التدقيق الداخلي

العدد 2
آذار / مارس 2016

جمعية التدقيق الداخلي الأردنية
JORDAN INTERNAL AUDIT ASSOCIATION

التدقيق الداخلي

جمعية التدقيق الداخلي الأردنية
JORDAN INTERNAL AUDIT ASSOCIATION

العدد ٢
آذار / مارس ٢٠١٦

كلمة العدد

الزميلات والزملاء

أشكركم بإسمي وبإسم كافة أعضاء الهيئة التأسيسية على إيمانكم برسالة الجمعية وعلى دعمكم منقطع النظير لها منذ إنشائها في أيلول 2015، ويسرني أن اعلمكم بأن عدد أعضاء الجمعية تجاوز 100 عضو في أقل من ستة أشهر. هذا كما أنها الآن تحظى بدعم من شركات ومؤسسات أردنية عريقة، مما يدل على ثقتهم بجمعيتكم وبرسالتها وأهدافها.

ومن أهم النشاطات والإنجازات التي قمنا بها خلال الفترة الماضية هي توقيع مذكرة تفاهم مع زملائنا بجمعية المدققين الداخليين في لبنان IIA-Lebanon للتعاون في مجال التدريب وتبادل الخبرات، حيث سيتمتع أعضاء جمعيتنا بالأولوية وبالأسعار التفضيلية لأي نشاطات تدريبية مهنية في لبنان. وعلى هامش مؤتمر رؤساء التدقيق الداخلي في دبي تم الاجتماع مع زملائنا رؤساء جمعيات المدققين والمراجعين من الإمارات العربية، والسعودية، وقطر، وسلطنة عمان، والجزائر، وفلسطين ، ومصر، كما تم الاتفاق على إنشاءالمجمع العربي للمدققين الداخليين العرب وذلك بهدف رفع مستوى مهنة التدقيق الداخلي في الوطن العربي وزيادة الوعي بها.

أما بالنسبة لرؤية الجمعية وخطة عملها في الأعوام القادمة فهي على اتساق تام مع الرؤية والإستراتيجية الوطنية التي تم رسمها في وثيقة الأردن #2025، حيث تتفق أهداف الجمعية مع رؤية الأردن #2025 في مسارات الرؤية المختلفة وخاصة مسار "قطاع خاص ديناميكي ومنافس عالمياً"، ومسار "حكومة ذات كفاءة وفاعلية".

وعند مراجعتنا لهذين المسارين نلاحظ أن أهم الأولويات هي تحديث التشريعات المتعلقة بالتدقيق والرقابة المالية لتتماشى مع أفضل الممارسات الدولية وإقرار برنامج جديد خاص بالمدقق الداخلي للنظام العام، ونشر ممارسات الحوكمة والشفافية وعقد ورش عمل توعوية بمضامين الحوكمة والشفافية، ووضع وتبني سياسات وبرامج للحوكمة الرشيدة وتضمينها في التشريعات ذات العلاقة تمهيداً لتطبيقها في القطاعين العام والخاص، ومتطلبات المجتمع المدني بحيث تصبح ثقافة مجتمعية ومؤسسية.

أما المبادرات ذات الأولوية في قطاع الأعمال فمن أهمها تطوير قانون الشركات ليواكب أفضل الممارسات العالمية وتطبيق دليل قواعد حوكمة الشركات بشكل إلزامي من خلال القانون، وتعديل قانون الأوراق المالية بما يتفق مع أفضل الممارسات والمعايير الدولية. وبلا شك فإن هذه المبادرات تعتبر ثورة ونقلة نوعية في سوق الأعمال الأردني. ويشكل التدقيق الداخلي عاملاً حيوياً في هذين المسارين لكونه أحد أهم ركائز ودعائم الحوكمة الرشيدة.

أما على الصعيد العالمي، فإن هذه الأوقات مميزة لمهنة التدقيق الداخلي من حيث التغييرات والتحديثات المقترحة للمعايير الدولية للممارسة المهنية للتدقيق الداخلي (المعايير). ومن هنا ندعوا أعضائنا للمشاركة وإبداء الرأي والملاحظات على هذه التغييرات مع مراعاة أن باب استقبال الملاحظات سيقفل في تاريخ 30 نيسان 2016 .
وستضم سنة 2016 عدة نشاطات وفعاليات منها التدريبية وورش العمل التي تتفق مع رؤية التدقيق الداخلي نحو #2025 والتي سيتم الإعلان عنها بشكل دوري على مدار العام من خلال وسائل التواصل الاجتماعي، بالإضافة للتواصل مع الجهات المعنية لتطوير المهنة ورفع مستوى الوعي والاهتمام بالمهنة.

فكونوا معنا في رحلة التدقيق الداخلي نحو #2025

هشام الشوا
رئيس هيئة الإدارة

"It's complicated. That's why we're bringing in BDO."

BDO Advisory Services

BDO's advisory professionals provide high-level strategic guidance to clients when they need it most. From litigation and dispute resolution, to business restructuring and risk management, our wide-ranging service offerings help clients navigate challenges and strengthen their businesses – whatever their needs may be.

Audit | Tax | Advisory | Internal Audit
www.bdo.com.jo

BDO

■ باسم حجاز ■ أيمن عبدالرحيم ■ عاصم الناصر ■ مازن شحادة ■ أمجد البيايضة

يمكنكم التواصل مع فريق إعداد النشره عبر البريد الإلكتروني jia.newsletter@gmail.com

أولاً: القيمة المضافة للتدقيق الداخلي:

وفقا لتعريف التدقيق الداخلي فإن التدقيق الداخلي يسعى لإضافة قيمة للمنشأة، ويختلف ممارسي التدقيق حول العالم بطرق إضافة القيمة، إلا أن التعقيد المتزايد في عالم الأعمال المتواجد في عالم مترابط يعني أن هناك تزايد في الطرق التي يستطيع من خلالها المدققين الداخليين تحقيق قيمة لمنشآتهم. وفقاً لتقارير الإطار المعرفي العام أو فيما يعرف بال "CBOK" تم إجراء مسح عالمي لممارسي المهنة بما يقدم نظرة شاملة على أنشطة وخصائص المدققون الداخليون في جميع أنحاء العالم. حيث شارك في المسح 14,500 ممارس لمهنة التدقيق الداخلي من 166 دولة حول العالم. وقد كانت إجابات المشاركين حول السؤال الخاص باختيار أنشطة التدقيق الداخلي التي تحقق أكبر قيمة للمنشأة كما هو موضح في الجدول المقابل، مع العلم بأن السؤال كان موجه لرؤساء التدقيق التنفيذيين، حيث شارك في الإجابة 2,636 رئيس تنفيذي للتدقيق.

#	الأنشطة المختارة من قبل الرؤساء التنفيذيين لإضافة قيمة للمنشأة	نسبة الاختيار
1	تقديم ضمان كفاية وفعالية نظام الرقابة الداخلية	86٪
2	التوصية بتحسين الأعمال	55٪
3	تقديم ضمان حول عمليات إدارة المخاطر في المنشأة	53٪
4	تقديم ضمان حول الامتثال التنظيمي	50٪
5	إبلاغ وتقديم المشورة للإدارة	40٪
6	تحديد المخاطر الناشئة (Emerging risks)	37٪
7	تقديم ضمان حول عمليات الحوكمة بالمنشأة	37٪
8	التحقيق أو ردع الغش	29٪
9	إبلاغ وتقديم المشورة للجنة التدقيق	28٪
10	اختبار تقييمات الإدارة للمخاطر	23٪

في عام 2010 قدمت جمعية التدقيق الداخلي مقترح لقيمة التدقيق الداخلي (Value Proposition for Internal Auditing) حيث تم وصف قيمة التدقيق الداخلي بأنها مزيج من ثلاثة مكونات (عناصر) وهي تقديم الضمان والبصيرة والموضوعية. الأنشطة التي تم اختيارها من قبل الرؤساء التنفيذيين للتدقيق الداخلي لإضافة قيمة للمنشأة (في الجدول أعلاه) تنسجم تماما مع تلك المكونات الثلاثة ، بل يمكن أيضا ربط تسعة أنشطة مباشرة مع تلك المكونات الثلاثة كما يلي:

المكونات الثلاثة	وصف المكونات	الأنشطة المختارة من قبل الرؤساء التنفيذيين
تقديم الضمان	تقديم ضمان حول الحوكمة والخطر والرقابة، حيث يقدم التدقيق الداخلي ضمان حول حوكمة المنظمة وإدارة المخاطر وعمليات الرقابة لمساعدة المنظمة في تحقيق أهدافها الاستراتيجية والتشغيلية والمالية والامتثال.	1-تقديم ضمان كفاية وفعالية نظام الرقابة الداخلية 86٪ 3- تقديم ضمان حول عمليات إدارة المخاطر في المنشأة 53٪ 4- تقديم ضمان حول الامتثال التنظيمي 50٪ 7- تقديم ضمان حول عمليات الحوكمة بالمنشأة 37٪
البصيرة	البصيرة في التحفيز والتحليل والتقييم، حيث يقدم التدقيق الداخلي الحافز لتحسين كفاءة وفعالية المنشأة من خلال تقديم رؤية وتوصيات تستند على تحليل وتقييم البيانات والأعمال.	2- التوصية بتحسين الأعمال 55٪ 6- تحديدالمخاطر الناشئة (Emerging risks) 37٪
الموضوعية	الموضوعية وتشمل النزاهة والمساءلة والاستقلالية، عن طريق الالتزام بالنزاهة والمساءلة يقدم التدقيق الداخلي قيمة لهيئات الحوكمة والإدارة العليا كمصدر موضوعي للمشورة المستقلة.	5- إبلاغ وتقديم المشورة للإدارة 40٪ 8- التحقيق أو ردع الغش 29٪ 9- إبلاغ وتقديم المشورة للجنة التدقيق 28٪

ثانياً: اتجاهات ناشئة ستواجه التدقيق الداخلي

يمكن للمدققين الداخليين توقع التطورات المستقبلية من خلال النظر إلى ما هو أبعد من الوضع الحالي لأعمال منشأتهم.

