دليل تدقيق نظم المعلومات

الفهـرس

مقدمــة

إنّ 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 التكنولوجيات الجديدة للمعلومات فضلا عن التعقيد المتزايد لنظم المعلومات الآلية إلى قيام المجلس بإعداد هذا الدليل. يسمح الدليل بتوجيه وتسهيل أشغال المدقق المكلف بتدقيق نظم المعلومات بغض النظر عن نوع الهيئة المعنية. إنّ 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 الإعلام الآلي ولكن إتقانا جيدا لممارسات التدقيق.

يتوجه هذا الدليل إلى مدققين لديهم معرفة أولية على الأقل به، أي أنّهم حضروا جلسة توعية أو قاموا بالفعل بمهمة أو مهمتي تدقيق في المجال برفقة مدقق متخصص في مجال نظم المعلومات. تمّ إكمال الدليل ببطاقات التدقيق الواردة في الملحق، ويتمّ عرضها حسب الترتيب ضمن الدليل.

تعد هذه الوثيقة النسخة الأولى، وقد تكون هناك تعديلات ضرورية لجعلها مناسبة لنظام معلومات الهيئة الخاضعة للتدقيق.

I. نظم المعلومات: رهانات ومخاطر

أ. نظام المعلومات

1. التعريف

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

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 ERP (*Enterprise Resource Planning*) 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.

2. 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 هي كما يلي:

- مشاركة قوية للإدارة في تسيير نظام المعلومات. يتعين عليها على وجه الخصوص الإشراف 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 الإعلام الآلي؛
  - التسيير الجيد لمشاريع تطوير الإعلام الآلي؛
  - التكوين المستمر لمُستخدِمي وفرق الإعلام الآلي؛
  - عقد الصيانة.

- وجود نظام معلومات متكامل.

ب. مخاطر الإعلام الآلي الرئيسية

يمكن تجميع مخاطر الإعلام الآلي الرئيسية في 3 مجالات:

- المخاطر العملية (خلل في التطبيقات، مخاطر الوقوع في الأخطاء، الازدواجية، إلخ)؛

- المخاطر المالية (القوائم المالية أو الحسابات تعكس حالة خائطة)؛
- المخاطر القانونية لعدم المطابقة (تسيير التراخيص، القانون العضوي رقم 12-05 المؤرخ في 12 يناير 2012، يتعلق بالإعلام، المرسوم رقم 09-110 المؤرخ في 7 أفريل 2009 الذي يحدد شروط وكيفيات مسك المحاسبة بواسطة أنظمة الإعلام الآلي...)

تعتبر أنظمة تخطيط الموارد في المؤسسة (ERP) حالة خاصة، مع ما تحمله من مزايا وعيوب ومخاطر محددة.

تتمتع أنظمة تخطيط الموارد في المؤسسة (ERP) بميزة تغطية العديد من المجالات المهنية الخاصة بالهيئة بواسطة تطبيق واحد عن طريق الوحدات. على سبيل المثال، يتضمن نظام تخطيط الموارد في المؤسسة الأكثر شهرة المعروف بـ ("ساب"، والذي يرتكز عليه نظام كوريس "CHORUS") في شكل وحدات، الوظائف الرئيسية التالية:

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

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 الإعلام الآلي 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؛

- 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 المهارات في الداخل على تخطيط موارد المؤسسة؛
- وضع إعدادات حقوق الدخول وملفات المستخدِمين.

II. نطاق عمليات تدقيق نظم المعلومات

يمكن لتدقيق نظم المعلومات أن يشكل إما مجالا فرعيا لتدقيق عام (التنظيم، العملية، النظامية، الخ)، أو يكون موضوعا رئيسيا للمهمة (التطبيق، المشروع، الأمن، احترام التشريع، إلخ.).

أ. تدقيق نظم المعلومات بمناسبة المهام "العامة"

1. تدقيق التنظيم

تستخدم الهيئات أو الإدارات الإعلام الآلي 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 الإعلام الآلي تعقيدا. إن أدوات الإعلام الآلي 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 الإعلام الآلي لا تتقن دائما خفايا قيادته وتسييره وأمنه. تكون هذه الهيئات في بعض الأحيان قليلة أو ضعيفة التنظيم لجعل الاستفادة قصوى من هذه الموارد.

يجب أن يتضمن تدقيق الهيئة من الآن فصاعدا تدقيقا لعلاقتها بواقع الإعلام الآلي والإجابة على الأسئلة التالية:

- كيف تحدد الهيئة احتياجاتها الوظيفية؟
- كيف تخصص مواردها البشرية والمالية من أجل تلبية هذه الاحتياجات ؟
- هل تم تنظيمها وهل وَضعت العمليات التي تسمح لها بالحصول على إعلام آلي يتناسب مع احتياجاتها (الاتساق الوظيفي)، تفاعلي، آمن وفعال؟

2. تدقيق العمليات

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

لذلك يجب أن يتضمن تدقيق عملية ما تدقيقا لأدوات الإعلام الآلي 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 الإجراءات التي تشكلها العملية، والبنى التحتية للإعلام الآلي للمعالجة والاتصال التي تستخدمها هذه العملية.

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

1. تدقيق التطبيقات

يتم تصميم تطبيق وإنجازه ووضع إعداداته وإدارته 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 الإعلام الآلي. يمكن بالتالي أن يكون مصدر قوة أو ضعف–الاثنين في بعض الأحيان–للهيئة.

يستوجب تدقيق تطبيقٍ للإعلام الآلي فحصَ التماسك بين البرامج المعلوماتية والأجهزة التي تستخدمها، والمواءمة الاستراتيجية لنظام الإعلام الآلي مع أهداف المنظمة.

2. تدقيق مشاريع الإعلام الآلي

يمكن للمدقق أن يجد نفسه أمام مشروع، والذي، عوض احترام تماسك نظام الإعلام الآلي، يساهم على العكس في عدم التجانس، بل وربما في فوضى في نظام الإعلام الآلي.

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

يمكن لتدقيق مشروع ما، خاصة إذا كان الداعي إليه هو حالة غير مرضية، أن ينجر عنه إعادة النظر في:

- كيفيات التعبير عن الحاجات المهنية واستقبالها؛
- عملية التحكيم بين المشاريع المتنافسة؛
- تنظيم إبرام الصفقات مع المشرفين على الإنجاز (Maître d'œuvre) في الإعلام الآلي، بل ومع مساعدي صاحب المشروع (Assistants du maître d'ouvrage)؛
- تسيير العمليات داخل الهيئة، لاسيما العملية التي دعت إلى مشروع التدقيق؛
- تنظيم هذه العملية؛
- تنظيم حوكمة وظيفة الإعلام الآلي.

III. توجيه وتخطيط المهمة

تتم مراعاة خصوصيات بيئة الإعلام الآلي في المراحل الأساسية من مسعى التدقيق، وهي:

- الاطلاع على الإعلام الآلي في الهيئة؛
- وضع خريطة التطبيقات.

أ. الاطلاع على الإعلام الآلي في الهيئة

الخطوة الأولى في تدقيق نظم المعلومات هي الاطلاع على تنظيم الإعلام الآلي ونظم المعلومات للمنظمة الخاضعة للتدقيق. تضم الخطوة الأولى جمع المعلومات حول نظم وعمليات الإعلام الآلي 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 بالإعلام الآلي ونظم المعلومات؛
- خطة الإعلام الآلي و/أو المخطط التوجيهي المعمول به؛
- بنية الإعلام الآلي؛
- مطابقة المتطلبات القانونية؛
- الأمن المعلوماتي.

تم وصف خطوة تدقيق هذه الخطوة الأولى في الملحق 1- بطاقة تدقيق متعلقة بالاطلاع على الإعلام الآلي للهيئة.

يسمح إنجاز هذه المرحلة للمدقق بفهم بيئة الإعلام الآلي للهيئة الخاضعة للتدقيق وتقييم إتقان الهيئة لنظم المعلومات.

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 الإعلام الآلي الرئيسية

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

- إسم التطبيق؛
- المستخدِم؛
- الميزات؛
- إستضافة 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.

