

مراجعة النظم

Information Systems Audit

الفصل الثامن

أنواع المراجعة

• هناك نوعين من أنواع المراجعة يمكن استخدامها عند تنفيذ مهام المراجعة :

١. المراجعة المستمرة

• المراجعة السابقة

• تستخدم عند الرغبة في التحقق من جميع العمليات بشكل مستقل قبل البدء أو الانتهاء منها

• يتم القيام بهذا الشكل من المراجعة عند تنفيذ المراجعة الداخلية على مستوى إدارة أو قسم معين

• المراجعة اللاحقة

• تختلف عن سابقتها من حيث توقيت القيام بها فقط إذ يقوم بها المراجع بعد الانتهاء من العملية المراد فحصها

٢. المراجعة الدورية

• يقوم بها المراجع الداخلي بشكل دوري لتحقيق الفحص الدوري للعمليات أو أرصدة الحسابات

• أي نوع يستخدم المراجع الداخلي ؟

مراجعة النظم Systems Audit

- من أمثلة النظم المقومة من قبل المراجع الداخلي
 - نظام الرقابة الداخلية
 - النظام المحاسبي
- لكي يستطيع المراجع تقويم النظم يجب أن يكون لديه إلمام كافي بالمتطلبات المهنية التي يجب توافرها في النظام المعني لكي يكون فعالاً.

خطوات مراجعه النظم

- تحديد الهدف الأساسي الذي يسعى المراجع إلى تحقيقه من دراسة وتقويم النظام .
- مثال : عند مراجعه نظام الرقابة الداخلية هدفى كمراجع هو تحديد مدى الثقة في أن نظام الرقابة الداخلية المطبق يستطيع أن يمنع حدوث الأخطاء والغش أو يستطيع اكتشافهما عند حدوثهما وإجراء التصحيح اللازم.
- عند تقويم نظام الرقابة الداخلية في المنشآت التي تستخدم نظم معالجة البيانات إلكترونياً يقوم المراجع بتطبيق الخطوات التالية:
 - أولاً: الدراسة المبدئية للنظام
 - ثانياً: تقدير نتائج الدراسة المبدئية
 - ثالثاً: إجراء اختبارات مدى تنفيذ النظام والالتزام به

خطوات مراجعه النظم

• أولاً: الدراسة المبدئية للنظام

• يقوم المراجع بدراسة مبدئية للنظام بهدف تفهمه وتحديد معالمه الرقابية

• جميع النشاطات اليدوية ، والمالية ، والإلكترونية الهامة

• تحديد مدى الاعتماد على نظم المعلومات فيما يتعلق بعمليات المنشأة. Business process mapping

• العلاقات المترابطة بين إدارة معالجة البيانات إلكترونياً والإدارات المستخدمة أو المستفيدة لمعرفة كيفية تدفق العمليات خلال النظام ، ومدى استخدام النظام الإلكتروني في كل تطبيق من التطبيقات المحاسبية الهامة ، والهيكل الأساسي للرقابة المحاسبية

• الإجراءات الرقابية المستخدمة مثل :

• إدارة هوية المستخدم النهائي End user Identity management

• Authentication mechanisms, password standards, roles limiting or granting systems functionality Operating

• اعدادات النظام systems configurations

• أدوات التحكم في أمان التطبيق Application security controls .

• أدوات التحكم في الوصول لقاعدة البيانات Database access controls

• .database configuration, account access to the database, roles defined in the database

• Anti-virus/Anti-malware controls

• أدوات التحكم في الشبكات مثل Access control lists, and firewall rules

• مساندة ال IT للنظام (user account reviews, change management)

• عمليات Backup/Restore

خطوات مراجعه النظم

- يقوم المراجع بتجميع المعلومات الخاصة بدراسة النظام من خلال:
 - الاستفسارات من الموظفين
 - ملاحظة توزيع الأعمال وإجراءات التشغيل
 - الرجوع إلى الوثائق المكتوبة كما في حالة النظام اليدوي
 - دراسة النظام باستخدام قائمة استقصاء مثل تلك الخاصة عن نظام الرقابة الداخلية بحيث تكون مصممة لأغراض الأنظمة الإلكترونية

خطوات مراجعه النظم

• ثانياً: تقدير نتائج الدراسة المبدئية

- يستطيع المراجع أن يقرر من خلال تقييمه للمعلومات التي حصل عليها من الدراسة المبدئية ما إذا كان سيستمر في دراسته للنظام أو يتوقف عن ذلك.
- إذا أشارت نتائج الدراسة المبدئية للنظام إلى أن هناك ضعفاً في إجراءات الرقابة مثلا المتعلقة بنظام معالجة البيانات إلكترونيا في هذه الحالة لا يجب الاستمرار في دراسة نظام الرقابة الداخلية ويجب على المراجع أن يعد تقريره بأن النظام الرقابي المصمم غير جيد ويجب تضمين تقريره توصيات ومقترحات لتحسينه
- إذا أشارت نتائج الدراسة المبدئية للنظام إلى أن النظام الرقابي مصمم بشكل جيد فيجب على المراجع الانتقال إلى مرحلة التأكد من مدى الالتزام به عن طريق إجراء اختبارات مدى تنفيذ النظام والالتزام به
- يقوم باختبارات مدى تنفيذ الأنظمة الرقابية ، وتقويم الإجراءات الرقابية لتحديد مدى اعتماده عليها ومدى استقصر عليه اختباره لتحقيق العمليات

