دور التدقيق الخارجي في مكافحة الجرائم المالية الإلكترونية

– رؤية استشرافية نقدية على الساحة المهنية والعالمية –

The role of external audit in combating digital financial crime
- A critical outlook on the professional and global arena-

سعيداني محمد السعيد[1]*، زرقون عمر الفاروق[2]، بكيري جمال الدين[3]

[1] جامعة عمار ثليجي (الجزائر)، ms.saidani@lagh-univ.dz

[2] جامعة ورقلة (الجزائر)، zergounefarouk@gmail.com

[3] جامعة عمار ثليجي (الجزائر)، bekiridjameleddine@gmail.com

تاريخ الاستلام: 2023-02-27 **تاريخ القبول:** 2023-04-24 **تاريخ النشر:** 2023-06-12

ملخص:

تنتشر الجرائم المالية الإلكترونية، كمرض تقني، بسرعة خارقة في العصر الحالي؛ لا شيء آمن، والشركات تحت تهديدٍ كبير؛ لا تزال تكلفة الاحتيال الرقمي تمثل مشكلة للعديد من المؤسسات بمختلف الاقتصاديات، تستكشف الدراسة كيف يمكن للتدقيق الخارجي توفير وسائل للحد من الاحتيال المالي الإلكتروني وتعزيز فعالية التدقيق التنظيمي للكشف عن مجالات وحالات الاحتيال المحتملة، أصبح الوصول إلى الأدلة أكثر تعقيدًا بشكلٍ متزايدٍ وبأحجام أكبر بكثير مما كانت عليه في عقودٍ سابقةٍ، تقدم النتائج المزيد من الأسئلة المفتوحة والفرص لتطوير وترقية هذا المجال، هناك حاجة ماسة لتطوير برامج تدقيق آلية ومتخصصة لحل المشكلات الرقمية، وثانيًا، توفير المهارات الجديدة المطلوبة من قبل المدققين ليكونوا فعالين في قطاع أعمال ذكي.

كلمات مفتاحية: البيئة الرقمية؛ جرائم الإنترنت؛ معايير التدقيق؛ البيانات المالية الاحتيالية.

تصنيفات JEL : H70؛ K29؛ L25؛ M41؛ M42؛ O33.

Abstract:

Cybercrimes as a technology disease are spreading very speedily in present era. Nothing is secure now and institutions are under a great threat. The cost of fraud continues to be a problem for many organizations in the global economy. This study explores how external audit may offer a way forward for organizations to reduce fraud and advance organizational audit effectiveness for detecting potential fraud areas and cases. the access to evidence is increasingly more complex and in far greater volumes than in previous decades. The research results offer more open-ended questions and opportunities to develop and upgrade this specific area, There needs to be the development of automated and specialist problem-solving auditing software and secondly, the new skills required by auditors to be effective in an intelligent workplace.

Keywords digital environment; Cybercrime; ISA; Fraud Financial statements..

JEL Classification Codes: H70, K29, L25, M41, M42, O33.

* المؤلف المرسل

1. مقدمة:

يتغير العالم بسرعة، لكن لا يبدو أن مهن المحاسبة والتدقيق تلاحظ ذلك، تمارس المحاسبة لأكثر من 500 عام بإجراءات وضمانات قديمة الطراز (القيد المزدوج **Fra Luca Pacioli** عام 1492 م)، بينما جرى العرف المهني على اعتبار التدقيق الخارجي آلية للكشف عن أي انحراف أو خطأ أو مبالغة غير عادية بالتركيز على عينة من المعاملات وموثوقية البيانات المالية، وإبداء الملاحظات في التقرير، من المتوقع أن يتألف النظام البيئي المعلوماتي القادم من سلسلة ضخمة من مصادر البيانات المترابطة والوكلاء الخارجيين التي تتجاوز الحدود التقليدية للشركة، في الواقع، أصبحت بيانات العملاء أكبر وأكبر بكثير مما يتعامل معه المدقق، ما يدفع بشكلٍ معقولٍ إلى افتراض أن إعداد التقارير سوف يتطور إلى مجموعة أوسع بكثير من **IFRS** أو **US GAAP** أو **ISA**، وفقًا لذلك، يتم تقديم المزيد من الإرشادات المهنية للمدققين للتعامل مع بيئة البيانات الضخمة **Big Data**.

في الوقت نفسه، تعد الجرائم الإلكترونية واحدة من تحديات عالم اليوم، توفر العولمة **globalization** فرص لتجاوز الحدود الإقليمية، بينما تولد شبكات التوزيع **networks distributed** فرصاً لتكوين ضحايا جدد، وتوفر مسارات البيانات **trails data** مواد جديدة لارتكاب الجريمة، يشير المنتدى الاقتصادي العالمي **World Economic Forum** أن العائدات غير المشروعة من النشاطات الإجرامية تقدر بنحو 2-5 **%** من الناتج المحلي الإجمالي العالمي أو 02 تريليون دولار[1]،

2.طرح إشكالية الدراسة:

في سياق البيئة الرقمية المعقدة، يلعب التدقيق الخارجي دورًا مهمًا في كشف عمليات الاحتيال الإلكتروني، وعليه يمكن طرح إشكالية الدراسة بالشكل الآتي:-

ما مدى فعالية التدقيق الخارجي في مكافحة الغش والتحايل المالي الإلكتروني في سياق البحث عن شفافية بيئة التقارير المالية واستدامتها؟؛

3.فرضية الدراسة:

يعتبر التدقيق الخارجي أحد الأدوات الرقابية الهامة الكفيلة بتحجيم مخاطر الغش والتحايل المالي الإلكتروني بمختلف الاقتصاديات مما يساهم بدورٍ محوريٍ و هامٍ في تحقيق شفافية بيئة التقارير المالية واستدامتها؟؛

4.محاور الدراسة:

وللبحث في مختلف الجوانب تضمنت الدراسة المحاور التالية:-

1.4. الغش والتحايل المالي في ظل البيئة الرقمية الإلكترونية المعاصرة؛

2.4. دور المراجعة الخارجية في مكافحة الغش والتحايل المالي الإلكتروني بقطاع الأعمال.

