

## 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:

<b>ضوابط التحقق من الصلاحية</b> تضمن إدخال ومعالجة البيانات الصالحة فقط	<b>ضوابط الاكتمال</b> تضمن معالجة السجلات من البداية إلى النهاية
<b>ضوابط المصادقة</b> توفر آلية مصادقة لنظام التطبيق	<b>ضوابط التحقق من الهوية</b> تضمن تحديداً فريداً وقاطعاً لجميع المستخدمين
<b>ضوابط الإدخال</b> تضمن دقة البيانات المدخلة من مصادرها في نظام التطبيق	<b>ضوابط التفويض</b> تضمن الوصول إلى نظام التطبيق من قبل المستخدمين المعتمدين فقط
<b>ضوابط التحقيقات</b> 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 في ما يتعلق بتنفيذ دورة حياة استمرارية الأعمال ومستوى المرونة المطلوب من خلال خمسة خطوات أساسية للمراجعة:

<b>المراجعة:</b> عملية مراجعة رسمية محايدة تقيس برنامج استمرارية الأعمال والتعافي من الكوارث التابع للمنشأة مقارنة بمعيار متفق عليه مسبقاً.	<b>التقييم الذاتي:</b> تقييم برنامج المنشأة في مجال استمرارية الأعمال في حد ذاته.
<b>ضمان الجودة:</b> ضمان إيفاء النتائج المختلفة من برنامج استمرارية الأعمال بالمتطلبات.	<b>تقييم الأداء:</b> تقييم أداء الأفراد المكلفين بأدوار ومسؤوليات ضمن برنامج استمرارية الأعمال.
<b>أداء الموردين:</b> مراجعة الموردين الرئيسيين 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:

<b>التأكد من أن المستخدمين المصرح لهم فقط لديهم حق الوصول المحدد إلى خدمات تقنية المعلومات</b>	<b>حوكمة تقنية المعلومات</b>
<b>التأكد من أن جميع الخدمات والضوابط المتعلقة بالبنية التحتية لتقنية المعلومات والخدمات يتم تقديمها وفقاً لمستويات الخدمات المتفق عليها</b>	<b>التطوير المناسب والترخيص والاختيار والموافقة على التغييرات لأنظمة المعلومات</b>
<b>ضمان أن كافة الإجراءات تضمن سرية وسلامة وتوافر نظام المعلومات إلى جانب وجود معايير للأمان والإعدادات</b>	<b>التحقق من قدرة المنشأة على استمرارية الأعمال</b>
<b>تقييم مدى توافق ومواءمة أهداف أنظمة الإدارة مع التوجه الاستراتيجي للمنشأة</b>	<b>تقييم قدرات الجهة الخاضعة للمراجعة على تحديد المخاطر الخاصة بتقنية المعلومات والفرص وتحديد وتنفيذ الإجراءات الفعالة لمواجهتها</b>

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

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

## مراجعة تقنية المعلومات

### ما هي مراجعة تقنية المعلومات؟

هي فحص وتقييم الضوابط العامة لتقنية المعلومات وضوابط التطبيقات في المنشأة بناءً على المعايير المعتمدة والمعترف بها عالمياً والسياسات المعمول بها وتقوم عمليات المراجعة بتقييم الضوابط من ثلاثة أوجه مختلفة تشمل: التصميم، والتنفيذ، والفعالية بالإضافة إلى تقييم السرية والنزاهة والتوافر.

### أهداف مراجعة تقنية المعلومات

<b>تقييم ومراجعة الضوابط الداخلية للأنظمة والعمليات المعمول بها والتي تحفظ بيانات المنشأة</b>	<b>تحديد المخاطر التي تتعرض لها أصول معلومات المنشأة، والمساعدة في تحديد طرق تقليل هذه المخاطر</b>
<b>التأكد من أن عمليات إدارة المعلومات تتوافق مع القوانين والسياسات والمعايير الخاصة بتقنية المعلومات</b>	<b>تحديد أوجه القصور في أنظمة تقنية المعلومات والإدارة المرتبطة بها</b>

### مراحل تنفيذ عملية مراجعة تقنية المعلومات

<b>1 - التخطيط</b> هي عملية جمع المعلومات الأساسية، وتحديد النطاق والأهداف، وتحديد أصحاب المصلحة الرئيسيين، وطلب المستندات اللازمة وإعداد مصفوفات المخاطر والضوابط وجداول الاجتماعات.	<b>2 - العمل الميداني</b> تنفيذ أنشطة المراجعة وتقييمها بما في ذلك جمع معلومات أكثر تفصيلاً وحضور اجتماعات لفهم العملية.
<b>3 - التقرير</b> هي أنشطة إعداد تقارير المراجعة من توثيق الملاحظات التفصيلية، وعقد اجتماعات التحقق مع أصحاب المصلحة الرئيسيين، وإعداد تقرير التقييم والذي يتضمن ملخصاً تنفيذياً وملاحظات تفصيلية وتوصيات وخطط عمل الإدارة.	<b>4 - المتابعة</b> هي إجراءات متابعة الملاحظات: 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 (ITGC - IT General Controls)

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:

<b>حوكمة تقنية المعلومات</b> عنصر من عناصر حوكمة المنشآت، وتهدف إلى تحسين الإدارة العامة لتقنية المعلومات وإيجاد قيمة مضافة من الاستثمار في المعلومات والتقنية.	<b>تطوير النظام وإدارة التغيير</b> نهج منظم للتعامل مع الانتقال أو التحول لأنظمة أو تقنيات المنشأة. لتنفيذ التغييرات مع الحد الأدنى من التأثير السلبي على خدمات تقنية المعلومات.
<b>عمليات تقنية المعلومات</b> عملية شاملة لإدارة عمليات الشبكة ومكوناتها، والنسخ الاحتياطي، وإدارة الحوادث والأعطال، والدعم الفني.	<b>إدارة الصلاحيات</b> إطار للسياسات والتقنيات يضمن أن المستخدمين المصرح لهم فقط لديهم حق الوصول المحدد إلى خدمات تقنية المعلومات.
<b>إدارة استمرارية الأعمال</b> هي عملية شاملة لإدارة التهديدات المحتملة على المنشأة وأثرها على العمليات الأساسية.	<b>أمن المعلومات</b> حماية المعلومات والبيانات المتداولة من أي خطر يهددها.

