الأكاديمية العربية الدولية
Arab International Academy

اسم المادة: التدقيق الأمني لنظم المعلومات

المحاضِر: م. خليل المحمد

الأكاديمية العربية الدولية – منصة أعد

مقدمة

إ ن التدقيق الذي يتم إنجازه ضمن بيئة معلوماتية قد يشكل صعوبات للمدققين من حيث التنفيذ ومن حيث المقاربة وكذا طبيعة عمليات الرقابة التي يتعين إنجازها واستغلال النتائج المتحصل عليها في ختام عمليات الرقابة.

أدى ظهور التكنولوجيا الجديدة للمعلومات فضلا عن التعقيد المتزايد لنظم المعلومات الآلية إلى القيام بدراسة التدقيق الأمني لنظم المعلومات.

يسمح الدليل بتوجيه وتسهيل أشغال المدقق المكلف بتدقيق نظم المعلومات بغض النظر عن نوع الهيئة المعنية.

إ ن الغرض من هذا الدليل هو تزويد المدقق بحلول عملية في إطار مراعاة البيئة المعلوماتية في تدقيقه.

لا تتطلب معظم أشغال التدقيق المتعلقة بنظام المعلومات معرفة معمقة جدا في نظم المعلومات، ولكن إتقانا جيدا لممارسات التدقيق.

ا. نظم المعلومات: رهانات ومخاطر

يمثل نظام المعلومات مجمل الموارد البشرية والمادية المشاركة في جمع وتخزين وتسيير ومعالجة ونقل وايصال المعلومات داخل الهيئة. ويرتكز في كثير من الأحيان على نظم المعلومات.

يكون نظام المعلومات متكاملا عندما تتواصل جميع التطبيقات مع بعضها البعض بشكل آلي باستخدام وسائط بينية. وبالتالي، لا يتم إدخال المعلومات سوى مرة واحدة فقط في النظام، ويكون تبادل البيانات موضوع عمليات رقابة آلية.

وبالتالي فإن تدخل الإنسان، وهو مصدر محتمل جدا للخطأ أو التزوير، محدود للغاية.

إن نظام تخطيط موارد المؤسسة الذي هو ترجمة عربية لمصطلح Enterprise Resource Planning:ERP هو عبارة عن مجموعة من التطبيقات المتكاملة التي تغطي جميع أنشطة الهيئة: تسيير الطلبات، وتسيير المخزونات، وتسيير المحاسبة، وتسيير الميزانية، ورقابة التسيير، والمرتبات. وتأتي هذه التطبيقات من مورد وحيد للبرمجيات. يسمى كل تطبيق وحدة.

العوامل الرئيسية لنظام معلومات

نظام المعلومات المثالي:

- يتماشى مع استراتيجية المنظمة والأهداف المهنية
- يمتثل للالتزامات القانونية
- آمن
- سهل الاستخدام
- موثوق
- تطوري
- مستدام
- متاح
- فعال.

العوامل الرئيسية لنظام معلومات عالي الأداء

- مشاركة قوية للإدارة في تسيير نظام المعلومات.

يتعين عليها على وجه الخصوص الاشراف على تسيير نظام المعلومات عن طريق وضع أدوات التوجيه التالية:

- سياسة أمن المعلومات
- احترام التشريع بخصوص نظام المعلومات
- وضع الإعدادات بشكل صحيح لحقوق الدخول إلى تطبيقات نظم المعلومات
- التسيير الجيد لمشاريع تطوير نظم المعلومات
- التكوين المستمر لمستخدمي وفرق نظم المعلومات
- عقد الصيانة .

- وجود نظام معلومات متكامل.

مخاطر نظم المعلومات الرئيسية

- المخاطر العملية: خلل في التطبيقات، مخاطر الوقوع في الأخطاء، الازدواجية، ,,,,,,,,,,إلخ
- المخاطر المالية)القوائم المالية أو الحسابات تعكس حالة خاطئة.
- المخاطر القانونية لعدم المطابقة.