1.4. الغش والتحايل المالي في ظل البيئة الرقمية الإلكترونية المعاصرة

1.1.4. تعريف الغش والتحايل المالي الإلكتروني في قطاع الأعمال

يشير مصطلح الجرائم الإلكترونية إلى الأعمال غير القانونية التي يرتكبها الفرد أو الأفراد عبر الفضاءات الإلكترونية باستخدام تكنولوجيا المعلومات والاتصالات وأدوات القرصنة وتقنيات التواصل الاجتماعي لغرض وحيد هو تحقيق مكاسب اقتصادية غير مشروعة أو ميزة مالية أو مهنية2، يُعرفْ الاحتيال الحاسوبي Computer Fraud بأنه: "سلوكٌ غيرُ شرعيٍ فردي أو جماعي قائمٌ على نية الغش بهدف تحصيل منافع أو دفع أضرارٍ مالية باستخدام الحاسوب مما يترتب عليه ضررٌ بالغير بتفويته مصلحة أو تحمله خسارةٍ ماديةٍ أو معنويةٍ"3، فالجريمة الإلكترونية: "فعلٌ ضارٌ يأتيه المواطن عبر استعماله الوسائط الإلكترونية كالحواسيب، أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الإنترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية"4، ويعرفها مؤتمر الأمم المتحدة لسنة 2000 م بأنها: "الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أو في بيئة إلكترونية"5، وتُعرَّف سرقة الهوية بأنها: "استخدام شخص آخر لمعلوماتك الشخصية لإنشاء حسابات احتيالية وسرقة بطاقات الائتمان والشيكات المطبوعة من البريد"6، وتعرفها وزارة العدل الأمريكية The U.S Department of Justice بأنه: "فعلٌ غير شرعي يتطلب المعرفة بتكنولوجيا الحاسوب لأجل ارتكابه أو تحقيقه إما بغرض إنجاز أهدافٍ خاصة فردية كانت أو جماعية بما في ذلك غسيل الأموال، والتهرب الضريبي، والاحتيال المالي، سرقة الهوية والحسابات الشخصية للموظفين، تغييرات في كشوف المرتبات، الترقية الوهمية للموظفين، وتوليد الموظفون الوهميون أو الشركاء الخارجيون أو المورّدون، والاحتيال التسويقي بإنشاء معاملات وهمية وزيادة تحصيل المستحقات، أو المبالغة في تقدير الأصول والإيرادات والأرباح أو التقليل من الالتزامات والخسائر وغيره"7، حسب التعاريف ستكون أجهزة الحاسوب إما موضع الجريمة كتدمير البيانات وتخريب أجزائها وبرامجها، أو أداة لارتكاب الجريمة بالتجسس وسرقة بطاقات الائتمان وإجراء التحويلات من حسابٍ لآخر، وقد تكون هي ضحية للجريمة الإلكترونية سواءٌ على كيانها المادي hardware أو المعنوي software كتعطيل خادم موقع الشركة أو هجوم الفيروسات، وهذه الجرائم تستخدم فيها شبكة الإنترنت باعتبارها أداةٌ لارتكاب الجريمة أو لتسهيل ارتكابها8، يرى Saether & Gottschalk 2011 م بأن أحد أسباب انتشار الغش المالي الإلكتروني في السنوات الأخيرة يعود إلى ضعف أنظمة الشركات في فحص المستندات وجمع الأدلة الالكترونية لإثبات حدوث الجريمة المالية، وينقسم المهاجمون عمومًا إلى ثلاث فئات رئيسية9:-

المهاجم ذو الدوافع المالية الذي يرغب بتجاوز الأنظمة لإجراء عمليات تحويل مالية إلكترونيًا؛

المهاجم بدافع التجسس الذي ينوي سرقة المعلومات لبيعها لطرفٍ ثالثٍ؛

المهاجم ذو الدوافع السياسية الذي ينوي المساومة على المعلومات أو الأنظمة لتحقيق هدف مشترك داخل مجموعة ذو توجهات سياسية معينة.

2.1.4. أنواع الغش والتحايل المالي الإلكتروني في الشركات

يمكن تصنيف الغش المالي الحاسوبي إلى خمسة أصنافٍ أساسية وهي:-

1. احتيال المدخلات Input: وهي أسهل طرق الاحتيال الإلكتروني بتعديل مدخلات الجهاز التي تتطلب القليل من المهارات الحاسوبية تشمل فقط فهم كيفية تشغيل النظام ثم إخفاء الأثر؛

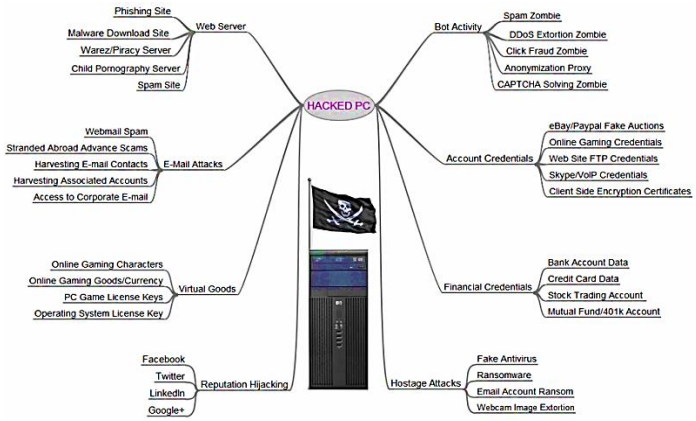
2. احتيال المعالج Processor Fraud: وذلك بالاستخدام غير المصرح به للأنظمة الحاسوبية من داخل الشركة أو خارجها، تتبنى كثير من الشركات سياسة عدم استخدام الأنترنيت من قبل موظفيها للأغراض الشخصية، ويعتبر انتهاك هذه السياسة احتيالاً من قبل موظفيها؛

3. احتيال تعليمات الأنظمة الحاسوبية Computer Instructions Fraud: يقوم هذا الاحتيال على التلاعب ببرمجيات الأجهزة والأنظمة الحاسوبية لتشغيل وإعداد البيانات والتقارير والتعديل فيها وأخذ نسخ غير قانونية عن البرمجيات واستخدامها في أنشطة غير مسموح بها أو تطويرها للقيام بأنشطة غير مصرح بها؛

4. احتيال المخرجات Output Fraud: وهو احتيال يقوم على إساءة استخدام مخرجات الأجهزة والأنظمة الحاسوبية للشركة بنسخها أو طبعها أو تغيير مخرجاتها وعرضها للمزاد في المواقع الإلكترونية.

يمكن عرض مخاطر الاختراق الإلكتروني في الشكل الموالي:-

الشكل (01): مخاطر اختراق أجهزة الحاسوب



Source : The Scrap Value of a Hacked PC, Revisited, site: https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/, date : 15/10/2012, date : 27/08/2022, p 01.

3.1.4. مجالات الجرائم المالية الإلكترونية في الشركات وقطاع الأعمال

تتعدد أنواع الجرائم المالية الإلكترونية في الشركات إلى الأنواع التالية10:-

1. الجرائم المرتبطة بالبورصات وأسواق الأسهم والأوراق المالية

يسمح سوق الأوراق المالية للمتعاملين باستثمار أموالهم إلكترونياً بغرض تحقيق عائد إيجابي متوقع، ومع ذلك، يتجه البعض إلى ارتكاب نشاط استثماري احتيالي بالتلاعب بأسعار الأوراق المالية والأصول الأساسية، يمثل التداول غير المشروع من الداخل أحد أخطر نماذج الاحتيال المالي بالأسواق المالية

2. عمليات غسل الأموال

غسل الأموال أسلوب يستخدمه المجرمون الذين يمتلكون أموالاً "قذرة" بممارسة نشاطات غير قانونية بهدف تحويلها إلى الحالة الشرعية في أعين القانون والمجتمع والحكومة.

3. سرقات الحسابات الشخصية والهوية الإلكترونية

SIM-Swapping هو هجوم يسمح لمجرمي الإنترنت بالتحكم غير المصرح به في أرقام الهواتف المحمول والبريد الإلكتروني والمواقع الإلكترونية للعملاء وموظفي الشركة، ، في هذا الشأن ذكرت سلطات كاليفورنيا أن طالبًا جامعيًا Joel Ortiz البالغ 20 عامًا سرق ما يقارب 05 مليون دولار لأكثر من 40 رقم هاتف باستخدام تقنية SIM-Swap لمستثمري العملات المشفرة في إجماع مؤتمر block Chain conference Consensus بمدينة نيويورك New York City11،12.

