١٣
مارس ٢٠٢٢

مجلة المنصة

مجلة
منصة المراجعة الداخلية

شراكة معرفة تطوير

منصة المراجعة الداخلية
Internal Audit Platform

مقال

المراجعة الداخلية على ضوابط إدارة الهوية والوصول: المتطلبات والإرشادات

جمع وتلخيص وكتابة

محمد قيس عادل القنبري

moh.ali_std@academy.edu.ly

شراكة معرفة تطوير

أصبحت عملية تبادل البيانات والمعلومات تتم على نطاق واسع بفضل انتشار التجارة الإلكترونية، والاعتماد على تقنيات الحوسبة السحابية (Cloud Computing) وغيرها من تقنيات أحدث لنشر البيانات عبر الإنترنت، وازدادت حاجة المستخدمين من خارج الشركة إلى الوصول للبيانات والمعلومات، وبالتالي كان من الواجب على الشركات ضمان أن يتم هذا الوصول بشكل أمن، من خلال وضع ضوابط معينة (Dhamdhere & Karande, 2017). تُسمى الضوابط ذات الصلة بالوصول إلى البيانات بإدارة الهوية والوصول Identity and Access Management (IAM).

تتطلب عملية إدارة الهوية والوصول قيام الشركة بتحديد كل شخص وآلة وبرنامج وعملية داخلها، وإنشاء معرّفات رقمية (IDs) وتمليكها إلى كل هؤلاء لضمان مساءلتهم وفق صلاحيات وتفويضات معينة، وباستخدام هذه المعرّفات يمكن لهم الوصول إلى أنظمة وموارد تكنولوجيا المعلومات بالشركة، بعد التأكيد على أنهم من يمتلكون هذه المعرّفات. إن هذه العملية المختصرة في كلمات قليلة لا تتم بالشكل الأمن إلا من خلال صياغة سياسات وتصميم عمليات وتوفير أدوات تضمن ذلك، وبالتنسيق بين إدارة تكنولوجيا المعلومات وإدارة الموارد البشرية ووحدات الأعمال الأخرى داخل الشركة. يحاول الجدول التالي تلخيص عملية إدارة الهوية والوصول (IIA, 2021):

المرحلة	التساؤل	كيف تتم المرحلة؟
الهوية	من أنت؟	بإنشاء معرّفات رقمية للمستخدمين المتمثلين في الأشخاص والآلات والبرامج وأي كيان يحتاج إلى الوصول لأنظمة وموارد الشركة؛ لأداء وظائف معينة حسب طلب صاحب العمل.
التفويض	ماذا يمكنك أن تفعل في هذا النظام؟	بتحديد الأذونات أو التصريح المناسب لكل وظيفة، من خلال التنسيق مع إدارة تكنولوجيا المعلومات (مسؤولي النظام) وصاحب العمل (وحدة الأعمال المستفيدة)، والمستخدمين النهائيين والمشرفين عليهم.
المصادقة	هل أنت من تدعي أنك؟	باستخدام آليات التحكم المختلفة، مثل: كلمات المرور أو رموز الوصول المؤقتة أو البيانات البيومترية* (Biometric data)؛ للتحقق من هوية الكيان الذي يحاول الوصول إلى الأذونات المرتبطة بالمعرّف، وأداء الوظيفية المرتبطة بالحصول على هذه الأذونات.

* تعد بمثابة توقيعات بشرية فريدة يمكن قياسها، مثل: بصمات الأصابع، مسح قزحية العين، طريقة شخص في فعل شيء ما.

