# اراء ووجهات نظر عالمية

## الاحتيال

**الجزء الأول: الاحتيال في مجال الكريبتو( مجال التشفير)**
**الجزء الثاني: المدققون الداخليون ومحققو الاحتيال: شراكة قيّمة**
**الجزء الثالث: المخلفات: الاحتيال في عصر ما بعد كوفيد**

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام الأستاذ ناجي فياض

The Institute of Internal Auditors

المعهد الدولي
للمدققين الداخليين

# Contents

# الجزء الأول

## الاحتيال في مجال الكريبتو (مجال التشفير)

## حول الخبراء

### دانا لورنس، CIA, CRMA, CFSA, CAMS, CRVPM

دانا لورانس هي مديرة الامتثال في Fideseo. وهي خبيرة معترف بها ورائدة في مجال الامتثال المعقد، وإدارة مخاطر المؤسسة (ERM)، والتدقيق الداخلي، وإنشاء برامج الحوكمة، وتوسيع نطاقها، ومعالجتها. تمتد مسيرة لورنس المهنية في مجال التكنولوجيا والخدمات المالية إلى الرهن العقاري، والخدمات المصرفية المجتمعية، والبنوك الكبرى في الولايات المتحدة والعالم، وشركاء البنوك المفتوحة، والتكنولوجيا المالية، والعملات المشفرة. شغلت مناصب قيادية عليا، وعملت مباشرة مع المنظمين المصرفيين والمدققين الداخليين / الخارجيين Lawrence . هو متحدث عام ومضيف حدث شهير، يتحدث في الأحداث المحلية والوطنية والعالمية مع ما يصل إلى 40000 مشارك. إنها متطوعة ملتزمة وقائدة فكرية، تخدم مجموعات مختلفة مثل معهد المدققين الداخليين.(IIA)

### لورد ميراندا، CAMS, CCE, CCFI, CEIC, CFE, CRC, FIS, MS

لورد ميراندا هو كبير مسؤولي الامتثال فيSendCrypto ، وهي شركة تكنولوجيا blockchain. وهي مسؤولة سابقة في وكالة المخابرات المركزية ومحللة في مكتب التحقيقات الفيدرالي تتمتع بخبرة تزيد عن 20 عامًا في الحكومة والشركات، وهي متخصصة في التحقيقات في الجرائم المالية وجمع المعلومات الاستخبارية وتحليلها على مستوى العالم. لديها خبرة ميدانية واسعة في استهداف مبيضي الأموال وممولي الإرهاب. منذ عام 2017، يعمل ميراندا في FinTechsكمحقق أول في مجال التشفير، وضابط امتثال أول، ومدير مخاطر، وبناء فرق الامتثال والتحقيق والتشفير والاستخبارات وبرامج التدريب. وهي أيضًا مؤلفة ومعلمة ومساهمة في العديد من الدورات التدريبية عبر الإنترنت كخبير في الموضوع. بالإضافة إلى ذلك، ميراندا عضو في المجلس الاستشاري لمؤسسة Toronto Compliance & AML (TCAE)ومقرها كندا .

# مقدمة

## العملات المشفرة والاحتيال في المحادثة العالمية

**سام بانكمان فرايد،** كان المؤسس لبورصة العملات المشفرة *FTX*، وتقدر ممتلكاته يومًا ما بقيمة تُقدر بـ 26.5 مليار دولار. وبوصفه زعيمًا لما كان في وقت ما ثالث أكبر بورصة في سوق العملات المشفرة، كان بانكمان-فريد و *FTX* من بين المحبوبين لدى مستثمرين عالميين مثل بلاكروك ولاعب كرة القدم الأمريكية توم برادي. ومع ذلك، فقد كل ثروته على الفور تقريبًا في واحدة من أكثر انهيارات الشركات دراماتيكية في التاريخ الحديث.

تم القبض على بانكمان فرايد في 13 ديسمبر 2022 في جزر الباهاما. وفقًا للتقارير المنشورة، يواجه تهماً مختلفة بما في ذلك الاحتيال الإلكتروني، والتآمر على الاحتيال، والاحتيال في الأوراق المالية، والتآمر على الاحتيال في الأوراق المالية، وغسيل الأموال.

في حين أن هناك اهتمامًا بشريًا بالمشهد الهائل لمثل هذا الانهيار المذهل، فقد أثار الحدث أيضًا أسئلة أكبر بشأن الأصول الرقمية. مع وجود أوجه تشابه مع فضائح مثل *Tornado Cash* و*Bitzlato* ، أدى انهيار *FTX* والتأثير اللاحق على الصناعة التي تمثلها إلى تشكيك الكثيرين في الجدوى طويلة الأجل لأصول التشفير - على الأقل في حالتها الحالية، وهو رئيس لجنة الأوراق المالية والبورصات الأمريكية أطلق غاري جينسلر على "الغرب المتوحش."

على الرغم من كونها مبنية على تقنية*blockchain* ، والتي تعد من بين أكثر الطرق أمانًا للحفاظ على أصول ومعلومات التشفير، إذا كان الرئيس المرئي للغاية لواحدة من أبرز بورصات العملات المشفرة في العالم يمكن أن يرتكب أعمال احتيال على نطاق واسع، فما هي نقاط الضعف الأخرى التي قد تكون موجودة للشركات التي تعمل في القطاعات الاخرى مع بعض القدرات؟ كيف تغير مشهد المخاطر مع الارتفاع السريع لأصول التشفير، وكيف تستجيب بعض المؤسسات ووظائف التدقيق الداخلي الخاصة بها بنجاح لهذه التغييرات؟

سيتناول الجزء الأول من هذه السلسلة المكونة من ثلاثة أجزاء حول الاحتيال هذه الأسئلة من خلال فحص مخططات الاحتيال الشائعة التي شوهدت في المراحل الأولى من عالم الأصول المشفرة. لمزيد من المعلومات حول هذا الموضوع، سيستضيف معهد المدققين الداخليين إعادة عرض لندوة الويب الأخيرة "وجهات نظر الاحتيال *Blockchain :و Crypto و KYC* "، جنبًا إلى جنب مع أسئلة وأجوبة مباشرة مع الخبراء المتخصصين المذكورين في هذا الموجز.

# عدم اليقين في مجال الكريبتو

## مستقبل مثير، لكنه محفوف بالمخاطر

### المؤسسات متنبهة في هذه الأوقات

على الرغم من أن آثارها واسعة ولا تقل عن كونها ثورية، إلا أن تقنية *blockchain* سهلة الفهم نسبيًا من الناحية المفاهيمية على أنها ليست أكثر من سجل مستمر ومتزايد باستمرار لمعاملات الأصول الرقمية التي يمكن مشاركتها وتخزينها في أي بنية شبكة تقريبًا. ما يميزه هو أنه يستخدم منهجيات التحقق التي تقوم بتشفير الكتلة باستمرار مع كل معاملة جديدة، مما يجعلها أكثر أمانًا.

قال لوردس ميراندا، كبير مسؤولي الامتثال في*SendCrypto* ، وهي شركة تكنولوجيا*blockchain* ، "إن التكنولوجيا نفسها معقدة للغاية وتستغرق سنوات من التدريب والتعليم لتحليلها، لكنني أعتقد أن *blockchain* نفسه بمثابة بيان مالي". "يحتوي *blockchain* على معلومات تتعلق بمن أرسل الأصول، ومكان إيداعها، وما إذا كان هناك أي عمليات سحب، والرصيد الناتج".

يمكن القول إن العملة المشفرة هي الأصول الأكثر شهرة التي تستخدم هذه التكنولوجيا، والتي تخلق نظامًا نقديًا لامركزيًا مفتوح المصدر (أو أنظمة) محصنًا من تأثير الكيانات، مثل البنوك المركزية - ولكن تشمل الأمثلة الأخرى لأصول التشفير القائمة على *blockchain* الرموز غير القابلة للاستبدال *(NFTs)* وتقنيات دفتر الأستاذ الموزع *(DLTs)* ورموز الألعاب وغيرها.

ومع ذلك، نظرًا لأن الصناعات تتعلم بسرعة، لمجرد أن الأصول المشفرة مبنية على تقنية آمنة يكاد يكون من المستحيل التلاعب بها بالطرق التقليدية لا يعني أن متبنيها محصنون من المخاطر. يوضح انهيار *FTX* هذا بأكثر من طريقة. على سبيل المثال، أوضح مدى الضرر الذي قد يلحقه الافتقار إلى الحوكمة السليمة للشركات والضوابط الداخلية، ليس فقط للمؤسسة، ولكن للمستثمرين في جميع أنحاء المشهد الصناعي بأكمله.

كانت هذه نقطة أدلى بها رئيس *IIA* ومديرها التنفيذي أنتوني بوغليس في خطاب حديث إلى الكونجرس الأمريكي دعاهم فيه إلى وضع متطلبات جديدة لتعزيز حوكمة الشركات في بورصات العملات المشفرة، وشركات تكنولوجيا*blockchain* ، وأسواق*NFT* ، ومنصات *Web3* العاملة في الولايات المتحدة.. قال بوغليس: "يدفع عدد لا يحصى من المستثمرين الآن ثمن إخفاقات" *FTX* ". من الواضح أننا لا نستطيع الاعتماد على عمليات تبادل العملات المشفرة غير المنظمة للقيام بالشيء الصحيح بمفردها - نحتاج إلى فرض معايير أقوى لحوكمة الشركات وضمان المساءلة عندما لا تحمي هذه التبادلات عملائها. عندما يفشل الفاعلون السيئون في الشركات، لا ينبغي أن يكون المستثمرون هم من يمسكون بالحقيبة."

شدد *Pugliese* على انهيار*FTX* ، وكان من الممكن التخفيف من عواقبه السوقية من خلال إجراءات وظيفة التدقيق الداخلي السليمة. وقال: "إن انهيار *FTX* هو أحدث تذكير بأن المؤسسات التي ليس لديها وظيفة تدقيق داخلي قوية، في أفضل الأحوال، تلعب بالنار، وفي أسوأ الأحوال، تضع نفسها وأصحاب المصلحة في حالة انهيار كارثي - ويمكن منعه تمامًا."-

هذه المخاوف من *Pugliese* وآخرين لم تلق آذانًا صاغية. في 3 يناير 2023، أصدر الاحتياطي الفيدرالي، وشركة تأمين الودائع الفيدرالية *(FDIC)* ومكتب المراقب المالي للعملة *(OCC)* أول بيان مشترك على الإطلاق بشأن العملة المشفرة. في ذلك، سلطوا الضوء على مجموعة متنوعة من المخاطر التي يمكن أن تلعبها المؤسسات المصرفية العاملة في العملة المشفرة في شكل ما، بما في ذلك:

- مخاطر الاحتيال والاحتيال بين المشاركين في قطاع الأصول المشفرة.
- حالات عدم اليقين القانونية المتعلقة بممارسات الحفظ والاسترداد وحقوق الملكية.
- الإقرارات والإفصاحات غير الدقيقة أو المضللة من قبل شركات الأصول المشفرة.
- تقلبات كبيرة في أسواق الأصول المشفرة، والتي تشمل آثارها التأثيرات المحتملة على تدفقات الودائع المرتبطة بشركات الأصول المشفرة.
- مخاطر العدوى داخل قطاع الأصول المشفرة الناتجة عن الترابط بين بعض المشاركين في الأصول المشفرة، بما في ذلك من خلال عمليات الإقراض غير الشفافة والاستثمار والتمويل والخدمات والترتيبات التشغيلية.

- إدارة المخاطر وممارسات الحوكمة في قطاع الأصول المشفرة التي تظهر نقصًا في النضج والقوة.
- المخاطر المتزايدة المرتبطة بالشبكات المفتوحة و / أو العامة و / أو اللامركزية، أو الأنظمة المماثلة.

في حين أن كل هذه المخاطر جديرة بالمناقشة (وفي كثير من الحالات تنطبق على المؤسسات التي تتجاوز البنوك التي تشتغل بالعملات المشفرة)، فإن هذا الموجز سيحد من التركيز على أعمال الاحتيال التي يرتكبها المشاركون في العملات المشفرة والأشكال البارزة التي يتخذونها في البيئة الحالية.

