البنيان المؤسساتي
Enterprise Architecture (EA)

ITIS411 >> LEC 6#

د.حنان الداقيز

الاهداف

Audit and compliance
التدقيق و الامتثال

Audit and compliance
التدقيق و الامتثال

أصبحت ثورة المعلومات والتكنولوجيا(صناعة المعلومات) أحد أهم الصناعات الحديثة في الوقت الحاضر فهي تقف وراء نجاح الشركات وتعطيها القوة والاستمرارية والمنافسة فظهرت الحاجة إلى ضوابط رقابية للحد من المخاطر الجديدة الناجمة عن التطورات الحديثة في بيئة تكنولوجيا المعلومات.

إن التدقيق على تكنولوجيا المعلومات يضمن أن تحقق عمليات تطوير و تطبيق وصيانة أنظمة تكنولوجيا المعلومات أهداف العمل، و يحمي أصول المعلومات و يحافظ على نزاهة البيانات، وبعبارة أخرى، فإن التدقيق على تكنولوجيا المعلومات يعتبر اختبارا لكيفية تنفيذ نظم تكنولوجيا المعلومات و الضوابط المطبقة عليها لضمان تلبية هذه النظم احتياجات العمل في الجهة دون المساس بالأمن، والخصوصية، والتكلفة، وغيرها من محاو ر العمل الهامة.

أهداف تدقيق تكنولوجيا المعلومات

- إن الهدف من عمليات تدقيق تكنولوجيا المعلومات هو التأكيد على أن موارد تكنولوجيا المعلومات تؤدي إلى تحقيق الاهداف التنظيمية بفعالية واستخدام الموارد بكفاءة، و قد يشمل تدقيق تكنولوجيا المعلومات أنظمة تخطيط موارد المؤسسات ERP، و أمن نظم المعلومات، والحصول على حلول لأعمال، و تطوير الانظمة، واستمرارية الاعمال والتي تعتبر كلها من مجالات تطبيق نظم المعلومات، أو يمكن أن تكون للنظر في القيمة المفترضة التي وفرتها النظم المعلوماتية.

فيما يلي بعض الامثلة على أهداف التدقيق :

1. مراجعة ضوابط نظم تكنولوجيا المعلومات للتأكيد على دقتها وفعاليتها.
2. تقييم العمليات المرتبطة بعمليات مجال معين مثل نظام الرواتب، أو نظام المحاسبة المالية.
3. تقييم أداء النظام و أمنه.
4. فحص عملية تطوير النظام والاجراءات.