إن عملية إدارة الهوية والوصول لم تُترك بِلا أُطر أو إرشادات وتوجيهات من الجهات المتخصصة في تكنولوجيا المعلومات والاتصالات، ومن بين الأطر المستخدمة على نطاق واسع والتي بدورها توفر أوصافاً لعناصر أو ضوابط التحكم المتعلقة بإدارة الهوية والوصول: الإطار القياسي المعنون بأهداف التحكم لتقنيات المعلومات Control Objectives for Information Technologies (COBIT) الصادر عن جمعية المراجعة والمراقبة على نظم المعلومات Information Systems Audit and Control Association (ISACA) عام 2019م، والمكون من عدة أدوات تساعد المديرين على تقليل الفجوة والمخاطر بين نظم المعلومات والاحتياجات الفنية واحتياجات الأعمال الأساسية للشركة. بالإضافة إلى أهم 20 عنصر أو ضابط تحكم في الأمن الحرج (Top 20 Critical Security Controls) الصادرة عن مركز أمان الإنترنت Center for Internet Security (CIS)، وهي مجموعة من الإجراءات الموصى بها للدفاع السيبراني. علاوةً على المنشورات الخاصة بالمعهد الوطني للمعايير والتكنولوجيا(NIST) National Institute of Standards and Technology.

إن إهمال الضوابط المتعلقة بإدارة الهوية والوصول يعني ارتفاع المخاطر ذات الصلة بانتهاكات البيانات، خاصةً في ظل انتشار وتنوع موارد تكنولوجيا المعلومات ومنهجيات الوصول، التي سيؤثر بدوره على الشركة من خلال إلحاق الضرر بسمعتها، ونتائجها النهائية، وإضعاف ثقة المستثمرين فيها (Harel, 2018). لذا كان من الواجب الاهتمام بهذه القضية خاصةً في ظل التشكيلات الجديدة من التقنيات التي توعد بها الثورة الصناعية الرابعة؛ والتي تنذر بزيادة الهجمات السيبرانية وارتفاع المخاطر في هذا الجانب، مما يستدعي من الشركات الناضجة رفع درجة الاستعداد للدفاع والتصدي لأي هجمات من خلال إدارة المخاطر باعتبارها خط الدفاع الثاني، ثم إدارة المراجعة الداخلية التي تعتبر خط الدفاع الثالث.

وفي سياق بناء إطار للممارسات المهنية الدولية International Professional Practices Framework (IPPF) في مجال المراجعة الداخلية، ينشر معهد المراجعين الداخليين Institute of Internal Auditors (IIA)بانتظام أدلة لمراجعة التكنولوجيا العالمية Global Technology Audit Guides (GTAGs)، تحتوي على إرشادات غير إلزامية للمراجعين الداخليين في جميع أنحاء العالم، أي أنها ليست بنفس درجة الإلزام التي تكتسبها مدونة قواعد السلوك (Code of Ethics) أو المعايير الدولية للمراجعة الداخلية، وإنما تساعد المراجعين الداخليين على فهم كيفية تطبيق متطلبات التوجيهات الإلزامية والامتثال لها. من بين هذه الأدلة، دليل بعنوان مراجعة إدارة الهوية الوصول (Auditing Identity and Access Management)، الذي يزود المراجعين الداخليين بالمعرفة اللازمة لأداء خدمات التأكيد والاستشارة المتعلقة بمخاطر وضوابط كُلاً من تكنولوجيا المعلومات Information Technology (IT) وأمن المعلومات Information security (IS).

صدرت الطبعة الأولى من هذا الدليل عام 2009م، ثم صدرت الطبعة الثانية منه في عام 2021م (IIA, 2021). يتكامل هذا الدليل بدوره مع COBIT & Top 20 Critical Security Controlsومنشورات NIST.