عندما يكون التغيير مستمر، فإنه من الصعب توقع المستقبل. إلا أنه، وبشكل عام، هنالك اتجاهات ناشئة واضحة ستواجه المدققين الداخليين خلال الخمس أو العشر سنوات القادمة وهي: بيئة المخاطر المتقلبة، تزايد الفحوصات التنظيمية، وارتفاع توقعات أصحاب المصلحة، ومخاطر التكنولوجيا المعقدة، والتنافس على أفضل مواهب التدقيق. قد لا يكون المدققون الداخليون قادرين على تنبؤ كيف يمكن لهذه الاتجاهات الخمسة أن تتغير على المدى الطويل، ولكن التتبع الحالي للطريقة التي تتطور فيها تلك الاتجاهات يساعد التدقيق الداخلي للاستعداد لما هو قادم.

التغييرات المقترحة على المعايير الدولية. ما هي التغييرات المقترحة وما طبيعتها ؟

مقدمة:

كثُر الحديث في الآونة الأخيرة عن التحديثات في الإطار المهني الدولي للممارسة المهنية للتدقيق الداخلي وما واكبه من تعديلات في المعايير، وقد رأيت أن أوجز في هذا المقال مجمل التعديلات المقترحة على المعايير الدولية بحيث يمكن لأي مهتم أن يرجع بسهولة لهذه التعديلات ويأخذ فكرة واضحة ومجملة عنها.

كنّا قد أشرنا في العدد السابق من المجلة أن معهد المدققين الداخليين الدولي قد أقرّ تحديث الإطار المهني الدولي للممارسة المهنية للتدقيق الداخلي (IPPF)، وهو إطار يحتوي على مجموعة تصورات ومفاهيم تنظّم الإرشادات الصادرة عن معهد المدققين الداخليين (وهي الرسالة والمبادئ الأساسية والتعريف والمعايير وأخلاقيات المهنة والإرشادات التطبيقية والإرشادات التكميلية)، وقلنا أنه لا بد من إحداث بعض التغييرات الجوهرية في المعايير لتنسجم مع الإطار الدولي الجديد وما يحتويه من مبادئ ورسالة جديدة، بالإضافة لذلك فإن المعهد يقوم بشكل دوري بمراجعة المعايير الدولية ويقترح تعديلات لتنسجم مع التغييرات الحاصلة في المهنة وبيئة الأعمال الخارجية، حيث كان آخر تعديل على المعايير في عام 2013. وبناءً عليه فقد قام المعهد الدولي بنشر استطلاع آراء لجميع المدققين الداخليين والمهتمين في هذا الشأن لحصر الملاحظات ومدى قبول أو رفض هذه المقترحات، وسينتهي الاستطلاع بتاريخ 30 آبريل 2016.

والسؤال المهم حالياً هو ما هي التغييرات المقترحة في المعايير وما طبيعتها؟

يمكن تصنيف التغييرات المقترحة في معايير التدقيق الداخلي إلى عدة أقسام كالتالي:

أولاً: معايير جديدة كلياً وتشمل:

1. إضافة معيار جديد رقم 1112 بخصوص دور الرئيس التنفيذي للتدقيق خارج إطار التدقيق الداخلي: فقد تم إضافة معيار أنه عندما يكون للرئيس التنفيذي للتدقيق الداخلي أي دور أو مسؤولية تقع خارج إطار التدقيق الداخلي كالمسؤولية عن الالتزام أو المسؤولية عن إدارة المخاطر ، أو عندما يتوقع حدوث هذا الدور، فيجب أخذ الاحتياطات اللازمة لتقليل حجم التأثر السلبي على الاستقلالية والموضوعية. وبالتالي تم طرح هذا المعيار بحيث يتم أخذ الاحتياطات للتعامل مع التأثيرات السلبية المحتملة، مثل عمل تقييم دوري للتبعية والمرجعية للتدقيق الداخلي والمسؤوليات المناطة به، واستحداث إجراءات بديلة للحصول على تأكيدات بخصوص مجالات المسؤوليات الإضافية.

2. إضافة معيار جديد كلياً برقم 1130 ت3 بخصوص تقديم خدمات توكيد لمجالات خضعت سابقاً لخدمات استشارية: حيث لم يتطرق المعيار السابق إلى تقديم خدمات التأكيد بعد الخدمات الاستشارية، فأجاز المعيار الجديد للمدقق الداخلي تقديم مثل هذه الخدمات بشرط ألا تكون الخدمات الاستشارية قد أثّرت سلباً على الموضوعية وبشرط أن يتم التعامل بطريقة مناسبة مع الموضوعية الفردية عند تخصيص الموارد اللازمة للمهمة الجديدة.

جدول يلخص أهم التعديلات التي حدثت على المعايير

رقم المعيار	موضوع المعيار	توضيح
1112	دور الرئيس التنفيذي للتدقيق خارج إطار التدقيق الداخلي	معيار جديد
1130	تقديم خدمات توكيد لمجالات خضعت سابقاً لخدمات استشارية	معيار جديد
1320	برنامج تأكيد وتحسين الجودة	تعديل المعيار
1312	برنامج تأكيد وتحسين الجودة	تعديل المعيار
2000	فعالية إدارة التدقيق الداخلي	تعديل المعيار
2050	التنسيق مع الأطراف الأخرى	تعديل المعيار
2060	رفع التقارير إلى الإدارة العليا والمجلس	تعديل المعيار
2410	معايير التبليغ	تعديل المعيار

ثانياً: تعديل المعايير لتنسجم مع المهمة والمبادئ الأساسية الجديدة: حيث أن العديد من المعايير كانت تُشير إلى مكونات الإطار المهني القديم ولم تلتفت إلى رسالة التدقيق الداخلي الجديدة والمبادئ الأساسية الحديثة، فتم تعديل جميع هذه المعايير لتنسجم مع الإطار المهني الجديد. من جهة أخرى تم عمل بعض التعديلات الطفيفة على صياغة العديد من المعايير ومن ضمنها تعديل المقدمة لتوضيح هذه المعايير بشكل أفضل.

ثالثاً: تعديلات في فهرس تعريف المصلحات: حيث تم إحداث تغيير جوهري في تعريف المجلس فقد ألغت التعديلات الاقتراح الذي كان يشير إلى "رأس المنشأة" كبديل مقبول لمجلس مستقل، فقد تم إضافة عبارة أن المجلس يشمل عادة أعضاء ليسوا جزءاً من الإدارة وليس مكوّناً بالكامل من أعضاء من الإدارة. وفي حال عدم وجود مثل هذا المجلس فإن كلمة مجلس في المعايير تشير الى شخص أو مجموعة مكلّفة بالحوكمة.

وتم أيضا تعريف المبادئ الأساسية للممارسة المهنية للتدقيق الداخلي (المبادئ الأساسية) بأنها العناصر الأساسية التي تصف فاعلية التدقيق الداخلي وأنها تدعم وتعزّز ميثاق أخلاقيات المهنة والمعايير.

شملت التعديلات على المعايير تعريف المبادئ الأساسية للممارسة المهنية للتدقيق الداخلي (المبادئ الأساسية) بأنها العناصر الأساسية التي تصف فاعلية التدقيق الداخلي وأنها تدعم وتعزّز ميثاق أخلاقيات المهنة والمعايير.

