

المحاضرة الرابعة: تدقيق نظم المعلومات - مفاهيم أساسية

أولاً: المفهوم

1. التعريف

يعرف تدقيق نظم المعلومات بأنه عملية منظمة لفحص وتقييم النظام المحوسب بهدف التحقق من كفاءة وفعالية النظام، وسلامة البيانات، وأمان العمليات المحاسبية والإدارية داخل النظام. تتضمن هذه العملية مراجعة البنية التحتية والتأكد من أن البيانات تتم معالجتها وحمايتها بما يتماشى مع أهداف المؤسسة ومتطلباتها القانونية.

2. الأهداف الأساسية لتدقيق نظم المعلومات:

-التحقق من كفاءة النظام: التأكد من أن النظام يؤدي وظيفته بأفضل شكل ممكن من حيث استخدام الموارد.

-التأكد من السلامة والأمن: حماية البيانات من الوصول غير المصرح به والتأكد من عدم وجود مخاطر على المعلومات.

-دعم الامتثال: ضمان توافق النظام مع القوانين واللوائح والمعايير المعمول بها.

التعرف على نقاط الضعف والمخاطر: تحديد أي مشكلات قد تؤثر على الأداء والاستقرار الأمني للنظام.

ثانياً: عناصر تدقيق نظم المعلومات

تتكون عملية تدقيق نظم المعلومات من عدة عناصر أساسية تشكل خطوات مهمة في عملية التدقيق وتضمن دقة التقييم وموضوعيته. تتضمن هذه العناصر ما يلي:

1. التقييم الشامل للأنظمة

يشمل هذا العنصر فحص المكونات المادية والبرمجية للنظام، وفهم طريقة عمل النظام وكيفية تكامل مختلف الوحدات فيه. يتم ذلك من خلال مراجعة الوثائق الفنية للنظام، وتقييم التصميم، واختبار الوظائف.

يستلزم هذا أيضاً مراجعة متطلبات النظام ومدى تماشيها مع الاحتياجات التشغيلية للمؤسسة.

2. تقييم الأداء

يهدف هذا العنصر إلى قياس مدى كفاءة وفعالية النظام في تحقيق الأهداف التشغيلية المرسومة له. يتم فحص سرعة النظام واستجابته للطلبات، ومدى توافق أدائه مع المعايير المحددة مسبقاً.

يساعد تقييم الأداء في تحديد أي أوجه قصور في الأنظمة، كالبطء أو عدم الاستقرار في أداء بعض العمليات.

3. تحليل المخاطر

يتطلب هذا العنصر تحديد كافة أنواع المخاطر التي قد تؤثر على سلامة النظام وكفاءته، مثل التهديدات الإلكترونية، والاختراقات الأمنية، وأخطاء المستخدمين، والمشاكل التقنية.

تحليل المخاطر يساعد في وضع خطط استباقية للتعامل مع هذه المخاطر وتخفيف تأثيراتها المحتملة على النظام.

4. مراجعة السياسات والإجراءات

يتم فحص سياسات وإجراءات العمل ومدى توافقها مع المتطلبات الرقابية. وتشمل السياسات المتعلقة بالوصول إلى النظام، وتحديث البيانات، وحفظ السجلات.

الهدف من هذا العنصر هو التأكد من أن النظام يتبع السياسات المحددة بشكل دقيق.

5. التدقيق الأمني

يعتبر التدقيق الأمني أحد أهم جوانب تدقيق نظم المعلومات، ويتضمن فحص الإجراءات الأمنية لحماية البيانات والبرامج من التهديدات الخارجية والداخلية.

ثالثاً: معايير تدقيق نظم المعلومات

يتم تنظيم عملية تدقيق نظم المعلومات وفق معايير دولية ومعتمدة تضمن تحقيق أهداف التدقيق بفعالية وموضوعية. ومن أبرز هذه المعايير:

1. المعايير العامة

-الاستقلالية والموضوعية: يجب أن يكون المدقق مستقلاً عن الأطراف التي يدققها، وموضوعياً في تقاريره وأحكامه.

-الكفاءة المهنية: ينبغي أن يكون المدقق على دراية تامة بتكنولوجيا المعلومات وأنظمة الرقابة ومتطلبات الامتثال.

-التوثيق: ضرورة توثيق كافة خطوات التدقيق والإجراءات التي تم تنفيذها لضمان إمكانية مراجعة العمل ومصداقيته.

2. معايير العمل الميداني

-التخطيط الجيد: يجب إعداد خطة شاملة لعملية التدقيق تغطي كل جزء من النظام بشكل دقيق.