# بيئة مؤاتية للاحتيال

## بيئة لا متناهية للمخاطر

### أداة جديدة في صندوق من لا يُحسن الاستخدام

في حين أن الأصول المشفرة لديها مجموعة من الخصائص المفيدة مثل الشفافية والتشفير المتقدم بشكل ملحوظ ضد التلاعب، فإن هذه الخصائص نفسها جعلت هذه الأصول) وتكنولوجيا *blockchain* وراءها أداة قوية لأولئك الذين يتطلعون لارتكاب الاحتيال.

في الواقع، هذا النداء للفاعلين السيئين هو الذي لفت انتباه المنظمين وإنفاذ القانون. قال ميراندا، الذي بحث في الجرائم المالية لصالح وكالة المخابرات المركزية ومكتب التحقيقات الفيدرالي منذ ما يقرب من 30 عامًا: "السبب الوحيد وراء اهتمام المنتظمين بأصول العملات المشفرة هو أن الجهات الفاعلة السيئة يستخدمونها لتمويل العمليات وغسل الأموال". "من الصعب جدًا التلاعب بـ*Blockchain* ، ولكن يمكن استخدامها بطرق تعزز النشاط الشائن".

إحدى الطرق، على سبيل المثال، هي استخدام هويات تعريف مزيفة داخل *blockchain.* قال ميراندا: "هذا ضخم في الكريبتوسفير". "سيستخدم الفاعلون السيئون هويات شرعية وصالحة تم شراؤها من السوق السوداء لاجتياز عملية إعداد *KYC* [اعرف عميلك] عند فتح المحافظ. هذه الهويات ليس لها خلفية إجرامية وليست مدرجة في أي قائمة سوداء - فهي نظيفة تمامًا. بعد ذلك، تحت هذا الاسم النظيف، يمكنهم نقل الأموال دون أن يتم اكتشافهم إلى حد كبير حتى يتمكن المحققون من رؤية اتجاهات الاحتيال المنبثقة بأعينهم."

قدمت صناعة الأصول المشفرة أيضًا مجموعة متنوعة من الأدوات التي، في حين أنها مصممة لراحة المستهلك، لديها مجموعة متنوعة من الثغرات التي يمكن استغلالها. يمكن لبادئ الاحتيال، على سبيل المثال، الاستفادة من مركز معاملات التشفير مثل ماكينة الصراف الآلي للبيتكوين، جنبًا إلى جنب مع الهاتف الناسخ لتجنب الأصوات من تطبيق القانون.

"لنفترض أنني في نيويورك، وأريد نقل الأموال في التمويل، وعلي أن أدفع لبعض الاشخاص السيئين في ميامي. يريدون أن يتقاضوا رواتبهم بسرعة. لن أحصل على شيك، ولا يمكنني استخدام جهاز كمبيوتر أو كمبيوتر محمول، لأن عنوان *IP* يتم إرساله، لذلك ما أفعله هو الذهاب إلى ماكينة الصراف الآلي *Bitcoin*في نيويورك واستخدام النقود والهاتف الناسخ. بهذه الطريقة، يمكنني الدفع للناس و التحايل على بروتوكولات مكافحة غسيل الأموال. قال ميراندا.

### الاحتيال بطريقة "ذبح الخنازير"

هناك تكتيك شائع آخر للاحتيال يمكن للجهات الفاعلة السيئة استخدامه وهو معروف بمصطلح "ذبح الخنازير". قالت دانا لورانس، كبيرة مسؤولي الامتثال في شركة *Fideseo* للاستشارات التجارية والتقنية: "هذا هو مفهوم المحتال المجازي "بتسمين" ضحيته من خلال استثمار الكثير من الوقت معهم من أجل بناء الثقة". وفقًا للورانس، يمكن أن يحدث الوقت الذي يستثمره المحتالون في أي مكان، ولكن الأهم من ذلك أنه يتم إما على وسائل التواصل الاجتماعي أو من خلال الرسائل النصية على مدار أسابيع أو شهور. استشهد لورانس بـ *LinkedIn* على وجه التحديد كمنصة مفضلة، وكذلك مواقع اجتماعية مثل *Twitter*.

في هذه الحالات، عادة ما يقدم الممثل السيئ نفسه على أنه مؤثر أو من الداخل قد استثمر بنجاح في العملة المشفرة. بمرور الوقت، سوف يروجون لفوائد العملة المشفرة في محاولة لجعل الضحية تنقل أصولها إليهم. في بعض الحالات، قام المحتالون بتزويد الضحية ببيانات مالية مزورة لجعلها تبدو أنها تحقق عوائد كبيرة.

في حين أنه من السهل قراءة هذه العلامات والعثور عليها بشكل واضح إلى حد ما، إلا أن المحتالين في هذه الحالة أصبحوا متطورين للغاية. فرق الاحتيال في دول مثل كمبوديا والصين، على سبيل المثال، تلقت تدريبًا متعمقًا من قبل علماء النفس حول كيفية جعل الناس أكثر عرضة لاتخاذ قرارات غير سليمة. قال جيف روزين، المدعي العام في مقاطعة سانتا كلارا بكاليفورنيا، في مقابلة مع شبكة سي إن إن: "لقد تم تدريبهم من قبل علماء النفس لمحاولة اكتشاف أفضل طريقة للتلاعب بالناس". "أنت تتعامل مع أشخاص سوف يستخدمون تقنيات نفسية مختلفة لتجعلك عرضة للخطر ولجعلك مهتمًا بالتخلي عن أموالك1".

1. Josh Campbell, "Beware the 'Pig Butchering' Crypto Scam Sweeping Across America," December 26, 2022, https://www.cnn.com/2022/12/26/investing/crypto-scams-fbi-tips/index.html.

## الاحتيال بطريقة "الضخ والاغراق"

شكل الاحتيال الرئيسي الآخر الذي يتم رؤيته في الكريبتوسفير معروف جيدًا للمراقبين القدامى في سوق الأسهم: ما يسمى بخطة "الضخ والإغراق."

قال لورانس: "يبدأ هذا المخطط عادةً بمجموعة تجتمع معًا لبدء مشروع تشفير جديد مثل الرمز المميز، ثم تستخدم - عادةً بمساعدة المؤثرين - الموارد لإثارة ذلك على منصات مثل *Twitter* أو *Discord* ". يوجد حاليًا الكثير من التقلبات في سوق العملات المشفرة بسبب السيولة. لذلك، إذا حاول الكثير من الناس شراء شيء ما دفعة واحدة، فإن هذا نوعًا ما يصدم السوق ويؤدي إلى رفع السعر. إذا حدث هذا، فإن الجهات الفاعلة السيئة المعنية التي تحتفظ بكميات كبيرة من الأصول تبيعها فجأة لتحقيق ربح، مما يؤدي إلى انخفاض السعر فجأة وترك جميع المستثمرين الآخرين بشيء يساوي صفرًا بشكل أساسي".

قال لورانس إن اشارة التحذير *(Red Flag)* في هذه المواقف هو الافتقار الواضح للإفصاحات التي تشير للمستثمرين المحتملين أن خسارة كل شيء هو احتمال واضح. عادةً ما يستفيد الفاعلون بقوة من الرسائل التي يتم نسخها ولصقها على وسائل التواصل الاجتماعي ولوحات المناقشة المكتوبة بواسطة ملصقات تحمل أسماء عرض متشابهة. وبمجرد اكتمال المخطط، ستختفي عادةً أسماء الشاشات هذه، ولا يتم تغيير هويتها تمامًا.

## أمثلة الاحتيال الأخرى في سياق الأصول المشفرة

لا يجب أن يكون الاحتيال المستند إلى التشفير دائمًا متطورًا للغاية. داخل المؤسسات القائمة على التشفير، غالبًا ما يكون كل ما هو ضروري لممثل سيئ هو الفرصة المناسبة. على سبيل المثال، في حين أن *blockchain* نفسها ستحافظ على الأصول الرقمية آمنة، فإن كل ما هو مطلوب لتجاوز الأمان وإفراغ المحفظة المشفرة هو الحصول على مفتاح خاص - مجموعة طويلة من الأرقام التي يمكن وضعها في منديل مطعم وتركها في أي مكان لأي شخص لإيجادها.

قال لورانس: "إن مفتاحك الخاص هو هويتك الرقمية لسوق العملات المشفرة، ويمكن لأي شخص يحصل على هذا أن يقوم بمعاملات احتيالية أو يسرق عملاتك المشفرة.، لا يوجد شيء يمكنني القيام به حيال ذلك. لا يمكنني استعادته، لا يمكنني تقديم شكوى، ولا توجد وكالة حماية المستهلك أو منظم للخلاف معه - لقد اختفى تمامًا" .

مع نضوج سوق العملات المشفرة، ظهرت خدمات أمان التشفير المتخصصة في حماية مفاتيح الأفراد والشركات من وضعها في غير مكانها، ولكن في بعض الحالات تكون منهجياتهم بدائية بشكل مدهش. وفقًا للورنس، فإن الحل الذي تستخدمه بعض هذه الخدمات هو تخزين المفاتيح في خزائن على جانب الجبال المهجورة. يوجد تأمين العملات المشفرة أيضًا كشبكة أمان للشركات التي يمكنها تحمل تكاليفها، ولكن في هذه المرحلة، تكافح الصناعة بأكملها لتحقيق الربحية، مما يجبر شركات التأمين على أن تكون انتقائية بشكل لا يصدق مع تقديم تغطية في نفس الوقت تتقلص بحلول العام.

في مقال نُشر في صحيفة *Insurance Times* البريطانية، ناقش شريك مجموعة *RPC Insurance James Wickes* تحديات سوق التأمين على العملات المشفرة. وقال: "من المرجح أن يكون العدد الصغير نسبيًا من شركات التأمين النشطة حاليًا في مجال تأمين الأصول المشفرة حريصًا على مراجعة التفاصيل الدقيقة في صياغة السياسة للحد من التعرض المحتمل من تقلب أسواق العملات الرقمية، كما يتضح من الانهيار الأخير". "سوق التأمين على هذه الأصول في مهده ويبقى أن نرى ما إذا كانت مجموعة كافية من شركات التأمين مستعدة لتوفير سعة كافية لتلبية الطلب ومدى شجاعة السوق في توسيع نطاق التغطية بما يتجاوز مخاطر السرقة التقليدية". [2]

ومع ذلك، على الرغم من هذه الاحتياطات، لا تزال هناك بعض الأدوات التي يمكن للجهات الفاعلة السيئة استخدامها للاستمرار في استخدام أصول التشفير و *blockchain* دون تجاوز الحساب المحدد بشكل مباشر - أي الخلاطات، المعروفة أيضًا باسم البهلوانات. إحدى السمات الأساسية لـ *blockchain* هي شفافيتها. في أي مستكشف *blockchain*، يمكن لأي شخص عرض سجل جميع معاملات *blockchain* منذ إطلاق العملة المشفرة في عام 2009. تسمح الخلاطات للمستخدم بخلط كمية أصول التشفير المعنية بشكل أساسي قبل تسليمها إلى المستلمين المقصودين، مما يمنحهم درجة من عدم الكشف عن هويتهم منذ ذلك الحين من الصعب للغاية فك تشفير من أرسل بالضبط عدد الأصول إلى من. باستخدام الخلاط، كل ما سيظهره المستكشف هو أن شخصًا واحدًا، بالإضافة إلى العشرات من الأشخاص الآخرين، أرسلوا الأصول إلى خلاط، ثم أرسلوا الأصول بكميات متنوعة إلى مجموعة متنوعة من الأشخاص الآخرين. والنتيجة، في جوهرها، تشبه شكلًا مثاليًا لغسيل الأموال.

في مواجهة هذه الحقائق، يجب على المنظمات التي تختار أن تكون موجودة في مجال التشفير أن تقبل أنها إلى حد كبير بمفردها عندما يتعلق الأمر بتخفيف المخاطر في هذه المرحلة. هذا لا يعني أنه يجب تجنب التشفير، ولكن هذا يعني أن الامتثال والرقابة الداخلية السليمة واكتشاف الاحتيال وجهود الردع والتدقيق الداخلي يجب أن تلعب دورًا كبيرًا في محادثات التشفير من مستوى المجلس إلى أسفل.

2. Isobel Rafferty, “Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments,” Insurance Times, July 18, 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

# من أين يبدأ دور التدقيق الداخلي

## بعض القوانين موجودة والباقي قيد الإعداد

### التوجيهات الصادرة

كما ذكرنا سابقًا، فإن الأطر التنظيمية التي يمكن للشركات البحث عنها للتعامل مع الأمان والحوكمة فيما يتعلق بأصول التشفير والمخاطر المرتبطة بالاحتيال المرتبطة بها ضئيلة. ومع ذلك، فإن بعض الصناعات مثل الخدمات المالية ليست مجردة تمامًا من الموارد التي تتناول مبادئ الحوكمة المناسبة فيما يتعلق بحماية الأصول الرقمية - وكثير منها ينطبق على العملات المشفرة.