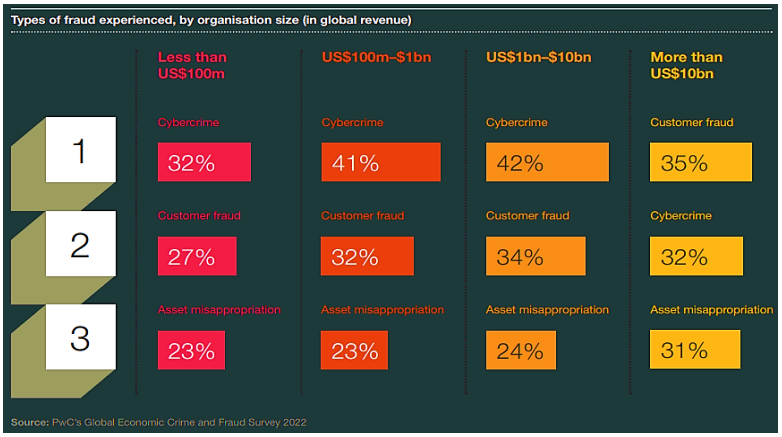
4. التزييف العميق و GPT-2 أو Deepfakes and GPT-2

يعتبر GPT-2 روبوت محادثة ذو ذكاء اصطناعي مفتوح أظهر أنه يمكن أن ينتج فقرات نصية تشبه البشر مثل المقالات الإخبارية، تم استخدام GPT2 لإنشاء مراجعات خاطئة لمواقع البائعين والعملاء الحقيقيين مثل Amazon، وبالتالي إجراء معاملات مع موردين وعملاء وهميين أو غير شرعيين أو مصنعي سلع ذات جودة منخفضة أو للإضرار بسمعة شركة منافسة.

4.1.4. واقع الجرائم المالية الإلكترونية في مناطق مختلفة من العالم

يشير تقرير USA Today reports لسنة 2014 م بأن المتسللين سرقوا أكثر من 500 مليون دولار على مدار الـ 12 شهرًا الماضية من البنوك والمؤسسات المالية الأمريكية دون دخول أي مبنى على الإطلاق على غرار بورصة نيويورك New York Stock Exchange و Bank of America و Capital One and ING و PNC Banks وغيرهميوضح الشكل التالي أنواع الجرائم المالية بالنظر إلى حجم الشركات كما يلي:-

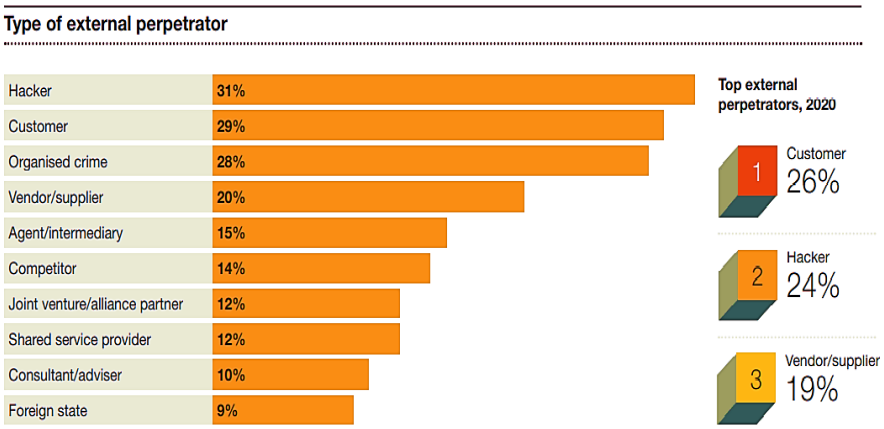
الشكل (02): علاقة أنواع الجرائم المالية بحجم الشركات



Source: PWC's (2022), Op cit, p 05.

وفقًا لتقرير PWC فإن 70 % من الجرائم المرتكبة هي إما هجوم خارجي أو بالتواطؤ مع الداخل، توافق الشركات بأن أدوات منع الاحتيال التقليدية كالتحقيقات وقواعد السلوك لم تعد تردع المحتالين الخارجيين، وصل الاحتيال الخارجي إلى 43 % مقابل 41 % في 2020 م ، وتعتبر مخاطر سوء السلوك هي أكثر محفزات التحايل الداخلي بنسبة 35 % مقارنةً بمخاطر الهجوم الرقمي بنسبة 16 %، وهو ما يوضحه الشكل التالي:-

الشكل (03): أهم مرتكبي التحايل الخارجي في الشركات

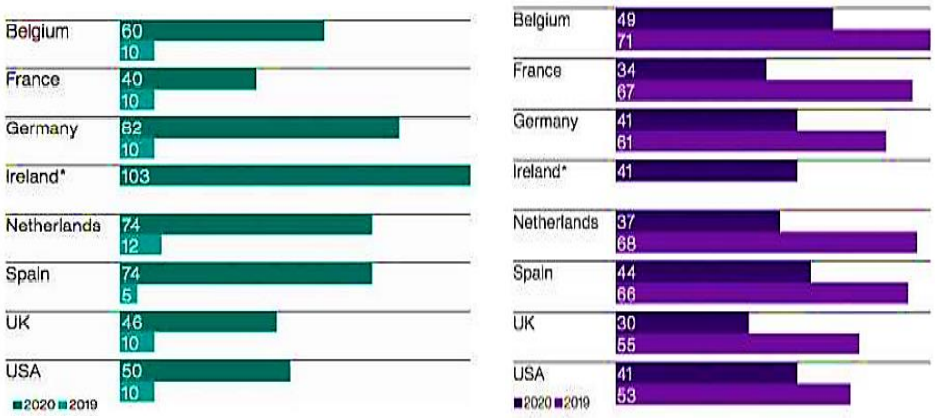


Source: PWC's (2022), Op cit, p 05.

على المستوى الدولي، وفي أوروبا، ذكرت بورصة ناسداك أواخر 2015 م بوقوع عدة هجمات إلكترونية في التداول عبر الإنترنت لاسيما في شركة FXCM للتداول بالعملات الأجنبية عبر الإنترنت، حصل المتسللون خلالها على وصول غير مصرح به إلى معلومات العملاء وتم إجراء بعض التحويلات من حساباتٍ معينةٍ، وفي سنة 2016 م أشار تقرير مؤسسة Crime Russia إلى تمكن قراصنة من سرقة أكثر من 1.7 مليار روبل (28.3 مليون دولار) من حسابات البنوك الروسية قبل احتجازهم من قبل الحكومة الروسية، تراوحت خسائر كل بنك من 2.5 مليون دولار إلى 10 ملايين دولار، بينما ذكر تقرير The Week Newsletter أوائل 2017 م أن بنك HSBC أحد أكبر بنوك أوروبا عانى من هجوم إلكتروني لم يتمكن عملائه بسببه من الوصول إلى الخدمات المصرفية عبر الإنترنت للمرة الثانية في شهرٍ واحدٍ، في حادثة مماثلة ذكرت Turkey Insurance Journal أن المتسللون استهدفوا في هجومٍ إلكتروني نظام تحويل الأموال العالمي SWIFT التابع للبنك التركي Akbank مما جعله يواجه مسؤولية قانونية تصل إلى 04 مليون دولار جراء الحادث.

الشكل (04):

الشكل (04): الإنتهاكات الرقمية لنفس الدول



Source : Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, Anurag Kumar Jaiswal (2021), A Systematic Literature Review on the Cyber Security, International Journal of Scientific Research and Management, Vol 09, n° 12, p 678-679.