تحديد الوسائط الرئيسية

لا يهتم فريق الرقابة بجميع العمليات الموجودة داخل الهيئة، ولكن فقط بتلك" التي تساهم بشكل مباشر أو غير مباشر بإنتاج بيانات مالية".

الخريطة هي أداة رئيسية لبيئة الإعلام الآلي الخاصة بالهيئة.

تم وصف مسعى التدقيق لهذه الخطوة في الملحق 2- بطاقة تدقيق متعلقة بخريطة التطبيقات فضلا عن الملحق 3-بطاقة تدقيق متعلقة بتحديد عمليات يتعين تحليلها.

IV. تقنيات التدقيق بمساعدة الحاسوب

خطوات تنفيذ تقنيات التدقيق بمساعدة الحاسوب هي:

1. الخطوة 1: استرجاع ملفات الإعلام الآلي

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

- تحديد البرامج المعلوماتية التي تشكل خطرا (رهانات مهمة، مبالغ كبيرة، وظائف رئيسية، الخ)؛
- تحديد البيانات الضرورية التي يتعين استغلالها؛
- استرجاع الملفات الضرورية لإنجاز اختبارات الإعلام الآلي 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) مُكيفيْن هي مرحلة أساسية ولكن معقدة، مع مراعاة تنوع نظم الإعلام الآلي في الهيئات (برامج معلوماتية خاصة، حزمة برمجية، اختلاف التكنولوجيا...) يكون نسق وسائط البيانات المستلمة متنوعا جدا.

2. الخطوة 2: التحقق من صحة الملفات

يكون التحقق من صحة الملفات على الخصوص بمقاربة الملفات المستلمة مع المحاسبة. يتعلق الأمر بالتحقق، قبل إجراء 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.

V. مقاربة مواضيعية للمجالات الرئيسية لتدقيق نظم المعلومات

تتداخل المواضيع السابقة "توجيه وتخطيط المهمة" و"وصف نظام معلومات الهيئة". ينبغي اعتبار المواضيع التالية على أنها تأتي كتكملة.

من المهم الإشارة إلى أنها تشكل نقاط رقابة قاعدية ذات طابع تمثيلي والتي ينبغي تكييفها مع السياق، الرهانات والمخاطر الخاصة بالتدقيق المنجز. لا ينبغي بالتالي اعتبارها على أنها شاملة أو أنها كافية بالضرورة لأشغال التدقيق.

وهي، علاوة على ذلك، مكيفة مع تنظيمات ودورات تطوير كلاسيكية، ولا يمكن بالتالي أن تكون مطبقة أو مناسبة بشكل تام لبعض أنماط التنظيم.

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: الأمن المادي لقاعات الإعلام الآلي، إجراءات حفظ تطبيقات وملفات العمل، خطة احتياطية في حالة كارثة، أمن الدخول إلى بيانات الهيئة، إجراءات مصلحة الإعلام الآلي، عملية تسيير مشاريع الإعلام الآلي.

يسمح حصول المدقق على الوثائق التالية، قبل الشروع في مهامه، بتقييم استراتيجية أمن الإعلام الآلي:

- السياسة الأمنية؛
- معايير ومقاييس معمول بها؛
- الأشخاص والفرق المشاركين في استغلال الشبكة وحظيرة الإعلام الآلي 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).

تم وصف تدقيق الأمن في الملحق 6 – بطاقة التدقيق المتعلقة بأمن الإعلام الآلي.

ب. تدقيق المشاريع

ينتج مشروع للإعلام الآلي عموما تطبيقات جديدة و/أو يحافظ على تطبيقات موجودة. ويمكن أن يتعلق الأمر أيضا بتجديد رئيسي في الأجهزة.

تعتبر إدارة المشروع عملية تسمح بالتحكم في إنجاز مشروع ما وإنجاحه.

يمر هذا التحكم بتقسيم المشروع إلى عمليات، وخطوات ومراحل وأنشطة ومهام. من الضروري أن يكون لدينا تحديد واضح لمدخلات العمليات والخطوات والمراحل والمنتجات المتوقعة وشروط المرور من مرحلة لأخرى. ينبغي تحديد دور ومسؤوليات الجهات الفاعلة بوضوح.

تنطوي إدارة مشروع ما على الخطوات التالية:

- دراسة الفرص والتعبير عن الاحتياجات: هاتين هما الخطوتان الأوليان لمشروع ما. وهما تبرزان محفزات وأسباب تنفيذ المشروع. تُتبع دراسة الفرص غالبا بدراسة التأثيرات. 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.

- 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.

يقدم الملف العناصر الضرورية لاتخاذ القرار من حيث البنية، والتجزئة والتكاليف والمخاطر والآجال.

- 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.

  تتضمن هذه المرحلة تطوير وسائط داخلية وخارجية، مواصفة الاختبارات وإعداد سيناريوهات استرداد البيانات.

  نميز بين احتمالين أثناء خطوة الإنجاز: إما أن هناك بالفعل حلا في السوق يلبي الحاجة (حزمة برمجية) والذي ينبغي وضع إعداداته حينئذ، أو يجب تطوير حل مخصص. ويتضمن الإعداد تكييف حزمة برمجية بالسياق التنظيمي التقني المستهدف من أجل الاستجابة للحاجات المعبر عنها من طرف المستخدِمين.

- الاختبارات واختبار القبول: على كل تطبيق للإعلام الآلي أن يتم اختباره قبل المرور إلى عملية الإنتاج، من طرف المشرف على التنفيذ بداية، ومن ثمَّ من طرف صاحب المشروع (اختبار المستخدِم).
  يؤطر الإجراء 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:

  - 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.

تم وصف مسعى تدقيق أمن المعلومات في الملحق 7 – بطاقة التدقيق الخاصة بمشروع الإعلام الآلي.

VI. الرقابة الداخلية في وسط الإعلام الآلي

يمكن لتكنولوجيات المعلومات أن تقضي بشكل قوي على المخاطر المتصلة بنظام يدوي، وتدخل مع ذلك مخاطرها الخاصة بها. علاوة على ذلك، بالنظر إلى طبيعة نشاطات الإعلام الآلي، يمكن لهذه المخاطر أن تؤثر على بعضها البعض:

- **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، سوء التنظيم أو كارثة على سبيل المثال، يكلف الكثير.

- **أخطاء نظامية.** تقلل تكنولوجيا المعلومات من الأخطاء العشوائية، لاسيما خلال إدخال البيانات، غير أن النظم الآلية يمكنها تكرار الأخطاء باستمرار، من خلال رمز خاطئ على سبيل المثال.

- **إدخال بشري أقل/ فصل أقل للوظائف.** تقلل العديد من النظم المعلوماتية تكاليف العمل عبر نظام آلي.
  تتضمن رقابة التخفيف التدقيق في فصل الوظائف والتدقيق من طرف المستخدِمين النهائيين لمخرجاتهم على مستوى تجميع ضعيف كفاية من أجل التمكن من الكشف عن المشاكل.

- **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. يعتمد ضمان الترخيص على عمليات رقابة البرامج المعلوماتية وسلامة الملف الرئيسي.

- **أعمال ضارة طواعية.** يمكن للأجراء/الأعوان غير الأوفياء أو المستاءين الذين لهم دخولهم الخاص فضلا عن الأفراد الخارجيين المحفزين بالربح أو التدمير أن يتسببوا في أضرار كبيرة لمنظمة ما. يمثل الزملاء الموثوق بهم الخطر الأكبر.

تتضمن رهانات تدقيق تكنولوجيات المعلومات تحديد وتقييم رقابة المخاطر المتصلة بتكنولوجيات المعلومات بشكل صحيح، وعلى المدقق:

- فهم هدف رقابة الإعلام الآلي، نوع الرقابة المعنية والأمر الذي تُوجه له؛
- تقييم أهمية رقابة الهيئة: الفوائد التي تعود للهيئة بواسطة الرقابة (على سبيل المثال، المطابقة القانونية أو المزايا التنافسية) والأضرار التي يمكن أن تحدث رقابة ضعيفة أو غير موجودة؛
- تحديد الأفراد أو الأجهزة المسؤولة عن تنفيذ مختلف المهام؛
- موازنة الخطر الذي تفرضه متطلبات إنشاء الرقابة؛
- تنفيذ إطار رقابة وخطة تدقيق مناسبين.