في أكتوبر 2022، قدم الاتحاد الأوروبي النص المتفق عليه للائحة الأسواق في الأصول المشفرة *(MiCA)*، والتي تعد واحدة من المحاولات الأولى عالميًا للتنظيم الشامل لتسويق العملات المشفرة، على الرغم من طرح التشريع حتى أبريل 2023 إلى ترجمه إلى 24 لغة مختلفة. في حالة اعتمادها رسميًا، فإن اللائحة سوف:

- تحديد الأصول المشفرة رسميًا على أنها "تمثيل رقمي للقيمة أو الحقوق التي يمكن نقلها وتخزينها إلكترونيًا، باستخدام تقنية دفتر الأستاذ الموزع أو تقنية مشابهة." بالإضافة إلى ذلك، فإنه يقدم أربع فئات مختلفة من الأصول المشفرة: الرموز المميزة للأصول، ورموز النقود الإلكترونية، والرموز المميزة للمرافق، والفئة الرابعة للأصول المشفرة التي لا تندرج في الفئات الثلاث الأخرى.
- جعل مزودي التشفير مسؤولين رسمياً إذا فقدوا أصول التشفير الخاصة بالمستثمرين.
- يتطلب من الجهات الفاعلة في أسواق الأصول المشفرة الإعلان عن المعلومات المتعلقة ببصمتهم البيئية والمناخية.
- التداخل مع التشريعات المحدثة بشأن مكافحة غسيل الأموال، وسوف تكلف الهيئة المصرفية الأوروبية *(EBA)* بالحفاظ على سجل عام لمقدمي خدمات الأصول المشفرة غير المتوافقين.
- مطالبة مزودي الأصول المشفرة بالحصول على إذن للعمل في الاتحاد الأوروبي.
- توفير إطار عمل قوي ينطبق على "العملات المستقرة" (عملة مشفرة مرتبطة بأصل مرجعي خارجي)، الأمر الذي سيتطلب مطالبة كل صاحب عملات ثابتة في أي وقت من قبل المُصدر، مجانًا [3].

في الولايات المتحدة، يقدم بيان مشترك صادر عن مجلس الاحتياطي الفيدرالي والمؤسسة الفيدرالية للتأمين على الودائع *(FDIC)* ومكتب المراقب المالي للعملة *(OCC)* بعض الموارد للشركات الأمريكية التي تقدم إرشادات مصممة لمساعدة "المؤسسات المصرفية على الانخراط في أنشطة قوية المناقشات الإشرافية المتعلقة بالأنشطة المقترحة والحالية المتعلقة بالأصول المشفرة.[4] " وتشمل هذه:

- خطاب تفسير *" OCC 1179* تفسير المستشار الرئيسي الذي يوضح: (1) سلطة البنك للانخراط في بعض أنشطة العملة المشفرة ؛ و (2) سلطة *OCC*في ميثاق بنك استئماني وطني" .
- الاحتياطي الفيدرالي *SR* 22-6 *" :CA 22-6/*المشاركة في الأنشطة المتعلقة بالأصول المشفرة من قبل المؤسسات المصرفية التي يشرف عليها الاحتياطي الفيدرالي".

3. General Secretariat of the Council, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," Council of the European Union, October 5, 2022, https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.

4. "Joint Statement on Crypto-Asset Risks to Banking Organizations, Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Office of the Comptroller of the Currency, January 3, 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

- *FDIC FIL-16-2022* إجراءات ملاحظات الإشعار والإشراف للمؤسسات الخاضعة لإشراف مؤسسة التأمين الفيدرالية *(FDIC)* المنخرطة في الأنشطة المتعلقة بالتشفير.

هذه ليست الموارد الوحيدة المتاحة. في أعقاب انهيار *FTX*، أصدرت هيئة الأوراق المالية والبورصات أيضًا إرشادات نصحت الشركات بالكشف عن مشاركتها مع شركات السلع الرقمية.

## قيمة التعليم

بافتراض أنه تم تبنيها، فإن التشريع الأوروبي المقترح سيدخل حيز التنفيذ في عام 2024، ولكن من شبه المؤكد أنه لن يكون الأخير. مع ملء المشهد التنظيمي المرقع من شهر لآخر، فإن الإجراء الأكثر قيمة الذي يمكن للمدقق الداخلي اتخاذه هو بذل قصارى جهده لمواكبة التغييرات وتوضيح هذه التغييرات لمجلس الإدارة وأصحاب المصلحة المعنيين.

في البيئة الحالية، يجب أن يوضح المدققون الداخليون أيضًا لأصحاب المصلحة ما هي اللوائح الأخرى الموجودة والتي قد تكون قابلة للتطبيق على جهود التشفير الخاصة بهم. على سبيل المثال، قال لورانس، الشركة التي تقدم عملتها المشفرة الخاصة بها قد تتطلب التسجيل في شبكة إنفاذ الجرائم المالية الأمريكية - وهي تفاصيل مهمة يمكن التغاضي عنها بسهولة لأن التشفير لم يتم ذكره على وجه التحديد في التشريع. قالت: "هناك الكثير من عدم اليقين الآن". "الأمر متروك للمدققين الداخليين لإبلاغ القادة بما هو قابل للتطبيق وما هو غير قابل للتطبيق".

لا ينبغي أن يؤدي التركيز على التقنيات الجديدة أيضًا إلى صرف انتباه الشركات عن أفضل الممارسات الأساسية فيما يتعلق بحماية الأصول الرقمية، بما في ذلك استخدام شبكة افتراضية خاصة *(VPN)* والأمان المناسب والتجميع والتخلص من معلومات ملف تعريف المستخدم عند الحاجة - خاصة المستهلكين. قال ميراندا: "تعد ملفات تعريف المستخدمين عنصر تحكم تنظيمي بالغ الأهمية". "إذا كنت أقوم بتدقيق شركة، فسوف أتحقق للتأكد من أن ملفات تعريف المستخدمين تتطابق مع نشاط المعاملات. على سبيل المثال، المعلومات الجغرافية مهمة بشكل لا يصدق في الامتثال والتحقيقات. تحتاج المنظمات إلى الحفاظ على أمان هذه المعلومات، وكذلك معرفة مكان تواجدها ". في هذه النقطة، أشار ميراندا إلى أن المؤسسات غالبًا ما تتجاهل اتفاقيات عدم الإفشاء*(NDAs)* ، والتي تحتوي على معلومات شخصية مهمة مثل العناوين المادية التي يمكن أن تكون حاسمة في تحقيق الاحتيال.

لمزيد من المعلومات، يقدم التوجيه التكميلي لمعهد المدققين الداخليين" *(IIA)* التدقيق الداخلي والاحتيال: تقييم إدارة مخاطر الاحتيال" توجيهًا واضحًا فيما يتعلق بالأدوار والمسؤوليات التنظيمية لإدارة وإدارة مخاطر الاحتيال بشكل سليم، بالإضافة إلى توصيات للحصول على إرشادات إضافية مثل دليل إدارة مخاطر الاحتيال من *COSO*.

# الخلاصة

## التدقيق الداخلي جاهز

تعد العملة المشفرة والتكنولوجيا التي تعتمد عليها ثورية للغاية بحيث لا يمكن للمدققين الداخليين تجاهلها، و تستحق اهتمام كبير من مجلس الإدارة. تقييمات المخاطر التي تتجاهلها لها نقطة عمياء حرجة. قد تكون العملة المشفرة مفهومًا جديدًا نسبيًا بالنسبة للكثيرين، لكنها لا تقلل من قيمة إطار عمل إدارة مخاطر الاحتيال السليم الذي يمكن قياسه واختباره عن طريق التدقيق الداخلي.

في حين أنه من السهل التحسر على منطقة مخاطر أخرى لإضافتها إلى رادار التدقيق الداخلي المتزايد باستمرار، إلا أن الخبر السار هو أنه لا توجد إدارة تنظيمية أخرى في وضع أفضل للتعامل معها. تمامًا كما فعل قانون *Sarbanes-Oxley (SOX)* في عام 2002، فإن تطور تنظيم العملة المشفرة يضمن فعليًا للتدقيق الداخلي مكانة قيّمة على الطاولة لسنوات قادمة. حتى إذا كانت الوظيفة لا تعرف العملات المشفرة بعد، فإنها تعرف الاحتيال وتعرف المخاطر ؛ هذا وحده كافٍ لتولي التدقيق الداخلي منصبًا قياديًا يتصدى للتحديات المستقبلية.

# الجزء الثاني

**المدققون الداخليون ومحققو الاحتيال: شراكة قيّمة**

## عن الخبراء

### ماسون وايلدر، CFE

ماسون وايلدر هو محقق معتمد في عمليات الاحتيال، ومدير أبحاث لـ *ACFE*. في هذا المنصب، يشرف على إنشاء وتحديث مواد *ACFE* للتعليم المهني المستمر، ويساعد في تخطيط وإنتاج جميع أحداث التدريب الخاصة بـ*ACFE* ، ويعمل على المبادرات البحثية مثل تقرير الأمم المتحدة وتقارير قياس الأداء، وإجراء التدريبات، والكتابة لـ *ACFE* المنشورات، والاستجابة لطلبات الأعضاء ووسائل الإعلام. قبل انضمامه إلى *ACFE*، عمل وايلدر في استخبارات وتحقيقات أمن الشركات لأكثر من عقد، وتخصص في الخلفية وتحقيقات العناية الواجبة وتحليل المعلومات الاستخبارية للأمن المادي الدولي والاستجابة للأزمات. قامت *Mason* ببناء مهنة في جمع المعلومات ذات الصلة من جميع المصادر لتحليلها وتقطيرها لدعم اتخاذ القرارات الحاسمة، وهي متحمسة لمساعدة المتخصصين في مكافحة الاحتيال على تحسين قدراتهم باستمرار لمكافحة الاحتيال بشكل فعال.

### شونا فلاندرز، CRISC, CISA, CISM, SSGB, SSBB

شونا فلاندرز، مديرة تطوير المنتجات في معهد المدققين الداخليين(*IIA*) ، هي تقني شغوف ومتخصص في صناعة التدريب التقني لديه شغف لتكييف المحادثات التقنية مع لغة تجارية مشتركة. تقدم *Shawna* مزيجًا فريدًا من المهارات الفريدة لكل مشاركة، بما في ذلك: تطوير محتوى الشركات الصغيرة والمتوسطة / المساهمة، التحدث / التدريب، المخاطر المتعلقة بتكنولوجيا المعلومات، تدقيق تكنولوجيا المعلومات، المعلومات والأمن السيبراني، الامتثال لتكنولوجيا المعلومات، حوكمة تكنولوجيا المعلومات، إدارة البائعين، اختصاصي تكنولوجيا المعلومات في الاتصالات، البرمجة، تصميم / مراجعة العمارة المتعلقة بالصوت والبيانات، الهندسة، إدارة التحليلات والتكامل، إدارة عمليات الأعمال، تحليل الأعمال، إدارة المشاريع، إدارة البرامج وتحسين العمليات / 6 سيغما.

# المقدمة

يوفر المدققون الداخليون رؤى بناءة حول الحوكمة والمخاطر والضوابط الداخلية التي تساعد المؤسسات على إدارة المخاطر، بما في ذلك تحديد الاحتيال والتخفيف منه. ومع ذلك، في حين أن التدقيق الداخلي هو جزء فعال من الكشف عن الاحتيال وردعه، فإن العثور على الاحتيال ليس مهمة المدقق الداخلي. من ناحية أخرى، فإن فاحص الاحتيال المعتمد *(CFE)* مكلف على وجه التحديد بتحديد والتحقيق في الاحتيال. يجلب *CFE* مهارات متخصصة في المعركة ضد الاحتيال. نتيجة لذلك، من المنطقي أن يتعاون نوعا المحترفين في شراكة تخدم أفضل مصالح المنظمة.

يتناول هذا الموجز، وهو الثاني في سلسلة من ثلاثة أجزاء حول الاحتيال، فوائد بناء علاقة تكافلية بين المدققين الداخليين والمراقبين الماليين التقليديين.