2.4. دور المراجعة الخارجية في مكافحة الغش والتحايل المالي الإلكتروني بقطاع الأعمال

1.2.4. تعريف التدقيق الرقمي أو الإلكتروني

يُعرَفْ التدقيق الإلكتروني E – Auditing أو Computer Auditing بأنه: "عملية تطبيق أي نوع من الأنظمة بإستخدام تكنولوجيا المعلومات لمساعدة المراجع في التخطيط والرقابة وتوثيق أشغال المراجعة"13، وأيضاً: "عملية جمع وتقييم لتحديد ما إذا كان استخدام الكمبيوتر يساهم في حماية أصول الشركة، ويؤيد سلامة بياناتها، ويحقق أهدافها بفعالية، ويستخدم مواردها بكفاءة"، وكذا: "عملية تجميع الأدلة لتحديد مدى كون نظم المعلومات المحاسبية المحوسبة مصممة للإحتفاظ بالبيانات المتكاملة وتخزين وإسترجاع المعلومات وتحمي الأصول وتسمح بتحقيق الأهداف التنظيمية وفعالية إستخدام الموارد، والحصول على تأكيدٍ معقولٍ بأن ضوابط الرقابة الموجودة كافية لحماية قواعد البيانات والتطبيقات وخادم الموقع من الوصول غير المسموح به"14، وأيضاً: "عملية فحص وتقييم نظم تشغيل المعلومات الآلية وغير الآلية والتفاعل فيما بينها، بهدف تقديم تأكيد معقول بأن ضوابط الرقابة الداخلية تحقق متطلبات تكنولوجيا المعلومات"، من خلال التعريفات، يشير Mike Suffield 2020 م إلى المهارات الواجب توافرها في مراجعي النظم الإلكترونية وقواعد البيانات الضخمة Big Data في15:-

المهارات الفنية والأخلاقيات Technical skills and ethics (TEQ): وهي القدرات اللازمة لأداء أنشطة التدقيق باستمرار مع الحفاظ على أعلى معايير النزاهة والاستقلالية والشك المهني؛

الذكاء Intelligence (IQ): وهو القدرة على اكتساب واستخدام المعرفة–التفكير والاستدلال لحل المشكلات في الوقت المناسب؛

الإبداع Creative (CQ): أي القدرة على استخدام المعرفة الموجودة في موقف جديد، لإجراء الاتصالات، واستكشاف النتائج المحتملة، وتوليد الأفكار الجديدة؛

الرقمية Digital (DQ): أي الوعي بتطبيق التقنيات الرقمية والقدرات والممارسات والاستراتيجيات الجديدة بكل أريحية وفعالية؛

العاطفة Emotional (EQ): وهي القدرة على تحديد مشاعر المدقق ومشاعر الآخرين وتسخيرها وتطبيقها على المهام وتنظيمها وإدارتها بما يخدم مهمة التدقيق؛

الرؤية Vision (VQ): القدرة على توقع الاتجاهات المستقبلية بدقة من خلال استقراء الحقائق الموجودة وملء الفجوات المعرفية من خلال التفكير بشكلٍ مبتكر للوقائع ومصداقية توقعاتها؛

الخبرة Experience (XQ): فهم توقعات العملاء وتلبية النتائج المرجوة وخلق القيمة.

2.2.4. أهمية التدقيق الرقمي وحدوده وعقباته

إن أتمتة التدقيق استنادًا إلى معايير التدقيق يقلل العمل اليدوي المكثف ويوفر قدرًا ملحوظًا من الوقت ويضمن عدداً أقل من الأخطاء ، هذا "التعاون بين الإنسان والآلة" هو الشكل المستقبلي للتدقيق، فالتحول الرقمي في التدقيق مجالٌ واعد، إلا أن هناك عقبات يمكن أن تبطئ هذه العملية، أولاً، تخدم شركات التدقيق عملاء متعددين في مختلف القطاعات والاقتصاديات، والأرجح أن كل عميل لديه بيانات بتنسيقاتٍ مختلفة، ما يجعل عدم تجانس بيانات العملاء متباين بشكلٍ واضحٍ مما يصعب من استخدام أدوات التحليل الرقمي لنفس الصناعات/القطاعات، لذلك هناك حاجةٌ ماسة لتوحيد بيانات العملاء، ثانياً، هناك العديد من المدققين لم يكتسبوا بعد المهارات اللازمة وليسوا مستعدين للتحول الرقمي الكامل، يشعر الكثيرون بالقلق إزاء مشكلة "الصندوق الأسود 'black box" لبعض التقنيات التكنولوجية التي يمكنها وضع تنبؤات للأحداث المستقبلية بناءً على البيانات التاريخية واستخراج الأنماط من البيانات الضخمة، إن صعوبة شرح كيفية وصول الخوارزمية إلى قرارها الحكمي يجعل الاستنتاج الذي تم إنشاؤه آليًا أقل ملاءمة لقبوله كحكم مهني حول وضعية الشركة الفعلية وهذا يتضح من لوائح التدقيق المعمول بها اليوم التي تبقى تؤكد على أهمية الحكم المهني.

3.2.4. مراحل تدقيق ومراجعة الغش المالي الإلكتروني في الشركات

تمر عملية مراجعة الغش المالي الإلكتروني وفقاً لرؤية المدقق المهنية عادةً بالمراحل التالية16:–

1. التأكد من وقوع الجريمة المالية الإلكترونية من داخل أو خارج الشركة؛
2. تحديد نمط وطبيعة الجريمة المالية الإلكترونية المرتكبة والمستوى الإداري المرتبطة به؛
3. التعرف على التقنيات التكنولوجية والإلكترونية المستخدمة في ارتكابها؛
4. محاولة تحديد الجناة المحتملين بتعقب تدفق الأموال أو المعلومات من مصدرها إلى مكان استلامها؛

5. معرفة الخطوات اللازمة لتجريم المشتبه بهم من الناحية القانونية، ومحاولة معرفة الأسباب والدوافع المحتملة لارتكاب الجريمة المالية الإلكترونية؛

6. وضع مخططات وقواعد معلومات عن حالات الغش المالي الإلكتروني وأنواعه خاص بالشركة و القطاع؛

7. الاستدلال على الشهود في حالة وجودهم؛

8. توضيح طبيعة الأدلة الجنائية الرقمية ومصادرها وكيفية استخدامها كدليل في المحكمة؛

9. التقرير: يعد استخدام مهارات الاتصال أمرٌ مطلوبٌ لجعل الحجج المدعومة ذات منطقية في الإثبات، يصرح David Dunckley الرئيس التنفيذي لشركة التدقيق The CEO of auditing firm Grant Thornton في فبراير 2019 م بقوله: "إن الإجراءات الحالية للتدقيق معيبة هيكليًا للكشف عن الاحتيال لأنها تتجه فقط نحو الوصول إلى استنتاج ما إذا كانت حسابات الشركات معقولة أم لا، نحن لا نبحث عن الاحتيال ولا ننظر للمستقبل لأننا ننظر إلى الماضي"17، وتم التأكيد في هذا السياق على نوعين فقط من أنواع الاحتيال وهما الاحتيال في التقارير المالية واختلاس الأصول (التحايل الداخلي والمشترك)، و ربما قد يظهر تبريرٌ آخر لتبني هذه الفرضية (نقل المسؤولية) وهو محاولة إسقاط تكاليف التقاضي عن شركات التدقيق ونقلها إلى كاهل الشركات والاقتصاديات (المجتمع)18.

في جانب المعايير، صدرت عدة معايير من قبل مجلس معايير التدقيق والتأكيد الدولية (IAASB) تتطرق إلى الغش والتحايل في قطاع الأعمال، كالمعيار الدولي ISA200 الأهداف العامة للتدقيق؛ المعيار الدولي 315 فهم الكيان وبيئته وتقييم مخاطر التحريف الجوهري؛ المعيار الدولي ISA 240 مسؤولية المدقق المتعلقة بالاحتيال في تدقيق البيانات المالية، كما أصدر مجلس معايير التدقيق التابع لـ AICPA معيار التدقيق (SAS 99) سنة 2002 م بشأن الاحتيال وتدقيق البيانات المالية، بينما أصدر مجلس الرقابة على المحاسبة العامة للشركة (PCAOB) سنة 2002 م بياناً بشأن الاحتيال وتدقيق البيانات المالية، على سبيل المثال، يطلب المعيار الدولي ISA 240 من المدققين قيام بـ19: (أ) تحديد وتقييم مخاطر التحريف الجوهري في البيانات المالية بسبب الاحتيال، فقط إذا كان له تأثيرٌ جوهريٌ على البيانات المالية؛ (ب) الحصول على أدلة تدقيق كافية ومناسبة لخطر التحريف الجوهري بسبب الغش بتصميم وتنفيذ برنامج مناسب؛ (ج) الاستجابة بشكلٍ مناسبٍ للاحتيال المشتبه به؛ كما يتطلب المعيار أيضًا من المدققين تصنيف الاستجابة لمخاطر الاحتيال إلى ثلاث فئات: (1) مخاطر الدوافع أو الضغوط لارتكاب التحايل، (2) خطر الفرص ارتكاب الاحتيال، (3) وخطر تبرير الاحتيال، وفيما يتعلق بالإبلاغ عن الاحتيال المشتبه به يتطلب المعيار من المراجعين الخارجيين إبلاغ الإدارة والمكلفين بالحوكمة في الوقت المناسب بأية أمور تتعلق بالاحتيال، وفي حالة اشتباه بتواطؤ الإدارة أو المكلفين بالحوكمة في الاحتيال يطلب المعيار من المدققين تحديد ما إذا كانت هناك مسؤولية للإبلاغ عن الحدث أو الشك لطرفٍ خارج الكيان كالهيئات الرقابية للبنوك والهيئات العمومية إذا أمكن20.

