر .

هـ - رقابة برامج الكمبيوتر : Programming Controls

ويقصد بها الاحتياطات الرقابية التى تتخذها الشركة لتتأكد من أن النظام المستخدم يحقق الهدف التشغيلى الذى تم وضع التصميمات له . أو بمعنى آخر التأكد من أن مصمم برنامج الكمبيوتر لم حيور في خطواته لتحقيق غش مالى / أو اختلاس تلقائى عندما يتم تشغيل البرنامج [١] .

٢- طبيعة الغش المالى من خلال أنظمة المعلومات الالكترونية
The Nature of Computer Fraud

يعرف الغش عموما على أنه الفعل العمدى الذى يؤدى الى تضليل أو خداع الطرف الآخر. أما من الناحية القانونية، فهناك نوعين من الغش. الأول، وهو الغش العمدى الذى ينجم عنه ضرر للغير ومنافع للطرف مرتكب الغش (Actual Fraud) أما النوع الثانى : الغش غير العمدى وهو الذى لا يتوافر فيه نية الكسب من وراء تضليل الحقائق ، أى أن

---

(١) فعلى سبيل المثال : قد يقوم مصمم برنامج الاجور بوضع برنامج جانبى يقضى بقيد أجور وهمية واصدار شيك لعامل وهمى مع كل مائة عامل أصلى ، وارسال الشيكات على صندوق بريد تلقائيا ودوريا دون أن يظهر هو فى الصورة على الاطلاق . وبالطبع فإن اكتشاف مثل هذا البرنامج (المدفون) لا يمكن اكتشافه الا بعد فترة طويلة .

عنصر (العمد) الاصرار غير متوافر. وهذا ما يسمى بـ (Constructive Fraud) ، وهو أقرب منه الى الخطأ.

وفى المحاسبة والتقارير المالية، فانه يمكن تعريف الغش المالى على أنه الفعل العمدى (عموما تحوير/تزييف البيانات المحاسبية)والذى يقصد منه تضليل مستخدم البيانات ، أو اخفاء حقائق اقتصادية غير مرغوب فيها. وهذا التضليل عادة ما ينجم عنه خسائر للوحدة الاقتصادية التى تم التلاعب بحساباتها ، أو لمستخدمى البيانات المالية (وهذه الخسائر تشمل الخسائر الفعلية أو خسائر الفرصة الضائعة). فعلى سبيل المثال ، اذا تسترت الادارة العليا على بعض الاختلاسات أو الضياع فى المخزون دون اثباتها بالدفاتر، فهذا فيه خسارة فعلية. حيث أن صافى أصول الوحدة الحقيقى أقل من المقيد بالدفاتر. أما اذا قامت ادارة الشركة بالتلاعب بالبيانات المحاسبية لاظهار أرباح وهمية، فهذا فيه خسارة الفرصة الضائعة.حيث أن المستثمرين فى سوق المال سوف يشترون أسهم هذه الشركة على فرض أنها ذات ربحية عالية.

أما الغش المالى من خلال أنظمة المعلومات الالكترونية فيقصد به :

الاختلاسات والتضليل فى البيانات المحاسبية التى تتم عن طريق أو باستخدام : أ) برامج الكمبيوتر، ب) أشرطة وسجلات حفظ الكمبيوتر، جـ) عمليات تشغيل الكمبيوتر والتى ينتج عنها خسائر للوحدة الاقتصادية التى تم التلاعب بنظام الكمبيوتر فيها . ويعرفه البعض الآخر على أنه يشمل أى عمل غير قانونى والذى تلعب فيه المعرفة/ الخبرة بتكنولوجيا الكمبيوتر دورا أساسيا.

".... Computer - related crime, then is any illegal act in which Knowledge of Computer technology plays a role in its preparation. "Vasarhelyi and Lin 1988, P. 184.

٢ . ١ اشتراك الكمبيوتر فى عملية الغش المالى
(How Computer is Involved in Fraud)

وفقا لتحليل القضاء الجنائى (جنايات الكمبيوتر) بأمريكا[١]، أن نظم المعلومات الالكترونية قد تشترك فى الغش المالى كهدف أو كوسيلة (Either Object or Instrument) فالكمبيوتر يعتبر هدفا فى جريمة الغش عندما يقوم الاشخاص من خارج النظام وغير المصرح لهم بالاستخدام بمحاولة استخدام الكمبيوتر من أجل الاطلاع على الارقام السرية للتشغيل. وكذلك أيضا يعتبر هدفا عندما يتم سرقة الاصول التى بداخلها (أو تعمل عن طريق) برامج كمبيوتر .

أما العلاقة الثانية، وهى الاكثر انتشارا، وهو أن يستخدم الكمبيوتر كوسيلة لارتكاب أو تغطية الغش المالى فى النظام. ويحذر الباحثون وخبراء نظم المعلومات من خطورة الدور الذى يلعبه الفنيون فى قسم الكمبيوتر مثل مصممى برامج الكمبيوتر والعاملين على الكمبيوتر فى التشغيل اليومى للنظام. (Fisher, 1984; Paul, 1981) وذلك لان هؤلاء الافراد يستطيعون التعامل مع الكمبيوتر فنيا، وتنفيذ عمليات الغش أو التحوير فى البيانات المسجلة دون ترك أية آثار تساعد على اكتشاف الغش أو التضليل فى البيانات المسجلة.

ونعرض فيما يلى بعض الاساليب الفنية التى يتبعها مرتكبى الغش المالى من خلال النظم الالكترونية، والتى تم اكتشافها بعد فترة طويلة من الزمن وتحملت فيها الوحدات خسائر مالية طائلة[٢] :

(1) Computer Crime-Criminal Justice, U.S. Department of Justice Pamphlet Page : 4 (1979)
(2) Computer Crime, Ibid. P. 17.