# نطاق الاحتيال

## معدل الخسائر حوالي 1.8 مليون دولار

### ويبقى الاحتيال خطراً منتشراً

الاحتيال هو أي عمل غير قانوني ينطوي على خداع أو إخفاء أو انتهاك للثقة يتم إجراؤه لتحقيق مكاسب مالية أو شخصية. قد يسعى الأشخاص أو المنظمات التي ترتكب الاحتيال إلى سرقة الأموال أو الممتلكات أو الخدمات؛ لتجنب الدفع مقابل شيء ما أو فقدانه؛ أو للحصول على ميزة شخصية أو تجارية. بالإضافة إلى المحتالين الخارجيين، يمكن أيضًا ارتكاب عمليات الاحتيال من قبل موظفي الشركة الذين يعانون من ضغوط مالية أو الذين يشعرون أنهم مستحقون للأموال أو الخدمات التي يأخذونها لأنهم يرون أن المنظمة قد عاملتهم بشكل غير عادل أو بسبب بعض المظالم الأخرى. قد يكون أي نوع من المنظمات ضحية للاحتيال، بغض النظر عن حجمه أو ما إذا كان عامًا أو خاصًا، أو وكالة غير هادفة للربح، أو وكالة حكومية أو مرفق عام أو خاص، أو كيان آخر.

الاحتيال هو خطر جسيم ومنتشر للمنظمات. يمكن أن تتراوح عواقب الاحتيال من التخريبية إلى الرهيبة. يمكن أن تشمل ليس فقط التحديات والخسائر المالية، ولكن أيضًا أوجه القصور التي تضر بالعمليات أو الإيرادات أو الأرباح ؛ إلغاء المشاريع. واعتمادًا على نطاقها، من المحتمل أن يكون فشل المنظمة[5].

غطت دراسة استقصائية حول *CFEs* في جميع أنحاء العالم أجرتها جمعية مدققي الاحتيال المعتمدين *(ACFE) 2110* حالة احتيال من 133 دولة. ضمن هذه المجموعة، بلغ إجمالي الخسائر العالمية بسبب الاحتيال أكثر من 3.6 مليار دولار، بمتوسط خسارة لكل حالة يقارب 1.8 مليون دولار. في الواقع، تقدر المؤسسات المالية التقليدية أن المؤسسات تخسر 5٪ من إيراداتها بسبب الاحتيال كل عام. من الواضح أن الشركات الصغيرة كانت الأكثر عرضة لخطر الاحتيال: فقد عانى أولئك الذين لديهم أقل عدد من العمال من أعلى متوسط للخسارة، وهو 150 ألف دولار.

بينما قد يكون من السهل اكتشاف خسائر بهذا الحجم، غالبًا ما يحدث الاحتيال بزيادات أقل بمرور الوقت. يمكن أن يؤدي مخطط احتيال نموذجي إلى خسارة 8300 دولار شهريًا ويمكن أن يستغرق اكتشافه 12 شهرًا، وفقًا للاستطلاع. من المهم أيضًا أن تدرك أن العملة المشفرة متورطة في بعض عمليات الاحتيال. وجدت *ACFE* أنهم متورطون في 8 ٪ من الحالات. تضمنت السيناريوهات المعتادة دفع الرشوة والرشوة وتحويل الأصول المختلسة[6].

#### أصناف الاحتيال المهني

هناك ثلاث فئات أساسية من الاحتيال المهني، وفقًا لتقرير *ACFE 2022* للأمم:

**مخططات الاحتيال في البيانات المالية** أو التسبب في خطأ جوهري أو حذف في البيانات المالية للمنظمة، هي الأقل شيوعًا (9 ٪) ولكنها الأغلى، حيث بلغت 593000 دولار في الخسائر لكل حالة.

**اختلاس الأصول**، حيث يسرق الموظف موارد الشركة أو يسيء استخدامها، حدث في 86٪ من الحالات. ومع ذلك، كانت مسؤولة عن أدنى متوسط للخسائر: 100،000 دولار لكل حالة.

**الفساد**، الذي يغطي الرشوة وتضارب المصالح والابتزاز، كان متورطًا في 50٪ من الحالات وأدى إلى خسائر قدرها 150 ألف دولار لكل حالة.

*المصدر:* **Association of Certified Fraud Examiners**, *Occupational Fraud 2022: A Report to the Nations*

[5] [5] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[6] *Occupational Fraud 2022: A Report to the Nations*, the Association of Certified Fraud Examiners.

# مهمة المدقق الداخلي

## التأكيد وتقديم المشورة لمكافحة الاحتيال

### كشف الاحتيال / ردعه أحد أساسيات مهام التدقيق الداخلي

*وفقًا لمعهد المدققين الداخليين*(IIA)، فإن "التدقيق الداخلي هو نشاط استشاري مستقل وموضوعي يهدف إلى إضافة قيمة لعمليات المنظمة وتحسينها. ويشمل دورها الكشف عن مخاطر الاحتيال ومنعها ومراقبتها ومعالجة تلك المخاطر في عمليات التدقيق والتحقيقات[7]."

*لا ينبغي للمنظمات أن تتوقع مجموعة مهارات التدقيق الداخلي لتشمل التحقيق في الاحتيال. إذا كانت الظروف تتطلب أن يتولى التدقيق الداخلي دورًا استقصائيًا، فيجب على المدققين الداخليين توخي العناية المهنية الواجبة وعدم المضي قدمًا إذا لم يكن لديهم الخبرة والخبرة اللازمتين.*

*في حين أن منع الاحتيال هو دور الإدارة، فإن التدقيق الداخلي يدعم جهود إدارة مكافحة الاحتيال من خلال توفير خدمات التأكيد اللازمة على الضوابط الداخلية المصممة لاكتشاف وردع الاحتيال. غالبًا ما يحدث الاحتيال بسبب الضوابط سيئة التصميم والحوكمة الضعيفة التي تقوض عمليات المؤسسة. يُعزى ما يقرب من نصف الحالات في مسح* ACFE *إلى الافتقار إلى الضوابط الداخلية (29٪) أو تجاوز الضوابط الحالية (20٪). ينظر المدققون في احتمالية مخاطر الاحتيال ومدى كفاية الضوابط الداخلية في المجالات التي يفحصونها. عندما تكون ضوابط مكافحة الاحتيال في مكانها الصحيح، تميل إلى انخفاض خسائر الاحتيال واكتشاف أسرع للاحتيال، وفقًا للمسح.*

لا ينبغي الاستهانة بمساهمة التدقيق الداخلي في جهود مكافحة الاحتيال. عندما طلب معهد المدققين الداخليين *(IIA)* من الرؤساء التنفيذيين للتدقيق *(CAE)* ذكر الأماكن التي شاركت فيها وظائف التدقيق الداخلي بشكل كبير، أشار 57٪ إلى الاحتيال وأشار 56٪ إلى التقييم العام للمخاطر. وفي الوقت نفسه، وجد استطلاع *ACFE* أن متوسط خسارة الاحتيال كان أعلى بنسبة 50٪ (150 ألف دولار مقابل 100 ألف دولار) عندما لم يكن هناك قسم للتدقيق الداخلي.

Considerations Integrated into Audits


في الواقع، تشير البيانات الواردة من التقريرالقادم من "نبض أمريكا الشمالية" لعام 2023 عن التدقيق الداخلي إلى أن الاحتيال هو أكثر الاعتبارات التي يتم الاستشهاد بها بشكل متكرر والمضمنة في عمليات التدقيق الداخلي. طلب الاستطلاع السنوي للرؤساء التنفيذيين للتدقيق في أمريكا الشمالية من أكثر من 500 مشارك الإشارة إلى المجالات التي يشملونها كجزء من عمليات تدقيقهم بشكل عام. "تشير الإجابات إلى أن المدققين غالبًا ما يتخذون نهجًا شاملاً ويأخذون في الاعتبار مجموعة واسعة من القضايا، بما في ذلك الأمن السيبراني والجهات الخارجية والحوكمة"، وفقًا للتقرير، الذي سيُعرض لأول مرة في مارس في مؤتمر *GAM 2023.* بشكل عام، قال 89٪ من الرؤساء التنفيذيين للتدقيق إنهم يدرجون اعتبارات الاحتيال في كل عملية تدقيق بشكل عام، والتي كانت أكثر فئات المخاطر التي يتم الاستشهاد بها بشكل متكرر مع احتلال اعتبارات تكنولوجيا المعلومات في المرتبة الثانية بنسبة 80٪.

[7] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.

وفقًا لورقة موقف معهد المدققين الداخليين *(IIA)* حول *الاحتيال والتدقيق الداخلي: التأكيد على ضوابط الاحتيال أمر أساسي للنجاح* [8]، يجب أن يمتلك التدقيق الداخلي المعرفة اللازمة بالاحتيال حتى يتمكن من:

- *تحديد العلامات الحمراء التي قد تشير إلى حدوث احتيال.*
- *فهم خصائص الاحتيال والأساليب المستخدمة لارتكابه، وكذلك أنواع مخططات وسيناريوهات الاحتيال.*
- *أن تكون قادراً على تقرير ما إذا كان من الضروري اتخاذ مزيد من الإجراءات أو ما إذا كان ينبغي التوصية بإجراء تحقيق.*
- *تقييم فعالية الضوابط لمنع أو الكشف عن الاحتيال وتحديد فرص التحسين.*

[8] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019

# مهمة محقق الاحتيال

## التحقيق في الخداع

### تحقيق الاحتيال الماهر أمر بالغ الأهمية

يشارك فاحص الاحتيال في برامج فحص الاحتيال الشاملة للمؤسسة ويدعمها. يفعلون ذلك جزئيًا من خلال إجراء تحقيقات الاحتيال التي "تسعى للحصول على الحقائق والأدلة للمساعدة في إثبات ما حدث، وتحديد الطرف المسؤول، وتقديم التوصيات عند الاقتضاء"[9]. إحدى القضايا التي يأخذها الفاحص في الاعتبار عند بدء التحقيق هي التوقع، مما يعني أن مجمل الظروف يجب أن تجعل من المعقول للمهني المدرب جيدًا وقوع الاحتيال.

قد تشمل الخطوات التي يتخذها فاحص الاحتيال في التحقيق الحصول على أدلة، والإبلاغ عما تم العثور عليه، والإدلاء بشهادة بشأن هذه النتائج حسب الحاجة، والمساعدة في اكتشاف الاحتيال ومنعه. هناك غرضان شائعان لفحص الاحتيال هما التحقيق في ادعاء احتيال أو احتيال محتمل ومراجعة سياسات وضوابط مكافحة الاحتيال الخاصة بالمؤسسة. قد تتضمن الأهداف الأكثر تحديدًا وراء فحص الاحتيال ما يلي:

- اكتشاف السلوك غير اللائق المرتبط أو المحتمل ارتباطه بالاحتيال، بالإضافة إلى تحديد المسؤول عن أي سلوك غير لائق.
- تحديد الخسائر أو الالتزامات الفعلية أو المحتملة من الاحتيال.
- إظهار التزام المنظمة بتحديد وتخفيف الاحتيال.
- المساعدة في تسهيل استرداد الخسائر.
- منع الاحتيال في المستقبل والخسائر أو الالتزامات ذات الصلة.
- معالجة العواقب بخلاف الخسائر المالية.
- الكشف عن نقاط الضعف في الضوابط الداخلية وتعزيزها.
- عند الاقتضاء في بعض الحالات، الامتثال للقوانين أو اللوائح أو العقود أو واجبات القانون العام.[10]

[9] "Planning and Conducting a Fraud Examination," *Fraud Examiners Manual: 2022 Edition*, ACFE.
[10] ibid

## مقارنة المناهج

يقدم هذا الجدول نظرة عامة على بعض الاختلافات المهمة بين الأدوار والأساليب والأهداف للمدققين الداخليين والمراقبين الماليين التقليديين.