حالياً؛ تتجه المواقف الدولية إلى توسيع دائرة مسؤوليات المدققين لاكتشاف الغش داخل الاقتصاديات، كان أحد العوامل الأساسية هو الاعتراف بأن هؤلاء المتخصصين هم مكوناتٌ أساسيةٌ لكل اقتصاد متطور ونزاهة في المنظمات، ولا يمكن تحقيق التنمية الاقتصادية بدون خدماتهم، مع هذه الأهمية تأتي أيضًا مسؤولية مكافحة الجرائم المالية الإلكترونية، فالمدققون مدعوون للعمل إلى حدٍ معينٍ كحراس الاقتصاد والمجتمع المستقلين للمراقبة ووكلاء إنفاذ القانون في الدولة، بالتوازي مع هذا الواجب العام يتعين عليهم أن يكونوا مخلصين لعملائهم الذين يدفعون رسومهم باكتشاف التلاعبات، عامل إضافي ساهم في إبراز واجبات المدققين بصفتهم وكلاء لمكافحة الغش الفضائح الواسعة النطاق في العقدين الماضيين بما في ذلك Enron و Worldcom و SwissLeaks و LuxLeaks و LIBOR وغيرهم، أدت هذه الأحداث إلى زيادة القبول الدولي بأن المدققين لديهم إمكانية الوصول إلى التفاصيل الدقيقة للأنشطة والمعاملات التجارية ويقع عليهم واجبٌ قانوني للكشف عن الأنشطة المشبوهة والإبلاغ عنها إلى السلطات المختصة ومساعدتهم في تعقب الأصول الإجرامية واستعادتها، إلى جانب هذه الحقيقة، فإن تطور التقنيات التكنولوجية على الصعيدين الوطني والدولي يعني أنه أصبح من المعقول والإمكان توقع قيام المراجعين بفحص جميع المعاملات واكتشاف الاحتيال بمختلف أنواعه وطرقه في مراحله المبكرة21.

بالرغم من افتراض أن المدققين هم أوصياء المجتمع ومن المتوقع بطريقةٍ ما أن يكونوا في خط الدفاع الأول ضد الجرائم المالية، فإن معدل نجاح الكشف عن الجرائم المالية من قبل هؤلاء في العديد من الاقتصاديات المتقدمة منخفضة للغاية، يشير تقرير جمعية مدققي الاحتيال المعتمدين the Association of ACFE Certified Fraud Examiners لسنة 2020 م أن التدقيق الخارجي يساهم فقط بـ 04 % في كشف حالات الغش المالي، بينما تتحدد عوامل ضعف نظام الرقابة الداخلية لكشف الغش المالي الإلكتروني في: عدم وجود ضوابط داخلية بنسبة 32 %؛ عدم وجود المراجعة الإدارية بـ 18 %؛ تجاوز الضوابط الداخلية الموجودة 18 %؛ فلسفة رقابية ضعيفة في القمة بـ 10 %؛ عدم وجود آلية للإبلاغ أقل من 1 %؛ عدم وجود عمليات تدقيق مستقلة 5 %؛ عدم وجود موظفين أكفاء في الأدوار الرقابية 6 %؛ و عوامل أخرى بـ 6 22%، بعبارةٍ أخرى، إن محاولة توسيع دائرة الواجبات القانونية للمدققين لا تكفي لتحقيق التمكين الفعال في استراتيجيات وسياسات مكافحة الاحتيال المالي أولاً، ثم الإلكتروني ثانياً، من جهةٍ أخرى، إن تخوف الهيئات المهنية الدولية من زيادة المتطلبات والإرشادات المهنية ناتج عن إتساع فجوة التوقعات و درجة التباين في المعايير عبر الحدود الدولية نتيجة هذه التوسعة المتعلقة باكتشاف الاحتيال، وفي سياق مكافحة الجرائم المالية الإلكترونية، تم تبني المبادرة الوطنية لمكافحة الاحتيال The National Anti– Fraud Audit Initiative (NFI) بقرارٍ من رئيس وزراء المملكة المتحدة 1998 م لكشف الاحتيال في القطاع العام باستخدام التكنولوجيا وتقنيات البيانات المتقدمة لمعالجة مجموعة واسعة من مخاطر الاحتيال التي يواجهها القطاع العام23.

وبما أن مكافحة الغش الإلكتروني هي من مسؤولية الشركات، يشير تقرير PWC لسنة 2022 م أن 02 من أصل 03 شركات تعمل على تحسين إجراءات الرقابة الداخلية وأخلاقيات العمل وقواعد الحوكمة وتدريب

الموظفين والعملاء على الخطوط الساخنة (الإبلاغ بالجرائم المالية) بمعدل زيادة 06 % في 24 شهراً الأخيرة، لكن يبقى التحايل الداخلي مخفي عن الأعين لفترة طويلة فإنه يمكن محاربة التحايل الخارجي المزدهر سنوياً من خلال ثلاثة عوامل أساسية وهي:-

1. فهم العلاقات والنهايات لدورة حياة المنتج-المستهلك Understand the end – to – and life cycle of Customer-facing products: يجب تحديد الفرص التي يمكن من خلالها للمتحايلين استغلال العلاقة بين المنتَج والسبب المالي، هل هو قانوني أم متعلق بالسمعة؟، والكيفية التي قد يقع بها التحايل الإلكتروني؟، وكيفية إثبات وقوعه؟، وكيفية التقرير عنه؟، ولمن يقدم التقرير؟.

2. تحقيق التوازن بين الخبرة والسيطرة على التحايل Strike the proper balance between user experience and fraud controls: يجب حماية سلسلة الإنتاج – العملاء من خلال تحقيق التوازن بين الخبرة وسياسات وإجراءات كشف الاحتيال ودعم الأهداف الاستراتيجية والإجرائية والتكنولوجية.

3. إعداد قواعد البيانات Orchestrate data: يجب تبني مؤشرات كشف الشذوذ وبرامج الحماية داخل قواعد البيانات الخاصة بسلاسل القيمة الإلكترونية الخاصة بالشركة.