خطوات مراجعه النظم

• ثالثاً: إجراء اختبارات مدى تنفيذ النظام والالتزام به

• الهدف هو التأكد من أن الإجراءات الرقابية المصممة يتم تطبيقها فعلا وأنها تؤدي وظيفتها بطريقة مرضية

• تشمل هذه المرحلة :

A. اختبار تنفيذ الإجراءات الرقابية العامة و الإجراءات الرقابية على قاعدة البيانات

B. اختبار إجراءات الرقابة التطبيقية

اختبارات مدى تنفيذ النظام والالتزام به

A. اختبارات تنفيذ الإجراءات الرقابية العامة و الإجراءات الرقابية على قاعدة البيانات

- الغرض هو إعطاء تأكيد معقول بأن الإجراءات الرقابية يتم تنفيذها كما هي موضوعة
- تتعلق اختبارات تنفيذ أنظمة الرقابة الداخلية أساساً بالأسئلة الآتية :

١. هل تم تنفيذ الإجراءات الرقابية الضرورية؟

٢. كيف تم تنفيذها؟

٣. من الذي قام بالتنفيذ؟

- اختبارات المراجع لها عن طريق الاستفسار والملاحظة وفحص الوثائق المختلفة

اختبارات مدى تنفيذ النظام والالتزام به

B. اختبار تنفيذ إجراءات الرقابة التطبيقية (مراجعة برامج الحاسب)

- تركز على اختبار تنفيذ برامج الحاسب الآلي المستخدمة و تشمل إجراءات الرقابة على مراحل البرنامج الثلاثة (المدخلات ، عمليات التشغيل ، المخرجات)
- أنواع الاختبارات :
 - ا. اختبار تنفيذ إجراءات الرقابة التطبيقية بدون الحاسب
 - اا. اختبار تنفيذ إجراءات الرقابة التطبيقية بالحاسب

اختبارات مدى تنفيذ النظام والالتزام به

1. اختبار تنفيذ إجراءات الرقابة التطبيقية بدون الحاسب

- في بعض نظم معالجة المعلومات إذا كان هناك مسار مستندي يمكن الاعتماد عليه (مستند ونتائج مطبوعة) بحيث يمكن متابعة العمليات من مصادرها الأصلية إلى نهايتها فيستطيع المراجع في هذه الحالة اختبار وجود وفعالية إجراءات الرقابة التطبيقية يدويا بدون استخدام الحاسب
- يتم ذلك بالحصول على المستندات الأصلية وتشغيلها يدويا ثم يقوم المراجع بمقارنة النتائج التي توصل إليها بمخرجات الحاسب المطبوعة
- يطلق على هذا النوع من المراجعة في بعض الأحيان "المراجعة حول الحاسب" ولا تختلف أساليب المراجع في هذه الحالة عن الأساليب المتبعة في مراجعة الأنظمة المحاسبية اليدوية

اختبارات مدى تنفيذ النظام والالتزام به

II. اختبار إجراءات الرقابة التطبيقية بالحاسب

- تستخدم في حالة نظم معالجة البيانات إلكترونياً التي لا يملكها وجود مستندات، أو العمليات المراد اختبار ذات حجم ضخم
- الأساليب التي يمكن للمراجع استخدامها عند استخدام الحاسب في اختبار إجراءات الرقابة التطبيقية :
 1. أسلوب البيانات الاختبارية
 2. البرامج الخاضعة لرقابة المراجع
 3. أسلوب المحاكاة المتوازية كأحد تطبيقات برامج المراجعة العامة
 4. أسلوب فحص تعليمات البرامج
 5. أسلوب تحقيق خريطة التدفق

اختبار إجراءات الرقابة التطبيقية بالحاسب

١. اسلوب البيانات الاختبارية

- يقوم المراجع بتحضير عمليات وهمية Dummy Data ثم يتم تشغيل هذه العمليات تحت رقابة المراجع بواسطة البرنامج الذي تطبقه الأقسام الأخرى
- بعد الحصول على نتائج العمليات التي تم تشغيلها تقارن هذه النتائج بالنتائج التي تم تحديدها مقدما لمعرفة ما إذا كانت البيانات الاختبارية قد تم تشغيلها بطريقة صحيحة
- ما هي صفات هذه البيانات :
 - مشابهة للعمليات التي تقوم الأقسام الأخرى بتشغيلها عادة
 - تشتمل على عمليات تعكس الأوضاع الصحيحة وغير الصحيحة التي يريد المراجع اختبارها
- يلاحظ أن اسلوب البيانات الاختبارية يختبر البرنامج المطبق في نقطة معينة من الزمن وليس خلال مدة المراجعة بأكملها
- هذا الاسلوب لا يعطي المراجع أي معلومات عن العمليات التي يتم تشغيلها فعلا فهو مجرد اختبار لوجود وتنفيذ الإجراءات الرقابية التي يتضمنها البرنامج محل الاختبار