-جمع الأدلة: تتضمن استخدام طرق متعددة لجمع الأدلة، مثل فحص السجلات واختبار النظام بشكل مباشر، لضمان الحصول على معلومات دقيقة.

-تحليل الوثائق: يتم تحليل كافة الوثائق الخاصة بالنظام للتأكد من مدى تطبيقها عملياً.

3. معايير إعداد التقرير

-الوصف الواضح للنتائج: يجب أن تكون النتائج واضحة ودقيقة، بحيث تقدم توصيات محددة وقابلة للتطبيق.

-التوصيات للتحسين: يجب على المدقق تقديم توصيات لتحسين الأداء أو معالجة الثغرات، مع عرض هذه التوصيات بطريقة واضحة ومفهومة.

-التوازن بين الشفافية والموضوعية: يُفترض أن يكون التقرير متوازناً، فيركز على جوانب التحسين والإيجابيات كذلك.

رابعاً: مجالات تدقيق نظم المعلومات

يتطلب تدقيق نظم المعلومات فحص وتقييم مختلف المجالات التي تؤثر على كفاءة النظام وفعاليتها، وتشمل:

1. التقييم الاقتصادي (Economy)

يتعلق بتقييم قدرة النظام على استخدام الموارد المتاحة بشكل اقتصادي دون إسراف أو هدر، بما في ذلك الموارد المالية والمعدات البشرية.

يشمل ذلك دراسة تكاليف التشغيل والصيانة وإمكانية تخفيض التكاليف وزيادة العائد على الاستثمار.

2. الكفاءة (Efficiency)

يقيس مدى سرعة وفعالية النظام في أداء العمليات المختلفة بموارد أقل وبدون تعقيدات زائدة. تحليل الكفاءة يساعد في تحديد أوجه القصور والعمليات التي يمكن تحسينها لزيادة سرعة وكفاءة النظام.

3. الفعالية (Effectiveness)

تركز هذه المعايير على مدى تحقيق النظام للأهداف التي تم تطويره لأجلها، أي أنه يعمل على إنجاز الأهداف التشغيلية بفاعلية.

يقاس مدى القدرة على تلبية احتياجات المستخدمين وأهداف المؤسسة بدقة وموثوقية.

4. تقييم نظام الرقابة الداخلية

يتضمن مراجعة الضوابط والسياسات التي تحكم النظام وأي إجراء وقائي يهدف إلى الحفاظ على البيانات وضمان صحة العمليات.

يتم فحص مدى استجابة النظام للضوابط الرقابية وكفاءته في الحد من مخاطر الوصول غير المشروع.

5. تدقيق الحسابات

يعنى بمراجعة دقة وصحة الحسابات والمعاملات المالية المخزنة ضمن النظام، ويشمل التأكد من تسجيل البيانات بدقة في السجلات المحاسبية الإلكترونية.

خامسا: مكونات تدقيق نظم المعلومات

تتطلب عملية التدقيق فحص عدة مكونات أساسية للنظام لضمان تحقيق الرقابة الشاملة، وهذه المكونات هي:

1. رقابة الموارد البشرية

تتعلق بمراقبة سياسات الموارد البشرية ومدى توافر الكفاءة والتدريب اللازمين للعاملين في إدارة النظام.

يشمل ذلك إجراءات الأمن المرتبطة بالمستخدمين مثل تعيين الصلاحيات، والتحقق من الهوية.

2. الرقابة على الجانب المادي (Hardware Control)

تهدف إلى حماية البنية التحتية للنظام، مثل الخوادم وأجهزة الكمبيوتر، من التلف أو الوصول غير المشروع.

تشمل هذه الرقابة تأمين مراكز البيانات، واستخدام أجهزة مراقبة، وتحديد إجراءات الصيانة اللازمة.

3. الرقابة على البرامج (Software Control)

تشمل حماية البرامج من التعديل غير المصرح به ومن البرمجيات الخبيثة، مثل الفيروسات.

يتم تحديث البرامج بانتظام، وتحديد الصلاحيات الخاصة بالمستخدمين، والتأكد من استخدام أدوات الأمان اللازمة.

4. الرقابة على قواعد البيانات

تتعلق بحماية المعلومات المخزنة، وضمان سريتها وسلامتها وتوافرها عند الحاجة. تشمل استخدام التشفير، وتحديث قواعد البيانات، والتحكم في الوصول وفقاً للصلاحيات المحددة.