أ - البرامج المدفونة : (Torjan Horse) [١]

ووفقا لهذا الاسلوب يقوم مرتكب الغش بوضع برنامج تزويرى مع البرنامج الاساسى للنظام، والذى بمقتضاه يقوم البرنامج التزويرى مستقلا عن البرنامج الاصلى باجراء بعض العمليات فى الدفاتر (لتنفيذ هدف معين)، ثم بعد ذلك يقوم البرنامج أيضا بمحو (erase) كل الادلة التى تشير الى أن عملية غير قانونية قد حدثت .

ب - البرامج الملازمة فى التشغيل وغير الظاهرة فى التدوين :
(Asynchronous Attack)

ويقضى هذا الاسلوب أن يضع مرتكب الغش برنامجا ملازما للبرنامج الاصلى، أى عندما يقوم عامل التشغيل باجراء عمليات على البرنامج الاصلى ، فيتم اجرائها وفقا للبرنامج الملازم أيضا، ولكن عند اثبات النتائج تثبت النتائج كما لو كان النظام الاصلى هو السائد فقط. والفرق بين أسلوب البرامج المدفونة والبرامج المتلازمة هو أن البرامج المدفونة يكون لها هدف واحد فقط، بمعنى أن البرنامج ينفذ عملية واحدة فقط وبعدها يحذف نفسه تلقائيا . أما الغش عن طريق البرنامج الملازم فيستمر فى التشغيل طالما أن البرنامج الاصلى مستمر هو الآخر فى التشغيل .

---

(١) ويأخذ هذا اسمه من الحيلة التاريخية التى استخدمها اليونانيون لفتح أسوار مدينة تورجان . حيث صنعوا تمثالا كبيرا لحصان ولكنه مفرغ من الداخل. ووضعوا بداخله مجموعة من الجنود ثم ألقو به فى الليل عند باب المدينة . ولما أمر حاكم المدينة بوضع التمثال داخل الاسوار، خرج الجنود من داخل الحصان ليلا وفتحوا الاسوار للجيش اليونانى الذى ايتسطاع أن يغزو المدينة حينذاك .

جـ - التلاعب فى توجيه البيانات : (Data Diddling / Manipula-tion)

والفئة التى تقوم بهذا النوع من الغش المالى تشمل القائمين على تشغيل الكمبيوتر (Operators) ، والذين يقومون بوظيفة ادخال المعلومات. ويعتبر هذا النوع من الغش المالى أكثر انتشارا بين موظفى البنوك (Bank - tellers) وشركات التأمين، وفى الشركات الصناعية أيضا .

ومن العرض السابق يتضح أن أكثر الطوائف فى الوحدة الاقتصادية ارتكابا للغش المالى والتلاعب فى البيانات المحاسبية هم مصممى برامج الكمبيوتر فى نظام المعلومات وكذلك القائمين على التشغيل اليومى للنظام. ولعل ذلك هو ما يدفع الكثيرين للقول بأن درجة الخطورة فى استخدام نظم المعلومات الالكترونية تأتى من القائمين على شئونه.

"...The Computerized system is never Vulnerable than in the hands of those who feed and care for it."
Vasarhelyi and Lin (1988), P. 186.

٢ . ٢ الخصائص التشغيلية لنظم المعلومات الالكترونية :

صعوبة اكتشاف الغش المالى :

تتميز أنظمة المعلومات الالكترونية ببعض الخصائص التى تجعل اكتشاف الغش المالى أو التلاعب بالبيانات المحاسبية أمرا أكثر صعوبة. وتشمل هذه الخصائص :

أ - تركيز المعلومات : Concentration of Information

تتصف معظم نظم الكمبيوتر بمركزية وتكامل المعلومات فى ملفات الكترونية أو نقط تشغيلية فى النظام. هذا التكامل والتركيز فى دوائر المعلومات يجعل الامر أكثر سهولة لمرتكب الغش المالى لاجراء كل التسويات اللازمة لتغطية الغش فى السجلات الاصلية والمكملة (Krauss and MacGahon, 1979) .

وهذا بخلاف الانظمة اليدوية، فاجراء أى تعديل فى سجل القيد الاولى (اليومية) يتطلب اجراء تعديل مماثل فى دفاتر الاستاذ والارصدة المرحلة - أما فى النظام الالكترونى فانه بمجرد اجراء التعديل فى دفتر اليومية (Raw Input Data) يتم الترحيل الى دفتر الاستاذ وتعديل الارصدة تلقائيا. ومن هنا فإن خاصية التكامل التلقائى بين أجزاء النظام (القيد .. الترحيل .. الترصيد ..) تخفى الآثار التى يمكن أن تدل على أية حالة غش أو تلاعب فى البيانات المحاسبية قد حدثت .

ب - السجلات الدائمة للنظام غير مرئية : (Lack of Visible Records)

تتمثل السجلات الدائمة (Permanent Records) للانظمة الالكترونية فى أشرطة أو اسطوانات مغناطيسية . وتتم عمليات المراجعة عن طريق طبع محتويات / أو أرصدة هذه السجلات فى أوقات أو لفترات زمنية معينة. ومن ثم ، فإن البيانات المطبوعة لا تكشف عن ما اذا كان هناك تغيير فى البيانات الاصلية . وذلك عكس السجلات اليدوية، حيث أن وجود سجل دائم يحتوى على العمليات بتسلسل تاريخى ومن ثم يسهل على المراجع الداخلى / أو الخارجى تتبع التغيير فى الارصدة والتأكد من عدم وجود تلاعب بالبيانات المدونة . (Allen, 1977)

جـ - أمن المعلومات : (Information Security)

على عكس السجلات اليدوية، حيث تكون تحت مسئولية موظف مختص أو حيث يتم حفظها ليلا فى خزائن معينة، فإن سجلات الكمبيوتر يمكن الاطلاع على محتوياتها أو اجراء عمليات غير قانونية بها بمجرد التعرف على الكود السرى لتشغيل الكمبيوتر. وفى كثير من الاحيان ما يتم تشغيل / الاطلاع على سجلات الكمبيوتر من خارج الوحدة الاقتصادية عن طريق التليفون (On-Line Access) .