رابعاً: تعديلات على معايير سابقة، نوجز أهمها كالتالي:

1. تعديل تفسيرات المعيار رقم 1312 وتعديل المعيار رقم 1320 الخاص ببرنامج ضمان وتحسين الجودة: حيث تم إضافة العديد من التعديلات التي تزيد من بساطة ووضوح هذا المعيار، فقد تم إضافة عبارة أنه في حالات التقييمات الخارجية لجودة التدقيق الداخلي أصبح إلزامياً على المراجع الخارجي للجودة أن يتوصل إلى قرار بخصوص التقيّد بالمعايير، ويمكن أن يُضمِّن استنتاجاته تعليقات عملية أو استراتيجية. وتم إضافة عبارة أنه يجب على الرئيس التنفيذي للتدقيق الداخلي أن يشجع مشاركة مجلس الإدارة في برنامج تأكيد وتحسين الجودة. وتم تفصيل طبيعة الإفصاحات لنتائج التقييم التي يجب على الرئيس التنفيذي للتدقيق أن يرفعها إلى الإدارة العليا ومجلس الإدارة وتشمل: نطاق ووتيرة التقييم الداخلي والخارجي، واستنتاجات المراجعين، والخطط التصحيحية، ومؤهلات واستقلالية المراجع أو فريق المراجعة وتضارب المصالح المحتمل.

2. تعديل تفسير المعيار 2000 المتعلق بفعالية إدارة نشاط التدقيق الداخلي: فمن أجل إظهار المبادئ الاساسية الجديدة بشكل أوضح ، مثل محاذاة العمل مع استراتيجيات و أهداف و مخاطر المؤسسة؛ وإعطاء تأكيدات مبنية على المخاطر؛ والتمتع بنظرة ثاقبة واستباقية وتركز على المستقبل، تم إضافة عبارة أن يأخذ نشاط التدقيق بالاعتبار الاتجاهات الشائعة والقضايا الناشئة التي يمكن أن تؤثر في فعالية نشاط التدقيق الداخلي، ويضيف نشاط التدقيق الداخلي قيمة للمنشأة والأطراف المعنية عندما يأخذ في الاعتبار الاستراتيجيات والأهداف والمخاطر ويَجهد لتوفير سبل تحسين مسارات الحوكمة وإدارة المخاطر والرقابة وتقديم تأكيدات ذات صلة بطريقة موضوعية.

3. تعديل المعيار رقم 2050 والمتعلق بالتنسيق مع الأطراف الأخرى: فتم إضافة كلمة " الاعتماد " إلى جانب التنسيق وتم إضافة عبارات عدة أهمها أنه يمكن للرئيس التنفيذي للتدقيق الاعتماد على جهات أخرى تُقدِّم خدمات تأكيد أو خدمات استشارية وأنه يجب تأسيس مسار ثابت ومتسق للأسس الواجبة للاعتماد على عمل الآخرين. ويجب على الرئيس التنفيذي للتدقيق أيضاً أن يكوّن فكرة واضحة عن نطاق وموضوعية ونتائج العمل المنجز من قبل الجهات الأخرى، وأنه عند الاعتماد على عمل جهات أخرى فإن الرئيس التنفيذي للتدقيق يبقى مسؤولاً وعرضة للمحاسبة عن تأمين الدعم الكافي للاستنتاجات والآراء التي توصّل اليها نشاط التدقيق الداخلي.

4. تعديل المعيار رقم 2060 والمتعلق برفع التقارير إلى الإدارة العليا والمجلس: حيث تم تحديد الأمور التي يجب أن تتضمنها تقارير ومراسلات الرئيس التنفيذي للتدقيق الداخلي إلى الإدارة العليا ومجلس الإدارة وهي كالتالي: ميثاق التدقيق الداخلي، واستقلالية نشاط التدقيق الداخلي، وخطة التدقيق وتقدم سير العمل بها، والموارد اللازمة، ونتائج عمليات التدقيق، ومدى التقيّد بالمعايير والخطط الموضوعة لتصحيح أي خلل جوهري في موضوع التقيّد، والمخاطر المقبولة من الإدارة والتي قد تكون غير مقبولة للمنشأة.

5. تعديل معيار رقم 2410 المتعلق بمعايير التبليغ: حيث تم إضافة أن التبليغات يجب أن تتضمن أهداف المهمة ونطاق المهمة ونتائجها. وتم تفصيل ما يجب أن يتضمنه التبليغ النهائي لنتائج المهمة بأنها الاستنتاجات القابلة للتطبيق، ويجب أن تتضمن أيضاً التوصيات و/أو خطط العمل ذات الصلة. وتم إضافة أنه حينما يكون ذلك مناسباً فإن رأي المدققين الداخليين يجب أن يكون موجوداً. فتم توضيح أنه ليس من الضروري دائماً تضمين التوصيات وخطط العمل في تبليغات المهمة، وعليه فإن "و/أو" تستعمل للإشارة أن أحدهما أو كلاهما مقبول.

تجدر الإشارة إلى أن التحديثات المقترحة على المعيار ستكون جاهزة للاعتماد من أكتوبر 2016 وبالإمكان البدء بالالتزام بها بشكل اختياري، ولكن ستكون مُلزمة ابتداءً من يناير 2017، وللعلم فإن هناك جهاز إشرافي في معهد المدققين الداخليين الدولي يقوم بمراجعة كامل عملية الاستقصاء والتأكد من اكتمالها والالتزام بما تم التوصل اليه.
فيما يلي هنا الإطار الزمني والخطوات القادمة للتغييرات المقترحة على المعايير:

التواريخ	النشاط
1 فبراير- 30 آبريل 2016	فترة المراجعة والتغذية الراجعة
مايو – سبتمبر 2016	مراجعة التعليقات واعتماد التغييرات النهائية
1 أكتوبر 2016	الإعلان عن المعايير المُعدّلة
1 يناير 2017	ستصبح المعايير الجديدة والمُعدّلة إلزامية

في النهاية، ينبغي على المدققين الداخليين أن يُتابعوا ويتفاعلوا مع الاستقصاءات التي يتم إصدارها من معهد المدققين الداخليين الدولي أولاً بأول لإحداث التغيير الإيجابي المطلوب، وينبغي أن يتم تحديث أوراق وأنظمة التدقيق الداخلي بالمعايير الجديدة ونشرها وتعريف الإدارة العليا والموظفين بها، وهذا له أثر كبير في نشر الوعي بأن أدبيات التدقيق الداخلي متغيرة بتغيّر المحيط الداخلي والخارجي وبأن نشاط التدقيق الداخلي في المنظمة متفاعل مع التغييرات في المهنة ويحرص على متابعة كل ما هو جديد في عالم التدقيق الداخلي.

للتعليق على المقال الرجاء مراسلة الكاتب على البريد الإلكتروني: mrbasem1@hotmail.com

فيما يلي نعرض لكم بعض نتائج الإحصائيات التي شملتها تقارير الإطار المعرفي العام (CBOK) التي تضمنت استطلاع رأي (14518) شخص معني بمهمة التدقيق الداخلي حول العالم والتي صدرت مؤخرا عن معهد المدققين الداخليين:

أهم الكفاءات التي يجب أن يمتلكها المدققين الداخليين:

المصدر: CBOK – Mapping Your Career

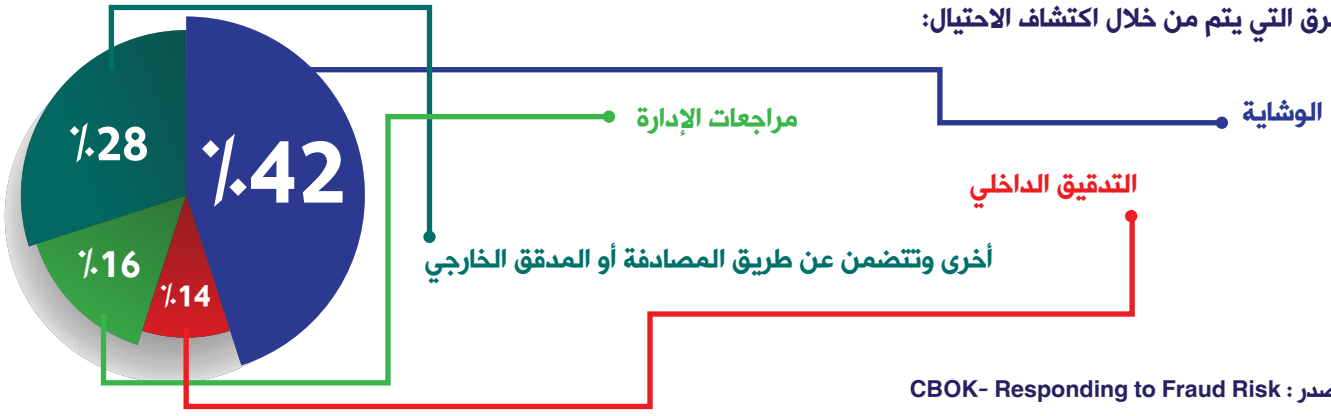
مدى التوافق مع المعيار رقم 1300 المعني ببرنامج ضمان وتحسين الجودة لإدارات التدقيق لعام 2015 :

المصدر: CBOK- Driving Success in a Changing World

مدى استخدام الوسائل الإلكترونية في عمليات التدقيق الداخلي لإدارات التدقيق في الشرق الأوسط:

المصدر : CBOK- Staying a Step Ahead

الطرق التي يتم من خلال اكتشاف الاحتيال:



المصدر : CBOK- Responding to Fraud Risk

التدقيق الداخلي محرك رئيسي لتطوير المؤسسة وليس خط دفاع عنها فقط.