أ. عمليات الرقابة العامة والتطبيقية لنظم المعلومات

يمكن أن نصنف عمليات الرقابة بحيث نفهم أهدافها ونعرف أين يتم إدراجها داخل نظام الرقابة الداخلية. يسمح فهم هذه التصنيفات للمدقق بمعرفة أفضل لوضعيتها داخل نظام الرقابة والاستجابة للمسائل الجوهرية مثل:

- هل عمليات الرقابة الكشفية مناسبة من أجل تحديد الأخطاء التي من شأنها أن تفلت من عمليات الرقابة الوقائية؟

- هل عمليات الرقابة التصحيحية كافية من أجل تصحيح الأخطاء بعد الكشف عن هذه الأخيرة؟

يتضمن تصنيف حديث لعمليات رقابة نظم المعلومات فصل عمليات الرقابة العامة عن عمليات الرقابة التطبيقية.

ب. عمليات الرقابة العامة

تُطبق عمليات الرقابة العامة (عمليات الرقابة العامة لتكنولوجيات المعلومات) على مجمل مكونات، عمليات، وبيانات تنظيم معين أو بيئة نظام. من غير أن ينحصر الأمر على هذه المجالات، تتضمن عمليات الرقابة العامة حكم نظام المعلومات، تسيير المخاطر، تسيير الموارد، استغلال وتطوير وصيانة التطبيقات، تسيير المستخدِمين، الأمن المنطقي، الأمن المادي، تسيير تغيرات النظم، حفظ واسترجاع البيانات، أو استمرار النشاط.

ترتبط بعض عمليات الرقابة العامة بالمهن (على سبيل المثال، فصل وظائف أو تنظيم الحكم)، فيما تكون أخرى أكثر تقنية (مثل عمليات رقابة نظم البرامج معلوماتية، وعمليات رقابة الشبكات) وهي مرتبطة بالبنية الضمنية.
تتم مراجعة عمليات الرقابة العامة من طرف المدقق لأنها تعد أساس بيئة رقابة نظم المعلومات. إذا كانت عمليات الرقابة العامة قليلة الموثوقية (رقابة الإدخال والتغييرات على سبيل المثال)، يتعين على المدقق أن يعدل مقاربته للاختبارات للمناطق المتأثرة.

عمليات الرقابة العامة لتكنولوجيات المعلومات هي:

- عمليات رقابة الدخول المنطقي للبنية، للتطبيقات والبيانات؛

- عمليات رقابة على تسيير التغييرات في البرامج؛
- عمليات رقابة الأمن المادي على مركز المعالجة المعلوماتية؛
- عمليات رقابة حفظ واسترجاع النظم والبيانات؛
- عمليات رقابة الاستغلال.

تم عرض استعراض عمليات الرقابة العامة لتكنولوجيات المعلومات في الأقسام الأولى من هذا الدليل، وسيركز باقي الوثيقة على استعراض عمليات الرقابة التطبيقية.

ج. عمليات الرقابة التطبيقية

تغطي عمليات الرقابة التطبيقية عملية التنظيم أو تطبيقاتها وتشمل عمليات الرقابة على مستوى مدخلات، معالجات ومخرجات التطبيقات. يتعلق الأمر بالخصوص بالتصديق على البيانات، فصل المهام (مثل إدخال والترخيص لمعاملة)، ميزان المجاميع الرقابية، تسجيل المعاملات وتقارير الأخطاء.
يعد دور الرقابة أساسيا من أجل تقييم تصميمه وفعاليته. يمكن على العموم أن نميز بين عمليات الرقابة الوقائية، الكشفية والتصحيحية.

عمليات الرقابة الوقائية

تسمح عمليات الرقابة الوقائية بتجنب وقوع الأخطاء، السهو أو حوادث الأمن المعلوماتي. يتعلق الأمر على سبيل المثال بقواعد بسيطة للتصديق على البيانات بمجرد إدخالها، والتي تمنع إدخال أحرف أبجدية في حقول رقمية وعمليات رقابة الدخول والتي تصبح بفضلها البياناتُ الحساسة أو موارد النظام غير قابلة للدخول من قبل أفراد غير مأذون لهم، أو أيضا عمليات رقابة تقنية ديناميكية ومعقدة مثل برامج معلوماتية مكافحة للفيروسات، والجدران النارية وأنظمة مكافحة التسلل.

عمليات الرقابة الكشفية

تهدف عمليات الرقابة الكشفية إلى تحديد أخطاء أو حوادث تفلت من عمليات الرقابة الوقائية. يمكن لرقابة كشفية بالتالي تحديد عدد الحسابات غير النشطة أو الحسابات التي تم الإبلاغ عنها على أساس أنها يجب أن تكون موضوع مراقبة من أجل الكشف عن أنشطة مشكوك فيها.

يمكن لعمليات الرقابة الكشفية ان تأخذ أيضا شكل مراقبة أو تحليل يهدف إلى تحديث الأنشطة أو الأحداث خارج الحدود المأذون بها أو المخططات المعروفة لبعض البيانات. التي يمكن أن تخضع لمعالجة غير مناسبة. بالنسبة لتبادلات البيانات الحساسة، يمكن أن يوصى بعمليات رقابة كشفية إذا كانت رسالة ما فاسدة أو إذا لم يكن بالإمكان التحقق من هوية المرسل.

عمليات الرقابة التصحيحية

تهدف عمليات الرقابة التصحيحية إلى تصحيح الأخطاء أو الحوادث بمجرد كشفها. يمكن أن يتعلق الأمر بتصحيح بسيط لخطأ في الإدخال وتحديد وحذف المستخدِمين أو البرامج المعلوماتية غير المأذون لها، في نظام أو شبكة، أو أيضا استئناف العمل بعد الحادث أو العطل أو الكارثة.

عموما، من الناجع أكثر توقع الأخطاء أو اكتشافها على مستوى أقرب ما يكون من المصدر من أجل تسهيل تصحيحها.

تسهر نقاط الرقابة الداخلية التي تمس التطبيقات على ما يلي:

- أن كل إدخال للبيانات دقيق، كامل، مأذون به وصحيح؛
- أن كل البيانات معالجة كما كان مخططا له؛
- أن كل البيانات المخزنة دقيقة وكاملة؛
- أن كل النتائج دقيقة وكاملة؛
- أن معالجة البيانات تكون موضوع تقفي (سجلات) بدءا من إدخال إلى تخزين وإنتاج بيانات الإخراج.

تشكل رقابة التطبيق مجالا لمدققي نظام الإعلام الآلي، ومع ذلك، فهذا النوع من عمليات الرقابة التي تمثل حاليا مكونا أساسيا في التحكم في الأنشطة. يجب على جميع المدققين (الداخليين/الخارجيين) جعل ذلك أولوية.

يجب أن تكون مختلف أنواع عمليات الرقابة الشائعة موجودة في كل تطبيق:

- عمليات رقابة بيانات الإدخال: تفيد أساسا في تدقيق سلامة البينات المدخلة في تطبيق ما وأن يتم إدخالها مباشرة من طرف المستخدِمين، عن بعد من طرف شريك أو من خلال تطبيق على الويب. يسمح التدقيق في البيانات بضمان أن تحترم المقاييس المحددة.

- عمليات رقابة المعالجة: تقدم وسيلة آلية لضمان أن المعالجة كاملة ودقيقة ومأذون بها.

- عمليات رقابة بيانات الإخراج: تغطي ما تم إنجازه من البيانات. وينبغي أن تقارن بين النتائج المتحصل عليها مع النتائج المرجوة، والتدقيق فيها بالنسبة لما تم إدخاله.

- عمليات رقابة السلامة: يمكن أن تطبق بشكل دائم على البيانات قيد المعالجة و/أو المخزنة، من أجل ضمان أن تبقى متماسكة ودقيقة.