وهذا بدوره يزيد من الخطر فى الاعتماد على البيانات المسجلة، ويتطلب نوعا خاصا من أساليب الرقابة وكذلك مراجعة أمن المعلومات (Srinivasaor and Duscher, 1978) .

د - خطورة دور الفنيين فى النظام : (Technical Personnel)

يلعب مصمم النظام (Computer Programmer) دورا خطيرا فى أمن المعلومات. فيقرر بعض المحللين أنه حتى اذا كان النظام الاصلى يحتوى على نقط رقابية تلقائية لتعطى اشارات عن العمليات غير المسموح بها (Fraud) فان مصمم البرامج داخل المشروع، أو المتخصصين فى اعداد النظم التشغيلية (Software Specialists) يمكنهم تعديل النظام ليعطى اشارات أن العمليات تتم دون خلل بينما حقيقة الامر أن الدفاتر تحتوى على بعض الاختلاسات أو التعديل غير المسموح به .

٢ - ٣ تحليل لبعض حالات الغش المالى

(Analysis of Some Computer Fraud Cases)

يعتبر تحليل بعض الحالات العملية للغش المالى أفضل أسلوب لتحديد الثغرات فى نقط الرقابة والتى يستغلها مرتكبى الغش المالى فى تنفيذ أهدافهم. ولذلك نعرض فى القسم التالى لبعض الحالات العملية[١].

Case 1 : A 25-year old computer terminal operator arranged to receive pension checks under thirty different names. Her scheme was a simple one. When a notice of a pension recipient's death came in, she was supposed to enter it on the computer in order to terminate the payments. Instead of entering the death notices she would enter an address change and send the check to a post office box. When auditors sent out letters to verify that the pensioners were still a live, the letters went to the fraudulent address. It was a simple matter for the terminal operator to respond affirmatively.

Case 2 : A computer consultant for the Los Angeles Bank, visited the bank's wire transfer room, where he obtained the electronic funds transfer code. Later, posing as a branch manager, he called from a public telephone and used the code to send money to a Swiss account. By the time the switzerland, converted the funds into diamonds, and returned to the U.S.A. only when he boasted of the feat was he identified.

Case 3 : An accountant employed by a fruit wholesaler made off with three million dollars over a period of six years. The scheme used was to inflate prices on invoices by small amounts and then to disburse the extra money to any of 17 dummy vendors. Underlying the scheme was an environment in which fruit prices often varied widely to facilitate his scheme, the perpetrator developed a computer system that simulated his employer's accounting system. Using his own system, which ran at a service bureau, he was able to determine

---

(1) These cases are taken From :

- U. S. Department of justice Pamphlet, 1979.
- U. S. Chamber of commerce " A Handbook of White Collar Crime", 1979.

which invoice could be inflated and by how much without attracting attention. The accountant then padded invoicess accordingly and disbursed the extra money to fictitious vendors he had created. The fraud was so skillfully executed that the firm's external auditors never detected it, the fraud was discovered only because the perpetrator go tired of covering his tracks.

من تحليل الحالات السابقة، يتضح ان هناك خصائص مميزة لحالات الغش المالى المصاحبة لأنظمة الكمبيوتر :

أ - ان معظم حالات الغش تشتمل على اجراء عمدى لاختلاس بعض اصول الشركة قبل تضخيم حجم المصروفات المقيدة، أو قيد مصروفات لخدمات أو بضاعة لم يتم استلامها. ويتضح ذلك من الحالة رقم (١) والحالة رقم (٣). كذلك أيضا التزوير فئ نقل الارصدة بين الحسابات . وهذا يتم عادة فى البنوك وشركات التأمين . وقد يتم عن طريق عملية واحدة ذات حجم كبير اذا كان مرتكب الاختلاس من خارج الشركة كما فى الحالة رقم (٢) أو بأحجام صغيرة ولفترات زمنية طويلة كما حدث فى الحالة رقم (٣).

ب - أن مرتكب الغش يقوم بادخال أسماء موردين وهمية، أو حسابات وهمية فى النظام وذلك حتى يمكن اخراج النقدية الى هذه الحسابات .

جـ - استخدام صناديق البريد كعنوان للاسماء الوهمية التى ترسل اليها الشيكات .

د - أن عملية الغش أو التزوير عادة ما تتم على مدار فترة زمنية طويلة. لتجنب جذب انتباه القائمين على المراجعة الداخلية أو التعارض مع نقط الرقابة الداخلية فإن معظم مرتكبى الغش أو الاختلاس يفضلون اجراء اختلاسات بأحجام صغيرة ولكنها متكررة. حيث أن اجراء اختلاس بقيمة كبيرة سرعان ما يشد انتباه نقط الرقابة فى النظام .

هـ - الاطلاع على الارقام والكود السرى لتشغيل الكمبيوتر . ويمثل ذلك خطرا على سرية المعلومات والعمليات ، حيث أن الاطلاع على الكود السرى (أو معرفة الكود السرى) بواسطة غير المصرح لهم بهذا سواء من داخل الوحدة أو خارجها يمكنهم من استعمال الكمبيوتر لتنفيذ أو تغطية الغش المالى بسهولة لان استخدام الكود السرى للعمليات يلغى وظيفة نقط الرقابة الخاصة باكتشاف الاستخدام غير المصرح به .