يشير تقرير ACFE 2020 م إلى أن ضوابط مكافحة الاحتيال الإلكتروني في الشركات شملت تعزيز مدونة قواعد السلوك بنسبة 81 % من الشركات الضحية، وإدارة التدقيق الداخلي بنسبة 74 %، وشهادة إعداد البيانات المالية بنسبة 73 %، كما تساهم أربعة ضوابط لمكافحة الاحتيال على وجه الخصوص في تخفيض 50 % من خسائر الاحتيال ومدته وهي: مدونة قواعد السلوك؛ قسم التدقيق الداخلي؛ تصديق الإدارة على البيانات المالية؛ مراجعة الإدارة المنتظمة للضوابط أو العمليات أو الحسابات أو المعاملات النهائية؛ بينما وجد أن الشركات الصغيرة تطبق ضوابط مكافحة الاحتيال بمعدل أقل بكثيرٍ من نظيراتها الكبيرة، كانت أكثر ضوابط مكافحة الاحتيال شيوعًا وهي التدقيق الخارجي للبيانات المالية موجودة فقط في 56 % من الشركات الصغيرة، و48 % فقط من هذه الشركات لديها قواعد سلوك مقارنةً بـ 92 % و 91 % على التوالي في المؤسسات التي لها أكثر من 100 موظف.

يبقى عدم وضوح مسؤوليات المدققين الخارجيين فيما يتعلق بالغش المالي الإلكتروني يؤدي إلى زيادة خسائر الشركات و تكاليف التقاضي، لا يزال المدققين بحاجة لإرشادات حول كيفية الاستجابة لمخاطر الغش الإلكتروني خاصةً عندما لا تتخذ الإدارة العليا الإجراءات الرقابية الصحيحة في هذا الجانب، حالياً تتوجه التوقعات نحو إشارات التحذير في وقتٍ مبكرٍ بما فيه الكفاية لأصحاب المصلحة لاتخاذ الإجراءات التصحيحية للتخفيف من حدة مخاطر الاحتيال، بالإضافة إلى ذلك، ليست مسؤولية المدققين وحدهم لاكتشاف الغش المالي ولكنها تتطلب جهودًا تعاونية من الحكومة و وكالات إنفاذ القانون والسلطة القضائية والإعلام، من الواضح أن التدقيق عالي الجودة يمثل رادع للاحتيال، وبالتالي ينبغي على المدققين تحسين مهاراتهم في اكتشاف الاحتيال الإلكتروني أو على الأقل الإبلاغ عن العلامات والمؤشرات المبكرة عنه24.

5.1.4. تحليل العلاقة الإحصائية ما بين التدقيق الخارجي والغش والتحايل المالي في الشركات

1.5.1.4. منهجية الدراسة: الإشكالية والفرضية البحثية، صياغة النموذج الإحصائي، العينة

1.1.5.1.4. التذكير بالإشكالية والفرضية البحثية الرئيسية

تنص إشكالية الدراسة على:-

ما مدى فعالية التدقيق الخارجي في مكافحة الغش والتحايل المالي الإلكتروني في سياق البحث عن شفافية بيئة التقارير المالية واستدامتها؟؛ ومنه يكون الشكل الإحصائي كالتالي:

H01: هل توجد أي علاقة إحصائية معنوية يمكن تمثيلها ما بين صلابة معايير التدقيق والتقارير المالية الدولية والفساد المالي في الشركات على الساحة العالمية خلال الفترة 2007 م – 2021 م؟؛

في حين تنص الفرضية الرئيسية الدراسة على:-

يعتبر التدقيق الخارجي أحد الأدوات الرقابية الهامة الكفيلة بتحجيم مخاطر الغش والتحايل المالي الإلكتروني بمختلف الاقتصاديات مما يساهم بدورٍ محوريٍ و هامٍ في تحقيق شفافية بيئة التقارير المالية واستدامتها؟؛ ويعطى شكلها الإحصائي كالآتي:-

H11: هناك علاقة ذات دلالة إحصائية معنوية هامة ما بين ما بين صلابة معايير التدقيق والتقارير المالية الدولية و الفساد المالي في الشركات على الساحة العالمية خلال الفترة 2007 م – 2021 م.

2.1 شكل النموذج الإحصائي Estimating Model

يمكن كتابة شكل النموذج الإحصائي وفق نموذج الإنحدار الخطي البسيط لـ Robert F. Engle And C.W.J. Granger كما يلي:-

$$\hat{y}t = B0 + B1\ Xt + et\ ,\qquad et = Yt - \hat{y}t$$

3.1 العينة، البيانات ومصادرها Sample and Data Source

لدراسة العلاقة تم إختيار مؤشرين دوليين هما: مؤشر صلابة معايير التدقيق والتقارير المالية Strength of auditing and reporting standards: الذي يعكس مدى تطبيق معايير التدقيق الدولية على الساحة العالمية خلال الفترة 2007 م – 2021 م، ومؤشر الفساد المالي في الشركات Corporate ethics and corruption: يعكس هذا المؤشر مدى انتشار الفساد المالي والأخلاقي في الشركات على المستوى الدولي لنفس الفترة، ليصل حجم البيانات 30 معطية للفترة المدروسة (15 سنة)، اعتماداً على المصادر الدولية لاسيما تقارير التنافسية العالمية الصادرة عن مؤسسة World Economic Forum التي تعتبر قواعد بياناتها المصدر الرئيس لمعطيات الدراسة: https://reports.weforum.org/global-competitiveness-index-2017-2018/downloads/.

2.1.5.1.4.. تحديد النموذج الإحصائي وإختبار معنويته الإحصائية الكلية والجزئية

لإستخلاص النموذج تم إستخدام البرنامج الإحصائي SPSS 24 والذي تعطى نتائجه كالآتي:

الجدول (01): تقدير معاملات النموذج الإحصائي

Coefficientsa						
Modèle		Coefficients non standardisés		Coefficients standardisés	T	Sig.
		B	Erreur standard	Bêta		
1	(Constante)	10,288	1,084		9,487	0,000
	STROIND	-1,480	0,252	-0,852	-5,874	0,000
a. Variable dépendante : COORIND						

المصدر: بناءاً على مخرجات SPSS 24.

ومنه تُعطى معادلة خط الإنحدار للنموذج الإحصائي بالشكل الآتي:-

$$COORINDt = 10.288 - 1.48\ STROINDt + \varepsilon i$$

تُفَسر العلاقات الدالية بأنه في الحالة العامة طويلة الأجل يؤثر متغير معايير التدقيق والتقارير المالية سلباً على مؤشر الفساد المالي في الشركات بمقدار 1.48، بمعنى آخر، كلما زاد مؤشر معايير التدقيق والتقارير المالية بوحدة واحدة أو 1 % كلما انخفض مؤشر الفساد المالي في الشركات بوحدة ونصف أو 1.48 %.

2.2 إختبارات جودة التوفيق والمعنوية الجزئية والكلية للنموذج

يتم إختبار معنوية معالم النموذج المقدر بإستخدام الفرضيات التالية:-

H0 : B0=0 H1 : B0≠ 0	H0 : BCOORIND, STROIND=0 H1 : B BCOORIND, STROIND ≠0

من الجدول السابق نلاحظ أن معنوية معاملات المتغيرات هي أقل تماماً من 5 % (0.000؛ 0.000 < 5 %)، ومنه نرفض الفرضية الصفرية H0 ونقبل الفرض البديل H1 القائل بمعنوية جميع معاملات النموذج الإحصائي ودلالة قيمتها المعنوية المقدرة عند مستوى معنوية 5 %، بينما يتم إختبار المعنوية الإحصائية الكلية وفق الفرضية الإختبارية الصفرية بالشكل التالي:-

H0 : B0= B BCOORIND, STROIND =0
H1 : B0 ≠ B BCOORIND STROIND ≠ 0

كانت النتائج كما يلي:

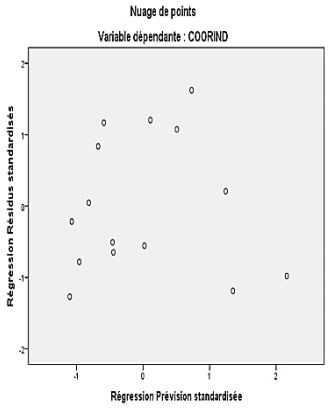
الجدول (02): إختبار المعنوية الكلية جودة التوفيق للنموذج الإحصائي