- قابلية التعقب: تسمح معالجة تاريخ عمليات الرقابة السابقة، ما نسميه عادة بمسار التدقيق، للإدارة بتتبع المعاملات من المصدر وصولا إلى النتيجة النهائية أو الصعود ابتداء من النتائج إلى المعاملات والأحداث المسجلة التي ولّدتها. على عمليات الرقابة هذه أن تسمح بمراقبة فعالية مجمل عمليات الرقابة والكشف عن الأخطاء بشكل استباقي قدر الإمكان.

1. خطة التدقيق

على المدققين إعداد خطة لكل مهمة تدقيق. على هذه الخطة أن تذكر أهداف، نطاق، موارد وبرنامج العمل. تسمح الأهداف للمدقق بتحديد ما إذا كانت عمليات الرقابة التطبيقية مصممة جيدا وتعمل بشكل فعال، من أجل تسيير المخاطر المتعلقة بالاتصال المالي، واحترام التنظيم والمقاييس العملية.

تهدف عمليات الرقابة التطبيقية إلى التدقيق في:

- أن بيانات الدخول دقيقة، كاملة، مأذون بها وصحيحة؛
- أن البيانات معالجة وفقا للأهداف وفي أجل مقبول؛
- أن البيانات المخزنة دقيقة وكاملة؛
- أن نتائج الخروج دقيقة وكاملة؛
- أن عمليات دخول، تخزين وإخراج البيانات محفوظة في الأرشيف.

نقترح خطة التدقيق التالية التي يمكن تكييفها بحسب الوضعية التي يتم مواجهتها:

مثال على خطة تدقيق يحدد فحص البيانات الخاصة بالهيئة فضلا عن نطاق التدقيق خطوات الاستعراض المفَصل للنشاطات التالية.	
الهدف 1: بيانات الدخول دقيقة، كاملة ومأذون بها وصحيحة	
عمليات الرقابة	**الأنشطة المتصلة بالمراجعة**
عمليات الرقابة التي تغطي بيانات الدخول مصممة وتعمل بفعالية بحيث تسهر على كون جميع المعاملات تم الإذن بها والتصديق عليها قبل إدخال البيانات.	الحصول على إجراءات إدخال البيانات، وفهم عملية الإذن والتصديق، وتحديد ما إذا كان هناك عملية فحص وتصديق، وما إذا تم إبلاغ المستخدِمين المكلفين بالحصول على التراخيص الموافقة لها. فحص كون مالك التطبيق أو العملية يسهر على كون جميع البيانات مأذونا بها قبل إدخالها. يمكن تحقيق هذا الضمان من خلال تقسيم الأدوار والمسؤوليات وفقا لوظائف كل منصب. الحصول على نسخة من مستويات التراخيص وتحديد ما إذا تم تكليف شخص للتدقيق في الاحترام الدائم للتراخيص الموافقة.
عمليات الرقابة التي تغطي بيانات	الحصول على إجراءات إدخال البيانات والتدقيق في كون الأفراد المسؤولين عن

الدخول مصممة وتعمل بفعالية بحيث تسهر على كون جميع المعاملات التي جرى إدخالها معالجة بشكل صحيح وكلي.	إدخال البيانات قد تم تكوينهم على إعداد وإدخال ورقابة بيانات الدخول. تحديد هل وتيرة الإصدار مدمجة في التطبيق الذي يتحقق ثم يرفض المعلومات التي لا تستوفي بعض المعايير: تواريخ غير صحيحة، أحرف غير صالحة، أطوال الحقول غير الصحيحة، بيانات ناقصة، وإدخالات/ أرقام المعاملات المزدوجة (القائمة ليست شاملة). فحص وجود وعمل عمليات الرقابة اليدوية لتجنب الإدخالات المتكررة. قد تتضمن عمليات الرقابة اليدوية الترقيم المسبق للوثائق المصدر ووضع عبارة "مُدخل" بعد الإدخال. التدقيق هل البيانات المضافة تأتي من مصدر مقبول ويتم مقاربتها بهذا المصدر باستخدام المجاميع الرقابية وعدد التسجيلات والتقنيات الأخرى، مثل تقارير المصدر المستقلة. تحديد ما إذا كان فصل الوظائف كافيا لتجنب أن يقوم المستخدِمون بالإدخال ويعطوا إذنا للمعاملات. التحقق من أن فصل الوظائف كاف بين الأفراد الذين يدخلون البيانات وأولئك الذين كُلفوا بمقاربة والتدقيق في دقة وشمولية بيانات الخروج. التحقق من أن عمليات الرقابة موجودة لتجنب التغييرات غير المأذون بها.
عمليات الرقابة التي تمس بيانات الدخول مصممة وتعمل بفعالية بحيث تسهر على كون جميع المعاملات التي تم رفضها قد تم تحديدها وإعادة معالجتها بشكل صحيح وكلي.	الحصول على إجراءات إدخال البيانات من أجل معالجة المعاملات المرفوضة والتصحيح البعدي للأخطاء والتحقق من أن المستخدَمين المسؤولين عن تصحيح الأخطاء وإعادة إدخال البيانات قد تلقوا التكوين المناسب. التحقق من أن هناك آلية تسمح بتحذير مالك العملية بأن المعاملات قد تم رفضها أو أن أخطاء قد حدثت. التحقق من أن العناصر المرفوضة تتم معالجتها بشكل صحيح وفي الآجال المحددة، وفقا للإجراءات.
عمليات الرقابة مصممة وتعمل بفعالية بحيث تسهر على كون البيانات المرسلة بشكل آلي، من نظام آخر، معالجةٌ بشكل صحيح	الحصول على الإجراءات والتحقق من وجود المعلومات المفصلة عن إجراء إذن الوسائط الآلية وعن العناصر التي تطلق المعالجة الآلية. التحقق من أن رزنامات المعالجة مودعة في وثيقة وأن المشاكل محددة ومصححة

وكامل.	سريعا. تحديد هل عد التسجيلات من النظام إلى النظام ومجموع القيم النقدية مدقق فيها بشكل نظامي للوسائط الآلية وهل هناك منع للعناصر المرفوضة حتى تظهر وهل تم تدوينها من أجل المتابعة والمعالجة. التحقق من أن كل الملفات وكل البيانات، التي يتم إنشاؤها لتُستعمل من قبل تطبيقات أخرى أو التي يتم نقلها لتطبيقات أخرى، محمية ضد جميع التعديلات غير المأذون بها خلال كل عملية التحويل.
عمليات الرقابة مصممة وتعمل بفعالية بحيث يتم استعمال الملفات الجيدة للبيانات وقواعد البيانات أثناء المعالجة.	التأكيد على أن البيانات والبرامج التجريبية مفصولة عن الإنتاج.
الهدف 2: تتم معالجة البيانات طبقا للأهداف وفي أجل مقبول	
عمليات الرقابة	**الأنشطة المتصلة بالمراجعة**
عمليات الرقابة على المعالجة مصممة وتعمل بفعالية حتى تكون جميع المعاملات معالجة بشكل سريع وخلال الفترة المحاسبية الموافقة.	التحقق من أن بيانات الاخراج يتم فحصها أو مقاربتها مع وثائق المصدر من أجل تأكيد شموليتها ودقتها، لاسيما عن طريق التدقيق في المجاميع الرقابية. تحديد ما إذا كان التطبيق يحتوي على وتيرة تضمن أن جميع العمليات، المُدخلة بشكل صحيح، معالجة ومسجلة جيدا كما كان متوقعا للفترة المحاسبية الموافقة.
عمليات الرقابة على المعالجة مصممة وتعمل بفعالية حتى تكون جميع المعاملات المرفوضة محددة ومعالجة بشكل سريع.	الحصول على إجراءات معالجة المعاملات المرفوضة وتصحيح الأخطاء وتحديد ما إذا كان المستخدَمون المكلفون بتصحيح الأخطاء وإعادة إدخال البيانات قد تلقوا التكوين المناسب. التحقق من أن آلية تقوم بتحذير مالك العملية بأن المعاملات قد تم رفضها أو أن أخطاء قد حدثت. التحقق من أن العناصر المرفوضة تتم معالجتها بشكل صحيح وسريعا، طبقا للإجراءات، وأن الأخطاء يتم تصحيحها قبل إعادة إدخالها في النظام.
الهدف 3: البيانات المخزنة دقيقة وكاملة	
عمليات الرقابة	**الأنشطة المتصلة بالمراجعة**
عمليات رقابة الدخول المنطقي مصممة وتعمل بفعالية من أجل	الحصول على إعداد وإجراءات استعمال كلمات السر والتحقق من وجود معايير إلزامية بخصوص كلمات السر، تجديد كلمات السر، قفل الحساب وإعادة استعمال