الوظائف الرئيسية لنظام كوريس CHORUS في شكل الوحدات التالية:

- وحدة المالية FI: Financial المحاسبة العامة
- وحدة الرقابة CO: Controlling مراقبة التسيير أو المحاسبة الفرعية
- وحدة تسيير المعدات MM: Material Management المشتريات وتسيير المخزونات
- وحدة العقار RE: Real Estate تسيير العقارات.

ERP :Enterprise Resource Planning

المزايا الرئيسية لأنظمة تخطيط الموارد في المؤسسة ERP هي كما يلي:

- تقليل الآجال الإدارية عن طريق التحديث الآني للبيانات
- إدخال البيانات مرة واحدة في نظام معلومات الهيئة
- توافر فوري للمعلومات
- ضمان تتبع العمليات، مسار التدقيق "مضمون" من حيث المبدأ
- يتم في بعض الأحيان إبراز تخفيض تكاليف نظم المعلومات على الرغم من الاستثمار الأولي المرتفع.

في المقابل، يتم فرض متطلبات معينة بشكل عام من خلال وضع نظام لتخطيط الموارد في المؤسسة ERP

- تنفيذ صارم وحازم
- مراجعة البنية التقنية التي يمكن أن تؤدي إلى استبدال البنى التحتية للأجهزة والشبكات
- ملاءمة العمليات والتنظيم لنظام تخطيط الموارد في المؤسسة ERP وهو ما يمكن أن يوفر فرصة للتحول إذا كان هذا الأخير متوقعا أو تمت تجربته أو، على العكس من ذلك، يمكن أن يشكل عائقا للمشروع إذا لم يكن مرغوبا فيه ولا مفترضا

ERP :Enterprise Resource Planning

- تبادل المعلومات الذي قد يؤدي إلى رفض من بعض الجهات الفاعلة
- التحكم الشامل في الحل مع مرور الوقت حيث يمكن أن تعيق بعض الحوادث الهيئة بأكملها

المخاطر المرتبطة بأنظمة تخطيط الموارد في المؤسسة ERP هي كما يلي:

- خروج المشاريع عن مسارها في الوقت والتكلفة مع مراعاة التعقيد والرهانات.
- تطوير برامج "خاصة" التي تبعد الأداة من المقياس مما يتسبب في مشاكل في التحكم في تخطيط موارد المؤسسة، بل وأيضا مشاكل من حيث قابلية التدقيق (تغيير ممكن في مسار التدقيق).
- عدم الملاءمة في نهاية المطاف بين تخطيط موارد المؤسسة والتنظيم في حالة لم يتم تعديل الإجراءات وتنفيذه من طرف المديرية العامة؛
- مستخدمون لم يتلقوا التكوين الكافي والذين يرفضون التطبيق
- اعتماد قوي على المقاولين من الباطن وعدم كفاية نقل المها ا رت في الداخل على تخطيط موارد المؤسسة
- وضع إعدادات حقوق الدخول وملفات المستخدِمين

II. نطاق عمليات تدقيق نظم المعلومات

أ. تدقيق نظم المعلومات بمناسبة المهام "العامة"

1 . تدقيق التنظيم

تستخدم الهيئات أو الإدارات نظم المعلومات يوميا. ويمكن أن يأخذ ذلك شكلا مكتبيا بسيطا، وتطبيقات مخصصة، تجعلها مرتبطة، إذا لزم الأمر، بمتعامليها المتعاقدين أو مستخدميها عبر الإنترنت، أو حتى أكثر نظم المعلومات تعقيدا.

إن أدوات نظم المعلومات هذه ضرورية للسير السليم للهيئة. فهي في بعض الأحيان في صميم أدائها.

ومع ذلك، فإن الهيئات ليست دائما على علم بها.

إن الهيئات التي تدرك أهمية نظم المعلومات لا تتقن دائما خفايا قيادته وتسييره وأمنه. تكون هذه الهيئات في بعض الأحيان قليلة أو ضعيفة التنظيم لجعل الاستفادة قصوى من هذه الموارد.