أفاد الدليل بأن عناصر أو ضوابط التحكم المتعلقة بإدارة الهوية والوصول يتم تنفيذها في كل طبقة من موارد تكنولوجيا المعلومات، بما في ذلك معدات البنية التحتية للشبكة (Network Infrastructure Equipment)، مثل: المحولات أو المبدلات (Switches)؛ أجهزة التوجيه (Routers)؛ أنظمة إدارة الشبكة (Network Management Systems). مع الخوادم (Servers)، وقواعد البيانات (Databases)، وخدمات البرامج الوسيطة (Middleware Services)، والتطبيقات (Applications). كما أن هذه الضوابط تعتبر القاعدة الأساسية لحوكمة تكنولوجيا المعلومات وتحقيق استراتيجياتها وأهدافها داخل الشركة، ومن أجل جني هذه الفوائد فسيتمثل دور أصحاب المصلحة في ضمان أن ضوابط تكنولوجيا المعلومات، بما في ذلك إدارة الوصول إلى موارد تكنولوجيا المعلومات، مصممة بشكل جيد ويتم تنفيذها بشكل فعّال (IIA, 2021).

أما عن دور المراجعين الداخليين فأشار الدليل إلى أنه يتمثل في دراسة كيفية سيطرة الشركات على الوصول، وفهم أن عمليات المراجعة الداخلية يمكن تطبيقها على مستوى الشركة أو تكون محددة لمورد معين. مع ضرورة أن يعرف المراجعين الداخليين بأن ليس جميع موارد تكنولوجيا المعلومات تحتاج إلى نفس المستوى من الحماية، وأنه لهذا السبب صممت الشركة ضوابط إدارة الهوية والوصول بشكل مثالي بحيث تتناسب مع فئة أمان كل نظام، مع معرفتهم بطبيعة مخاطر الاحتيال ومتطلبات الامتثال التنظيمي ذات الصلة. كما أشار الدليل إلى ضرورة أن يتأكد المراجعين الداخليين من أن الشركة تقوم بتطبيق مبدأ الامتياز الأقل أو مبدأ الحد الأدنى من الامتيازات (Principle of least privilege)، الذي ينص على أن الوصول إلى الأنظمة يقتصر فقط على ما هو ضروري لأداء وظائف الأعمال المصرح بها، أي أن تكون كل وحدة قادرة على الوصول إلى البيانات والمعلومات الملائمة للغرض فقط، وليس الوصول المفتوح لكل البيانات والمعلومات، إلى جانب التحقق من التزام الجميع بهذا المبدأ. قد ينصح المراجعون الداخليون حول كيفية قيام الشركة بزيادة فعالية ضوابط إدارة الهوية والوصول، وبالتالي المساهمة في تقليل المخاطر الأمنية والتنظيمية، وباتباع هذا النهج سيظهر المراجع الداخلي التزاماً بالمعيار رقم (1220) الصادر عن IIA والمعنون ببذل العناية المهنية (IIA, 2021).

وعلى الرغم من أهمية قضية إدارة الهوية والوصول، وضرورة وجود دليل يسترشد به المراجعون الداخليون لمراجعة هذه القضية، إلا أن الدليل الصادر عن IIA واجه بعض الانتقادات، حيث أوصى Marks(2021) معهد المراجعين الداخليين (IIA) بحذف الطبعة الثانية من هذا الدليل، ووضعه جانباً وعدم الأخذ به؛ لأنه رأى أن هذا الدليل وقع في