منع الدخول والتعديل أو الإفشاء غير المأذون به لبيانات النظام	كلمات السر. التحقق من أن الأحكام الموصوفة أعلاه مطبقة بشكل جيد على التطبيقات الخاضعة للفحص. التحقق من أن عمليات رقابة الدخول عن بعد مصممة وتعمل بفعالية. التحقق من أن المستخدِمين لا يمكنهم تنفيذ سوى وظائف محددة، طبقا للمسؤوليات المتأصلة في منصبهم (الدخول القائم على الأدوار). التحقق من أن أرقاما وحيدة للتعريف بالمستخدِم قد تم منحها لكل المستخدِمين، بما في ذلك المستخدِمين المُميزين، وأن حسابات المستخدِمين والإداريين لا يتم مشاركتها. التحقق من أن إنشاء أو تعديل حسابات المستخدِمين مأذون بها قانونيا قبل منح الدخول أو تعديله. (المستخدِمون هم المستخدِمون المميزون، الإجراء، المقاولون من الباطن، الموردون والمندوبون). التحقق من أن الدخول محذوف مباشرة مع نهاية عقد العمل. التحقق من أن مالك التطبيق يسهر على إنجاز فحص سداسي لحسابات المستخدِمين والنظام من أجل تأكيد أن الدخول للبيانات المالية والتطبيقات والنظم العملياتية الحرجة صحيح وخاضع للتحديث.
عمليات الرقابة مصممة وتعمل بفعالية من أجل السهر على كون حفظ البيانات صارما وكاملا وسريعا.	التحقق من أن إنشاء أو تعديل حسابات المستخدِمين مأذون بها قانونيا قبل منح الدخول أو تعديله. (المستخدِمون هم المستخدِمون المميزون، الإجراء، المقاولون من الباطن، الموردون والمندوبون). التحقق من أن الدخول محذوف مباشرة مع نهاية عقد العمل. التحقق من أن مالك التطبيق يسهر على إنجاز استعراض سداسي لحسابات المستخدِمين والنظام من أجل تأكيد أن الدخول للبيانات المالية والتطبيقات والنظم العملياتية الحرجة صحيح وخاضع للتحديث.
عمليات الرقابة مصممة وتعمل بفعالية من أجل السهر على كون البيانات مخزنة بشكل مادي في مكان آمن، خارج الموقع وفي بيئة	التحقق من أن آليات منصبة من أجل تخزين بيانات خارج الموقع في مكان آمن وبيئة خاضعة للرقابة.

خاضعة للرقابة.	
الهدف 4: بيانات الخروج دقيقة وكاملة	
عمليات الرقابة	**الأنشطة المتصلة بالمراجعة**
عمليات الرقابة على المخرجات مصممة وتعمل بفعالية بحيث تسهر على كون جميع النتائج المتحصل عليها من المعاملات كاملة ودقيقة.	الحصول على إجراءات خروج البيانات، وفهم عملية الفحص والتحقق من أن الأفراد المسؤولين عن الإدخال مكونين على التحليل والتدقيق في مخرجات البيانات. التأكد من أن بيانات الخروج يتم فحصها ومقاربتها مع الوثائق المصدر من أجل التحقق من شموليتها ودقتها، بما في ذلك ما يكون من خلال التحقق من مجاميع الرقابة.
عمليات الرقابة على المخرجات مصممة وتعمل بفعالية بحيث تسهر على كون جميع النتائج المتحصل عليها من المعاملات منشورة للمستخدَمين المناسبين وأن المعلومات الحساسة والسرية محمية خلال النشر.	فحص الإجراءات القائمة حول مخرجات البيانات وتحديد ما إذا كانت تحدد أيٌ من المستخدَمين (personnel) يتلقاها وكيف يتم حماية هذه البيانات خلال نشرها.
عمليات الرقابة على المخرجات مصممة وتعمل بفعالية بحيث تسهر على انشاء تقرير الخروج في الوقت المحدد، ويغطي الفترة المشار إليها.	التحقق من إنشاء تقرير الخروج وأن تاريخ ووقت التقرير يتطابقان جيدا مع الوقت المحدد. التحقق من أن التقرير يغطي الفترة المشار إليها بالمقاربة مع الوثائق المصدر لهذه الفترة.
الهدف 5: عمليات إدخال البيانات وتخزينها وإخراجها تتم أرشفتها	
عمليات الرقابة	**الأنشطة المتصلة بالمراجعة**
عمليات الرقابة مصممة وتعمل بفعالية من أجل السهر على توليد مسار تدقيق وتحديثه لكل البيانات المتعلقة	التحقق من وجود مسارات ويوميات التدقيق التي تؤكد أن كل الملفات تمت معالجتها وتسمح بتتبع المعاملة من إدخال البيانات إلى تخزينها وإخراجها. التحقق من وجود تقارير تدقيق تقتفي تحديد وإعادة معالجة المعاملات المرفوضة. على هذه التقارير أن تحتوي على وصف واضح للمعاملة المرفوضة، والتاريخ والوقت المشار إليه.

2. عمليات الرقابة التطبيقية الجارية واقتراح الاختبارات

تصف الفقرات التالية عمليات الرقابة التطبيقية (أنظر الملحق 7) المشتركة مع الاختبارات المقترحة لكل رقابة.

أ. رقابة المدخلات

يتم تصميم عمليات الرقابة هذه من أجل إعطاء ضمان معقول أن البيانات المستلمة من أجل المعالجة بالإعلام الآلي مأذون بها قانونا ومحولة إلى شكل يمكن أن يتم استيعابه آليا، وألا يتم فقدان بيانات ولا حذفها ولا إضافتها ولا تكرارها أو تعديلها بشكل غير قانوني. تتضمن عمليات رقابة المدخلات الآلية إجراءات تدقيق وتصديق على البيانات مثل الأرقام الرئيسية، وعدد التسجيلات، والمجاميع الرقابية والمجاميع المالية للرقابة، بينما تجمع وتيرة الإصدار الآلي، المصممة للكشف عن الأخطاء في البيانات، عمليات رقابة صحة الحروف، وعمليات رقابة البيانات الناقصة، واختبارات التتابع وعمليات تدقيق المعقولية.

يُظهر الجدول أدناه عمليات رقابة الإدخالات والاختبارات الموصى بها.

عمليات رقابة المدخلات والدخول		
تسمح عمليات الرقابة هذه بفحص كون كل بيانات الإدخال دقيقة وكاملة ومأذونا بها.		
المجال	**الرقابة**	**الاختبارات الممكنة**
الفحص والتحقق من صحة البيانات	• عمليات تدقيق المعقولية على القيم المالية. • عمليات الرقابة على النسق والحقول المطلوبة، شاشات الإدخال القياسية • عمليات رقابة التتابع (على سبيل المثال: العناصر الناقصة)، رقابة الحدود والأرقام الرئيسية. • تدقيق إسنادي (لا تكون بعض السياسات صحيحة إلا مع وجود بعض رموز جدول فرق القيمة). • التحقق من صحة البيانات (على سبيل المثال: جدول الذاكرة والقائمة المنسدلة للعناصر الصحيحة). • تحديد من يمكنه تغاضي عمليات الرقابة.	• اختبار العينات لكل سيناريو. • ملاحظة محاولات ادخال بيانات غير صحيحة. • تحديد من يمكنه التغاضي عن عمليات الرقابة. • تحديد من يمكنه تغيير التعديلات ومستويات السماح إذا كانت مسيرة بالجداول.
الإذن والموافقة الآليين والتجاوز (contournement)	• يتم منح حقوق الإذن (بالنسبة للنفقات مثلا، دفع الديون أو الاعتمادات فوق عتبة معينة) لمستخدِمين معينين على أساس أدوارهم وحاجتهم إلى استعمال التطبيق.	• مباشرة اختبارات على أساس حقوق دخول المستخدِمين. • فحص امتيازات الدخول لكل وظيفة أو معاملة حساسة.