و - التعاون بين أكثر من شخص (أو قسم) داخل النظام . (conclusion among two or more parties in the company) حتى يمكن تغطية الغش المالى فى الدفاتر، فكثيرا ما يلجأ مرتكب الغش المالى الى استخدام ممثلين من الاقسام المختلفة وذلك لاجراء التعديل المطلوب فى السجلات المكملة بالاقسام الاخرى. ويعتبر الاختلاس عن طريق التعاون بين الاقسام أكثر صعوبة فى اكتشافه بواسطة نظم الرقابة الداخلية حيث أن التعديل يتم فى كل السجلات، ومن ثم لم يترك أثرا أو تضارب فى الارصدة ليكشف عن وجود خلل أو تزوير فى العمليات .

٣ - تطوير أساليب الرقابة الداخلية لمواجهة الغش المالى :

يتضح من العرض السابق لخصائص نظم المعلومات الالكترونية، وكذلك من تحليل بعض حالات الغش المالى العملية أن مرتكبى الغش المالى يستخدمون ثغرات ملازمة لطبيعة تشغيل النظم الالكترونية (Vasarhelyi and Lin, 1988) ومن ثم يجب تطوير نظام الرقابة الداخلية ليشمل نقط رقابية لتغطية هذه الثغرات أو الخصائص . ونعرض فيما يلى بعض الاقتراحات الخاصة بتطوير نظام وأساليب الرقابة الداخلية لتضييق / كشف الغش المالى فى المشروع .

أولا : رقابة العمليات (Transaction Control)

تعتبر الرقابة على المدخلات فى النظام من أهم نقط الرقابة . ففى معظم حالات الغش السابقة، استطاع مرتكب الغش أن يضيف عمليات من اختراعه أو أن يغير مضمون العمليات ، وذلك كما هو فى الحالة رقم (١) فبدلا من اجراء قيد التسوية لاخطار وفاة تم اجرائه على أنه تغيير عنوان. وقد ساعدها فى ذلك خاصية تركيز النظام (Concentration) حيث أن اجراء تغيير العنوان يتم بواسطة عامل فى نقطة واحدة وبعدها يقوم الكمبيوتر باجراء التعديل فى كل السجلات والنقط الرقابية اللاحقة.

ويمكن تحسين أساليب الرقابة الداخلية للعمليات عن طريق اتباع الآتى :

١ - تقسيم النظام العام الى نظم مساعدة ومستقلة
(Independent Computer Sub-Systems)

ويهدف هذا الاسلوب الى وضع رقابة مضادة لخاصية تركيز التشغيل فى النظم الالكترونية. حيث لا يستطيع مرتكب الغش اجراء التسويات اللازمة لتغطية التزوير أو الاختلاس فى السجلات المساعدة والمكملة بمفرده (Elliot and William, 1980) فعلى سبيل المثال يمكن تقسيم دورة الشراء والسداد للموردين الى ثلاثة دوائر مستقلة (وفى نفس الوقت مكملة بعضها للبعض) :

أ - دائرة الطلب، ب - دائرة الاستلام والتخزين ، جـ - دائرة سداد الموردين. والاستقلال / أو التقسيم هنا لا يعنى تقسيم العمل فقط، وانما يعنى عدم استطاعة الموظف المختص بالطلب من الاطلاع أو القيد أو اجراء أى تسويات فى النظام الخاص باستلام الطلبيات أو سداد الموردين. أى منع الموظف الخاص بنظام مساعد معين من تشغيل أو

الاطلاع على النظم المساعدة الاخرى. وهنا تكون النظم المساعدة بمثابت نقط رقابة (أو مطابقة) على بعضها البعض .

والجوهر هنا (من استخدام النظم المساعدة) هو خلق نوع من المطابقة الحتمية مع اختلاف العامل الذى يقوم بادخال البيانات للكمبيوتر وكذلك اختلاف مستند المدخلات. وهذا فيه تضييق أو منع الفرصة من قيام موظف بمفرده من اجراء تعديل (تزوير) فى سجلات الكمبيوتر دون اكتشافه .

على أنه يجب ملاحظة أن تطبيق النظم المساعدة لا يضمن سلامة البيانات المحاسبية اذا اتفق موظفى المدخلات فى الاقسام الثلاثة على اجراء تزوير معين، وهذا ما يطلق عليه : Operators Collusion أى تعاون موظفى المدخلات فى الاقسام المختلفة على اجراء تزوير / تعديل معين فى سجلات الكمبيوتر. وهذا يتطلب وضع نقط رقابة مضادة اضافيه (مثل التناوب المفاجئ لموظفى المدخلات)، وهذا سوف يتناوله البحث بالتفصيل فى جزء لاحق.

٢ - السجلات الثنائية فى المدخلات : (Dual - File - Recording)

ويقضى هذا الاسلوب الى تزويد نظام الاستقبال فى الكمبيوتر بسجل اضافى يعمل تلقائيا عندما يقوم الموظف المختص بادخال بيانات أو تعديل أو تسويات فى السجل الاصلى وهذا الاسلوب يعرف فى لغة البيانات الالكترونية بـ (Back-up Copy) والهدف من الاحتفاظ بالنسخة الاضافية (Back-up Copy) هو وجود مصدر احتياطى للبيانات اذا تم اتلاف أو محو البيانات من السجل الاصلى عن طريق الخطأ .