فخ منشورات المعهد الوطني للمعايير والتقنية (NIST)، أي أن الدليل يتحدث عن أصول المعلومات عندما يجب الحديث عن التأثير المحتملة لقضية إدارة الوصول على الأعمال التجارية. علاوةً على أن الدليل اختزل إدارة الوصول في تحديد من يمكنه الوصول إلى أنظمة المعلومات والبيانات فقط، في حين أن الوصول يشمل حتى الوصول إلى المخزون والمرافق والأشخاص والمعدات. هنا يرى الباحث أن القول بأن IIA وقع في فخ NIST قد لا يعتبر صحيحاً؛ لأن دليل مراجعة إدارة الهوية والوصول أشار في ملخصه التنفيذي أنه سيُركّز على وصول المستخدم إلى موارد تكنولوجيا المعلومات، التي يُشار إليها أحياناً باسم الوصول المنطقي، وأنه لا يتطرق إلى إدارة الوصول المادي. كما أن ذلك واضحاً من خلال تتبع السلسلة التي يندرج تحتها هذا الدليل، وهي GTAGs. أما فيما يتعلق بإهمال قضية إدارة الوصول على حساب الحديث عن أصول المعلومات، فإن الباحث يتفق مع Marks في أن هذه القضية لم تُعالج بالصورة الواضحة التي تبين للمراجعين الداخليين المخاطر المتعلقة بها وما يجب عليهم القيام به تجاه هذه المخاطر. مع افتقار الدليل لأي إرشادات توضح كيف يتم تخطيط عملية المراجعة الداخلية التي تشمل التحقق من إدارة الهوية والوصول (وليس منفصلة) بناءً على المجالات التي تمثل مخاطر عالية في هذا الجانب، بحيث يستطيع المراجعون الداخليون إضافة قيمة فعلاً. كما لم يُحدد الدليل حسب وجهة نظر Marks المكان الذي تقع فيه إدارة الوصول مقابل المصادر الأخرى لمخاطر الأعمال؛ للمساعدة في تحديد النطاق التفصيلي لأي عملية مراجعة داخلية. بالإضافة إلى أن الدليل ترك الكثير من التساؤلات بدون إجابة، على سبيل المثال لا الحصر: ما هو الوصول الذي يجب أن يكون محدوداً، ولماذا؟ حتى يتمكن المراجعين الداخليين من التركيز على ما يهم الشركة. ما هي آلية تغيير الوصول في الوقت المناسب حسب تغير احتياجات الفرد (بالنقل أو الإنهاء مثلاً). واختتم Marks انتقاده بأن النقطة الأساسية هي أن أي عملية مراجعة داخلية يجب أن تعتمد في تصميمها وتنفيذها على مستوى مخاطر العمل، وليس على معيار عام أو قائمة معينة لأصول المعلومات.

في هذا الصدد، يوجّه الباحث المراجعين الداخليين إلى المقالات التي تناولت مراجعة إدارة الهوية والوصول لتغطية أي نقص في الدليل الصادر عن IIA. فمثلاً مقال Harel (2018) استعرض قائمة مختصرة تتضمن ما يجب أن يتحقق منه المراجعين الداخليين فيما يتعلق بإدارة الهوية والوصول، يأتي في مقدمتها أنهم بحاجة إلى التحقق من قيام الإدارة بوضع نهج شامل أو سياسة أمنية واضحة تختص بإدارة الهوية والوصول، مع التأكد من قيامها بإضفاء الطابع الرسمي عليها ومراجعتها وتنقيحها على فترات منتظمة وبمشاركة جميع الأطراف ذات العلاقة. فضلاً عن التحقق من شمول هذه السياسة لقائمة بأدوار كل فرد أو آلة أو برنامج أو عملية، مع تحديد الصلاحيات والسلطات والإجراءات والوقت المطلوب لكل منهم فيما يتعلق بإكمال المهام

المنوطة بهم، وبمراعاة التغير المستمر في المهام المكلفين بها. يحتاج المراجعون الداخليون أيضاً إلى التحقق من أن الامتيازات التي تُمنح بشكل مؤقت للمستخدمين يتم إلغاؤها بعد انتهاء الفترة المؤقتة، حتى لا يكون لدى بعض المستخدمين امتيازات غير مناسبة، مما يترك باب الموارد التكنولوجية التي لا ينبغي الوصول إليها مفتوحاً على مصراعيه.