	• يتم تخصيص القدرة على التغاضي (الإذن بديون بمبلغ مرتفع خلافا للعادة) لبعض المستخدِمين، على أساس أدوراهم وحاجتهم لاستعمال التطبيق.	• فحص حقوق الدخول التي تثبت وتعدّل الحدود القابلة للضبط للموافقة أو الإذن.
الفصل الآلي لوظائف وحقوق الدخول	• لا يمكن للأفراد الذين يقررون من هم الموردون المعتمدون التزام معاملات الشراء. • ينبغي ألا يكون بوسع الأفراد، الذين يستطيعون الدخول إلى معالجة الديون، تحديد سياسة أو تعديلها.	• إجراء اختبارات على أساس حقوق دخول المستخدِمين. • فحص حقوق الدخول التي تثبّت وتعدل الأدوار القابلة للضبط أو بنية القائمة.
عناصر قيد الانتظار	• يفحص المشرفون يوميا أو مرة في الأسبوع التقارير الزمنية التي تظهر عناصر جديدة للسياسات التي تكون معالجتها غير كاملة. • الملفات قيد الانتظار والتي تكون المعلومات المتوفرة بشأنها غير كافية حتى تسمح بمعالجة للمعاملة.	• فحص نتيجة التصنيف الزمني ودليل إجراءات الفحص الذي يجريه المشرف. • السير ضمن عينة نحو وابتداء من التقرير الزمني أو الملف قيد الانتظار.

عمليات رقابة إرسال الملفات والبيانات		
تسمح عمليات الرقابة هذه بفحص كون كل الملفات والمعاملات مرسلة داخليا أو خارجيا بشكل إلكتروني من مصدر محدد ومعالجة بشكل دقيق وكامل.		
المجال	**الرقابة**	**الاختبارات الممكنة**
عمليات رقابة إرسال الملفات	• رقابة شمولية وصحة المحتوى، بما في ذلك تاريخ ووقت وحجم البيانات، وحجم التسجيلات والتصديق على المصدر.	• مراقبة تقارير الإرسال والأخطاء. • مراقبة إعدادات الصحة والشمولية والضبط. • فحص حقوق الدخول إلى تحديد وتعديل الإعدادات القابلة للضبط لتحويل الملفات.
عمليات رقابة إرسال البيانات	• تطبيق بعض عمليات الرقابة على المدخلات من أجل التصديق على البيانات المستلمة (على سبيل المثال: الحقول الرئيسية، المعقولية، الخ)	• اختبار عينات لكل سيناريو • مراقبة محاولات إدخال بيانات غير صحيحة. • تحديد من يمكنه التغاضي عن الرقابة.

		• تحديد من يمكنه تغيير الاصدارات ومستويات السماح.

ب. عمليات رقابة المعالجة

يتم تصميم عمليات الرقابة من أجل جلب ضمان معقول أن معالجة البيانات جرى كما كان متوقعا، من غير سهو أو تسجيل مزدوج لها. إن رقابة المعالجة هي في جزء كبير منها نفس رقابة المدخلات، خاصة بالنسبة لنظم المعالجة عبر الانترنت، أو في الوقت الفعلي، غير أنها مطبقة خلال مراحل المعالجة. عمليات الرقابة هذه هي المجاميع الوسيطة، تقارير المجاميع الرقابية، عمليات رقابة الملفات والمتعاملين، مثل العلامات الخارجية والداخلية للنوعية، يوميات نظامية لعمليات الإعلام الآلي واختبارات المعقولية.

عمليات رقابة المعالجة		
تسمح عمليات الرقابة هذه بفحص كون بيانات الإدخال صحيحة وتمت معالجتها بشكل دقيق وكامل.		
المجال	**الرقابة**	**الاختبارات الممكنة**
تحديد الملفات والتحقق الآلي من صحتها.	• الملفات التي يتعين معالجتها موجودة وكاملة.	• فحص عملية التحقق من صحة الملفات وعمل الاختبار.
الميزات الآلية وعمليات العد.	• عد محدد منجز على مدخل واحد أو عدة مدخلات وعناصر البيانات المخزنة التي تُنتج عناصر بيانات أخرى. • استعمال جداول بيانات موجودة (على سبيل المثال: الملفات الرئيسية أو البيانات المرجعية مثل السُلّم).	• مقارنة قيم المدخلات والمخرجات لكل السيناريوهات حسب المسلك وحسب إعادة التنفيذ. • فحص عمليات رقابة صيانة الجداول ومن بإمكانه تغيير الإصدارات ومستويات السماح.
مسارات التدقيق والتجاوز (contournement)	• متابعة آلية للتغييرات التي تم إدخالها على البيانات، مع إسناد التغيير إلى مستخدِم محدد. • متابعة آلية وإبراز تجاوز الإجراءات العادية.	• فحص تقارير وأدلة عمليات التدقيق. • فحص حقوق تجاوز الإجراءات العادية.
استخراج وتمحيص وإيصال	• معقولية وشمولية مخرجات وتيرة	• فحص تصميم وتيرة الاستخراج

البيانات	الاستخراج قد تمت رقابتها. • التخصيص الآلي للمعاملات (على سبيل المثال: لأغراض إعادة التأمين، عمليات اكتوارية أخرى أو تخصيص للأموال). • تقييم البيانات المستخدِمة من أجل الشروع في التقديرات لأعراض الاتصال المالي.	بالنسبة لملفات البيانات المستخدِمة. • فحص تقييم المشرفين لنتائج وتيرة الاستخراج من أجل التحقق من أن فحصا منتظما يتم القيام به وهل هناك من مشاكل. • فحص الأساس الصحيح لعينة تخصيص. • فحص عملية تقييم شمولية وصحة البيانات المستخرجة.
توازن في الواسطة	• الفحص الآلي للبيانات المستلمة من النظم القبلية (على سبيل المثال: بيانات حول المرتبات، الديون، الخ) من طرف مستودعات البيانات أو الدفاتر الكبيرة. • فحص آلي للمطابقة بين أرصدة النظامين. في حالة عدم المطابقة، يتم توليد واستعمال تقرير استثناء.	• تفتيش تقارير الأخطاء في الواسطة. • تفتيش إعدادات وضبط الصحة والشمولية. • فحص حقوق الدخول إلى عملية الضبط وإلى تعديل الإعدادات القابلة للضبط على الوسائط. • فحص أدلة تقارير المطابقة، وفحوص ومعالجة الملفات التي تحتوي على أخطاء.
الميزات الآلية والتصنيف الزمني	• مستخرجات ملفات قوائم المدينين من أجل تقديم معلومات لمسؤولي البينات عن المعاملات حسب ترتيب زمني.	• اختبار عينات للمعاملات على هذه القوائم من أجل التحقق من صحة عملية التصنيف الزمني.
عمليات رقابة الازدواجية	• مقارنة كل معاملة بالمعاملات السابقة المسجلة من أجل تحقيق تطابق الحقول. • مقارنة كل ملف مع التواريخ، الأوقات، الأحجام المتوقعة، إلخ.	• فحص حقوق الدخول إلى عملية الضبط وإلى تعديل الإعدادات القابلة للضبط على المعاملات أو الملفات المزدوجة. • فحص عملية استعمال الملفات أو المبادلات المرفوضة.

ج. عمليات رقابة المخرجات

تم تصميم عمليات الرقابة هذه حتى تجلب ضمانا معقولا أن نتائج المعالجة دقيقة ومنشورة حصريا للمستخدَمين المخولين بذلك. من المناسب إجراء مقارنة ومقاربة مجاميع رقابة الإخراج خلال المعالجة بمجاميع رقابة الإدخال والمجاميع الرقابة البينية المنتجة أثناء المعالجة. من المناسب مقارنة تقارير التعديل التي يولدها الحاسوب للملفات الرئيسية بالوثائق المصدر الأصلية من أجل التحقق من أن المعلومات صحيحة.