ويوحى الباحث هنا بأن يتم تصميم برنامج الكمبيوتر بحيث لا يمكن للموظف (القائم بادخال البيانات) التعامل مع النسخة الاضافية (Back-up Copy) بمعنى أنه لا يمكنه

الاطلاع عليها أو اجراء تعديلات بها . أى أنها تعتبر بمثابة سجل رقابى على الموظف المختص فى عملياته على الكمبيوتر دون أن يكون له تأثير عليها. ومن ثم فإنه فى حالة عدم مطابقة البيانات (أرصدة الحسابات مثلا) بين السجل الاصلى (المرئى) والسجل الاضافى (غير المرئى)، فإن هذا يعتبر اشارة الى قسم المراجعة الداخلية لتحليل أسباب التضارب. وبناء على ذلك فإن موظف المدخلات لا يستطيع تعديل (أو تزوير) البيانات الواقعة تحت مسئوليته الا بعد الحصول على ترخيص بذلك من الجهة الادارية المختصة .

والجدير بالذكر أن معهد المحاسبين الامريكيين فى دراسة خاصة عن مراجعة نظم المعلومات الالكترونية أوصى بضرورة زيادة الاهتمام باجراءات وقيود التسويات فى سجلات الكمبيوتر[١]. الا أن المعهد لم يذكر بالتحديد الخطوات العملية لرقابة هذه التسويات .

٣ - تناوب / نقل موظفى الكمبيوتر بين الانظمة المساعدة دوريا :

Periodic / Random Rotating of Operators

ويهدف هذا الاسلوب الى الكشف عن ما يكون قد تكوّن بين الموظفين (كل فى دائرة اختصاصه) من اتفاق بغرض التغلب على النظام (Operators Collusion)، وتغطيه التلاعب فى البيانات والسجلات بين الانظمة المساعدة والمكملة. فقد أثبتت دراسات التنظيم الادارى بأن الافراد داخل المشروع كثيرا ما يتفقون على بعض الخطوات غير الرسمية بهدف كسر أنظمة الرقابة . وهذا ما يطلق عليه(Counter implementation) ، أى الاجراءات المضادة لتنفيذ ما تتطلبه اللوائح والانظمة الداخلية [٢] .

---

(1) AICPA, "The Auditor's Study and Evaluation of Internal Control in EDP Systems, New York, 1977.

(٢) لقد جذبت مشاكل ادخال وتشغيل الكمبيوتر فى الوحدات انتباه الباحثين ليس فى مجال المحاسبة والمراجعة فقط . فقد اهتم العلوم الاجتماعية بأثر النظم الالكترونية على عادات وسلوك الافراد فى المشروع . كما اهتم علم التنظيم بدراسة التغيرات المتوقعة فى أساليب التنظيم . ويمكن الرجوع فى ذلك الى :

- Kling, R. "Social Analysis of Computing : Theoretical Perspectives in Recent Empirical Research", Computing Survey 12, (MNarch, 1980) PP. 61-110.

وقد يرى البعض أن النقل الدورى أو تناوب موظفى الكمبيوتر بين الانظمة المساعدة قد يقلل من كفاية الموظف نظرا لان خبرته سوف تكون موزعة بين أقسام مختلفة وهذا ليس بالخطأ، الا أن الفوائد المقابلة تفوق التكلفة المتوقعة. فإنه بالرغم من توزيع الخبرة بين أقسام متعددة الا أن التوزيع ليس توزيعا جوهريا حيث أن الموظف ما زال يعمل فى مجال الكمبيوتر وان كان فى قسم آخر .

ثانيا : رقابة البرامج / مصممى البرامج : Programming Controls

ويهدف هذا الاسلوب الى التأكد من أن برنامج الكمبيوتر المستخدم يقوم بتحقيق الهدف المنشود منه. أو بمعنى آخر التأكد من أن مصمم برنامج الكمبيوتر لم يحور فيه ، أو لم يضيف اليه (أو يختزل منه) بعض الاجزاء لتغطية اختلاسات أو حذف بيانات غير مرغوب فيها .

تحقيق هذا الهدف عن طريق الفحص الدورى للبرامج المستخدمة . وفى ذلك كثيرا ما تلجأ الشركات الى اجراء عمليات صغيرة يدويا، ثم اجراء نفس العمليات مرة ثانية عن طريق برامج الكمبيوتر المرغوب فحصها، ثم مقارنة النتائج اليدوية مع مخرجات الكمبيوتر. وقد تلجأ بعض الشركات الى تغيير مصممى برامج الكمبيوتر دوريا، حيث يطلب من المصمم الجديد فحص البرنامج القديم واعداد تقرير عما يوجد به من ثغرات .

وقد تلجأ بعض الشركات الى اتمام عملية مراجعة البرامج وفحصها بطريقة غير علنية. حيث تقوم الشركة بايفاد مصمم البرامج الى مهمة ميدانية لفرع آخر للشركة لمدة أسبوع أو أسبوعين. وفى خلال هذه الفترة يتم استدعاء أحد المتخصصين من خارج الشركة لفحص والتأكد من سلامة البرامج المستخدمة.

٤ - تطوير أساليب المراجعة الخارجية

على الرغم من أن المراجع الخارجى ليس مسئولا بالدرجة الاولى عن اكتشاف الغش أو التزوير فى البيانات المحاسبية، الا أنه يعتبر مسئولا عن فحص وتقييم نظم الرقابة الداخلية للتأكد من كفايتها فى حماية أصول المنشأة وكذلك تحقيق الدقة فى البيانات المحاسبية [١].

ولما كان نظام المحاسبة الالكترونى أحد أجزاء النظام العام للشركة ، فإن مراجع الحسابات يعتبر مسئولا عن التأكد من مدى كفاية أساليب الرقابة الداخلية من خلال ذلك النظام. ومع استمرار اختراع واستخدام النظم الالكترونية فى المنشآت، أصبحت أساليب المراجعة فى حاجة الى تطوير مستمر حتى تتفق وتساير خصائص النظم السائدة فى الوقت المعاصر.