II. نطاق عمليات تدقيق نظم المعلومات

2 . تدقيق العمليات

يمكن أن تعتمد العمليات بشكل كبير جدا على أدوات نظم المعلومات. في أفضل الحالات، تعتمد على نظام إعلام آلي يلبي احتياجاتها.

لذلك يجب أن يتضمن تدقيق عملية ما تدقيقا لأدوات نظم المعلومات التي يرتكز عليها.

ويجب أن يتضمن هذا التدقيق فحصا للمعطيات والمعلومات التي تتم معالجتها أثناء سير العملية، بما في ذلك تلك التي تأتي من عمليات أخرى وتطبيقات تستخدم أو تعمل على أتمتة جزء من أو كل المهام أو الاجراءات التي تشكلها العملية، والبنى التحتية لنظم المعلومات للمعالجة والاتصال التي تستخدمها هذه العملية.

II. نطاق عمليات تدقيق نظم المعلومات

ب. مهام التدقيق التي ينتمي موضوعها الرئيسي إلى مجال نظم المعلومات

1 . تدقيق التطبيقات

يتم تصميم تطبيق وانجازه ووضع إعداداته وادارته وصيانته واستعماله من طرف أعوان ينتمون أو لا للمنظمة.

يمكن أن يكون التطبيق مفيدا لعملية واحدة أو عدة عمليات، وأن يكون متكيفا معها، أو بالعكس، يكون عائقا أمام سيرها الجيد. يمكن أن يساهم في التجانس أو الازدواجية، بل وربما في خلل في نظام نظم المعلومات. يمكن بالتالي أن يكون مصدر قوة أو ضعف الاثنين في بعض الأحيان للهيئة.

يستوجب تدقيق تطبيقٍ لنظم المعلومات فحصَ التماسك بين البرامج المعلوماتية والأجهزة التي تستخدمها، والمواءمة الاستراتيجية لنظام نظم المعلومات مع أهداف المنظمة.

2 . تدقيق مشاريع نظم المعلومات

يمكن للمدقق أن يجد نفسه أمام مشروع، والذي، عوض احت ا رم تماسك نظام نظم المعلومات، يساهم على العكس في عدم التجانس، بل وربما في فوضى في نظام نظم المعلومات.

على المدقق أن يفحص جودة التعبير عن الحاجات واستقبالها وترجمتها. في الواقع، لا يمكن للتوصيات الصادرة في نهاية التدقيق تجاهل هذه البيئة.

III. توجيه وتخطيط المهمة

أ. الاطلاع على نظم المعلومات في الهيئة

الخطوة الأولى في تدقيق نظم المعلومات هي الاطلاع على تنظيم نظم المعلومات للمنظمة الخاضعة للتدقيق.

تضم الخطوة الأولى جمع المعلومات حول نظم وعمليات نظم المعلومات للهيئة واستنتاج أثرها على الإجراءات الداخلية للعمل.

يتعلق الأمر بالخصوص بمعرفة وتقييم:

- الهيكل التنظيمي المكلف بنظم المعلومات ومكوناته (الهيئات، تعداد المستخدمين، التجهيزات والموارد) الأجهزة والتطبيقات والموارد البشرية.
- مهام، أهداف وغايات الهيكل المكلف بنظم المعلومات.
- خطة نظم المعلومات و/أو المخطط التوجيهي المعمول به.
- بنية نظم المعلومات.
- مطابقة المتطلبات القانونية.
- الأمن المعلوماتي.

III. توجيه وتخطيط المهمة

ب. وصف نظام معلومات الهيئة

تتضمن الخطوة الثانية إعداد خريطة التطبيقات.

يتضمن وصف نظام معلومات الهيئة:

- إضفاء الطابع الرسمي على خريطة التطبيقات
- تقييم درجة تعقيد نظام المعلومات
- تحديد العملية التي يتعين تحليلها.

