الرقابة الماليــة
Financial Control

تحول الرقابة المالية

العدد 10 | أغسطس 2022

مراجعة تقنية المعلومات

ما هي مراجعة تقنية المعلومات؟

هـي فحـص وتقييـم الضوابـط العامـة لتقنيـة المعلومـات وضوابـط التطبيقـات فـي المنشأة بناءً علـى المعايير المعتمدة والمعترف بها عالمياً والسياسات المعمول بها. تقـوم عمليـات المراجعـة بتقييـم الضوابـط مـن ثلاثـة أوجـه مختلفـة تشـمل: التصميـم، والتنفيـذ، والفعاليـة بالإضافـة إلـى تقييـم السـرية والنزاهـة والتوافـر.

أهداف مراجعة تقنية المعلومات

تقييــم ومراجعــة الضوابــط الداخليــة للأنظمـة والعمليـات المعمـول بها والتي تحفــظ بيانـات المنشـأة

تحديـد المخاطـر التـي تتعـرض لهـا أصـول معلومات المنشأة، والمساعدة في تحديد طـرق تقليـل هـذه المخاطـر

التأكـد مــن أن عمليـات إدارة المعلومـات تتوافـق مـع القوانيـن والسياسـات والمعايير الخاصـة بتقنيـة المعلومـات

تحديـد أوجـه القصـور فـي أنظمـة تقنيـة المعلومـات والإدارة المرتبطـة بهـا

مراحل تنفيذ عملية مراجعة تقنية المعلومات

1 - التخطيط

هـي عمليـة جمـع المعلومـات الأساسـية، وتحديـد النطـاق والأهـداف، وتحديـد أصحـاب المصلحـة الرئيسـيين، وطلـب المسـتندات اللازمـة وإعـداد مصفوفـات المخاطـر والضوابـط وجـداول الاجتماعـات.

2 - العمل الميداني

تنفيذ أنشـطة المراجعة وتقييمها بما فـي ذلـك جمـع معلومـات أكثـر تفصيلاً وحضـور اجتماعـات لفهـم العمليـة.

3 - التقرير

هـي أنشـطة إعـداد تقاريـر المراجعـة مـن توثيـق الملاحظـات التفصيليـة، وعقـد اجتماعـات التحقـق مـع أصحـاب المصلحـة الرئيسـيين، وإعـداد تقريـر التقييـم والـذي يتضمـن ملخصاً تنفيذياً وملاحظـات تفصيليـة وتوصيـات وخطـط عمـل الإدارة.

4 - المتابعة

هي إجراءات متابعة الملاحظات المكتشفة؛ للتأكد من تطبيق واتخاذ الإجراء المناسب. وهذا يشمل التواصل مع أصحاب المصلحة، وإجراء اختبارات التحقق من الصحة، وعقد اجتماعات المتابعة، وتوثيق النتائج والحالة في سجل المراقبة.

أنواع الضوابط في تقنية المعلومات

1 - الضوابط العامة لتقنية المعلومات (IT General Controls - ITGC)

تعتبر من أسس التحكم والضبط في تقنية المعلومات. فهي تساعد على ضمان موثوقية البيانات التي يتم إنشاؤها بواسطة أنظمة تقنية المعلومات، ودعم التأكيد على أن الأنظمة تعمل بالطريقة والآلية المنشودة، وأن المخرجات موثوق بها. وتنقسم إلى التالي:

تطوير النظام وإدارة التغيير

نهج منظم للتعامل مع الانتقال أو التحول لأنظمة أو تقنيات المنشأة. لتنفيذ التغييرات مع الحد الأدنى من التأثير السلبي على خدمات تقنية المعلومات.

حوكمة تقنية المعلومات

عنصر من عناصر حوكمة المنشآت، وتهدف إلى تحسين الإدارة العامة لتقنية المعلومات وإيجاد قيمة مضافة من الاستثمار في المعلومات والتقنية.

إدارة الصلاحيات

إطار للسياسات والتقنيات يضمن أن المستخدمين المصرح لهم فقط لديهم حق الوصول المحدد إلى خدمات تقنية المعلومات.

عمليات تقنية المعلومات

عملية شاملة لإدارة عمليات الشبكة ومكوناتها، والنسخ الاحتياطي، وإدارة الحوادث والأعطال، والدعم الفني.

أمن المعلومات

حماية المعلومات والبيانات المتداولة من أي خطر يهددها.

إدارة استمرارية الأعمال

هي عملية شاملة لإدارة التهديدات المحتملة على المنشأة وأثرها على العمليات الأساسية.