وفى اطار تطوير أساليب المراجعة قد استعرض الباحثين والمهنيين (AICPA) بعض طرق تقييم نظم الرقابة الداخلية لانظمة المعلومات الالكترونية. فقد اقترح كل من Cushing (1974) Bonder (1975), Vasarhely (1980) and Srinidi and Vasarhely (1986) استخدام أسلوب اختبار فاعلية النظم الهندسية Engineering Reliability Models لتقييم فاعلية الرقابة الداخلية فى النظم الالكترونية . ويقوم هذا النظام على أساس حساب احتمالات وقوع الخطأ فى كل جزء من أجزاء النظام مسبقا، ثم تركيز واجراءات الفحص على الاجزاء ذات احتمال الخطأ العالية. ويعيب البعض على هذا الاسلوب أنه لا يأخذ فى الحسبان الظروف السلوكية والمناخية لتشغيل النظام .

كما قد اقترح معهد المحاسبين الامريكيين فى دراسته عام ١٩٧٩ (AICPA Section 320-65) استخدام الاسلوب المنطقى (Conceptual Logical Approach) ويقضى هذا الاسلوب أن يركز المراجع اهتمامه على الاخطاء والتحويرات فى النظام التى يمكن أن تقع، بمعنى أن يتصور المراجع أو أن يسأل نفسه ما هى الاخطاء أو التحويرات التى يمكن أن تحدث فى كل جزء من أجزاء النظام . ثم يقوم بعد ذلك باجراء الاختبارات التى تؤكد / تثبت سلامة

---

(1) AICPA, Statement of Auditing Standards Number 1 (SAS No. 1). New York, 1972.

النظام من هذا النوع من الخطأ / أو الغش والذى سبق أن تصوره.

ونعرض فيما يلى بعض النقاط الهامة والتى يجب أن تؤخذ فى الحسبان عند مراجعة النظم الالكترونية :

أ - تحديد نقط الرقابة/ نقط الضعف فى النظام
(Control Point Identification)

يتضح من العرض السابق أن تحديد نقط الضعف أو الثغرات فى نظم المعلومات الالكترونية يعتبر عنصرا هاما في مراجعة أجزاء النظام والحكم على مدى فعاليته وتأتى هذه الاهمية فى اطار مستويات الأداء المهنى، حيث يقضى أساس المراجعة رقم : (AICPA SAS No.3) بضرورة أن يتفهم المراجع لطبيعة تدفق العمليات داخل النظام ودقة تنفيذها .

وحيث أن تدفق العمليات فى ظل أنظمة الحسابات الالكترونية قد يكون متشابكا ومتداخلا بعضه مع البعض، فإن أنسب أسلوب لفحص تدفق العمليات هو اختبار البيانات عند مرورها بنقط رقابة معينة فى النظام .

ولعل أسلم أسلوب لتحديد نقط الرقابة هذه هو أن يقوم مراجع الحسابات بدراسة خريطة تشغيل وتدفق العمليات والبيانات بين أجزاء النظام، ومن ثم تحديد نقط الرقابة التى يجب عليه فحصها، أو اجراء الاختبارات عندها. ويتطلب تنفيذ هذا الهدف ضرورة تأهيل مراقب الحسابات فنيا حتى يصبح قادرا على تحليل نظم المعلومات الالكترونية وخطوات تشغيلها، ومن ثم اكتشاف نقط (الضعف) الرقابة .

ب - مراجعة أمن المعلومات : (Information Security Audit)

يقصد بأمن المعلومات حماية البيانات والسجلات من الافعال التى تغير من محتواها أو اختفائها أو استخدامها بواسطة الافراد غير المصرح لهم سواء كانت هذه الافعال عن عمد Deliberate أو بطريق الخطأ Accidental ومن ثم يجب على نظام الرقابة الداخلية أن يوفر ضمانات أمن المعلومات فى الجوانب الآتية :

أمن المعلومات من الأفراد ، الأمن الادارى، أمن النظام نفسه، وأخيرا أمن المناولة ودور المراجع الخارجى هنا هو التأكد من وجود هذه الضمانات والتى تكفل حماية المعلومات فى النقط المشار اليها عاليا (Srinivasn and Dascher, 1978) فعلى سبيل المثال، نجد أن معظم أنظمة الكمبيوتر مزودة بأجهزة لتشهر أو تبلغ الادارة عن محاولة كسر الكود السرى والاطلاع على سجلات الكمبيوتر بواسطة أشخاص غير مصرح لهم بذلك. ومسئولية مراجع الحسابات فى هذا الموقف ليست فقط التأكد من وجود هذا الجهاز (ناقوس الخطر)، بل أيضا يجب أن تمتد لتشمل التأكد من أن ادارة الشركة قامت باتخاذ الاجراءات المناسبة لمنع حدوث هذه المحاولات ثانيا .

جـ - استخدام أسلوب فريق المراجعة : (Audit Team Approach)

تثبت الدراسات الميدانية فى مجال حكم المراجع على كفاية نظام الرقابة الداخلية ن مستوى آداء فريق المراجعة يفوق بكثير مستوى آداء المراجع الفردى فى حالات المراجع المتشعبة (أى حالات مراجعة الشركات الكبيرة)(١). ومن التحليل السابق يتضح أن عملية مراجعة نظم المعلومات الالكترونية متشعبة ومن ثم يرى الباحث ضرورة استخدام أسلوب فريق المراجعة فى مراجعة نظم المعلومات الالكترونية.