يسمح إنجاز خريطة تطبيقات بفهم وتوثيق مكونات نظام المعلومات. وهو يسمح علاوة على ذلك بإبراز المخاطر المحتملة المتعلقة بهذه البنية.

يستوجب إعداد خريطة نظام المعلومات تحديد تطبيقات ووسائط رئيسية، وينتهي بتحديد العملية التي يتعين تحليلها.

تحديد تطبيقات نظم المعلومات الرئيسية

يتعلق تحديد تطبيقات نظم المعلومات بتعداد التطبيقات التي تشكل نظام المعلومات الخاص بالهيئة. لكل من هذه التطبيقات، من الضروري معرفة:

- اسم التطبيق
- المستخدِم
- الميزات
- استضافة على خوادم داخلية أو استضافة خارجية على خوادم خارجية
- النوع: تطوير داخلي، تطوير من قبل الغير، حزمة برمجية، ملف مكتبي
- تاريخ الوضع
- مقدم خدمة الصيانة
- تاريخ آخر تعديل
- التاريخ المتوقع لانتهاء الاستخدام

نظام التشغيل الخاص بخادم استضافة التطبيق: يونكس، ويندوز، AS400؛...

- قاعدة البيانات: خادم إس كيو إل SQL Server؛...
- مشروع التطور
- الوظائف الرئيسية
- طبيعة المخرجات
- تقدير الحجم الذي تمت معالجته
- درجة الاعتماد على التطبيق

تحديد الوسائط الرئيسية

يخص تحديد الوسائط الرئيسية الروابط الموجودة بين مختلف التطبيقات. يمكن لهذه الروابط أن تكون آلية، نصف آلية أو يدوية. لكل واسطة تم تحديدها، من الضروري معرفة:

- نوع الواسطة: آلية، نصف آلية أو يدوية
- التطبيقات القبلية) المصدر(/ البعدية) الوجهة
- نوع التدفقات: مبيعات، مخزونات، زبائن...
- بروتوكول تبادل البيانات
- الدورية: يومية، أسبوعية، شهرية
- الإطلاق
- البيانات المتبادلة
- عمليات الرقابة

١٧. تقنيات التدقيق بمساعدة الحاسوب

1 . الخطوة 1 : استرجاع ملفات نظم المعلومات

من المناسب أن نحدد مع الهيئة طبيعة الاختبارات التي سيتم إنجازها على أساس تحليل خريطة التطبيقات، يتعلق الأمر ب:

- تحديد البرامج المعلوماتية التي تشكل خطرا مثل رهانات مهمة، مبالغ كبيرة، وظائف رئيسية، الخ.
- تحديد البيانات الضرورية التي يتعين استغلالها
- استرجاع الملفات الضرورية لإنجاز اختبارات نظم المعلومات اللازمة للتدقيق.

تظهر الصعوبة الأولى من حقيقة وجود، داخل الهيئات، نظم متنوعة وبرامج معلوماتية من مصدر مختلف، والتي لا تسير نفس نوع البيانات.

إن استرجاع الملفات في نسق معين وحامل (support)مكيفيْن هي مرحلة أساسية ولكن معقدة، مع مراعاة تنوع نظم المعلومات في الهيئات) برامج معلوماتية خاصة، حزمة برمجية، اختلاف التكنولوجيا...(يكون نسق وسائط البيانات المستلمة متنوعا جدا).

١٧. تقنيات التدقيق بمساعدة الحاسوب

2 . الخطوة 2 : التحقق من صحة الملفات:

يكون التحقق من صحة الملفات على الخصوص بمقاربة الملفات المستلمة مع المحاسبة. يتعلق الأمر بالتحقق، قبل اجراء الاختبارات ، من أن البيانات المستلمة شاملة ولا يطرأ عليها أي تعديل أثناء الاستخراج.