لو تم طرح سؤال عام على الإدارة العليا ومجلس الإدارة ما الدور الذي يلعبه التدقيق الداخلي في المؤسسة؟ .... بالتأكيد ستكون أغلب الإجابات بأنه خط الدفاع الذي يعمل على حماية أصول المؤسسة واكتشاف نقاط الضعف في الرقابة الداخلية، إلا أن هذه النظرة السائدة عن التدقيق الداخلي غير صحيحه وبحاجه إلى توضيح أكثر من المهنيين في التدقيق الداخلي لكي يعكسوا الدور الصحيح للتدقيق الداخلي الذي أضحى شريكاً رئيسياً في المضي قدماً مع الإدارة العليا في تطوير المؤسسة ومساعدتها على تحقيق أهدافها كما أن التغيرات الأخيرة على الإطار المهني الدولي لممارسة مهنة التدقيق الداخلي تؤكد صحة هذا الشيء وبالأخص المبادئ التي تم تبنيها والمتعلقة بأن يكون التدقيق الداخلي ذو بصيرة ومبادر وذو نظرة مستقبلية ويدعم تطوير وتحسين المؤسسة. إلا أن هناك بعض التناقضات التي تستدعي منا كممارسين لمهنة التدقيق الداخلي أن نكون على وعي بها.

إضافة قيمة أم حماية المؤسسة؟

يعرف التدقيق الداخلي على أنه "نشاط مستقل وموضوعي، يقدم تأكيدات وخدمات استشارية بهدف إضافة قيمة للمؤسسة وتحسين عملياتها. ويساعد هذا النشاط في تحقيق أهداف المؤسسة من خلال اتباع أسلوب منهجي منظم لتقييم وتحسين فاعلية عمليات الحوكمة وإدارة المخاطر و الرقابة." فالتعريف حدد بشكل واضح هدفين للتدقيق الداخلي وهو إضافة قيمه للمؤسسة ثانيا تحسين عملياتها فهل إضافة القيمة للمؤسسة تقتصر على تحديد الفجوات الرقابية و وضع توصيات لتحسينها أم تتعدى ذلك من خلال تحديد المجالات التطويرية للمؤسسة والتي تتطلب تفكير استراتيجي عند المدقق وبصيرة وبعد نظر في شأن المؤسسة للأحداث المتوقعة التي قد تؤثر في اتخاذ قرارات مستقبليه من شأنها تطوير أداء المؤسسة.

من وجهة نظر أخرى، قام معهد المدققين الداخليين بوضع رساله للتدقيق الداخلي حيث نصت الرسالة على " تعزيز وحماية المؤسسة من خلال تقديم التوكيد والمشورة و البصيرة الموضوعية المستندة على المخاطر لأصحاب المصلحة". فالرسالة إلى حد ما قد تتعارض بشكل واضح مع هدف التدقيق الداخلي والمبادئ التي تم تبينها والمتعلقة بأن يكون التدقيق الداخلي ذو بصيرة ومبادر وذو نظرة مستقبلية ويدعم تطوير وتحسين المؤسسة.

تطوير وتحسين المؤسسة جزء من تعريف التدقيق الداخلي

لو نظرنا مرة أخرىإلى تعريف التدقيق الداخلي سنلاحظ أيضا أنه وضع مهمة واضحه على التدقيق الداخلي تتعلق بتحسين عمليات المؤسسة والسؤال الذي يطرح نفسه هل هذا التعريف اقتصر على تحسين العمليات من خلال تحديد مجال الضعف في الرقابة و إدارة المخاطر والحوكمة فقط أم تحسين كافة العمليات التي تتعدى ذلك. فهدف الحوكمه المؤسسية في النهاية هو تحسين الأداء كما أن أحد أهداف إدارة المخاطر هو إدارة موارد المؤسسة واستغلالها. والسؤال هنا، هل تقييم الرقابة وإدارة المخاطر والحوكمة تلبي المبادئ التي تم تبنيها والمتعلقة بالبصيرة والنظرة المستقبلية وتطوير وتحسين المؤسسة؟

لو نظرنا إلى تعريف التدقيق الداخلي لتبين لنا أن هدف التدقيق هو إضافة قيمة للمؤسسة وتحسين عملياتها وهو هدف لتطوير المؤسسة و ليس لحماية أصولها واكتشاف الثغرات الرقابية كما هو سائد عند الأغلبية.

إدارة المخاطر تتطلب التعامل مع كل من الخطر والفرصة

يعرف معهد التدقيق الداخلي الخطر على انه " إمكانية وقوع حدث يكون له اثر على تحقيق أهداف المؤسسة." ونحن نعرف بأن إدارة المخاطر تتعامل مع الأحداث غير المؤكدة وأن الخطر ليس بالغالب شيء يؤدي إلى الضرر، فقد تكون الأحداث غير المؤكدة إيجابية وتمنح فرص للمؤسسة وبالتالي يجب التعامل مع هذه الأحداث سواء كانت خطر أو فرصة.

تتبع الكثير من إدارات التدقيق الداخلي بناء خطة تدقيق مبنيه على تقييم المخاطر، إلا أن هذه الطريقة تتجاهل الفرص التي تعتبر الجانب الجوهري الذي يمكن من خلاله إضافة قيمه كبيرة للمؤسسة. من جانب أخر، لو تم تقييم برامج التدقيق التي يتم إعدادها من قبل المدققين سنلاحظ بأنها على الأغلب تخلو من إجراء يتعلق بتحديد فرص التحسين الممكنة سواء كانت إدارية أو ماليه كما أنها قد تخلو أيضا من ربط أهداف التدقيق بأهداف المؤسسة وهذا مؤشر بأن مهمة التدقيق الداخلي قد لا تتوافق مع ما تطمح له المؤسسة.

نموذج خطوط الدفاع الثلاثة، لماذا الدفاع في حين أن المؤسسة بحاجه إلى التقدم إلى الأمام؟

قد يزيد من حدة هذه التناقضات أن نموذج خطـوط الدفاع الثلاثة اكد على أن التدقيق الداخلي هو خط دفاع ثالث وتجاهل هدف التدقيق الداخلي والدور الذي تم الإشارة له ضمن تعريف التدقيق الداخلي، وعلى الرغم من تحفظي الشخصي على مسمى هذا النموذج حيث أنه ليس نموذج دفاع وإنما نموذج لتقديم توكيد كما أن الجهات التي تم الإشارة لها في الخط الثاني لا يقتصر عملها على الدفاع عن المؤسسة وإنما تطوير المؤسسة فعلى سبيل المثال ضمن المستوى الثاني تم الإشارة إلى الوظائف المتعلقة بالجودة والتي تعتبر أهم مهامها تطوير المؤسسة وليس الدفاع عنها وحمايتها، فهل يعقل أن كافه الأطراف في النموذج تعمل على الدفاع عن المؤسسة دون النظر إلى مستقبلها وتطويرها.

تغيير الثقافة جزء صعب يتطلب فكر ووعي لدى ممارسي المهنة

في بداية حياتي المهنية أذكر أول مهمة تدقيق قمت بها وقد يشاركني نفس التجربة العديد من المدققين حيث طلب مني القيام بالتدقيق على مركز عمل وكنت أهدف خلال مهمة التدقيق إلى كتابة أكبر عدد من الملاحظات تتعلق بضعف الضوابط الرقابية وعدم الالتزام بإجراءات العمل.... ومع تطور التفكير المهني لدي أصبحت على وعي أن الالتزام بالإجراءات ليس هدف بحد ذاته فقد تكون الإجراءات التي تم وضعها لا تساعد في تحقق الأهداف التي تطمح لها المؤسسة فبدأت خلال مهام التدقيق بالنظر إلى ضرورة الالتزام وفي حال عدم الالتزام ما هي الإجراءات التي يمكن اتباعها لتطويرها ... وبعد عدد من السنوات مع تطور مرحلة أخرى من الفكر كان لابد من النظر لمستوى أعلى من الإجراءات فالنظر إلى استراتيجية المؤسسة ومدى تحقيق أهدافها الرئيسية كان ذا أثر أكبر عند الإدارة العليا والمشاركة في تقديم الاستشارات ذات البعد الاستراتيجي كان ذا أثر أكبر بكثير.... بالتأكيد أن المرحلة القادمة تتعدى ذلك حيث ركز معهد المدققين الداخليين ضمن المبادئ التي تبناها بان يكون التدقيق الداخلي ذو بصيرة و ذو نظرة مستقبلية ومبادر ويدعم تطوير المؤسسة.