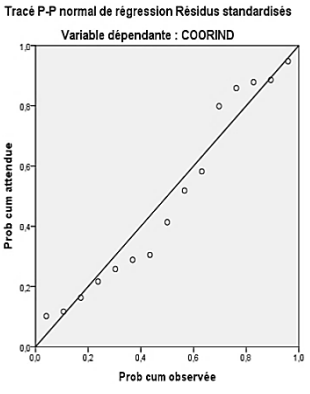
ANOVAa							Récapitulatif des modèlesb				
Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.	Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	Régression	0,662	1	0,662	34,499	,000b	1	,852a	0,726	0,705	0,138562887
	Résidu	0,250	13	0,019			a. Prédicteurs : (Constante), STROIND				
	Total	0,912	14				b. Variable dépendante : COORIND				
a. Variable dépendante : COORIND											
b. Prédicteurs : (Constante), STROIND											

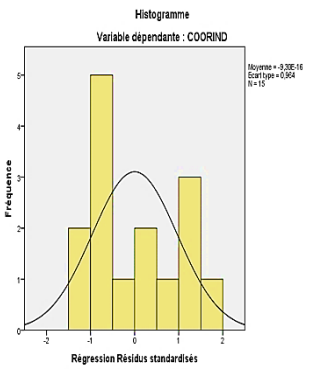
المصدر: بناءاً على مخرجات SPSS 24.

وكما يدل جدول ANOVA فإن النموذج معنوي عند 5 % بما أن قيمة (0.000)=Sig < 5 %، و F = [34.499] > FTable مما يؤكد المعنوية الكلية للنموذج المقدر، وبالتالي نرفض H0 ونقبل الفرض البديل H1 القائل بأن الإنحدار معنوي ولا يساوي صفر، وبالتالي صحة النموذج في تفسير العلاقة المدروسة بين تطور مؤشر الفساد المالي في الشركات ومؤشر صلابة معايير التدقيق والتقارير المالية، وفي قياس جودة التوفيق تبلغ قيمة الإرتباط المربع R-deux = 72,6 % مما يعني أنه يمكن تفسير التغيرات الفترية للفساد المالي في الشركات على الساحة الدولية من خلال التغيرات الفترية في معايير التدقيق والتقارير المالية بالنسبة المذكورة، وعليه يمكن إستنتاج أنه كلما كانت هناك إختلافات كبيرة في تبني معايير التدقيق والتقارير المالية الدولية كلما كانت هناك إختلافات جوهرية في مؤشرات الفساد المالي في الشركات، بينما توضح الأشكال البيانية التالية إستقرارية البواقي للنموذج الإحصائي كما يلي:-

الشكل (07): إختبارات التوزيع الطبيعي وإنتشارية البواقي للنموذج المقدر







المصدر: بناءاً على مخرجات SPSS 24.

يوضح رسم المدرج التكراري Histogramme أن بيانات النموذج المقدرة تتبع التوزيع الطبيعي، في حين يوضح الرسم البياني p-p plot أن البيانات تتجمع حول خط الإنحدار المقدر في إشارةٍ إلى أن البواقي Residuals تتبع هي الأخرى التوزيع الطبيعي، بينما يؤكد شكل سحابة إنتشار البواقي Residuals عدم وجود نمطٍ معينٍ لتشتت النقاط مما يؤكد على تحقق شرط الخطية وصدق النموذج في نمذجة العلاقة بين الفساد المالي في الشركات وصلابة تطبيق معايير التدقيق والتقارير المالية وقدرتها على التنبؤ به مستقبلاً.

6.1.4. الخطوات المستقبلية لمكافحة الغش والتحايل المالي الإلكتروني في قطاع الأعمال

تتضمن الخطوات المستقبلية لكشف الغش المالي الإلكتروني ما يلي25:-

1.6.1.4.. إصدار معايير خاصة بتدقيق البيانات الضخمة

لتحسين جودة التدقيق الإلكتروني من الأهمية بمكان تطوير معايير تدقيق وتقنيات تحليلية للبيانات الضخمة من قبل واضعي المعايير، يجب أن تشجع المعايير الشركات على إدارة البيانات الداخلية بطرقٍ فعالةٍ ومتسقة والتحقق من صحة البيانات الخارجية بشكلٍ مستمر للحصول على أدلة تأكيد كافية، كما يجب معايرة التقنيات التكنولوجية الجديدة والذكاء الاصطناعي للأغراض التحليلية وإجراءات التدقيق التقليدية،.

2.6.1.4.توعية مكاتب التدقيق

تواجه شركات التدقيق حاليًا كتلة من المهام تدفعهم نحو تبني التكنولوجيا الرقمية والتطبيقات الذكية، وبالرغم من إدراكهم المعلن لأهميتها إلا أن 70 % من شركات التدقيق لا تزال في المراحل الأولية لتبني هذه التطبيقات في إجراءات التدقيق الخاصة بهم، يجب على هذه الشركات وضع خطط إستراتيجية وبذل جهود أكبر لتنفيذ هذه المنهجيات في مؤسساتهم بتوفير التدريب والحوافز المناسبة،

3.6.1.4.. الاعتماد على مصادر البيانات الخارجية

تلعب البيانات الخارجية دورًا مهمًا في ممارسات التدقيق بتوفير أدلة تدقيق مجانية تساعد المدققين الداخليين والخارجيين على تلبية متطلبات التحقيق الخاصة بهم، في العصر الحالي للبيانات الضخمة يمكن للمدققين جمع بيانات خارجية من مصادر مختلفة مثل وسائل التواصل الاجتماعي والإنترنت، تساعد تقنيات تحليل البيانات المتطورة المدققين بمعالجة البيانات بطرقٍ فعالةٍ وكفؤة بشكلٍ متزايدٍ، وبالتالي فإن المدققين الذين لديهم بيانات خارجية تم تحليلها جيدًا لديهم إمكانية الوصول إلى أدلة تدقيق أكثر ملاءمة ويمكنهم تقليل احتمالية الأخطاء الجوهرية وأخطاء التدقيق واكتشاف مجالات الغش الأكثر توقعاً مقارنةً بغيرهم.

5. خاتمة:

تتجه الأوساط المهنية الحالية إلى قبول مسؤولية المدققين في اكتشاف الغش والاحتيال لاسيما عند عدم الإلتزام بالمعايير المهنية والأخلاقية كالاستقلالية والشك المهني أثناء أداء الواجبات، بينما يتجه القانون والقضاء إلى جعل هذه المسؤوليات أكثر قسوة فيما يتعلق بمسؤولية المدققين للكشف عن الاحتيال في

الشركات، في الواقع، إن التبني المتزايد للتكنولوجيا الرقمية تجعل الأطراف الثالثة التي قد يكون المدققون مسؤولين أمامها مختلفة للغاية، ومع ذلك، فإن الضوابط الداخلية القوية التي تستخدم التكنولوجيا للكشف عن الاحتيال تجعل المدققين يكتشفون بسهولةٍ أي أخطاء في التقارير المالية، توصي الهيئات المهنية المدققين بضرورة إجراء تقييم فعّال لمخاطر الاحتيال مع مراعاة العوامل التي تمكّن من ارتكابه التي تشمل الافتقار للنزاهة داخل الشركات، ودوافع مرتكبيه، والفرص المتاحة مع القدرة على استغلالها، وبالرغم من أن معايير التدقيق الدولية تطلب من المدققين الخارجيين النظر في معظم هذه العوامل إلا أن المدققين بالكاد يأخذون في الاعتبار دوافع الاحتيال أو نزاهة الإدارة في تقييماتهم لمخاطر الاحتيال، بالمقابل، يجب تطوير لغة معايير التدقيق لتعكس من جهة الآثار المتوقعة للتكنولوجيا الرقمية على مهنة التدقيق ثم التقنيات المتبناة لتقييم مخاطر الاحتيال الإلكتروني وكيفية الاستجابة له، من جانبٍ آخر، يشكل عدم الإلمام بأنظمة الحوسبة السحابية والبيانات الضخمة وأمن المعلومات والتشفير والمعارف غير المحاسبية الأخرى من قبل المدققين هاجس آخر، لذا يتطلب الأمر