2 - ضوابط التطبيقات

ضوابط أمنية تمنع أو تقيد التطبيقات غير المصرح بها من التنفيذ بطرق تعرض البيانات للخطر. والهدف الرئيسي هو المساعدة في ضمان خصوصية وأمن البيانات المستخدمة من قبل التطبيقات والتي يتم نقلها بين التطبيقات. وتنقسم الى التالي:

ضوابط الاكتمال
تضمن معالجة السجلات من البداية إلى النهاية

ضوابط التحقق من الصلاحية
تضمن إدخال ومعالجة البيانات الصالحة فقط

ضوابط التحقق من الهوية
تضمن تحديداً فريداً وقاطعاً لجميع المستخدمين

ضوابط المصادقة
توفر آلية مصادقة لنظام التطبيق

ضوابط التفويض
تضمن الوصول إلى نظام التطبيق من قبل المستخدمين المعتمدين فقط

ضوابط الإدخال
تضمن دقة البيانات المدخلة من مصادرها في نظام التطبيق

ضوابط التحقيقات
تضمن أن جميع البيانات صحيحة علمياً وحسابياً، بناءً على المدخلات والمخرجات

يجب على المنشآت وضع خطط عمل لرفع قدرتها على الاستجابة الفعالة للحوادث من خلال التركيز على سلامة الأشخاص وحماية الأصول وتقليل التأثير السلبي على الأعمال من خلال عملية "إدارة استمرارية الأعمال".

إدارة استمرارية الأعمال

هي عملية شاملة لإدارة التهديدات المحتملة على المنشأة وأثرها على العمليات الأساسية. والتي تركز على استئناف الأنشطة التشغيلية الحيوية واستمرارها وإدارتها، والتعافي من الحوادث من خلال استعادة البنية التحتية المهمة لتقنية المعلومات والتطبيقات والوظائف بعد التعطل.

مراجعة إدارة استمرارية الأعمال

تقوم على مراجعة برنامج استمرارية الأعمال، وتحديد التوصيات للمنشأة فيما يتعلق بتنفيذ دورة حياة استمرارية الأعمال ومستوى المرونة المطلوب من خلال خمسة خطوات أساسية للمراجعة:

المراجعة: عملية مراجعة رسمية محايدة تقيس برنامج استمرارية الأعمال والتعافي من الكوارث التابع للمنشأة مقارنة بمعيار متفق عليه مسبقاً.

التقييم الذاتي: تقييم برنامج المنشأة في مجال استمرارية الأعمال في حد ذاته.

ضمان الجودة: ضمان النتائج المختلفة من برنامج استمرارية الأعمال تفي بالمتطلبات.

تقييم الأداء: تقييم أداء الأفراد المكلفين بأدوار ومسؤوليات ضمن برنامج استمرارية الأعمال.

أداء الموردين: مراجعة الموردين الرئيسين لبرنامج استمرارية الأعمال، أو مراجعة أداء موردين خدمات التعافي من الكوارث.

دور مراجعة تقنية المعلومات في رحلة تحول الرقابة المالية

يساعد التطبيق السليم لعمليات مراجعة تقنية المعلومات على تعزيز الرقابة الداخلية للجهات في رحلة التحول من خلال:

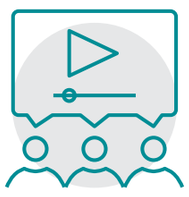
حوكمة تقنية المعلومات

التأكد من أن المستخدمين المصرّح لهم فقط لديهم حق الوصول المحدد إلى خدمات تقنية المعلومات

التطوير المناسب والترخيص والاختبار والموافقة على التغييرات لأنظمة المعلومات

تقييم مدى توافق ومواءمة أهداف أنظمة الإدارة مع التوجه الاستراتيجي للمنشأة

التحقق من قدرة المنشاة على استمرارية الأعمال



ضمان أن كافة الإجراءات تضمن سرية وسلامة وتوافر نظام المعلومات إلى جانب وجود معايير للأمان والإعدادات

تقييم قدرات الجهة الخاضعة للمراجعة على تحديد المخاطر الخاصة بتقنية المعلومات والفرص وتحديد وتنفيذ الإجراءات الفعالة لمواجهتها

التأكد من أن جميع الخدمات والضوابط المتعلقة بالبنية التحتية لتقنية المعلومات والخدمات يتم تقديمها وفقاً لمستويات الخدمات المتفق عليها

قدمت النشرة معلومات عامة عن مفهوم الالتزام كجزء من الحملة التثقيفية بمفاهيم الرقابة المالية، ونأمل أن يكون في سياقها معلومات توضيحية عن أهداف ودور الالتزام وأهميته في تعزيز التحول وتبني الرقابة الذاتية.

@

في حال وجود أي استفسارات، يسعدنا تواصلكم معنا عبر البريد الإلكتروني للرقابة المالية
sdfci@mof.gov.sa