اختبار إجراءات الرقابة التطبيقية بالحاسب

٢. البرامج الخاضعة لرقابة المراجع

- تستخدم هذه الطريقة كبديل أو كمكمل لمدخل البيانات الاختبارية
- في هذه الطريقة يقوم المراجع تحت ظروف خاضعة لرقابته بإعادة تشغيل عينات من البيانات الفعلية الخاصة بالفترة محل الفحص
- يمكن أن يستخدم أحد البرامج المطبقة التي سبق اختبارها أو يستخدم نسخة من برنامج يكون خاضعا لرقابته
- بعد إكمال عملية إعادة التشغيل تتم مقارنة نتائج العينة مع البيانات الأصلية المقيدة في سجلات العميل
- هذه الطريقة تتميز عن أسلوب البيانات الاختبارية في أنها تمكن المراجع من الحكم على برنامج العميل و صحة بعض العمليات محل المراجعة ، أيضا يمكن استخدامها على كمبيوتر خارجي دون استخدام الكمبيوتر الخاص بالأقسام التي تتم المراجعة عليها أو الاستعانة بموظفيها

اختبار إجراءات الرقابة التطبيقية بالحاسب

٣. أسلوب المحاكاة المتوازية Stimulations

- السبب في إطلاق تعبير "المحاكاة المتوازية" هو أن البرنامج مصمم لإعادة إنتاج (محاكاة) البيانات الحقيقية للأقسام الأخرى التي تم تشغيلها
- هذا المدخل يتمتع بالمزايا الآتية :
 - هذا المدخل لا يؤدي إلى تلوث ملفات العميل
 - يمكن إجراؤه في مركز كمبيوتر خارجي مستقل
 - بما أن البيانات الحقيقية هي التي تستخدم فيستطيع المراجع تحقيق العمليات بمتابعتها إلى مصادرها الأصلية (المستندات) المعتمدة
 - يمكن زيادة حجم العينة زيادة كبيرة بتكاليف ضئيلة نسبيا
 - يستطيع المراجع أن يقوم بتشغيل الاختبار بنفسه بطريقة مستقلة .
 - يمكن إجراؤها في أوقات مختلفة خلال السنة المالية محل المراجعة ويمكن أيضا استخدامها في إعادة تشغيل بيانات تاريخية
- يجب التأكد من أن تكون البيانات المختارة للمحاكاة ممثلة للعمليات الفعلية
- يلاحظ أنه من الممكن أن يقوم النظام المطبق بالوحدة بعمليات تخرج عن نطاق برامج المراجعة العامة التي تستخدم في عملية المحاكاة بحيث لا تستطيع هذه البرامج محاكاتها

اختبار إجراءات الرقابة التطبيقية بالحاسب

٤. أسلوب فحص تعليمات البرامج

- يتم فحص وتعديل التعليمات التي يتضمنها البرنامج الخاص بمعالجة عملية معينة للتحقق من أن هذه التعليمات تؤدي إلى المعالجة المطلوبة
- مع إجراء عملية الفحص بشكل مفاجئ وبصفة متكررة وإجراء المقارنات – في حالة وجود تعديلات – بين البرنامج قبل وبعد التعديل يمكن التعرف على أي تعديلات تكون قد تمت على البرنامج وإذا كانت هذه التعديلات مصرح بها أم لا
- هذا الأسلوب يتطلب توافر درجة كافية من الخبرة لدى المراجع بكيفية إعداد البرامج وكيفية صياغتها
- يستغرق وقت أطول من أي أسلوب آخر سبق عرضه ولاسيما في ظل النظم المعقدة لمعالجة البيانات حيث يكون من الصعب فحص كل سطر في مختلف البرامج المكتوبة

اختبار إجراءات الرقابة التطبيقية بالحاسب

٥. أسلوب تحقيق خريطة التدفق

- يتم فحص خريطة التدفق والتي تعكس منطق المعالجة الخاصة بتطبيق معين بدلاً من فحص كل سطر من سطور البرنامج المكتوب
- هذا الأسلوب يعتبر نسخة مطورة من أسلوب فحص تعليمات البرنامج
- يتم إعداد خرائط التدفق إما يدوياً (الأكثر انتشاراً) أو باستخدام الحاسب
- يمكن للمراجع أن يعد يدوياً خريطة تدفق تحتوي على التفاصيل اللازمة إلى المدى الذي يمكنه من متابعة كل سطر في البرنامج الذي يؤدي في النهاية إلى أسلوب فحص تعليمات البرنامج
- يتطلب ذلك معرفة من المراجع في إعداد البرامج وخرائط التدفق

المصادر

- الرقابة والمراجعة الداخلية في الأجهزة الحكومية والمؤسسات العامة – SOCPA
- ملاحظات و عروض الاستاذ هناء العقيل