مما سبق يمكن تقرير جملة التوصيات التي تتناول الجوانب التالية:-

- على المدققين الاطلاع على المعايير واللوائح والقوانين ذات الصلة بالجرائم الإلكترونية والفهم المعقول للمهارات التكنولوجية الأساسية و مخططات الاحتيال ومصادر البيانات الإلكترونية للشركات ليكونوا قادرين على تقدير التداعيات المختلفة للجرائم المالية الإلكترونية على تقاريرهم المهنية وقطاع الأعمال؛

- على منظمي مهنة التدقيق تقديم إرشادات للمراجعين حول كيفيات تقييم مخاطر الغش والاستجابة لها والأفعال غير القانونية التي يمكن أن يكون لها تأثيرٌ جوهريٌ على البيانات المالية، وهذا يحتاج من المدققين فهم طبيعة الجرائم الإلكترونية، وفئاتها، وكيف ارتكاب كلٍ منها، من المرجح أن يساعدهم هذا في تحديد الفرص المحتملة و فهم نطاق مسؤوليتهم؛

- ضرورة التكوين والتعليم المحاسبي التكنولوجي المستمر لا غنى عنه مع تطوير برمجيات و نماذج احتمالية لتوفير حلول سهلة الاستخدام للمهنيين والشركات؛

- وجود فجوة توقع في مجتمع الأعمال بين ضرورة تحمل المدققين لمسؤوليتهم في اكتشاف الغش المالي والمتطلبات القانونية الحالية، يمكن تحجيمها بتثقيف المستخدمين حول الدور والواجبات الفعلية للمدققين؛

6. قائمة المراجع:

[1] - World Economic Forum, **Nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat. What can they do about it?**, site: https://www.weforum.org/agenda /2022/07/fraud-cybercrime-financial-business/, Date : Jul 26, 2022, Or also, the site: https://www.Weforum .org/agenda/2018/01/we-need-to-talk-about-financial-crime, date : jan 12, 2018, date: 29/08/2022, p 01.

2 - Nida Tariq (2018), Impact of Cyberattacks on Financial Institutions, Journal of Internet Banking and Commerce, Vol 23, n° 02, p 03.

3 - Les Nunn, Brian L. McGuire, Carrie Whitcomb, Eric Jost (2006), Forensic Accountants: Financial Investigators, Journal of Business & Economics Research, Vol 4, N ° 2, p 06.
4 - Manoj Kumar Saxena, Nitika Sharma (2021), A Review on Cyber Crime: Some Educational Suggestions to Overcome, Horizons of Holistic Education, Vol 8, n° 02, p 65.
5 - Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer, Mulatu Fekadu Zerihun (2021), The Integration of Forensic Accounting and the Management Control System as Tools for Combating Cyberfraud, Academy of Accounting and Financial Studies Journal, Vol 25, n° 2, p 01-14.
6- Howard Silverstone, Stephen Pedneault, Michael Sheetz, Frank Rudewicz (2012), Forensic Accounting and Fraud Investigation, 3rd Edition, CPE Edition, p 90.
7 - Cameron S. D. Brown (2015), Investigating and Prosecuting Cyber Crime :Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology, Vol 09, n° 01, p 57.
8 - Amit Wadhwa, Neerja Arora (2017), A Review on Cyber Crime: Major Threats and Solutions, International Journal of Advanced Research in Computer Science, Vol 08, n° 05, p 2217.
9 - Luminița IONESCU (2017), Errors and fraud in accounting : the role of external audit in Fighting Corruption, Annals of Spiru Haret University, n° 04, p 04.
10 - Jack Nicholls, Aditya Kuppa, Nhien-an le-khac (2016), Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape, journal of IEEE ACCESS, Vol 04, p 05.
11 - Lorenzo Franceschi-Bicchierai, How a hacker allegedly stole millions by hijacking phone numbers, Online Available: https://www.vice.com/en/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping, date consultation : 26/08/2022, p 01.
12 - Convicted sim swapper gets 3 years in jail, Online Available: https://krebsonsecurity.com/2020/ 11/convicted-sim-swapper-gets-3-years-in-jail/, date: 20/11/2020, date consultation: 26/08/2022, p 01.
13 - Abdullah Mohammad Al-Zoubi, Fares Saoud Al-Qadi (2016), The Effect of Electronic Auditing in Reducing the Burden of Electronic Environment Complexity of Accounting Information System on the Auditor, Research Journal of Finance and Accounting, Vol 07, n° 14, p 178.
14 - Azizul Kholis, Wanda Prayogi (2020), Analysis Acceptance of E-Audit Application on the Financial Audit Board of the Republic of Indonesia in North Sumatera Regional Office, 4th Padang International Conference on Education, Economics, Business and Accounting (PICEEBA-2 2019), Advances in Economics, Business and Management Research, vol 124, p 31.
15 - Mike Suffield (2020), Auditors of the future – what are the skills needed in a digital age?, Journal of big data & digital audit, n° 01, p 25.
16 - Gojko Grubor, Nenad Ristić, Nataša Simeunović (2013), Integrated Forensic Accounting Investigative Process Model in Digital Environment, International Journal of Scientific and Research Publications, Vol 03, n° 12, p 03.
17 - Rasha Kassem and Umut Turksen (2021), Role of Public Auditors in Fraud Detection: A Critical Review, in Contemporary Studies in Economic and Financial Analysis, site: https://www.researchgate.net/ publication/337089583, p 15-17.
18 - Oyinlola, Ayobami Oluwagbemiga (2010), The role of Auditors in fraus Detection, Prevention and reporting in Nigeria, Library Philosophy and Practice (e-journal), site: https://digitalcommons.unl.edu/libphilprac/517, p 03.
19 - Gin Chong (2013), Detecting Fraud: What Are Auditors' Responsibilities?, Article in Journal of Corporate Accounting & Finance, Vol 24, n° 02, site: https://www.researchgate.net/publication/262947270, p 49.

20 - Dan Ioan TOPOR (2017), The Auditor's Responsibility for Finding Errors and Fraud from Financial Situations: Case Study, International Journal of Academic Research in Accounting, Finance and Management Sciences, Vol 07, n° 01, p 343-344.
21 - Rasha Kassem, Andrew W. Higson (2016), External Auditors and Corporate Corruption: Implications for External Audit Regulators, Current Issues in Auditing, American Accounting Association, Vol 10, n° 01, p 03-05.
22- Report to the nations (2020), Global study on occupational fraud and abuse, URL: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf, p 07.
23 - Hysen Ismajli, Edona Perjuci, Vlora Prenaj, Medina Braha (2019),The Importance of External Audit in Detecting Abnormalities and Fraud in the Financial Statements of Public Enterprises in Kosovo, Ekonomika, Vol 98, n° 01, p 26, site: https://doi.org/10.15388/Ekon.2019.1.8.
24 - Akwasi A. Boateng, Gilbert O. Boateng, Hannah Acquah (2014), A Literature Review of Fraud Risk Management in Micro Finance Institutions in Ghana, Research Journal of Finance and Accounting, Vol 05, n° 11, p 44-45.
25 - Miklos A. Vasarhelyi, Smart Audit: the digital transformation of audit, Journal of big data & digital audit, n° 01, p 28-29.