| الخصائص | التدقيق الداخلي | محققو الاحتيال |
|---|---|---|
| الهدف | قد تكشف إجراءات التدقيق الداخلي عن الاحتيال، لكنها لا تضمن اكتشافه. على سبيل المثال، قد يجد المدققون معاملة أو موقفًا مشبوهًا في المراجعة وقد يتم تحديدها في النهاية على أنها احتيال. ومع ذلك، فإن العثور على الاحتيال سيكون جانبًا واحدًا فقط من فحص أكبر للضوابط والإجراءات داخل المنطقة قيد المراجعة. | يركز محقق الاحتيال بشكل مباشر على الكشف عن الاحتيال والنظر في إجراءات أو أنشطة مكافحة الاحتيال. |
| التكرار | عادة ما تكون عمليات التدقيق متكررة بشكل منتظم، على الرغم من أنه يمكن استخدام عمليات التدقيق المنبثقة لمعالجة موقف أو أسئلة فريدة في منطقة واحدة. | عادةً ما يتم إجراء التحقيقات بالاحتيال فقط مع التحذير الكافي، على الرغم من أنها قد تحدث دون أي مشغل محدد كجزء من برنامج إدارة المخاطر أو تقييم مخاطر الاحتيال. ومع ذلك، يتم إجراء معظمها ردًا على نصيحة أو ادعاء. وجد استطلاع *ACFE* أن 43 ٪ من عمليات الاحتيال تم اكتشافها بسبب النصائح، وهو ما يقرب من ثلاثة أضعاف عدد الطريقة التالية الأكثر شيوعًا للعثور على الاحتيال. جاء أكثر من نصف جميع نصائح الاحتيال من الموظفين. |
| عدائي أم لا؟ | عمليات التدقيق الداخلية ليست ذات طبيعة عدائية. هدف المدققين هو تقديم رؤى ومعلومات يمكن لقادة وأعضاء الفريق استخدامها لتحسين الضوابط أو العمليات الأخرى، على سبيل المثال. | التحقيقات بالاحتيال هي بطبيعتها عدائية. جزء من الهدف هو إلقاء اللوم على من يرتكب الاحتيال. |
| المعايير | يتبع المدققون الداخليون المعايير الدولية للممارسة المهنية للتدقيق الداخلي، التي وضعها معهد المدققين الداخليين (*IIA*). | تتبع *CFEs* مدونة *ACFE* للمعايير المهنية. يمكن أن تستخدم *CFEs* أداة تقييم مخاطر الاحتيال *ACFE* في اختباراتهم. |

# التعاون لتحقيق الأهداف

## الاحترام المتبادل والمسؤوليات

### التعاون في المعركة ضد الاحتيال

هناك العديد من الفرص للتعاون المفيد بين المدققين وفاحصي الاحتيال. يمكنهم التشاور مع بعضهم البعض بشأن:

- بدء تحقيق احتيال
- التخطيط السنوي للتدقيق وامتحانات الغش
- تقييمات المخاطر
- تقييم وتقييم الضوابط وبرامج مكافحة الاحتيال
- نقل نتائج التدقيق مع الآثار المترتبة على الاحتيال
- معالجة أوجه القصور في السيطرة.

لدى العديد من المؤسسات قواعد تحكم في البروتوكولات عندما يسلم التدقيق الداخلي نتيجة احتيال إلى فريق فحص احتيال خارجي أو داخلي. يلاحظ فريق التدقيق الداخلي اكتشاف الاحتيال ثم يقوم بإعداد تقرير مشترك مع فاحص الاحتيال في نهاية المراجعة.

بالإضافة إلى ذلك، قد يقوم التدقيق الداخلي بمراجعة قسم مكافحة الاحتيال في المؤسسة للتأكد من أن ضوابطه الخاصة كافية. قد يقدم فريق مكافحة الاحتيال تقارير إلى الفرق القانونية أو فرق إدارة المخاطر المؤسسية، من بين مجالات أخرى، بما في ذلك التدقيق الداخلي. في حالة إبلاغ فريق الاحتيال إلى التدقيق الداخلي، يجب الاستعانة بمصادر خارجية لأي تدقيق لهذا القسم لضمان الموضوعية.

### دراسة الحالة توضح التعاون لشكل عملي

توضح دراسة الحالة التالية كيف يمكن للفريقين العمل معًا. ويستند إلى مناقشة أجراها كل من *Shawna Flanders* و *CRISC* و *CISA* و *CISM* و *SSGB* و *SSBB* ومدير تطوير المنتجات في*IIA* ، في ندوة عبر الويب أخيرة لـ *IIA* و*ACFE* ، بعنوان تعزيز التعاون: المدقق وفاحص الاحتيال.

عادةً ما يكتشف التدقيق الداخلي نمطًا يحاكي الاحتيال وينبه فاحصي الاحتيال. في الحالة التي قدمتها فلاندرز، تضمن التدقيق الداخلي مراجعة قروض السيارات. كانت إحدى الخطوات التي اتخذها فريقها هي تقييم الحسابات المتأخرة. في مجموعة من 40 من هذه الحسابات، برز خمسة منهم. تم تعيين النظام للإشارة إلى القروض المتعثرة التي ينبغي متابعتها، ولكن لبعض الأسباب لم يتم وضع علامة على هذه القروض الخمسة. بالإضافة إلى ذلك، تم إعدادهم جميعًا ليكونوا يتمتعون بخصائص غير عادية للغاية: معدل فائدة بنسبة 0٪، ومدة 72 شهرًا، ولا يوجد حد أدنى للدفع.

عندما حققت فلاندرز، وجدت أن معرف المستخدم المرتبط بالقروض ينتمي إلى ممثل خدمة العملاء، وهو أمر غير منطقي. شخص ما في هذا الدور لا يوافق عادة على القروض. ثم راجعت ملفات السجل المتعلقة بالقروض ووجدت أنه قبل حوالي ساعة واحدة من تقديم كل منها والموافقة عليها، تم منح صاحب هوية المستخدم وصولاً إضافيًا إلى النظام. تمت إزالة هذا الوصول بعد حوالي ساعة من الموافقة على القروض وتفعيلها. نظرًا لشروط القرض غير المعتادة، ومشاركة ممثل خدمة العملاء، والتغييرات في الوصول إلى النظام، أدرك فريق التدقيق أن الوقت قد حان لتحويل القضية إلى قسم الاحتيال في الشركة.

اعتمادًا على سياسات وإجراءات المؤسسة، تتضمن الخطوات التي قد يتخذها قسم الاحتيال في هذه الحالة عند تنبيهه بالنشاط المشبوه ما يلي:

- تأكد من صحة المعلومات الواردة من المراجعين.

- فحص النطاق الكامل للأنشطة المتعلقة بهذه الحسابات.
- تحديد ما إذا كان إنشاء هذه الحسابات الخمسة هو إجراء فريد أو جزء من مخطط محتمل مستمر.
- تحديد أي متآمرين.
- النظر في ما إذا كانت الفروع أو المكاتب الأخرى متورطة والنطاق العام للاحتيال.

قد يفكر فاحصو عمليات الاحتيال في هذه المرحلة أيضًا فيما إذا كان ينبغي إيقاف الاحتيال وكيفية إيقافه. إذا كانت هناك حاجة إلى مزيد من الأدلة أو المعلومات، فقد يتقرر السماح باستمرار الاحتيال مؤقتًا على الأقل. هذا قرار معقد سيعتمد على مقدار الخسارة التي خسرتها الشركة بالفعل، ومقدار الخسائر المحتملة إذا استمر الاحتيال، ورغبة المؤسسة في المخاطرة، وفقًا لماسون وايلدر، مدير الأبحاث في*ACFE* ، الذي شارك أيضًا في الندوة عبر الويب. في هذه الحالة، قد تتضمن الخطوات التي يجب اتخاذها قبل إيقاف الاحتيال إجراء مقابلة مع ممثل خدمة العملاء للحصول على مزيد من المعلومات وتحديد نطاق الاحتيال، وربما الكشف عن عمليات احتيال أو خطط إضافية لمزيد من المعلومات.

بمجرد جمع الأدلة وتحليلها، يقوم فاحصو الاحتيال بإبلاغ النتائج التي توصلوا إليها - شفهيًا أو كتابيًا - إلى الأشخاص المناسبين في المؤسسة. قد يشمل ذلك الإدارة أو مجلس الإدارة أو لجنة التدقيق. "تقرير فحص الاحتيال هو سرد للأنشطة المحددة لفاحص الاحتيال والنتائج والتوصيات، إذا كان ذلك مناسبًا"، وفقًا لدليل مدققي الاحتيال .*ACFE* يمكن لإدارة المؤسسة بعد ذلك استخدام التقرير لتحديد الخطوات التالية المناسبة.

إذا قام فاحصو عمليات الاحتيال بمراجعة الموقف ولم يعثروا على احتيال فعلي، فقد يعيدون القضية إذا قرروا أن العلم الأحمر الأصلي قد نشأ بسبب نقص في ضوابط إدارة مخاطر الاحتيال. يمكن للتدقيق الداخلي بعد ذلك تضمين هذا النقص في تقريره.

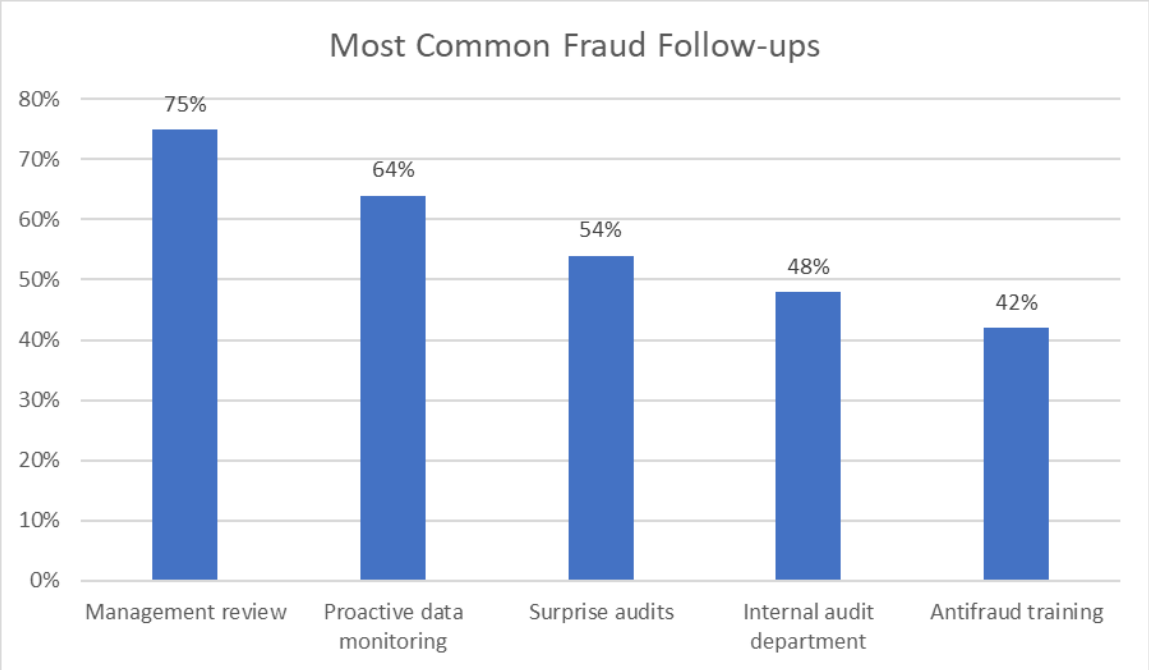
## توحيد الجهود

يجب على المعنيين بالاحتيال أن يتذكروا أن التخفيف مهم. أشار تقرير مسح *ACFE* إلى أن الخطوات الاستباقية للعثور على الاحتيال يمكن أن تؤدي إلى الكشف المبكر وتقليل الخسائر، بينما تسمح الجهود التفاعلية للمخططات باللعب على مدى وقت أطول وتزيد من التأثير المالي على الضحية.

ومع ذلك، لا يمكن للمنظمات تحديد أو القضاء على جميع مخاطر الاحتيال. إنهم يواجهون أنواعًا عديدة من الاحتيال، ومجموعة متنوعة من الدوافع وراءهم، ومجموعة واسعة من الجناة. ومع ذلك، كلما كان الناس أكثر دراية على جميع المستويات - الإدارة ومجلس الإدارة والموظفين - كان من الأفضل لهم بذل جهود التخفيف المعقولة وتحديد الاحتيال أو العلامات الحمراء التي قد تشير إلى وجودها. من خلال الجمع بين مهاراتهم وخبراتهم الفريدة، يمكن للمدققين الداخليين وفاحصي الاحتيال تقديم مساهمة قوية في جهود المنظمة الشاملة. يمكن للمؤسسات استخدام عملها لاتخاذ قرارات أكثر استنارة حول أساليب إدارة مخاطر الاحتيال.