وتتفق فلسفة فريق المراجعة مع طبيعة النظم الالكترونية من حيث أن فريق المراجعة

---

(١) يمكن الرجوع فى ذلك الموضوع الي دراسة تحليلية (تجميعيه) للأبحاث السابقة :
Soiomon , Ira " Multi- Auditor Judgment / Decision Marking Research " Joumal of " Accounting Literature " 6 (1987) , P.P. 1 - 25.

يؤدى الى الآتى:

- أن يوفر المناقشة الجماعية للجوانب المختلفة للنظام. بمعنى مراجعة أجزاء مختلفة (Systems من النظام بواسطة مراجعين مختلفين يعطى فرصة أكبر لتطابق (أو عدم تطابق) الحكم على فاعلية نظام الرقابة الداخلية.
- أن يوفر الفرصة لان يحتوى الفريق على أعضاء فنيين وفقا لطبيعة النظام. بمعنى أن يكون ضمن الفريق أحد خبراء نظم المعلومات وتصميم برامج الكمبيوتر .

والجدير بالذكر فى هذا الصدد أن معظم شركات المحاسبة (المراجعة) بدأت بالفعل تستعين بخبراء النظم ومصممى الكمبيوتر فى مراجعة نظم المعلومات الالكترونية (Arnes and Loebbecke , 1984) بل تقضى مبادئ التأهيل الشخصى للراجع (AICPA) بإستمرارية تدريب المراجع وزيادة معرفته بالتطور فى نظم المعلومات .

٥- خلاصة البحث وتوصياته :

لقد صاحب استخدام أنظمة الحاسبات الالكترونية ارتفاع فى عدد حالات الغش المالى والتلاعب بأصول الوحدات الاقتصادية. والجدير بالذكر أنه لم يتم اكتشاف هذه الحالات من خلال نظم الرقابة الداخلية أو المراجعة الخارجية. وقد دفعت هذه الملاحظة الكثير من الباحثين والمهنيين فى مجال المحاسبة والمراجعة الى اسناد ظاهرة انتشار الغش المالى من خلال الكمبيوتر الى عجز أساليب الرقابة الداخلية والمراجعة الخارجية عن مسايرة التطور المستمر فى نظم المعلومات .

وفى هذا البحث قام الباحث بتحليل خصائص نظم المعلومات الالكترونية والتى لها آثار سلبية على الرقابة الداخلية. وامتد البحث الى دراسة بعض حالات عملية لتحديد الثغرات التى يستخدمها مرتكبى الغش المالى من خلال الكمبيوتر ثم أخيرا قام الباحث باقتراح بعض أساليب الرقابة الداخلية لمواجهة خصائص النظم الالكترونية وسد الثغرات التى تسهل عملية الغش المالى . كذلك أيضا اقتراح بعض أساليب المراجعة الخارجية لاكتشاف

عمليات الغش المالى .

وتتصف نظم المعلومات الالكترونية بالخصائص التشغيلية الآتية :

١ - تركيز عمليات التشغيل وتلقائية القيد والتعديل فى السجلا. بمعنى أن نقط المدخلات أو/ التسويات مركزة. ومن ثم فإن عامل المدخلات يمكنه أن يغير محتويات السجلات الاخرى حتى ولو كانت واقعة تحت مسئولية قسم آخر .

٢ - أن السجلات الدائمة للنظام غير مرئية - بمعنى أن كل سجلات النظم الالكترونية عبارة عن أشرطة واسطوانات مغناطيسية ، وهذا يجعل عملية فحص المحتويات أو تحليل الاجماليات صعبا.

٣ - أمن المعلومات أكثر حساسية عن النظم اليدوية. بمعنى أنه يمكن محو (ازالة) بيانات أساسية بمجرد الاستخدام الخطأ، أو سهولة ازالتها بمجرد الضغط على مفتاح الكمبيوتر، أو اضافة بيانات لتغطية عمليات غير قانونية .

٤ - خطورة دور الفنيين فى النظام (مصممى برامج الكمبيوتر والقائمين على التشغيل) وهذا يلقى عبئا جديدا على نطاق الرقابة الداخلية، وعلى حجم ونوع الاختبارات التى يجريها المراجع الخارجى.

ويفيد تحليل الحالات العملية للغش المالى ، أن مرتكبى الغش قد استخدموا الثغرات الموجودة بالنظام والملازمة لخصائص النظم الالكترونية . فمثلا بسبب خاصية تركيز المدخلات واجراء القيد فى السجلات تلقائيا تمكن مرتكب الغش من تغطية اختلاساته عن طريق اجراء التسويات فى السجلات الاخرى حتى وان كانت تحت مسئولية أقسام أخرى . كما أن غياب أمن المعلومات (وخاصة الارقام السرية) لتشغيل النظام ونقل الارصدة مكنت بعض المختلسين من نقل أرصدة الى حسابات خاصة سواء داخل الدولة أو خارجها .

وفى مواجهة هذه الثغرات يقترح الباحث ضرورة تطوير نظام الرقابة الداخلية على الوجه التالى : أولا: رقابة العمليات . ويمكن تطوير رقابة العمليات عن طريق تقسيم النظام العام الى نظم مساعدة ومستقلة، أى القضاء على ظاهرة تركيز التشغيل والقيد التلقائى.

كذلك أيضا يمكن استخدام أسلوب السجلات الثنائية فى المدخلات (Dual - File - Record-ing) حيث يكون السجل الثانى رقيبا على عامل المدخلات. كذلك أيضا يمكن تقليل حجم الخطر عن طريق تناوب أو نقل موظفى الكمبيوتر دوريا . أما فى مجال أمن المعلومات ، فيجب على ادارة الوحدات أن تفحص دوريا برامج الكمبيوتر المستخدمة لتتأكد من سلامة تصميم النظام للكمبيوتر دوريا مع الخبراء الخارجيين . وكذلك تغيير الكود التشغيلى للكمبيوتر دوريا مع تحديد مسئولية المستخدمين. وأيضا استخدام أجهزة الانذار التى تفصح عن محاولات استخدام الكمبيوتر بواسطة غير المصرح لهم .