إن ثقافة التدقيق التي يتم تشكيلها لدى الإدارة العليا تعتمد على محتوى التقارير التي يتم رفعها فلو تطرقت التقارير إلى إضافة القيمة وتطوير المؤسسة لأصبح التدقيق الداخلي شريكاً استراتيجياً مع الإدارة العليا في قيادة المؤسسة وليس العقبة – وهي النظرة السائدة عن التدقيق - التي تمنع الإدارة من السير إلى الأمام. كما يلعب مدراء التدقيق الداخلي دوراً مهماً في إرشاد المدققين وتوعية الإدارة العليا عن الدور المنتظر من التدقيق الداخلي حتى يتحول من الدفاع إلى الهجوم.

تناقض المعايير مع المبادئ الجديدة للتدقيق الداخلي

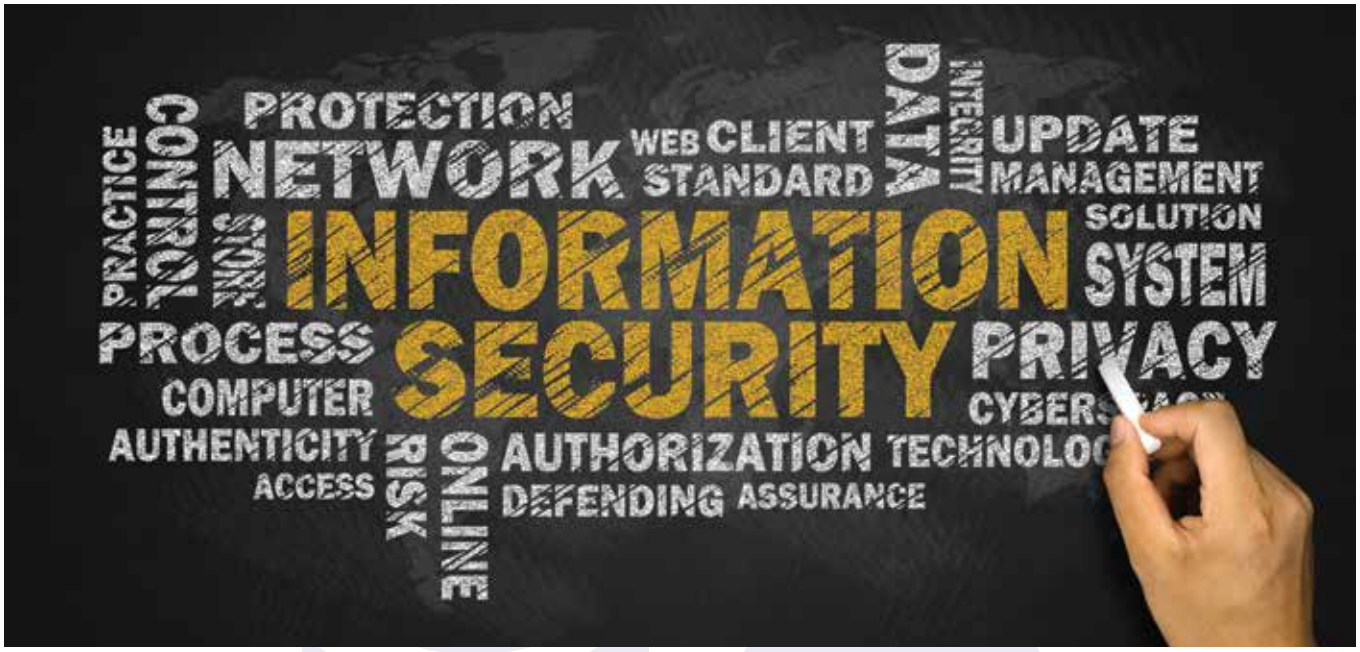
تضمنت المبادئ التي تم تبنيها من قبل معهد المدققين الداخليين أن يكون التدقيق الداخلي ذو بصيرة وذو نظرة مستقبلية ويدعم تطوير المؤسسة وجميعها تتطلب استخدام الحكم الشخصي والاجتهاد في إبداء الرأي في حين أن معايير التدقيق الداخلي بشكلها الحالي لا تساعد في تحقيق المبادئ التي تم تبنيها كما أن المعايير طلبت من المدقق أن يعتمد على معلومات كافية ومناسبة وذات علاقة ومفيدة وهذا قد يعيق إبداء الرأي وأنا هنا لا أقصد المشاركة في أخذ القرارات بدلاً من الإدارة بل مشاركتهم اهتمامهم وتوقعاتهم المتعلقة بتطوير المؤسسة وتحسين أداءها من خلال طرح مبادرات ذات بعد استراتيجي وعدم الاقتصار على رفع التقارير ذات الطابع النقدي فقط. والمثير بالموضوع أن مسودة النسخة المعدلة لم تراعي تغطية هذا الجانب فلماذا ذلك؟؟؟.

الخلاصة

وفي نهاية هذا المقال، قد يخالفني الرأي المتحفظون الذين يرون أن مهنة التدقيق الداخلي يجب أن تبقى كما هي عليه وقد تلعب توقعات الإدارة العليا دوراً كبيراً في بقاء هذا الدور كما هو عليه. وقد يوافقني الرأي من يرى أن مهنة التدقيق الداخلي على أعتاب منحى جديد وتطور كبير قد يزيد من أهميتها وشموليتها في تطوير المؤسسة. وأخيراً، هذه أفكار تطرح العديد من التساؤلات لدينا بطريقة تستدعي منا عدم أخذ أي تطورات على الاطار المهني الدولي لممارسة مهنة التدقيق الداخلي كما هو بل النظر في محتواه بشكل أكثر تعمقاً.

للتعليق على المقال الرجاء مراسلة الكاتب على البريد الإلكتروني: ayman.abdelrahim@outlook.com

تعددت مصادر التهديد وأمن البيانات هدف واحد.



كميات كبيرة من البيانات تتدفق إلى خارج المنشأة كل يوم عن طريق البريد الكتروني، وتحميل البيانات، ونقل الملفات والرسائل الفورية من الشبكات ...الخ. حيث حولت التكنولوجيا طريقة نقل البيانات من الشكل المنظم "الشكل الورقي" الذي كان يسهل نظرياً حمايته، إلى الشكل الرقمي غير المنظم ليشمل البريد الإلكتروني، والأجهزة المحمولة، ووسائل التواصل الاجتماعي.

تصف الدراسات الحديثة بأن المصادر الخارجية وبالأخص القرصنة الخارجية باعتبارها السبب الرئيسي لفقدان البيانات في عالم الشركات، ولذلك نجد اهتمام المنشآت بالأساليب التكنولوجية المتطورة مثل Firewall، وأنظمة كشف التسلل، ومسح نقاط الضعف واختبار الاختراق (vulnerability scanning and penetration testing)، والتي تهدف في المقام الأول لحماية الشبكة من التهديدات الخارجية. إلا أن المصادر الداخلية تشكل تهديداً كبيراً لأمن البيانات أيضاً، حيث تصل نسبة فقدان البيانات من مصادر داخلية وفقاً لبعض الدراسات إلى 35٪ (مرجع 1و 2)، ونجد بأن المنشآت لديها عدد قليل من الأدوات والآليات لتقييم وحماية فقدان البيانات من مصادرها الداخلية، والتي تتطلب اتباع منهجية مختلفة ترتكز غالباً على معالجة البيانات داخل المنشأة وتدفق البيانات خارجها.

مصادر فقدان البيانات

الموظفون هم المصدر الرئيسي لفقدان البيانات (57٪) ومن ثم الجهات الخارجية المتطفلة على المنشأة (32٪)، وتتوزع باقي المسؤولية على كل من المدراء والموردين والموظفين السابقين بالإضافة لجهات مجهولة أخرى(مرجع 3).

في كثير من الحالات، فإن فقدان البيانات ينتج عن الأنشطة الداخلية والسلوكيات الخاطئة للموظفين. وليس بالضرورة أن يكون مصدر الخطر الداخلي نتيجة لسلوك فاسد من قبل الموظفين (45٪ غير مقصود، 45٪ مقصود، 10٪ مجهول) (مرجع 3)، ولكن الحقيقة أن كل موظف أو جهاز يخلق ويحمل في جعبته مخزن من المعلومات. فقد يقوم الموظف بالتحدث بصوت عال عن بعض الخطط والمشاريع السرية، أو قد يفقد جهاز الكمبيوتر المحمول الذي يحتوي على معلومات حساسة.