3 . إنجاز الاختبارات:

يمكن حينئذ البدء في الاختبارات. من المهم أن يتم لاحقا إعادة انتاج الاختبارات المنجزة وأن يتم حفظ الخطوات الوسيطة.
بالتالي، يمكن أن يكون وجود دفتر للاختبارات المنجزة في البرنامج المعلوماتي للتدقيق مهما من أجل تحديدها. تؤدي هذه الخطوة إلى إنشاء ملف يحتوي على مختلف مراحل دورة الإنجاز والتحقق من صحة الملفات.

4 . التحليل والتلخيص:

تتضمن المرحلة الأخيرة تحليل وتفسير النتائج، التي تودع حينئذ في تقرير تلخيصي يصف بالخصوص الاختبارات المنجزة والتوصيات المنجرة عن ذلك.

٧. مقاربة موضوعية للمجالات الرئيسية لتدقيق نظم المعلومات

أ. تدقيق الأمن

تعد المعلومة عاملا ثمينا للهيئة، ولذلك لابد من حمايتها من الضياع، التغيير والكشف. يجب حماية الأنظمة التي تحمل هذه المعلومة بدورها من عدم التواجد ومن التسلل إليها.

تعطي دراسة الوظيفة المعلوماتية خريطة للمخاطر حول محاور الحيطة الرئيسية

يسمح حصول المدقق على الوثائق التالية، قبل الشروع في مهامه، بتقييم استراتيجية أمن نظم المعلومات:

- السياسة الأمنية
- معايير ومقاييس معمول بها
- الأشخاص والفرق المشاركين في استغلال الشبكة (نظم المعلومات المصغرة) الإدارة، الصيانة، الأمن, حامل المستخدِم، تحديد المسؤوليات
- إجراءات مطبقة أو مرتقبة (وضع الأداء الوظيفي المنخفض)
- خطط (الحفظ، الأرشفة، النسخ الاحتياطي، الاستئناف، إلخ).
- محاورون للتدقيق (المعلوماتي والمستخدِمون).

٧. مقاربة موضوعية للمجالات الرئيسية لتدقيق نظم المعلومات

ب. تدقيق المشاريع

- دراسة الفرص والتعبير عن الاحتياجات: هاتين هما الخطوتان الأوليان لمشروع ما.

يتعلق الأمر بتحليل فشل النظام الحالي من أجل الحصول في الأخير على وصف وحيد وتشاركي للجميع، ووصف لمجمل الحاجيات الواجب استيفاؤها (تطور الاحتياجات الموجودة أو احتياجات جديدة). ينبغي إعداد مختلف سيناريوهات الحلول بالإضافة إلى التقدير المتباين للتكلفة المتعلقة بذلك.

- التخطيط: على الهيئة أن تكون قادرة على تقييم وتنظيم وتخطيط إنجاز الأشغال القادمة.

وقد أصبح تشارك الموارد، سواء داخل مديرية نظم المعلومات أو الهيئات المهنية، ضرورة.

من الضروري ان نراقب هل المنظمة قادرة على تخطيط استعمال مواردها بشكل متماسك.

- هيئات الإدارة: هناك هيئات مختلفة للإدارة التي يمكن تنصيبها من أجل مرافقة مشروع ما.

يلعب كل من اختيار المؤشرات وشكلية تقديم التقارير دورا مهما أثناء اتخاذ القرار.

٧. مقاربة موضوعية للمجالات الرئيسية لتدقيق نظم المعلومات

- الطرق والأدوات: على المدقق السهر على استخدام فريق المشروع لإطار مرجعي منهجي. الصعوبات الرئيسية التي تتم مواجهتها هي نقص تناسق المخرجات، صعوبة استخدام الطريقة وعدم مطابقة الأدوات الموضوعة مع الطريقة.

- التصميم: يحدد ملف التصميم العام المعلوماتي سيناريوهات تطور نظام المعلومات مع:

  - وصف عام للحل التصميمي للتدفقات / المعالجة والبيانات
  - وصف عام للحل التنظيمي
  - وصف عام للبنية التقنية للحل (مركزية، لامركزية...)
  - الاتجاه العام لإجراءات تسيير التغيير وتنفيذه.