## خطوات لتفادي التكرار

قام ما مجموعه 81٪ من المؤسسات في استطلاع *ACFE* بإجراء تعديلات على ضوابط مكافحة الاحتيال بعد عملية احتيال. يوضح الرسم البياني أدناه التغييرات الأكثر شيوعًا لعناصر التحكم التي نفذتها المؤسسات أو عدلتها. تشمل ضوابط مكافحة الاحتيال الأخرى التي أوصت بها *ACFE* المراقبة الآلية للمعاملات / البيانات، والمراقبة، وتسوية الحسابات.




***المصدر:*** **Occupational Fraud 2022: A Report to the Nations, the Association of Certified Fraud Examiners.**

# الخلاصة

يتطلب **دور التدقيق الداخلي**، كونه المزود الثالث للضمانات حول الحوكمة وادارة المخاطر والرقابة الداخلية، هياكل وعمليات وممارسات تعزز ضمانًا موضوعيًا ومستقلًا. ولكن، كما هو مذكور في نموذج الخطوط الثلاثة لمعهد المدققين الداخليين*(IIA)* ، فإن الاستقلال لا يعني العزلة.

يجب أن يكون هناك تفاعل منتظم بين التدقيق الداخلي والإدارة لضمان أن عمل التدقيق الداخلي ملائم ومتوافق مع الاحتياجات الاستراتيجية والتشغيلية للمؤسسة. من خلال جميع أنشطته، يبني التدقيق الداخلي معرفته وفهمه للمؤسسة، مما يساهم في التأكيد والمشورة التي تقدمها كمستشار موثوق به وشريك استراتيجي "، وفقًا للنموذج.

من الواضح أن هذا هو الحال عندما يجد التدقيق الداخلي وفاحصو الاحتيال المعتمدون أرضية مشتركة كحلفاء في المعركة ضد الاحتيال.

# الجزء الثالث

**المخلفات: الاحتيال في عصر ما بعد كوفيد**

## عن الخبير

ديفد دومنغيز، **CIA, CRMA, CPA, CFE**

ديفيد هو مدير التدقيق والامتثال في *Itafos* في هيوستن. خلال مسيرته المهنية، عمل ديفيد مع شركات متعددة الجنسيات في صناعات مختلفة لتأسيس وتوجيه وتحويل وظائف التدقيق الداخلي للشركات والإقليمية. قاد ونفذ المشاريع المالية والتشغيلية والمتعلقة بالضمان والاستشارات في أمريكا الشمالية وأمريكا اللاتينية وأوروبا وآسيا. كما أدار وشارك في العديد من التحقيقات متعددة الاختصاصات ومبادرات تحليل البيانات ومجموعة واسعة من عمليات تدقيق المساهمين الدوليين والمشروعات المشتركة والموردين. تشمل مجالات خبرته حوكمة الشركات والمؤسسات، وإدارة مخاطر المؤسسات، وإدارة مخاطر الاحتيال، وقانون ساربينز أوكسلي لعام 2002، وبرامج الأخلاقيات والامتثال.

# مقدمة

خلال الجزء الاكبر من عامي 2020 و2021، تسبب *COVID-19* في حدوث اضطرابات في جميع المجالات، بدءًا من الطريقة التي يعمل بها الأشخاص، ومكان عملهم، وكيفية تعامل مؤسساتهم مع الموردين ومشكلات سلسلة التوريد، وكيفية تعاملهم مع المخاوف المهمة، مثل الصيانة الضوابط الداخلية واكتشاف ومنع الاحتيال.

اليوم، يتنفس العالم بسهولة حيث يتلاشى أسوأ وباء ببطء في التاريخ، ولكن مع ذلك، لا ينبغي للمرء أن يفترض أن المخاطر المرتبطة بـ *COVID-19* لم تعد مصدر قلق. في الواقع، يمكن للمنظمات التي تضع هذا الافتراض أن ترتكب خطأ فادحًا. يتناول موجز المعرفة العالمي هذا، وهو الثالث في سلسلة الاحتيال المكونة من ثلاثة أجزاء من معهد المدققين الداخليين*(IIA)* ، العديد من عوامل الاحتيال المرتبطة بالوباء المحددة في تقرير *ACFE* 2022 للأمم المتحدة، وكيف يمكن أن تؤثر على المنظمات، والتدقيق الداخلي. دور في الجهود التنظيمية للتخفيف من عوامل خطر الاحتيال تلك.

# الاحتيال ومخاطره أمور باقية

## المتغيرات التي أحدثها الكوفيد ستبقى مصدر قلق

### ستظهر أنواع احتيال جديدة مستوحاة من الكوفيد

في أحدث تقرير لها إلى الأمم المتحدة حول الاحتيال المهني، وجدت رابطة مدققي الاحتيال المعتمدين *(ACFE)* أن متوسط مدة عمليات الاحتيال - أي الوقت المعتاد بين وقت بدء الاحتيال ووقت اكتشافه - كان 12 شهرًا.[11] وهذا يعني أن المنظمات تستمر في مواجهة عمليات الاحتيال المتعلقة بالوباء والتي لم يتم اكتشافها بعد.

هناك العديد من الأسباب التي تجعل التغييرات المتعلقة بالوباء تستمر في التأثير على مخاطر الاحتيال. على سبيل المثال، كان القصد من اعتماد العمل عن بُعد أن يكون مؤقتًا، لكنه تحول إلى إجراء تشغيل قياسي في العديد من الشركات. غالبًا ما جلب العمل عن بُعد تغييرات كبيرة - وفي بعض الحالات تخفيف - للممارسات والإجراءات المصممة لتحديد أو تخفيف الاحتيال. ونتيجة لذلك، لا تزال المخاطر المرتبطة بها تشكل تهديدات للشركات حتى مع تضاؤل الاضطرابات المرتبطة بالوباء.

لقد لعب التدقيق الداخلي وسيظل يلعب دورًا رئيسيًا في التعامل مع مخاطر الاحتيال المستمرة المتعلقة بالوباء. في دراسة لأعضاء معهد المدققين الداخليين حول العالم أجرتها مؤسسة التدقيق الداخلي *(IAF)* وكرول، شعر العديد من المشاركين في الموائد المستديرة ذات الصلة أن الوباء "يضع التدقيق الداخلي أكثر في مقعد القيادة عندما يتعلق الأمر بإدارة مخاطر الاحتيال"[12]. وهذا يشمل مشاركة إضافية في الاعتبارات الإستراتيجية للتحديات التشغيلية، وتوفير ضمان مستمر، وزيادة التعاون عبر وظائف العمل - كل ذلك مع الحفاظ على استقلالية المدقق.

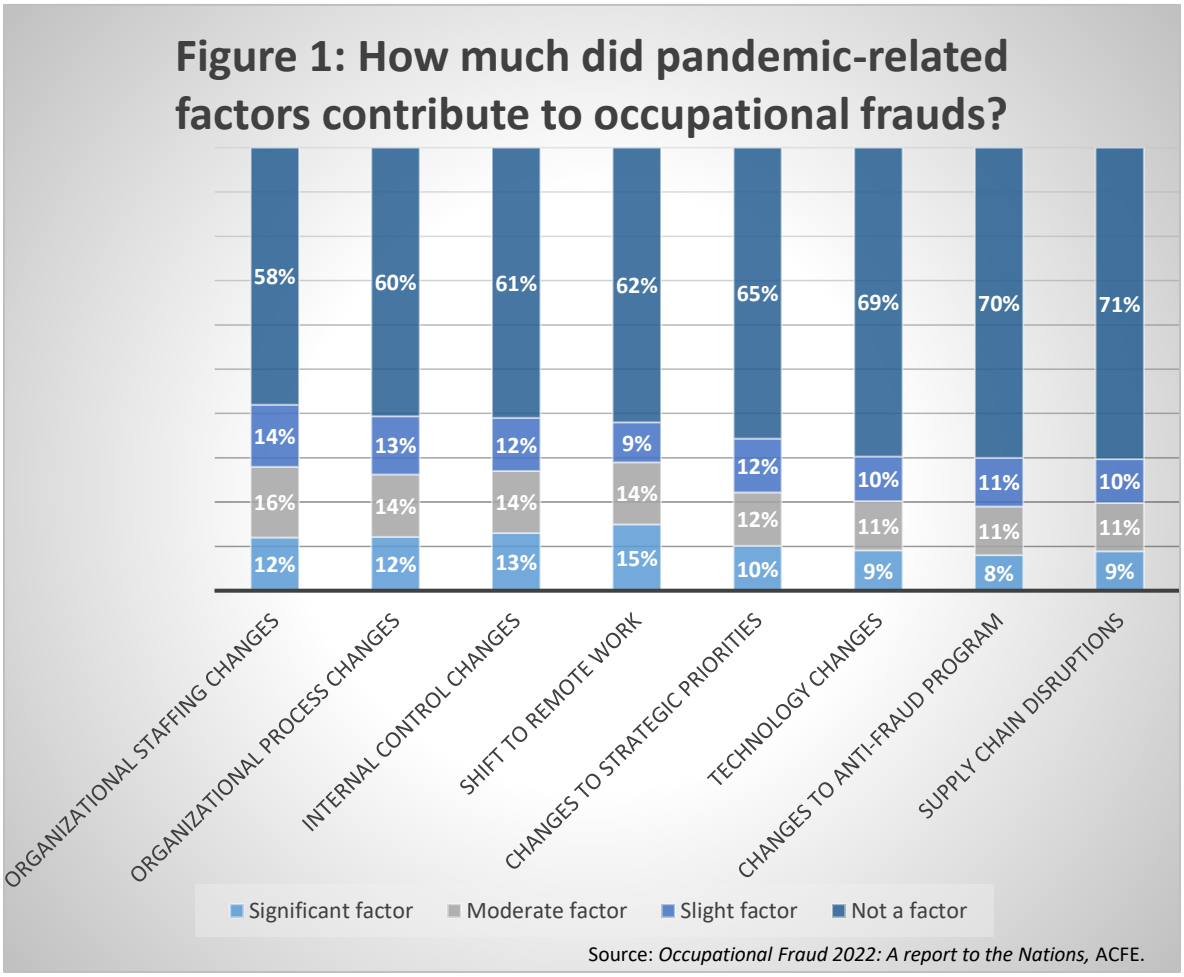
[11] *Occupational Fraud 2022: A Report to the Nations*, ACFE.
[12] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.

# أهم مخاطر الاحتيال المرتبطة بالأوبئة

## تغييرات التوظيف، العمل عن بعد أكبر مخاوف

### يرى أكثر من نصف المشاركين في الدراسة عوامل وبائية تسهم في الاحتيال

أثناء إعداد تقريره عن الاحتيال المهني، وجدت الهيئة أن 52٪ من المجيبين أفادوا أنه في حوادث الاحتيال التي حققوا فيها، ساهمت واحدة على الأقل من القضايا العديدة المتعلقة بالوباء في الاحتيال. من بينها، كانت التغييرات في التوظيف التنظيمي المرتبطة بالوباء هي الأكثر شيوعًا. قال ما مجموعه 42 ٪ من المستجيبين أن التغييرات في التوظيف كانت عوامل مهمة أو معتدلة أو طفيفة تساهم في الاحتيال المهني. كان التحول إلى العمل عن بعد هو العامل الأكثر شيوعًا الذي تم الاستشهاد به باعتباره مهمًا (15 ٪)، يليه الضوابط الداخلية (13 ٪).( Figure 1)




Source: *Occupational Fraud 2022: A report to the Nations,* ACFE.

يُظهر فحص أعمق لبعض أهم القضايا المتعلقة بالوباء التي تم تحديدها في تقرير *ACFE* أن التأثيرات يمكن أن تكون غالبًا معقدة ودقيقة.

## التغييرات في التوظيف تشكل مخاطر احتيال مختلفة

أجبر الوباء العديد من المنظمات على إيجاد حلول بديلة أو اختصارات من أجل التغلب على الاضطرابات العديدة التي كانوا يواجهونها، بما في ذلك تغيير أو توسيع مسؤوليات العمال أو جلب أشخاص جدد لديهم وقت محدود للتأقلم مع وظائفهم. بالإضافة إلى ذلك، غالبًا ما تصبح عمليات التسريح المؤقت أو الإجازات الناتجة عن عدم اليقين الاقتصادي المرتبط بالوباء دائمة، كما أشار ديفيد دومينكيز، مدير التدقيق والامتثال في شركة*Itafos*، وهي شركة متخصصة في الفوسفات والأسمدة. وقال: "لقد زاد بالتأكيد من المخاطر من زوايا مختلفة."