عمليات رقابة المخرجات		
تسمح عمليات الرقابة هذه بفحص كون بيانات الإخراج كاملة، دقيقة ومنشورة لمن يهمه الأمر.		
المجال	**الرقابة**	**الاختبارات الممكنة**
النقل على الدفتر الكبير العام	• كل عمليات نقل المعاملات الفردية والملخصة على الدفتر الكبير.	• رفع عينة من المعاملات المُلخّصة للإدخال وعينات من الدفتر الكبير المساعد إلى غاية الدفتر الكبير المساعد.
النقل على الدفتر الكبير العام	• كل عمليات نقل المعاملات الناجحة على الدفتر الكبير المساعد.	• رفع عينة من معاملات الإدخال إلى غاية الدفتر الكبير المساعد.

عمليات رقابة الملفات الرئيسية والبيانات المرجعية		
تسمح عمليات الرقابة هذه بفحص سلامة ودقة الملفات الرئيسية والبيانات الدائمة		
المجال	**الرقابة**	**الاختبارات الممكنة**
الإذن بالتحديث	• حقوق الدخول إلى عمليات التحديث المسندة إلى كبار المستخدِمين على أساس أدوارهم وحاجتهم إلى استعمال التطبيق.	• فحص حقوق الدخول على ضبط وتعديل الملفات الرئيسية والبيانات المرجعية.

VII. المعايير الدولية المرجعية

تشكل الأطر المرجعية للرقابة الداخلية لتسيير مخاطر المؤسسة للجنة المنظمات الراعية للجنة تريدواي (كوسو) مصادر معلومات يتم استقاء معلومات منها بشكل متكرر، ولكن هذه الأطر لا تتمركز بشكل خاص حول نظم المعلومات. ينبغي أن يتم إكمال بيئة الرقابة التي تعتمد على لجنة المنظمات الراعية للجنة تريدواي بأهداف أكثر تفصيلا لرقابة نظم المعلومات، والتي ستسمح بالتقييم بشكل أكثر فعالية لبيئة رقابة نظم المعلومات.

هناك عدد معين من الفرص في هذا الصدد، ويمكن للمعايير المذكورة أدناه أن يتم أخذها بعين الاعتبار:

1. أهداف الرقابة المتعلقة بالمعلومات والتكنولوجيات المتصلة بها (كوبيت)

نشر بدايةً سنة 1994 من طرف جمعية التدقيق والرقابة على نظم المعلومات (إيساكا)، يعتبر كوبيت أحد النظم المرجعية لرقابة وحكم نظم المعلومات شائعة الاستخدام.

تم نشر النسخة 0.5 من الكوبيت بتاريخ ديسمبر 2013، وليس القصد من الكوبيت أن ينافس الكوسو أو غير ذلك من النظم المرجعية، ويمكن أن يُستخدم كتكملة لها من خلال إثرائها بأهداف رقابية لنظم المعلومات أكثر استهدافا.

يقترح نظامٌ مرجعيٌ مثل الكوبيت سلسلة من الأهداف الرقابية لنظم المعلومات المقبولة عادة، والتي تساعد المدقق على تصميم سياسة تقييم وتسيير للمخاطر المتعلقة بنظم المعلومات.

2. إيزو 27001 – إيزو 27001

أصدرت المنظمة الدولية للمعايير (ISO) معيارا عاما معترف به دوليا حول سلامة نظم المعلومات. كان الأمر في البداية متعلقا بمعيار بريطاني (BS7799)، والذي تم تحويله إلى معيار إيزو والذي يعرف حاليا باسم إيزو 27001 – تقنيات الأمن– نظم تسيير أمن المعلومات.

يمثل هذا المعيار الممارسات الجيدة المقبول بها عادة فيما يتعلق بتسيير أمن نظم المعلومات، ويشكل وثيقة مرجعية نافعة يمكن من خلالها لمدققي نظم المعلومات أن ينجزوا مهامهم بشكل جيد.

http://www.iso.org

3. إيساي 5310 – توجيهات حول منهجية مراجعة أمن نظام المعلومات، باللغة الإنجليزية فقط (Information System Security Review Methodology)

تم تحرير التوجيهات حول رقابة أمن المعلومات (SSI) في ثلاث مجلدات:

- يقترح المجلد 1 على المؤسسات العليا للرقابة (ISC) طريقة لمراجعة سهلة ويدوية لنظام المعلومات، ولاسيما حينما تكون الموارد محدودة أو إذا كانت رقابة مفصلة أكثر غير ضرورية.
- يعتبر المجلد 2 طريقة أكثر تطورا مرتكزة إلى القيمة النقدية للمخاطر التي تتعرض لها نظم المعلومات. وهي تعتمد على منظور ينتقل " من القمة إلى القاعدة" فيما يخص المعلومة وما تمثله من حيث القيمة للمؤسسة، والمخاطر، ومخاطر الأمن، وهي تصوغ التوصيات.
- يظهر المجلد 3 المنهجيات المفصلة من أجل ضمان أمن نظام المعلومات. وتحاول هذه المنهجيات قياس التأثير النقدي الصافي لمخاطر أمن المعلومات والتدابير المضادة الموضوعة.

4. دليل التدقيق المعلوماتي 2014 (WGITA IDI)

تم وضع دليل التدقيق المعلوماتي (IT Audit Handbook) من طرف فريق عمل الإنتوساي المعني بتدقيق تكنولوجيا المعلومات (WGITA) ومبادرة الإنتوساي للتنمية (IDI)، والهدف الأساسي منه هو دعم المدقق في التخطيط لعمليات تدقيق الإعلام الآلي وإنجازها.

يقدم الدليل أداة عمل مكيفة مع المؤسسات العليا للرقابة والذي يتبع المبادئ العامة للتدقيق المنصوص عليها في المعايير الدولية للأجهزة العليا للرقابة المالية العامة (إيساي). يمكن للدليل أن يكمل الأطر المرجعية المنصوص عليها في النماذج الأخرى مثل نموذج إساكا كوبيت، وذلك الخاص بالمنظمة الدولية للمعايير (ISO) أو للمعايير، وبأدلة وكتيبات بعض المؤسسات العليا للرقابة.

وضع السيد كاردوسو (Cardoso) أداة في إطار النشاط أ.4.2.2. تعتمد هذه الأداة على دليل التدقيق المعلوماتي وتستعمل بيئة إكسيل: انطلاقا من استبيان يعتمد على تقييم المخاطر، تقترح هذه الأداة اختبارات يتعين على المدققين أن ينجزوها. تم تسليم الأداة من طرف السيد كاردوسو لأعضاء مجموعات عمل مجلس المحاسبة الجزائري.

الملاحق

الملحق 1. بطاقة تدقيق تفصيلية متعلقة بالاطلاع على الإعلام الآلي للهيئة

الديباجة

الهدف من التدقيق هو تقييم "النضج" المعلوماتي للتنظيم وملاءمة دور، وتموقع وأهداف مديرية نظم المعلومات (DSI) مع رهانات الهيئة.

الملفات التي يتعين طلبها هي:

- المخطط التنظيمي للبنية المكلفة بنظم المعلومات؛
- بطاقات مهام مختلف مسؤولي نظم المعلومات؛
- معلومات لها علاقة بالأهداف والسياسات والتوجيهات بخصوص نظم المعلومات والإعلام الآلي؛
- خطط الإعلام الآلي ومخططات توجيهية؛
- بنية وخريطة نظم المعلومات؛
- قائمة تجهيزات الإعلام الآلي (معدات، برامج معلوماتية، تطبيقات...) ؛
- ميثاق الإعلام الآلي؛
- إجراءات وسياسات الأمن المعلوماتي؛
- ميزانية الإعلام الآلي للسنوات الثلاثة الأخيرة فضلا عن الميزانيات التقديرية؛
- توصيل المشاريع الجارية أو المرتقبة؛
- العقود المبرمة مع متعاملي الهاتف النقال ومزودي الدخول على الأنترنت.