- التطوير والإنجاز ووضع الإعدادات: تتضمن مرحلة الإنجاز تقديم مجمل الرموز قابلة التنفيذ (البرامج) المهيكلة والموثقة التي تطابق المواصفات وتحترم أحكام خطة ضمان الجودة انطلاقا من ملف المواصفات المفصلة والمعايير والمقاييس الخاصة بإنتاج البرنامج المعلوماتي.

٧. مقاربة موضوعية للمجالات الرئيسية لتدقيق نظم المعلومات

- اختبار القبول: على كل تطبيق لنظم المعلومات أن يتم اختباره قبل المرور إلى عملية الإنتاج، من طرف المشرف على التنفيذ بداية، ومن ثمَّ من طرف صاحب المشروع (اختبار المستخدِم).

يؤطر الاجراء الرسمي قبول أو رفض التسليم.

يجب تحرير محضر بشكل منهجي في نهاية اختبار القبول (الفترة التجريبية).

يمكن تضمين جودة استرداد البيانات في المرحلة التجريبية هذه.

- إدارة التغيير والتنفيذ: زيادة على كونه رهانا حاسما في نجاح أو إخفاق مشروع ما، على التغيير من قبل المنظمات أثناء تطور نظام المعلومات أن يتم التحكم فيه وتسييره كعملية كاملة. يتعلق الأمر بمجمل الوسائل والموارد والطرق من أجل تحويل معرفة تطبيق فرقة المشروع نحو مستخدِمي ومستغلي التطبيق.

على هذه العملية أن ينجر عنها امتلاك حقيقي لنظام معلومات جديد من طرف جميع المستخدِمين منذ مرحلة البداية. يتم تنظيم مسعى إدارة التغيير/ التنفيذ في العادة في ستة مراحل:

٧. مقاربة موضوعية للمجالات الرئيسية لتدقيق نظم المعلومات

- تحديد وتقييم التغييرات
- خطة الإتصال
- خطة التكوين
- وضع نهائي للوثائق
- تنظيم الدعم
- في الحالات السهلة، يمكن لاسترداد البيانات أن يتم تضمينه في هذه المرحلة.

• الوثائق: حتى يكون التطبيق مستداما ويمكن أن يتطور، من المهم أن يتم إنتاج الوثائق. تساهم هذه الوثائق في نقل المعرفة من أجل صيانة التطبيق وتطويره واستعماله.

VI. الرقابة الداخلية في وسط نظم المعلومات

مسارات التدقيق المادية المستبدلة بمسارات البيانات. تم استبعاد عدد لا بأس به من الوثائق المادية للتدقيقات، وينبغي استعمال عمليات رقابة من أجل التدارك.

- **عطل في الأجهزة/ البرامج معلوماتية.** إن الفقدان المستمر للبيانات، بسبب ضرر بيئي، عدم التوافر.
- **أخطاء نظامية.** تقلل تكنولوجيا المعلومات من الأخطاء العشوائية، لاسيما خلال إدخال البيانات
- **إدخال بشري أقل/ فصل أقل للوظائف.** تقلل العديد من النظم المعلوماتية تكاليف العمل عبر نظام آلي.
- **ترخيص الدخول.** تزيد القدرة المتصاعدة على الدخول إلى المعلومات الحساسة عن بعد أيضا من خطر الدخول غير المصرح به.
- **ترخيص المعاملات الآلية:** إن المعاملات التي كانت تستلزم في السابق تدقيقا وترخيصا يمكن أن يتم تنظيمها كليا من طرف تطبيق معلوماتي. ئيسي.
- **أعمال ضارة طواعية:** يمكن للأعوان غير الأوفياء أو المستاءين الذين لهم دخولهم الخاص فضلا عن الأفراد الخارجيين المحفزين بالربح أو التدمير أن يتسببوا في أضرار كبيرة لمنظمة ما.

شكراً لحضوركم

آمل ان تكونوا قد حققتم الفائدة