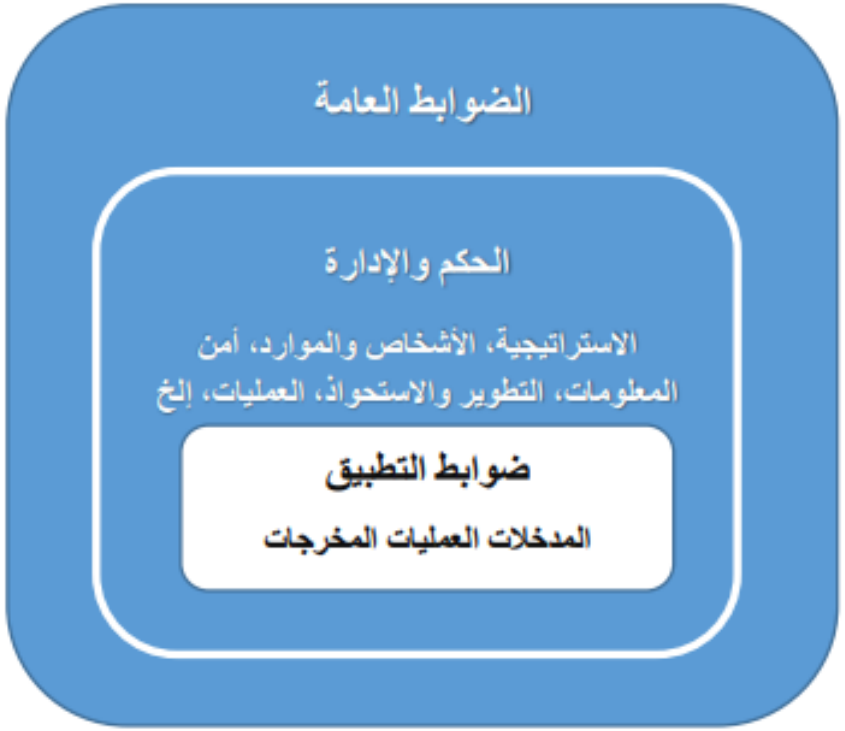
حدود او مجال تدقيق تكنولوجيا المعلومات

- عادة ما تقوم أجهزة الرقابة العليا بعمليات التدقيق على تكنولوجيا المعلومات مقترنة مع التدقيق على البيانات المالية، و مراجعة الضوابط الداخلية، وعمليات تدقيق الاداء لنظم و تطبيقات تكنولوجيا المعلومات.
- فمن امثلة عمليات تدقيق تكنولوجيا المعلومات الاتي:-
  - في عمليات التدقيق المالي (لتقييم صحة البيانات المالية للجهة).
  - في تدقيق الالتزام والتدقيق التشغيلي (تقييم الضوابط الداخلية) .
  - في تدقيق الاداء (بما في ذلك مواضيع نظم المعلومات).
  - في عمليات التدقيق المتخصصة (تقييم الخدمات المقدمة من خلال طرف ثالث كالاستعانة بمصادر خارجية)
  - في التدقيق القضائي و التدقيق على مشاريع تطوير نظم المعلومات .

بغض النظر عن نوع التدقيق، يجب على مدقق تكنولوجيا المعلومات أن يقوم بتقييم السياسات المطبقة والاجراءات المتبعة في بيئة تكنولوجيا المعلومات بصورة شاملة في الجهة الخاضعة للتدقيق، و ذلك للتأكيد على وجود الضوابط والاليات المناسبة في الموضع الصحيح، ويحدد مجال التدقيق مدى دقة الفحص، و نظم المعلومات التي سيتم تغطيتها و أي وظائف منها، و عمليات تكنولوجيا المعلومات التي ستخضع للتدقيق، و مواقع نظم تكنولوجيا المعلومات و الفترة الزمنية التي سيتم تغطيتها، أي أنه شيء أساسي أن يتم تحديد مجال التدقيق.

ضوابط تكنولوجيا المعلومات

- الضوابط هي مزيج من الأساليب والسياسات والإجراءات التي تكفل حماية أصول الجهة، و دقة و موثوقية سجالتها، والألتزام التشغيلي بمعايير الإدارة. تنقسم ضوابط تكنولوجيا المعلومات إلى قسمين: الضوابط العامة وضوابط التطبيق، وتعتمد نوعية هذه الضوابط على مدى تأثيرها وهل هي مرتبطة بأي تطبيق محدد.



اولاً : الضوابط العامة

- تعتبر الضوابط العامة أساس ضوابط تكنولوجيا المعلومات، و هي المعنية بالبيئة العامة التي يتم فيها التطوير والصيانة، تضع الضوابط العامة لتكنولوجيا المعلومات إطار عمل نظم تكنولوجيا المعلومات وتشغيلها وادارتها للرقابة الشاملة على أنشطة تكنولوجيا المعلومات وتقدم الضمان بتحقيق مستوى مرضي من أهداف الرقابة.
- يتم تطبيق الضوابط العامة باستخدام عدد من الأدوات كالسياسات والإجراءات والتوجيه وكذلك بوضع هيكل إداري ملائم، بما في ذلك هيكل إدارة نظم تكنولوجيا المعلومات في الجهة، وتشمل الأمثلة على الضوابط العامة تطوير وتنفيذ استراتيجية نظم المعلومات، والسياسة الأمنية لنظم المعلومات، و تشكيل لجنة توجيهية لتكنولوجيا المعلومات، وتنظيم موظفي نظم المعلومات لفصل المهام المتعارضة، والتخطيط للوقاية من الكوارث واستعادة الاوضاع.

ثانياً : ضوابط التطبيق

- ضوابط التطبيق هي ضوابط معينة تختلف بإختلاف التطبيق، ولها علاقة بالمعاملات والبيانات الموجودة، وتشمل ضوابط التطبيق التحقق من صحة إدخال البيانات، تشفير البيانات المراد إرسالها، وضوابط المعالجة، الخ، على سبيل المثال، من ضوابط المدخلات في تطبيق الدفع عبر الإنترنت، أن يكون تاريخ انتهاء بطاقة الائتمان أكبر من تاريخ المعاملة، و أن يتم تشفير المعلومات التي تم إدخالها.