المنشآت التي تواجه خطر أكبر لفقدان البيانات تشمل شركات البرمجيات، وشركات البيانات والتحليلات، ومقدمي الرعاية الصحية، والشركات التي تقوم بتخزين المعلومات الديموغرافية للعملاء التي تتعدى بيانات حامل البطاقة مثل أماكن تواجدهم وميولهم، بالإضافة للشركات التي تعتمد على أطراف خارجية لتحليل البيانات، مثل الاتصالات، والتجزئة، وشركات المنتجات الاستهلاكية. فعلى سبيل المثال، فإن تجاهل الضروريات

الجديدة في حماية الخصوصية والأمن يعتبر ثالث أهم المخاطر التي تواجه شركات الاتصالات في عام 2016م (مرجع 4).

• بعض جوانب الحوكمة

- استراتيجيات الحوكمة Strategy Governance

تحدد هذه الاستراتيجية المواقع الرئيسية لتخزين البيانات وطبيعتها ومن هو المسؤول عن الحفاظ عليها. قبل الشروع في تنفيذ أي مهام على التدقيق الداخلي الاستفسار عن وجود استراتيجية حوكمة تنظم حماية البيانات. من خلال العمل في مختلف مجالات العمل داخل المنشأة يمكن للتدقيق الداخلي الربط بين الاستراتيجيات المقترحة والحالية، والموضوعات الرئيسية لعملية التنظيم (Fundamental Themes of Regulation)، وما هو مطلوب من كل جهة تشغيلية من أجل الامتثال، بحيث يصبح التدقيق الداخلي مستشاراً موثوقاً به لمدراء الأعمال ويساعد على حماية حقوق المنشأة، وينبغي التأكيد على أهمية إطار أمن البيانات في جميع المحادثات مع مستويات الإدارة ومن خلال الأخذ بعين الاعتبار إطار أمن البيانات في جميع مهام التدقيق.

- سياسة تصنيف البيانات Data Classification Policy

تصنيف البيانات خطوة أساسية في محاولة حماية واحد من أهم أصول المنشأة – وهي البيانات والمعلومات. تصنيف البيانات هي عملية تحديد وتصنيف البيانات التي تعتبر بيانات حساسة للمنشأة وتحديد متطلبات الوصول إليها وآلية التعامل مع تلك البيانات، وتشمل عملية تصنيف البيانات إلى تقسيمها لمستويات محددة مسبقا، بحيث تقوم المنشأة بتحديد مستويات مختلفة من الضوابط الأمنية والحد من عدد الموظفين الذين يمكن لهم الوصول لتلك البيانات. مفهوم تصنيف البيانات ليس بالمفهوم الجديد، ولكن كما هو الحال مع المفاهيم التي تعتبر جزءاً من الأنظمة الموروثة في العمل فمن السهل أن ننسى مدى أهمية هذا المفهوم في الإطار الأمني للمنشأة. وإذا لم تقم المنشأة بتطبيق هذا المفهوم بشكل صحيح أو تعطيه التركيز المناسب، فإن كل الأنشطة المرتبطة بحماية البيانات قد تكون بخطر.

ينبغي أن يفهم المدقق الداخلي إطار تصنيف المنشأة ومن ثم تقييم مدى كفاية وفاعلية الضوابط الرقابية التي تم تحديدها لكل مستوى كما ينبغي على المدققين الداخليين تقييم واختبار هذه السياسة للتحقق من تطبيقها بشكل موحد في جميع أنحاء المنشأة، والتأكد من توافق السياسة مع مستوى تقبل المخاطر في المنشأة.

• الضوابط الرقابية

- التدريب والتعليم: كل موظف في المنشأة مسؤول عن أمن البيانات و ليست مسؤولية وحدات تكنولوجيا المعلومات فقط. ويكون الموظفون أكثر قدرة على تحديد ومنع أية حوادث أمنية في حال تصميم وتطبيق الضوابط الرقابية لحماية أمن البيانات لتكون جزءا من طبيعة أعمالهم اليومية. و يحتاج قياديو الأعمال في المنشآت لفهم مخاطر الأعمال والتأكد من أن كل فرد في المنشأة قد تلقى التدريب لاتخاذ الإجراءات المناسبة لحماية البيانات.

- تشفير البيانات Data Encryption

يعتبر تطبيق بروتوكولات تشفير البيانات أمراً أساسياً في حماية البيانات. تحتاج المنشآت لتحديد البيانات الحساسة وثم تشفيرها لضمان الحفاظ عليها، وتشفير البيانات على مستوى كل مستخدم نهائي يمكن أن يضمن أن البيانات محمية. وبشكل دوري، ينبغي على المنشآت إعادة تقييم سياسات تشفير البيانات لديها لتحديد التغييرات اللازمة في الوقت المناسب، بالإضافة لتقييم طرق تشفير البيانات المطبقة للتأكد من أن البيانات لا تزال محمية من أحدث الثغرات أو نقاط الضعف المحتملة. فعلى سبيل المثال، مقياس تشفير البيانات (DES) تم اختراقه عام 1999م وتم الاعتقاد بأن استخدام الخوارزمية بشكلها الثلاثي (TripleDES) سيكون آمناً من الناحية العملية، إلا أنه وفي عام 2008م تم كسر هذا التشفير وسحبه من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) واستبداله بمعيار التشفير المطور (AES – Advance Encryption Standard).

- الوقاية من فقدان البيانات (DLP- Data Loss Prevention)

المنشآت التي تستقبل وتخزن كميات كبيرة من البيانات بحاجة إلى تقييم الحاجة لاستخدام أدوات الوقاية من فقدان البيانات(DLP). حيث تقوم هذه الأدوات بالمساعدة في منع فقدان البيانات التي قد تحدث نتيجة نقاط ضعف داخلية و/أو خارجية. كما تقوم هذه الأدوات بتقييم حركة البيانات وعدم السماح للمعلومات الحساسة بمغادرة المنشأة وذلك بناء على سياسات محددة مسبقا. وقد تطورت حلول تقنية (DLP) بأشكال مختلفة منذ 2007/2006 لتكون منهج شامل لمنع وكشف والتصرف تجاه أي محاولة غير مصرح بها للتعامل مع البيانات الحساسة. وقد تم تحديد (DLP) كأحد أهم متطلبات الرقابة الآمنة في المنشآت (Top 20 most critical control requirements). إلا أن الاستطلاعات تشير إلى قلة الاعتماد على تقنية (DLP)، بالإضافة لاستخدامها في نطاق محدود مثل الإنترنت ومراقبة البريد الإلكتروني، وليس كحل متكامل.

أحد أشرس الهجمات التي حدثت لأحد تجار التجزئة هي وضع برامج خبيثة على أنظمة نقاط البيع، حيث تمكن المستفيد من الحصول على معلومات بطاقات الإئتمان للعملاء خلال أحد أكثر مواسم التسوق ازدحاما. وأستطيع القول نظريا، بأن استخدام أحد أدوات الوقاية من فقدان البيانات كان كفيلا بإنقاذ الجهة المتضررة من خسارة الملايين، حيث أن أحد القدرات التقليدية لأدوات الوقاية من فقدان البيانات هو عدم السماح لمعلومات البطاقات الائتمانية بمغادرة المنشأة بالإضافة لإشعار الإدارة عن أي محاولة لفعل ذلك. قد لا يكون تاجر التجزئة في المثال السابق متضرر ماليا من عملية الهجوم، حيث المبالغ المسحوبة على بطاقات الإئتمان سيتم تحميلها على العملاء. إلا أن الخاسر الأكبر باعتقادي هو تاجر التجزئة الذي فشل في حماية بيانات عملاءه من السرقة. وهذا بالتحديد ما أشارت إليه المعايير الإرشادية (2130) إلى أنه قد يترتب على عدم حماية المعلومات الشخصية نتائج لا يستهان بها بالنسبة لأي منشأة، كما أن ذلك يمكن أن يسيء لسمعة المنشأة ويعرضها لمخاطرعديدة منها قانونية وتدهور ثقة العملاء. وفقاً لدراسة عالمية أقامتها شركة جيمالتو للأمن الرقمي مؤخراً، فإن 64٪ من المشاركين بالدراسة أشاروا بأنهم لن يتعاملوا مرة أخرى مع المنشأة التي تعرضت لسرقة بيانات أو تم تسريب بياناتهم عن طريقها (5).