أما فيما يتعلق بالمراجع الخارجى ، فإن التطوير يتطلب تدريب المراجع على التحديد الدقيق لنقط الرقابة فى النظام، أى نقط الضعف فى النظام حتى يركز عليها الاختبارات الميدانية والفحص. وفى هذا الصدد يمكن الاستعانة بخبراء النظم ومصممى برامج الكمبيوتر لتحليل نظام معلومات العميل وتحديد نقط الرقابة التى يجب فحصها أو التركيز عليها . ويعتبر أسلوب فريق المراجعة أكثر ملاءمة حيث يحتوى الفريق عل يمتخصصين فى مجال النظم والكمبيوتر، هذا مع ضرورة فحص نظام الرقابة الداخلية للتأكد من كفاية اجراءات أمن المعلومات .

توصيات لدراسات أخرى :

لما كان هذا البحث يقوم على أساس دراسة تحليلية لمشكلة الغش المالى وفقا لخصائص النظم الالكترونية وأساسيات المحاسبة والمراجعة فيما يتعلق بالرقابة الداخلية، فإن الامتداد الطبيعى للبحث فى هذا المجال هو دراسة عملية يتم فيها تحديد سلوك مراجع الحسابات فى فحص ومراجعة النظم الالكترونية عن طريق ما يسمى بـ Protocol Analysis .

فعلى سبيل المثال يمكن اختبار عينة من محاسبى الجهاز المركزى للمحاسبات ووضعهم فى مناخ يصف حالة عميل يحتفظ بنظام حسابات الكترونى. ثم يطلب منهم اجراء عملية المراجعة بصوت مرتفع وخطوة بخطوة، وتحديد مواطن السهولة / الصعوبة فى اجراءات الفحص والمراجعة. والهدف من هذا هو تحديد احتياجات المراجع من النظم الالكترونية حتى يستطيع أن يبنى رأيا فنيا محايدا عن دلالة الحسابات (النظام).

أما اذا تعذر توفير هذا المناخ للبحث فى مصر، فانه يمكن استخدام أسلوب قائمة الاستقصاء (Questionnair) حيث يتم فيها الاستفسار عن الصعوبات المحتمل أن يواجهها المراجع فى مراجعة النظم الالكترونية، ما هى الخطوات العملية التى يلجأ اليها للتغلب على هذه الصعوبات ، وما هى اقتراحاته لتصميم نظام المعلومات حتى يكون أكثر قابلية للمراجعة ولتخفيض حجم الخطر فى البيانات المحاسبية الناتجة عن النظام .

REFERENCES

AICPA, "The Auditor's Study and Evaluation of Internal Control in EDP Systems, "**AICPA**, New York, 1977.

Allene, Brandt, "The Biggest Computer Frauds : Lessons for CPAS, "**The Journal of Accountancy** (May 1977), pp. 52-62.

Arnes, A., and J. Loebbecke, "**Auditing : An Integrated Approach**", Prentice-Hall, New Jersey, 1984.

Bondar, G., "Reliability Modeling of Internal Control Systems", **The Accounting Review** (October 1975), pp. 747 - 757.

Carmichael, D., "Behavioral Hypotheses of Internal Control", **The Accounting Review** (April 1970), pp. 235-245.

Cushing, B., "A Mathematical Approach to the Analysis and Design of Internal Control Systems", **The Accounting Review** (January 1974), pp. 24-41.

Davis, G., and R. Weber, "The Impact of Advanced Computer Systems on Controls and Audit Procedures, "**Auditing : A Journal of Practice and Theory** 5 (Spring 1986), pp. 35-40.

Elliot, R., and J. Wiulliam, "**Fraud Detection and Deterrence**", New York, 1980.

Kling, R., "Social Analysis of Computing : Theoretical Perspectives in Recent Empirical Research", **Computing Survey** 12 (March 1980), pp. 61-110.

Krauss, L., and A. MacGahan, "**Computer Fraud and Counter Measures**", Prentice-Hall, Englewood Cliffs, N.J. 1979.

Parker, D., "A Look at Computer Fraud and Embezzlement in Banking", **The Magazine in Bank Administration** (May 1976), pp. 18-23.

Perry, W., and H. Warner, "Systems Auditability : Friend or Foe?" **Journal of Accountancy** (February 1987), pp. 52-60.

Pomeranz, F., "Auditors Sensitivity to Fraud", **Journal of Accounting, Auditing, and Finance** (Winter 1980), pp. 1-25.

Sawyer, L., **"The Practice of Modern Internal Auditing"**, The Institue of Internal Auditors Inc., 1981.

Solomon, I., "Multi-Auditor Judgment / Decision Making Research", **Journal of Accounting Literature** 6 (1987), pp. 1-25.

Srinidhi, B., and M. Vasarhelyi, "Auditor Judgment Concerning Establishment of Substantive Tests Based on Internal Control Reliability", **Auditing : A Journal of Practice and Theory** 5 (Spring 1986), pp. 64-76.

Srinivasan, C., and P. Dascher, "Computer System Security and Auditing Implications, **"The National Public Accountant"** (January 1978), pp. 20-25.

U.S. Chamber of Commerce, **"A Handbook on White Collar Crime"**, Washington, 1974.

U. S. Department of Justice, **"Computer Crime"**, Criminal Justice Resource Manual, 1979.

Vasarhelyi, M., and W. Lin, **"Advanced Auditing"**, Adison Wesley, 1988.