العلاقة بين الضوابط العامة وضوابط التطبيق لتكنولوجيا المعلومات

- إن طريقة تصميم الضوابط العامة لتكنولوجيا المعلومات و طريقة تطبيقها لهما تأثير كبير على فعالية ضوابط التطبيق، تزود الضوابط العامة التطبيقات بالموارد التي تحتاجها للتشغيل وضمان عدم حدوث أي تغييرات غير مصرح بها على التطبيقات أو على قواعد البيانات الأساسية.
- فيما يلي أكثر الضوابط العامة شيوعا و التي تعزز ضوابط التطبيق لتكنولوجيا المعلومات :
  - ضوابط الدخول المنطقي على البنية التحتية والتطبيقات والبيانات.
  - ضوابط دورة حياة تطوير النظام.
  - ضوابط إدارة تغيير البرنامج.
  - ضوابط الدخول المادي على مركز البيانات.
  - ضوابط الاحتياطات الخاصة بالنظام والبيانات و استرجاع الاوضاع الطبيعية.
  - ضوابط عمليات الكمبيوتر.

تعمل ضوابط التطبيق على مستوى المعاملات بحيث تضمن صحة إدخالها ومعالجتها و مخرجاتها، تؤثر فعالية تصميم وتشغيل الضوابط العامة لتكنولوجيا المعلومات بصورة كبيرة على مدى اعتماد الإدارة على ضوابط التطبيق في إدارة المخاطر.

مدقق نظم المعلومات المعتمد
Certified Information Systems Auditor - CISA

- آيزاكا **ISACA** (Information Systems Audit and Control Association) هي جمعية تُعرف باسم جمعية ضبط وتدقيق نظم المعلومات. الاشهر في العالم في مجال تدقيق نظم المعلومات و التي اصبحت تمنح شهادات مهنية في التدقيق.
- CISA هي شهادة معلوماتية تختص في مراجعة نظم المعلومات وهي حجر الزاوية لجمعية ISACA، حيث يعمل اختبار CISA منذ عام 1978 على قياس كفاءة عملية التدقيق على نظم المعلومات وضبط أمن نظم المعلومات هي لغة المنهج والاختبار، وقد حصل على هذه الشهادة حتى الآن ما يزيد على 50 ألف متخصص. وقد حصلت الجمعية على اعتماد شهادة CISAمن المعهد الأمريكي الوطني للمعايير **ISACA**. ويمثل الحصول علي هذه الشهادة قيمة مضافة لحامليها حيث:
- أصبحت CISA رمزاً عالمياً للإنجاز والكفاءة في هذا المضمار، وهو المعيار المتعارف عليه بين أهل المهنة على مستوى العالم. فأصبحت CISA رمزاً للاحترافية والمعرفة في مجال تدقيق وضبط نظم المعلومات بوجه عام. أصبحت CISAالبرنامج المفضل الذي تبني عليه الشركات والهيئات في جميع القطاعات اختيارها لتوظيف كوادر نظم المعلومات.

التدقيق في نظم المعلومات

- يمكن القول بأنه لا توجد منظمتان تتقاسمان أهداف رقابية متطابقة أو تتعرضان لنفس المخاطر كما انه لا يتوفر نفس الموارد لهما للتعامل مع المواضيع الرقابية ومع ذلك فان جميع المنظمات ترغب في وجود ضوابط رقابية فاعلة وبكلفة متدنية نسبيا.
- وهنا تقع مهمة التدقيق والضوابط الرقابية حيث ينصب التركيز على فهم المتطلبات والمخاطر وتطبيق آلية الأمان والرقابة.
- يعتبر تقدير المخاطر مسألة حساسة للإدارة و أي تهديد لتحقيق استراتيجيات وأهداف منظمة الأعمال هو خطر للأعمال التجارية.
- **أنواع المخاطر:-**
- المخاطر الاستراتيجية :و التي تتعلق بعمل الأشياء الخطأ
- المخاطر التشغيلية:وهي تلك المخاطر التي تتعلق ببناء النظام من تحليل او تصميم او فقد المهارات المطلوبة لاستكمال او تشغيل جزء او كامل النظام.
- المخاطر المالية :وهي تلك المخاطر التي تتعلق بفقدان الموارد المالية أو حدوث التزامات غير مقبولة.
- مخاطر المعلومات :وهي تلك المخاطر التي تتعلق بالمعلومات الغير صحيحة أو غير ملائمة، ونظم ليست ذات مصداقية وتقارير غير صحيحة أو تقارير مضللة