- أجهزة المحمول Mobile Devices

أمن البيانات أصبح أساسيا بعد توسع المنشآت وعملائها في استخدامهم للهواتف الذكية، واللوحية وغيرها من الأجهزة المحمولة من أجل إنجاز الأعمال والحفاظ على التواصل. المنشآت التي توزع اجهزة على موظفيها تكون قادرة نظريا على الاحتفاظ بسيطرتها على البيانات. أما المنشآت التي تتبع سياسة استخدام الأجهزة الشخصية للموظفين (Bring Your Own Device-BYOD) تكون قادرة على تقليل التكاليف وإعطاء مرونة لموظفيها إلا أن هذه الممارسات تجلب أنواع جديدة من مخاطر أمن البيانات والامتثال ومخاطر الخصوصية. لإدارة هذه المخاطر تحتاج المنشآت لتطوير وتطبيق سياسات فعالة لاستخدام الأجهزة الشخصية (BYOD) بما في ذلك حلول خاصة لإدارة أجهزة المحمول (Mobile Device Management – MDM). الحلول الخاصة لإدارة أجهزة المحمول (MDM) تعتبر أحد أفضل الممارسات التي تمكن المنشآت من إدارة الأجهزة المحمولة لموظفيها وتنفيذ السياسات الأمنية عن بعد وذلك بمجرد تحميل الموظف للبرنامج والموافقة على الشروط والظروف الخاصة بالمنشأة. كما يمكن لبعض المنتجات فصل تخزين البيانات الخاصة للموظف عن بيانات العمل، بحيث يتمتع الموظف بكامل الخصوصية وتتيح للمنشأة القدرة على رقابة بيانات الأعمال.

ولتسليط الضوء على مخاطر استخدام أجهزة المحمول والتطبيقات والأنظمة التشغيلية التي تعمل عليها تلك الأجهزة نشير إلى تقرير نشره موقع CVE Details المتخصص بعرض الثغرات الأمنية الأكثر شيوعا (6)حيث حصد نظام تشغيل شركة أبل (MAC OS X) على المرتبة الأولى كأكثر البرامج والأنظمة اكتشافاً للثغرات في عام 2015م. حيث بيّن التقرير بأنه قد تم اكتشاف 384 ثغرة أمنية، كما حصل نظام تشغيل iOS للهواتف المتنقلة على المركز الثاني في هذا التقرير والذي احتوى على 375 ثغرة، يليهم برنامج Adobe Flash Player والذي احتوى على 314 ثغرة أمنية متنوعة الخطورة. من جهة أخرى حصدت متصفحات IE و Chrome و Firefox والتي تعتبر أكثر المتصفحات استخداماً على المراكز السابع والثامن والتاسع في هذه القائمة حيث احتوى كل منها بالترتيب على عدد الثغرات التالية 231، 187، 178. فيما حصلت شركات Adobe و Microsoft و Apple على المراكز الثلاثة الأولى كأكثر الشركات تم اكتشاف ثغرات في تطبيقاتها و أنظمتها.

وفي الختام أود الإشارة إلى وجود ندرة في المدققين الداخليين المختصّين في تكنولوجيا المعلومات (اكثر من 600,000 وظيفة شاغرة حول العالم) (7) إلا أنني أعتقد بأن العديد من الضوابط التي تحكم وتنظم أمن البيانات يمكن مراجعتها وتقييمها من قبل عموم المدققين الداخليين، حيث تصنف معظم تلك الضوابط ضمن الضوابط العامة، وعليه أوصي رؤساء التدقيق التنفيذيين بالمبادرة ومساعدة منشآتهم على حماية أحد أهم اصولها وعدم انتظار التوظيف.

المراجع:

1- KPMG – Data Loss Barometer.
2- Open Security Foundation's Data-Loss Database.
3- InfoWatch Analytical Center, Global Data Leakage Report, H1 2015.
4-Top Ten Risks In Telecommunication Revisited – EY.
5-http://www.gemalto.com/press/Pages/Global-survey-by-Gemalto-reveals-impact-of-data-breaches-on-customer-loyalty.aspx
6- http://www.cvedetails.com/
7- ISACA/RSA Conference Security Survey.

للتعليق على المقال مراسلة المؤلف على البريد الإلكتروني Amjad_afb@yahoo.com

"Thankfully, our auditor saw it coming."

BDO Audit Services

In today's rapidly evolving regulatory environment, knowledgeable and proactive guidance is more important than ever. BDO's partner-led audit teams draw on global resources and deep industry sector knowledge to help clients navigate change, bolster investor confidence, and build value.

Audit | Tax | Advisory | Internal Audit
www.bdo.com.jo

BDO

هل تعتقد بأن مؤسستك مستعدة لتأسيس قسم خاص بإدارة المخاطر؟

يعد النضوج المؤسسي أحد أهم العوامل التي يجب دراستها قبل اتخاذ القرار بتأسيس قسم متخصص في إدارة المخاطر المؤسسية، بالإضافة الى أن مرحلة نضوج المؤسسة تؤثر بشكل كبير على الطريقة المثلى لوضع القسم داخل الهيكل التنظيمي للمؤسسة.

تعتبر مرحلة نضوج المؤسسة مهمة جداً في عملية وضع الخطة المناسبة لتطبيق عناصر إدارة المخاطر وتحديد العلاقة فيما يخص رفع التقارير والتواصل داخل المؤسسة وتضمين إدارة المخاطر في كل عملية من عمليات المؤسسة الرئيسية.

ما هي المتطلبات الرئيسية لتأسيس إدارة المخاطر؟

إن القرار المتعلق بتأسيس قسم متخصص بإدارة المخاطر المؤسسية يجب أن يتخذ من قبل مجلس إدارة المؤسسة أو الملاك بعد القيام بتقييم تفصيلي لعوامل جاهزية المؤسسة والتى تشمل:

1- الثقافة المؤسسية ودرجة الدعم من مجلس الإدارة

يجب أن يكون لدى أعضاء مجلس الإدارة أو ملاك الشركة – بالحد الأدنى - فهم لهيكل ومكونات إدارة المخاطر المؤسسية. يجب عليهم أيضاً أن يقتنعوا بأهمية دور إدارة المخاطر وبناء سقف توقعات منطقي فيما يتعلق بدور ومسؤوليات إدارة المخاطر داخل المؤسسة.

بالإضافة الى ذلك، يعد وجود ثقافة تواصل منفتحة داخل المؤسسة عاملاً رئيسياً من أجل اكتشاف ومعالجة المخاطر الداخلية والخارجية التي قد تتعرض لها المؤسسة. من الضروري لمجلس الإدارة أو ملاك المؤسسة إدارك الحقيقة المتعلقة بأن إدارة المخاطر تضيف قيمة للمؤسسة فقط في حال وجود درجة عالية من الشفافية والدعم والتمكين في التعامل مع إدارة المخاطر. يجب عليهم أيضاً الاستعداد لقبول التغيير والأفكار والطروحات الجديدة كنتيجة حتمية لأداء إدارة المخاطر داخل المؤسسة.

الثقافة المؤسسية يجب أن تتوافق مع أهداف إدارة المخاطر فيما يتعلق بالتعامل مع المخاطر وتقليل أثرها على المؤسسة وتعزيز بيئة الرقابة الداخلية. يتم تعزيز ذلك من خلال التواصل المستمر وإرسال رسائل تؤكد هذه الثقافة من قبل مجلس الإدارة أو الملاك والإدارة العليا لجميع الموظفين بشكل دوري.

2- هيكل الحوكمة والرقابة على المخاطر

إن وجود مقومات الحوكمة الأولية في المؤسسة هو متطلب أساسي من أجل تحقيق الأهداف المرجوة من تأسيس إدارة المخاطر. من غير الممكن القيام بتأسيس إدارة فاعلة للتعامل مع المخاطر من دون وجود المكونات التالية بالحد الأدنى:

المرجع:
.CBOK, Delivering on the Promise: Measuring Internal Audit Value and Performance
Written By: Jane Seago

IIA magazine (Internal Auditor, February 2016). Five Trends

- مجلس إدارة أو أية هيئة إدارية تقوم بنفس دور الحوكمة الموكل الى مجلس الإدارة (مثال: هيئة المديرين). يجب أن تكون هذه الهيئة فاعلة في دورها الرقابي فيما يتعلق بالمخاطر من خلال المتابعة والتقييم للبيئة الرقابية داخل المؤسسة.

- وجود أهداف واضحة للمؤسسة وتوجه استراتيجي واضح والذي يتم ترجمته الى أهداف ومؤشرات أداء على مستوى العمليات والأقسام داخل المؤسسة.
- وجود هيكل تنظيمي واضح داخل المؤسسة يبين العلاقات الإدارية بشكل تفصيلي.
- أن يكون لدى المؤسسة تفويض صلاحيات يُمكن الإدارة الوسطى من اتخاذ قرارات تتعلق بالخطط المستقبلية المقترحة للتعامل مع المخاطر بحيث يكون هناك تحديد للمسؤوليات ومتابعة دورية على تنفيذ هذه الخطط.
- وجود سياسات واجراءات وأنظمة تدعم تحقيق أهداف المؤسسة.

3- خط الدفاع الأول (الإدارة التنفيذية)

خط الدفاع الأول في المؤسسة يتكون من الإدارة التنفيذية والموظفين الذين يقومون بإدارة مخاطر الأعمال من خلال تنفيذ مهامهم ومسؤولياتهم اليومية في المؤسسة.