بالنظر إلى التعديلات والتسهيلات العديدة لممارسات وبروتوكولات العمل التي قد يكون الوباء قد خلقها - ومنحنى التعلم المحتمل لأولئك الذين يقومون بمهام جديدة - يجب على المنظمات النظر في أنواع التأثيرات غير المقصودة التي قد تكون لهذه التغييرات. فيما يلي بعض المجالات التي يجب وضعها في الاعتبار:

### الثقافة

هناك عدد من الأسباب لإعادة تقييم ثقافة وقيم الشركة وربما إعادة تأكيدها في أعقاب الوباء. كان "إنجاحها" فضيلة أثناء الوباء، لكن هذا قد يعني أنه قد تم نسيان بعض الممارسات والمواقف الأخلاقية المهمة. قد لا يكون العمال الجدد قد جربوا أبدًا مقدمة مناسبة للقيم الأخلاقية للشركة. إذا كان الأمر كذلك، فمن المستحسن أن تذكر المنظمات الموظفين بتوقعاتهم بشأن السلوكيات الأخلاقية.

"ان ثقافة النهج الاستباقي يمكن أن تردع أنواع مختلفة من سوء السلوك ويعزز السلوكيات التي يمكن أن تعزز الروح المعنوية والإنتاجية،" حسب تقرير *ACFE*. "للثقافة قدرة قوية على التأثير في كيفية أداء الناس لوظائفهم ؛ كيف يتم اتخاذ القرارات المتعلقة بالجودة والامتثال والشواغل الهامة الأخرى ؛ وكيف يُنظر إلى المنظمة داخليًا وخارجيًا".[13]

### اعتبارات الموارد البشرية

أدى نقص العمالة وتحول السياسات في العمل الهجين والعمل عن بعد إلى قلب بعض ممارسات الموارد البشرية القديمة، مثل الخطوط الساخنة المجهولة للمبلغين عن المخالفات.

أحد الأدوات الهامة المتعلقة بالموارد البشرية في منع الاحتيال هو الخط الساخن للمبلغين المجهولين. في الواقع، تم اكتشاف 42٪ من عمليات الاحتيال بواسطة الابلاغ، وفقًا لتقرير*ACFE* ، أكثر من ثلاثة أضعاف الطريقة التالية الأكثر شيوعًا.

يمكن أن يدعم التدقيق الداخلي هذه العملية من خلال فحص ما إذا كان يعمل على النحو المنشود. قال دومينكيز إن الخطوة الأولى قد تكون تحديد مدى جودة مراقبة هذه الخطوط الساخنة وما إذا كان يتم متابعة الشكاوى وتتبعها. ويوصي بطرح أسئلة على مراقبي الخط الساخن، مثل:

- **كيف يصل الناس إلى الخط الساخن؟** تشمل الخيارات ترك النصائح في صندوق الإسقاط في المكتب أو الاتصال برقم الخط الساخن أو الإبلاغ عن الشكاوى عبر الإنترنت. ضع في اعتبارك أن الصندوق المنسدل - والملصقات التي تروج للخط الساخن - لن تساعد العمال عن بُعد.
- **هل يمكن توفير الخط الساخن بلغات مختلفة، إذا كان ذلك مناسباً؟**
- **ما مدى جودة تتبع الجهد؟** أشار دومينكيز إلى أن بعض الشركات تهنئ نفسها على أرقام الشكاوى المنخفضة. قد يكون هذا انعكاسًا دقيقًا لمؤسسة جيدة الإدارة، ولكنه قد يشير أيضًا إلى أن بعض مكالمات الخط الساخن لا يتم الرد عليها أو نادرًا ما يتم متابعة الشكاوى.

يمكن للتدقيق الداخلي مراجعة عملية الرد على الشكاوى لضمان التوقيت المناسب من الاستلام إلى الحل وما إذا كانت قرارات المتابعة أم لا تستند إلى أسس سليمة. تفوت المنظمات أحيانًا نصائح احتيال صحيحة بسبب الخوف من الانتقام بعد تقديم شكوى. يمكن للتدقيق الداخلي مراجعة ما إذا كان دليل الشركة أو مدونة قواعد السلوك تحظر صراحة الانتقام. وللمضي قدمًا، يمكن أن يساعد التدقيق الداخلي الشركة أيضًا على تتبع ما إذا كان المبلغون عن المخالفات أقل احتمالًا للحصول على ترقية أو أكثر عرضة لمراجعة أداء ضعيف، كما أشار دومينكيز. وقال إنه حتى عندما تكون الشكوى غير مدعمة بأدلة، فقد تجد الشركات من خلال سياسات عملية الاستجابة التي تحتاج إلى تحديث أو توضيح.

[13] *Assessing Corporate Culture: A Proactive Approach to Deter Misconduct*, Anti-Fraud Collaboration, March 2020.

تشمل الاحتياطات / الضوابط القيمة الأخرى التي يجب أن تستمر أو تنفذ ما يلي:

- مراجعة الخلفية لتحديد التاريخ الائتماني السابق أو المشاكل المالية الأخرى أو تاريخ الأجور أو الامتيازات أو الأحكام التي قد تكون مرتبطة بالاختلاس.
- التحقق من أوراق الاعتماد.

أفادت *ACFE* أن 50 ٪ من المحتالين أظهروا علامة حمراء واحدة على الأقل متعلقة بالموارد البشرية قبل أو أثناء وقت وقوع حادث الاحتيال. من حيث القرائن السلوكية، كان العيش خارج إمكانيات الفرد هو العلامة الحمراء الأكثر شيوعًا في كل دراسة لـ *ACFE* منذ عام 2008. وقد تم تحديده في 39٪ من الحالات، قبل العامل الثاني الأكثر شيوعًا، الصعوبات المالية، بنسبة 25٪.

### عدم اليقين الوظيفي

حدد *ACFE* عددًا من الأمثلة على عدم اليقين الوظيفي الذي يمكن أن يساهم في الاحتيال، ويمكن أن تؤدي الظروف الاقتصادية الصعبة إلى زيادة انعدام الأمن. تشمل العلامات الحمراء المحددة ما يلي:

- الخوف من فقدان الوظيفة.
- رفض زيادة أو ترقية.
- خفض الفوائد.
- خفض الأجور.
- قطع لا إرادي في ساعات.
- تخفيض الرتبة.

بينما استقر المناخ الاقتصادي منذ أسوأ أيام الوباء، لا تزال هناك تحديات داخل مناخ الأعمال العالمي. ليس من المستغرب أن يظل تأثير المشكلات المتعلقة بعدم اليقين الوظيفي قوياً في عام 2022، وفقًا لـ *ACFE*. من المنطقي أن بعض حالات عدم اليقين هذه قد تظل عاملاً في دفع سوء سلوك الموظف.

تنطبق هذه العلامات الحمراء على الموظفين بشكل عام، ولكن كانت هناك بعض العلامات الإضافية التي تنطبق بشكل خاص على المديرين التنفيذيين:

- **التنمر أو التخويف**. 23٪ للمالك / المديرين التنفيذيين ؛ 8٪ لغير المالكين / التنفيذيين.
- **قضايا التحكم**. 18٪ للمالك / المديرين التنفيذيين ؛ 12٪ لغير المالكين / التنفيذيين.
- **موقف "*Wheeler-dealer*"**. 17٪ للمالك / التنفيذيين ؛ 9٪ لغير المالكين / التنفيذيين.
- **الضغط المفرط من داخل المنظمة**. 13٪ للمالك / التنفيذيين ؛ 6٪ لغير المالكين / التنفيذيين.
- **المشاكل القانونية السابقة**. 11٪ للمالك / التنفيذيين ؛ 3٪ لغير المالكين / التنفيذيين.

## يجب إعادة النظر في تغييرات الرقابة الداخلية المتعلقة بكوفيد

الضوابط الداخلية هي الإجراءات المعتمدة لضمان أن الإجراءات والقرارات في جميع أنحاء المنظمة تتماشى مع سياساتها ومتطلبات إعداد التقارير وولايات الامتثال. يمكن أن تقلل ضوابط مكافحة الاحتيال من خسائر الاحتيال وتسهل اكتشاف الاحتيال بشكل أسرع. في دراسة *ACFE* ، يمكن إرجاع ما يقرب من نصف خسائر الاحتيال إلى عاملين: الافتقار إلى الضوابط الداخلية (29٪) وتجاوز الضوابط الحالية (20٪). من الواضح أن تنفيذ وتعزيز الضوابط الداخلية يمكن أن يوفر فائدة إيجابية كبيرة للمنظمات. يلعب التدقيق الداخلي دورًا مهمًا في الإبلاغ عن الضوابط الداخلية والتوصية بالتحسينات عليها. في الواقع، وجد استطلاع *ACFE* أن متوسط خسارة الاحتيال كان أعلى بنسبة 50٪ (150.000 دولار مقابل 100.000 دولار) عندما لم يكن هناك قسم تدقيق داخلي.

يعتقد المدققون الداخليون الذين ردوا على استبيان *IAF / Kroll* أن "إطار الرقابة الداخلية قد يضعف بسبب تحديات العمل عن بعد، وفي كثير من الحالات، تقليل الموظفين من خلال المرض والإجازة وعدد الموظفين[14]."

قال دومينكيز إن الأشخاص الجدد الذين ينضمون إلى المنظمات خلال أوقات الأزمات ربما لم يتلقوا التدريب الكافي أو نقل المعرفة، أو ربما تعلموا فقط بروتوكولات الطوارئ التي لم تتضمن عمليات وضوابط طويلة الأمد. قال: "تم تخفيف الضوابط أو ربما سقطت من خلال الشقوق". على طول الطريق، قد تصبح هذه الاختصارات - وقد تظل - إجراء تشغيل قياسيًا على الرغم من أنه كان من المفترض استخدامها فقط خلال إطار زمني محدد أو في موقف معين.

وقد أدى هذا القلق إلى تغييرات إيجابية في العديد من المنظمات. على سبيل المثال، قال ما يقرب من ثلاثة أرباع أعضاء لجنة التدقيق الذين أجابوا على استبيان مشترك أجراه مركز *Deloitte* لفعالية مجلس الإدارة ومركز جودة التدقيق إنهم قاموا بتحديث ضوابطهم الداخلية في العام الماضي بسبب بيئة العمل عن بُعد[15] .

يمكن أن تساهم نقاط الضعف في الضوابط الداخلية في الاحتيال من خلال خلق أو تعزيز بيئة يكون فيها إهمال أو تجاوز التدابير القوية لمكافحة الاحتيال أسهل. على سبيل المثال، أثناء الوباء، ربما تم استبعاد الفصل بين الواجبات - وهو إجراء شائع وفعال لمكافحة الاحتيال - لأنه كان من الصعب تحقيقه مع العمال المنتشرين في مواقع مختلفة أو بسبب تقليص عدد الموظفين أو النقص. هذا هو نوع الرقابة الداخلية التي يجب على الشركة مراجعتها الآن للتأكد من أنها قد أعيدت للعمل بشكل فعال.

يمكن أن يساعد التدقيق الداخلي المؤسسات على معالجة هذه المخاطر من خلال ضمان وجود البروتوكولات والعمليات الحيوية. باستخدام تقنية رسم الخرائط، يمكنهم تتبع العمليات خلال فترة حديثة - ستة أشهر أو سنة - وتحديد الاختلافات من الإرشادات المناسبة أو أفضل الممارسات. قال دومينكيز: "يمكنك رؤية الانحرافات عن الإجراءات أو السياسات القياسية وتحديد العمليات التي تحتاج إلى التحديث أو الإنفاذ."

تشمل المجالات الأخرى التي يجب إعادة النظر فيها الضوابط الداخلية المتعلقة بالمشتريات، وتحرير الشيكات، والتسويات المصرفية، وسداد النفقات، أو أي مجال معني بالاعتبارات المالية.