بالإضافة إلى ما تقدم، ينبغي أن يتحقق المراجعين الداخليين من قيام الإدارة بتقسيم المهام الحرجة إلى مهام أصغر متعددة، وفق مبدأ الفصل بين الواجبات أو المهام المتعارضة Segregation of duties (SoD)، بحيث لا يتحكم شخص واحد في العملية بأكملها. فحتى في حالة حدوث فشل في أمن الهوية، لن يتمكن المهاجم من الوصول إلى العملية أو البيانات بأكملها. قد يتحقق المراجعون الداخليون من الحسابات العامة للمستخدمين في حالة قيام الشركة بإعداد حسابات مستخدمين عامة على شبكتها، حيث تمثل هذه الحسابات مخاطر أمنية في حال كانت كلمات المرور ضعيفة، فبمجرد تمكن المهاجم من معرفتها سيصل إلى موارد الشركة باستخدام الإعدادات الافتراضية. من الضروري التأكد من قيام الشركة بمراجعة وحذف أي حسابات عامة لم تعد ضرورية، مع تعيين كلمات مرور قوية مثلاً. ولا تقتصر عملية مراجعة وحذف الحسابات على الحسابات العامة، فيجب أن تشمل أي حسابات غير نشطة حتى لا تتراكم ويُستغل خمولها في خرق البيانات. واختتم Harel مقاله بضرورة أن يحتفظ المراجعين الداخليين بالوثائق ذات الصلة بإدارة الهوية والوصول، مثل: وثيقة سياسة إدارة الهوية والوصول، والوثائق التي تعدها إدارة المخاطر في هذا السياق.

في الحقيقة، أن كل ما ورد في مقال Harel تم تضمينه في الدليل، ولكن ما يُعاب على الدليل هو أنه لم يكن واضحاً في تبيان ما يجب أن يقوم به المراجعين الداخليين، وكأنه اعتمد على مهارات هؤلاء المراجعين في استنباط الإجراءات والمهام والأنشطة التي سيؤدونها من خلال تحليل محتوى الدليل وربطه بما ورد في المعايير الدولية للمراجعة الداخلية الصادرة عن IIA. ربما ما يؤكد هذا القول هو الإشارة الصريحة من قبل IIA إلى أن الأدلة الصادرة عنه تعد إرشادات غير إلزامية، يُستعان بها في تطبيق المعايير.

أخيرا، يرى الباحث أنه من الضروري وضع برنامج مراجعة داخلية قائم على مخاطر إدارة الهوية والوصول سواءً التي تمت الإشارة إليها ضمنيًّا في الدليل، أو المخاطر الأخرى التي لم يتم الإشارة إليها، وهذا ما نص عليه المعيار رقم (2120) المعنون بإدارة الخطر، مما يتطلب بدوره من المراجعين الداخليين الوصول إلى مستوى معين من الفهم لبنية تكنولوجيا المعلومات والاتصالات داخل الشركة وخارجها، وتحسين مهاراتهم في هذا الجانب، وهو ما نص عليه المعيار رقم (1230) المعنون بالتطوير المهني المستمر. كما يوصي الباحث بأن يكون المراجعين الداخليين في اطلاع دائم على التشريعات في الدولة التي يعملون بها، ففي حال شملت التشريعات الحالية أو المستقبلية جوانب متعلقة بإدارة الهوية والوصول، فإنه من الضروري التحقق من مدى امتثال والتزام الشركة لأحكامها. أي يتأكد المراجعون الداخليون أينما كانوا من امتثال الشركة لكل ما يتعلق بإدارة الهوية والوصول سواءً في التشريعات النافذة أو المعايير المحلية أو الدولية.

المراجع

1. Dhamdhere, M. & Karande, S. (2017). Identity and access management: concept, challenges, solutions. *International Journal of Latest Trends in Engineering and Technology*, 8(1): 300-308. DOI: 10.21172/1.81.039
2. Harel. O. (2018). 8 steps for a complete IAM system audit. https://blog.plainid.com/8-steps-iam-system-audit-checklist Accessed on 1 March 2022.
3. IIA. (2021). Auditing identity and access management. 2nd Edition. Florida, United states.
4. Marks, N. (2021). Some thoughts on auditing identity and access management. https://internalaudit360.com/some-thoughts-on-auditing-identity-and-access-management/ Accessed on 19 December 2021.