من حيث المبدأ، لا يمكن للمؤسسة تفعيل خط الدفاع الثاني - إدارة المخاطر المؤسسية - من دون وجود إدارة تنفيذية مؤهلة والتي يقع على عاتقها الدور الأساسي والمسؤولية الرئيسية المتعلقة بإدارة المخاطر.

يجب على خط الدفاع الأول مساعدة إدارة المخاطر المؤسسية من خلال القيام بمسؤوليات معينة تشمل:

- مساعدة إدارة المخاطر على تحديد حجم المخاطر التي يمكن للمؤسسة تحمله (Risk Capacity) وحجم المخاطر التي ترغب المؤسسة في تحمله (Risk Appetite) ومحددات المخاطر على مستوى العمليات (Risk Tolerance) بناء على توجه مجلس الإدارة أو الملاك و الإدارة العليا من حيث قبول المخاطر.

- تقديم الدعم لإدارة المخاطر فيما يتعلق بالتعرف أو اكتشاف المخاطر التي تؤثر على المؤسسة.

- المساعدة في تحليل المخاطر المتعلقة بالعمليات والمخاطر المالية والرقابية من خلال الخبرة التي يتمتع بها المدراء التنفيذيون في إدارة عمليات المؤسسة.
- تحديد الضوابط الرقابية والإجراءات المطبقة فيما يتعلق بتخفيض أثر المخاطر التي تم اكتشافها خلال عملية تقييم المخاطر.
- المشاركة في تطوير خطط مستقبلية تتعلق بالتقليل من حدة المخاطر المكتشفة.
- أخذ زمام المبادرة وتحمل المسؤولية فيما يتعلق بقائمة المخاطر التي تم الاتفاق عليها مع قسم إدارة المخاطر من أجل تحديد المسؤوليات والمتابعة على تنفيذ التوصيات والخطط المستقبلية.

ليس من الضروري أن يتمتع موظفو خط الدفاع الأول بخبرة كبيرة في مجال إدارة المخاطر من أجل ضمان نجاح تطبيق برنامج إدارة المخاطر في المؤسسة، ولكن في نفس الوقت يجب أن يكون لديهم استيعاب لمفاهيم إدارة المخاطر والأهم من ذلك أن يتمتعوا بالكفاءة والنضج الإداري ليكونوا جزءاً فاعلاً في تحقيق الأهداف المرجوة من برنامج إدارة المخاطر.

يبين الشكل التالي مراحل النضج المؤسسي المختلفة مع وصف مختصر لأهم ما يميز كل مرحلة:

إن القرار المتعلق بتوقيت وكيفية تأسيس إدارة المخاطر في المؤسسة يعتمد على مراحل النضوج التي تمر بها المؤسسة والتي تم شرحها في الشكل السابق. الهيكل الموصى به لإدارة المخاطر في كل مرحلة من المراحل هو كما يلي:

• **بدائي:** في هذه المرحلة، تكون المؤسسة غير جاهزة لتبني ممارسات إدارة المخاطر لوجود ضعف في نظام الحوكمة وعدم وضوح الهيكل المؤسسي. يجب إعطاء الأولوية لبناء المكونات الأساسية لنظام الحوكمة. في الغالب يتم تأسيس إدارة تدقيق داخلي للقيام بدور توكيدي فيما يتعلق بعمليات المؤسسة.

• **مجزأ:** يكون التركيز في هذه المرحلة منصباً على اكتشاف الثغرات في نظام الحوكمة والعمل على تصحيحها بالإضافة الى تطوير السياسات الداخلية وسير العمليات. يعتبر استحداث "قسم تقييم المخاطر" ضمن مظلة إدارة التدقيق الداخلي من الممارسات الموصى بها في هذه المرحلة، حيث يعتبر النواة لإدارة المخاطر المستقلة في المستقبل ويعمل على المساعدة في اكتشاف وتقييم المخاطر ونشر الوعي حول إدارة المخاطر المؤسسية.

تقوم إدارة التدقيق الداخلي بأخذ زمام المبادرة في هذه المرحلة من حيث تأسيس وإدارة قسم تقييم المخاطر وذلك لعلاقة إدارة المخاطرة الوطيدة بعمليات التدقيق الداخلي وإمكانية إقناع الإدارة العليا بالحاجة الى هذا القسم كجزء من إدارة التدقيق الداخلي.

• **محدد ومتكامل:** تتميز هذه المرحلة بوجود نظام حوكمة جيد وتفويض صلاحيات مقبول. تكون المؤسسة جاهزة لتأسيس قسم مستقل لإدارة المخاطر بحيث يكون موصولاً بالرئيس التنفيذي مباشرة. يمنح هذا التنظيم الهيكلي مرونة أكبر لإدارة المخاطر للقيام بدورها الاستشاري بعيداً عن محددات الاستقلالية المتعلقة بإدارة التدقيق الداخلي.

يحتاج مجلس الإدارة والإدارة العليا الى جهة استشارية موثوقة في هذه المرحلة التي تمر فيها المؤسسة بتغيرات كبيرة على صعيد بناء نظام حوكمة قوي بجميع عناصره وضمان تحقيق أهداف المؤسسة في الوقت عينه. تعتبر إدارة المخاطر أفضل جهة للقيام بهذا الدور من خلال قدرتها على اكتشاف المخاطر بشكل مبكر وتقديم المشورة للإدارة العليا في الوقت المناسب فيما يتعلق بكيفية التعامل مع هذه المخاطر.

• **مثالي:** تكون المؤسسة قد طبقت أفضل الممارسات الرائدة المتعلقة بأنظمة الحوكمة في هذ المرحلة مع وجود ثقافة مؤسسية شفافة ومنفتحة. بالإضافة الى ذلك تم تفعيل دور لجان الحوكمة وقامت بدورها الرقابي على أكمل وجه. تم تضمين اجراءات إدارة المخاطر في كل العمليات الرئيسية في المؤسسة مع تبني برنامج الامتثال وأخلاقيات العمل ومنع الغش.

نتيجة لوجود مرحلة متقدمة من النضوج المؤسسي فإن أفضل علاقة تنظيمية لإدارة المخاطر تكون موصولة بلجنة المخاطر والتدقيق.
إن أولوية إدارة المخاطر في هذه المرحلة تكمن في التركيز على المخاطر الاستراتيجية والتأكد من أن مجلس الإدارة والإدارة العليا على علم بهذه المخاطر وأن الجهة المسؤولة في المؤسسة وضعت الخطط الكفيلة بإدارة هذه المخاطر وتقوم على تنفيذها. إن اتباع هذا النموذج يعود الى وجود خط دفاع أول قوي ومؤهل بشكل عالي لإدارة المخاطر التشغيلية والمالية والرقابية بشكل يومي ووجود نظام امتثال يعزز قدرة الإدارة على التعامل مع المخاطر التي قد تظهر بشكل يومي.

الخلاصة

بناءً على ما تم ذكره سابقاً، يجب أن يكون قرار تأسيس قسم لإدارة المخاطر في المؤسسة مبرراً ويجب أن يكون مبنياً على تحليل سليم لمرحلة النضوج التي تمر بها المؤسسة مع بناء سقف توقعات معقول فيما يتعلق بالإنجازات المتوقعة من قبل هذه الإدارة.

تسعى العديد من المؤسسات الى تأسيس أقسام مستقلة لإدارة المخاطر من أجل إرضاء الجهات الرقابية واستيفاءً لمتطلباتها من دون وجود مبرر فعلي يدعو الى مثل هذا القرار. تؤدي مثل هذه الممارسات الى اعتبار وتصنيف إدارة المخاطر كقسم كمالي غير ضروري ويمكن الاستغناء عنه في حال الحاجة الى تقليل التكاليف عند أول هزة تتعرض لها المؤسسة.

يجب دراسة جميع التجارب السابقة –ناجحة كانت أم فاشلة- المتعلقة بتأسيس أقسام مستقلة لإدارة المخاطر وتحليل هذه التجارب للوصول الى الأسباب الحقيقية التي ساهمت في نجاح أو فشل تلك التجارب. بناء على هذه الدراسات يجب مشاركة النتائج لجميع الأطراف المهتمة من أجل نشر الوعي حول الطرق المثلى لنجاح تطبيق برامج إدارة المخاطر.

للتعليق على المقال الرجاء مراسلة الكاتب على البريد الإلكتروني: ehab-saif@live.com

جمعيـة التدقيـق الداخلـي الأردنيــة
Jordan Internal Audit Association

لأي اقتراحات أو الرغبة في نشر مقال يرجى التواصل معنا عبر البريد الإلكتروني:
jia.newsletter@gmail.com

ملاحظة:
المقالات التي تتضمنها النشرة تعبر عن رأي كاتبها ولا تعبر عن رأي الجمعية ولا عن جهة توظيف كاتبها