## لا يزال العمل عن بعد عامل احتيال بالغ الأهمية

من المحتمل أن يكون المحور الدراماتيكي للعمل عن بُعد - إغلاق المكاتب والسماح للعمال بأداء وظائفهم في المنزل - هو التغيير الأكثر أهمية لمعظم المنظمات خلال الوباء. وبالتالي، كان هذا النهج الجديد هو العامل الأكثر ذكرًا كمساهم بشكل كبير في الاحتيال في تقرير *ACFE*. في الظروف العادية، قد تقضي الشركة شهورًا في التفكير في التأثير الاستراتيجي لمثل هذه الخطوة، لكن هذا كان مستحيلًا في الأساس وسط حالة عدم اليقين وإلحاح الأسابيع الأولى للوباء. إذا لم يكن هناك شيء آخر، فإن العمل بمفردك وبعيدًا عن أعين الزملاء والمشرفين يمكن أن يسهل ببساطة ارتكاب مجموعة متنوعة من عمليات الاحتيال. وفقًا لـ*ACFE* ، يجب على أولئك الذين ينتقلون بشكل دائم إلى العمل عن بُعد أو العمل الهجين أن ينخرطوا في تخطيط إدارة التغيير "لاكتشاف خطوط الصدع التي يمكن أن يكون لها عواقب كارثية إذا تُركت دون معالجة[16].."

من خلال هذه العملية، هناك العديد من خطوط الأعطال المحتملة التي يمكن أن يركز عليها التدقيق الداخلي. على سبيل المثال، تم الاستشهاد بصعوبات الإدارة الفعالة للأشخاص في بيئة نائية مجزأة وتأثيرها على الثقافة كمجالات رئيسية يجب معالجتها، وفقًا لتقرير *IAF / Kroll.* [17] غالبًا ما يكون السلوك الأخلاقي شيئًا يتم تعلمه وتعزيزه من خلال التفاعلات مع العمال الآخرين الذين يثبتون ذلك أثناء العمل. يمكن أن يساعد الوصول إلى الزملاء الأكثر خبرة الموظفين على فهم كيفية الاستجابة في الظروف المربكة أو المشبوهة، مثل عندما يبدو أن عامل آخر يتصرف بشكل غير لائق أو غير قانوني.

من بين أنواع الاحتيال المرتبطة على وجه التحديد بالعمل عن بُعد:

- **سرقة الوقت أو تقديم مطالبات غير دقيقة عن ساعات العمل**. يمكن أن يكون هذا أسهل عندما لا يكون شخص ما تحت إشراف مباشر.
- **سرقة البيانات أو إساءة استخدامها أو مشاركة معلومات سرية أو حساسة**. قد يتم ذلك عن طريق أولئك الذين يمكنهم الوصول إلى أجهزة الموظف أو بواسطة الموظفين الذين يشعرون براحة أكبر في إساءة استخدام البيانات عندما يكونون بعيدًا عن المكتب[18]..

[14] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[15] *Audit Committee Practices Report: Common Threads Across Audit Committees*, Deloitte's Center for Board Effectiveness and the Center for Audit Quality, January 25, 2022.
[16] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[17] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[18] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.

أحد الامور ذات الصلة هو تولي الموظفين عن بعد لوظائف ثانوية. على سبيل المثال، قد يقوم الموظف بإجراء استشارات أو مهام مؤقتة لشركة أخرى خلال الساعات التي من المفترض أن يعملوا فيها لدى صاحب العمل الأساسي، كما قال دومينكيز. هذه بالتأكيد سرقة للوقت، ولكن إساءة استخدام موارد الشركة، مثل أجهزة الكمبيوتر المحمولة أو الهواتف، قد يعرض الشركة أيضًا لقضايا الأمن السيبراني. قد تكون الوظيفة الجانبية أيضًا تضاربًا في المصالح إذا كان الموظف يقوم بعمل لصالح أحد المنافسين، خاصةً إذا كان يتبادل المعلومات المفيدة للمنافسة. قال دومينكيز إن التدقيق الداخلي يمكن أن يساعد في معالجة هذه المشكلة من خلال التشكيك في نوع التدريب الذي يتلقاه الموظفون وما إذا كان دليل الموظف والسياسات قد تم تحديثها لبيئات العمل الجديدة.

## التغييرات التكنولوجية تخلق فرصاً عديدة للاحتيال

يمكن للتكنولوجيا أن تمكن المنظمات من تنفيذ إجراءات فعالة في مجالات مثل الضوابط الداخلية والعمل عن بعد. تقوم المنظمات بالفعل بإجراء تحسينات واستثمارات في التكنولوجيا لمعالجة مخاوف الأمن السيبراني، وقد دفع الوباء الشركات إلى تسريع وتقوية أنظمتها. تم تضمين العديد من وظائف التدقيق الداخلي في تحديث التكنولوجيا. في الواقع، أضاف 29٪ من المدققين الداخليين تحليل البيانات كأداة لتحديد الاحتيال والفساد منذ بداية الوباء[19]..

في الوقت نفسه، يمكن أن يؤدي سوء استخدام أو إهمال الأدوات التقنية إلى تسهيل نجاح مخططات الاحتيال. كما لوحظ، تعد سرقة البيانات أحد الاهتمامات المرتبطة بالعمل عن بُعد. تشمل الحلول الممكنة لمخاطر سرقة البيانات، وفقًا لـ*ACFE* ، مطالبة العمال بتأمين شبكتهم المنزلية - وعدم مشاركتها مع أفراد الأسرة الآخرين. يعد استخدام شبكات *VPN* وكلمات مرور وإعدادات أقوى وأكثر تعقيدًا لتأمين أجهزة الكمبيوتر المنزلية أمرًا أساسيًا أيضًا. تشمل الخيارات الأخرى المصادقة متعددة العوامل والتدريب السنوي للموظفين على أمن البيانات والخصوصية. يجب على المؤسسات أيضًا تطوير سياسات بشأن الاستخدام المقبول للأجهزة الإلكترونية ووسائل التواصل الاجتماعي وبيانات الشركة، بالإضافة إلى مطالبة الموظفين بقراءة السياسات والإقرار بفهمهم لها.

ستحتاج المؤسسات التي تعمل في بيئة بعيدة أو هجينة أيضًا إلى التأكد من قيام الموظفين بتحديث البرامج وتصحيحات الأمان على أجهزتهم المنزلية، بالإضافة إلى تثقيف العمال حول أفضل الطرق لتجنب التصيد الاحتيالي وتهديدات القراصنة الأخرى. [20] بالطبع، يجب على الشركات التي تكافح لمواكبة تأثير الوباء مراجعة تدابير الأمن السيبراني الخاصة بها لضمان بقائها محدثة.

للمساعدة في معالجة هذه المخاوف، أوصى *Dominquez* بأن التدقيق الداخلي يمكنه التحقيق في بروتوكولات الأمان المعمول بها، وما هي أدوات منع فقدان البيانات التي تستخدمها المؤسسة، وإذا كانت تتطلب مصادقة متعددة العوامل وشبكات*VPN* ، وإذا تم إلغاء تنشيط الحسابات في الوقت المناسب عند مغادرة الموظفين.

## يؤثر "ترك العمل المبطن" على الامتثال والجهود الأخلاقية

يشير مصطلح " ترك العمل المبطن " إلى ممارسة يقوم فيها العمال بالحد الأدنى من متطلبات عملهم. وفقًا لأحد التقديرات الصادرة عن مؤسسة غالوب، فإن هؤلاء العمال يشكلون ما لا يقل عن 50٪ من القوة العاملة في الولايات المتحدة. كان مستوى العمال الملتزمون 32٪، لكن أولئك الذين تم فك ارتباطهم بنشاط كان 18٪. تلاحظ جالوب أن هذا يمثل مشكلة خاصة في وقت تكون فيه العديد من الوظائف تعاونية أو عندما يتطلب الأمر خطوة إضافية لتلبية احتياجات العملاء. وبينما حظي الاتجاه نحو الإقلاع الهادئ بالكثير من الاهتمام، يجب على أصحاب العمل أن يدركوا أن التاركين الصاخبين - أو الأشخاص الذين يعبرون بنشاط عن استيائهم وربما ينشرونه - لا يزالون موجودين [21] .

يمكن أن يكون هذا الاتجاه أخبارًا سيئة للإنتاجية والكفاءة والاحتفاظ. في الوقت نفسه، يمكن أن يكون لها تأثير سلبي على إدارة المخاطر. قال دومينكيز: "لا يولي الناس نفس القدر من الاهتمام لما يجب عليهم فعله". وكما تشير رؤى الامتثال المؤسسي، فإن برنامج الامتثال والأخلاقيات الناجح يتطلب مشاركة ودعم كل فرد في المؤسسة. وأشار إلى أنه "عندما تجمع بين النظرة السلبية نسبيًا للعمل مع نهج منتج العمل - الحد الأدنى القابل للتطبيق، فإن الإضافات التي يعتمد عليها المتخصصون في الامتثال والأخلاقيات للتأكد من أن الأشخاص يثيرون المشكلات غالبًا ما تختفي[22]..."

هذا صحيح بالتأكيد بالنسبة لبرنامج إدارة مخاطر الاحتيال. قد يقوم الموظفون بختم الموافقات والمعاملات أو يتجاهلون الحالات الشاذة، أو قد يصعدون حالة شاذة فقط ليجدوا أن مدير المستوى التالي قد تجاهلها لأنهم استقالوا بهدوء.

يمكن للتدقيق الداخلي فحص استطلاعات رضا الموظفين، ومعدلات الدوران، ومقابلات الخروج للتعرف على المشاكل في مشاركة الموظف. قال دومينكيز إنه يمكن مقارنة الاتجاهات الحديثة بالنشاط قبل الوباء لفهم التأثير الذي قد يكون له .

[19] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[20] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[21] "Is Quiet Quitting Real?" Jim Harter, Gallup Workplace, September 6, 2022.
[22] "Why 'Quiet Quitting' Could Harm Ethics and Compliance Functions," Lisa Beth Lentini Walker, *Corporate Compliance Insights*, September 14, 2022.

# الخاتمة

**ما الذي يضيفه كل هذا؟** وفقًا لـ*ACFE* ، تخسر المؤسسات ما يقدر بـ 5٪ من الإيرادات بسبب الاحتيال كل عام، بمتوسط خسارة 117000 دولار ومتوسط خسارة 1.783000 دولار. عادةً، يمكن أن يبلغ متوسط خسائر مخطط الاحتيال 8300 دولار شهريًا. هذه اعتبارات جدية لأي منظمة.

وأثناء أسوأ حالات الوباء ومنذ ذلك الحين، لجأت المنظمات إلى المدققين الداخليين لمساعدة صانعي القرار الاستراتيجيين في إعادة تقييم العمليات التشغيلية وتحسينها. يجب أن تستمر هذه الممارسة، لا سيما في تقييم الضوابط الداخلية لمكافحة الاحتيال. ربما يكون العالم قد خرج من الوباء، لكنه لم يتخلص بالضرورة من تهديدات الاحتيال المرتبطة بالوباء.

منذ أن بدأ الوباء، كان هناك تقدير أكبر للمساهمات التي يمكن أن يقدمها التدقيق الداخلي في تخفيف أو وقف الاحتيال. في الماضي، كان التدقيق الداخلي يأتي غالبًا بعد وقوع حادث احتيال بالفعل. هذا يتغير. من غير المرجح الآن أن تنتظر المؤسسات للكشف عن الاحتيال وتأمل في معالجته قبل حدوث الكثير من الضرر. وللمساعدة في تحقيق ذلك، فإنهم يقومون بإشراك المدققين الداخليين في محادثات قائمة على المنع، وبعبارة أخرى، يطلبون منهم التفكير في ضوابط مكافحة الاحتيال قبل حدوث الاحتيال، على حد قول دومينكيز. يعمل التدقيق الداخلي أيضًا على تسهيل المناقشات حول تقييم مخاطر الاحتيال وأطر تقييم مخاطر الاحتيال، مع الأخذ في الاعتبار تواتر وفعالية تلك التقييمات واختبارات الرقابة، وملاحظة أي تغييرات في ملف تعريف المخاطر المستمر للشركة. قال دومينكيز: "بدلاً من انتظار اكتشاف الاحتيال، يتجه المدققون الداخليون إلى الجانب الوقائي."

## عن معهد المدققين الداخليين (IIA)

معهد المدققين الداخليين *(IIA)* هو جمعية مهنية دولية غير ربحية تخدم أكثر من 230 ألف عضو عالمي وقد منحت أكثر من 185000 شهادة مدقق داخلي معتمد *(CIA)* في جميع أنحاء العالم. تأسس معهد المدققين الداخليين *(IIA)* في عام 1941، وهو معترف به في جميع أنحاء العالم باعتباره الرائد في مهنة التدقيق الداخلي في المعايير والشهادات والتعليم والبحث والإرشاد الفني. لمزيد من المعلومات، قم بزيارة *theiia.org*.

## تنويه



## حقوق النشر



نيسان 2023

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام الأستاذ ناجي فياض

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101