الأشخاص الذين تتم مقابلتهم في إطار تدقيق التنظيم المعلوماتي ونظم المعلومات هم:

- مديرية الهيئة الخاضعة للتدقيق؛
- مسؤولي الإعلام الآلي ونظام معلومات المنظمة الخاضعة للرقابة؛
- عينة تمثيلية للمستخدِمين والمسيرين المعنيين (مستخدِمين أساسيين تمثيليين).

تدقيق نظام المعلومات	البطاقة رقم: 1
أخذ البيئة المعلوماتية بعين الاعتبار	الطبعة: 0.1 مصادق عليه في: نوفمبر 2016 من طرف:

	سؤال حاسم

	الأجوبة	التأثير على موثوقية نظام المعلومات			التنقيط (على 3)	التعليقات
		ض	م	ع		
1. دور وتموقع الإعلام الآلي في الهيئة					2,08	
ما هي البنية التنظيمية لمديرية نظم المعلومات (م ن م) للهيئة؟		X			1	
بماذا يتم ربط مديرية نظم المعلومات؟ يتم ربطها بالمديرية العامة؟ (تقييم درجة إشراك وتحكم المديرية العامة في نظم معلومات الهيئة)				X	3	
هل هناك لجان "معلوماتية" (استراتيجية، توجيهية... تجمع مختلف مديريات الهيئة المكلفة بتعداد الحاجيات والفرص، وتسيير الأولويات ومتابعة المشاريع، وتقييم دور ووزن اللجان؟						
2. تنظيم وبنية مديرية نظم المعلومات					2,33	
فحص وجود ميثاق معلوماتي آلي أو أية وثيقة أخرى تحدد دور ونطاق مسؤولية م ن م.						
إذا لم تكن هذه الوثيقة موجودة، شرح كيف يتحدد مجال تدخل م ن م.			X		2	
وصف موجز للمسؤوليات والمهام والصلاحيات داخل م ن م.						
فحص وجود مخطط تنظيمي محين لـ م ن م.						
هل هناك تحديد لوظائف ومسؤوليات كل منصب مدرج في المخطط التنظيمي؟						
فحص كون مجمل مكونات وظيفة معلوماتية (استغلال، رصد تكنولوجي، أمن المعلومات، دعم المستخدمين، إدارة الخوادم...) محدد بشكل لائق في ميثاق الإعلام الآلي.						

ما تعداد المستخدمين المخصص لـ م ن م؟						
هل عدد المستخدمين يظهر لكم كافيا بالمقارنة مع رهانات الإعلام الآلي للهيئة؟ (ملائمة المستخدمين للحاجيات والرهانات).				X	**3**	
هل يمتلك مستخدمو م ن م المهارات التقنية المطلوبة؟						
تقييم الطابع "المعقول" لنسبة تجديد مستخدمي م ن م (5 إلى 15٪ في السنة) وتقييم توازن الفريق.						
هل تلجأ الهيئة إلى خدمات الإعلام الآلي؟ (عدد مقدمي الخدمات، درجة الاستقلالية تجاه مقدمي الخدمات والوظائف الممارسة).						
تقييم استقلالية الهيئة تجاه شخص واحد أو عدة أشخاص.			X		**2**	
هل يتلقى المختصون في الإعلام الآلي إشعارا مسبقا في حالة إنهاء مفاجئ لعقد العمل؟						
هل توجد خطة عمل لتكوين إسمي لمجمل المختصين في الإعلام الآلي؟						
هل جهد التكوين مكيف، وكاف وهل يندرج ضمن المدة؟						
هل توجد وثائق للمستعملين ولتسيير مختلف التطبيقات المعلوماتية؟ هل يتم نشرها؟						
3. التخطيط الاستراتيجي						
الاطلاع على التخطيط الرئيسي للهيئة وتحليل خطة الإعلام الآلي وخارطة الطرية الخاصة بنظم المعلومات (تحليل أهمية الخطة ومواءمتها الاستراتيجية، وتحليل مدى ملاءمة المهارات والموارد لأهداف الخطة).						
تحليل إجراءات إدارة وتحديث خطة الإعلام الآلي.						
تحليل آليات إدارة ومتابعة تنفيذ الخطة.						
تحليل دور لجان وإجراءات تحديث الخطة (الدورية السنوية الدنيا).						
وصف (بإيجاز) وتحليل الأهداف قصيرة ومتوسطة المدى.						
4. الميزانية وتكاليف الإعلام الآلي						
الاطلاع على الميزانية، هل يتم تفصيلها بشكل كاف؟						
هل تتضمن ميزانيات الحيازة على العتاد والبرامج المعلوماتية؟						
هل تتضمن ميزانيات الصيانة المعلوماتية؟						

وضع نسب وعناصر المقارنة (نسبة التكاليف/رقم الأعمال، نسبة ميزانية الإعلام الآلي/الميزانية العامة).						
5. الاطار التشريعي والتنظيمي						
هل المتطلبات القانونية والتنظيمية المعمول بها موثقة على مستوى الهيئة (المرسوم رقم 09-110 المؤرخ في 7 أفريل 2009).						
التصديق على نظام المعلومات من قبل هيئة خارجية (المرسوم XXX)						
احترام سرية البيانات.						
6. أهمية الإعلام الآلي في الهيئة						
ما مدى التأثير المعلوماتي على إنتاج معلومات محاسبية ومالية؟ (قوي، متوسط، ضعيف أو منعدم)؟						
وصف البنية الوظيفية لنظم المعلومات.						
ما هي مجالات النشاط التي يغطيها الإعلام الآلي؟						
ما مدى التشغيل الآلي؟						
ما هي المعالجات التي تمت بطريقة آلية؟ عدد المعالجات؟						
ما هي المعالجات التي تمت بطريقة غير آلية؟ (هل إجراءات وقواعد التسيير مرسمة)						
حجم النظام، عدد المعاملات التي تمت معالجتها.						
ما هي خصائص نظام المعلومات (احتياجات النشاط، حجم كبير من المعاملات، استخدام كبير للتكنولوجيات (تبادل البيانات غير المادية، الإنترنت)، الاستغلال في الوقت الفعلي، التوليد التلقائي للعمليات...)؟						
ما هو الوقت المسموح به لعدم الإتاحة؟ (تقدير).						
ما هي التأثيرات والنتائج (العملية والمالية) لانقطاع في نظام المعلومات فوق المدة الأقصى المسموح بها.						

Fiche audit - Prise connaissance environ

الملحق 2. بطاقة تدقيق متعلقة بخريطة التطبيقات

العمل الذي يتعين إنجازه

قائمة التطبيقات

التطبيق	المستعمل	الوظائف	الاستضافة (المكان إذا كانت الاستضافة مملوكة و/أو اسم الغير إذا كان منطبقا)	الاستضافة (محلية، خارجية)	النوع 1- تطوير داخلي 2- تطوير من طرف الغير 3- حزمة برامج معلوماتية 4- ملف مكتبي	تاريخ الوضع	مقدم خدمة الصيانة	تاريخ نهاية الاستعمال المتوقع (إذا كان منطبقا، وإلا ترك الخانة فارغة)	تاريخ آخر تحديث	نظام تشغيل الخادم المستضيف للتطبيق	قاعدة البيانات	مشروع التطور	طبيعة المخرجات	الحجم المعالج	الحرجية (1 إلى 5)
مثال															
مالية +	رقابة التسيير	محاسبة عامة محاسبة تحليلية	قاعة الخادم	محلية	حزمة برامج معلوماتية	2011/04/11	XX معلوماتي	2016/10/31		خادم ويندوز 2013	خادم SQL	ترقية الإصدار إلى v8.2 في جانفي 2013	وضع الحسابات	500 تسجيل في اليوم	1
تطبيقات مالية حرجة															
تطبيق أخرى مهمة															

قائمة الواسطات الرئيسية الداخلية والخارجية

إ م	المصدر	الوجهة	نوع التدفق	البروتوكول	الدورية	الاطلاق	البيانات المتبادلة	عمليات الرقابة

Fiche audit -
Cartopgraphie des ap

الملحق 3. بطاقة تدقيق متعلقة بتحديد العمليات التي يتعين تحليلها

الأشغال التي يتعين إنجازها

بالنسبة لكل العمليات التي تساعد بشكل مباشر أو غير مباشر على إنتاج بيانات مالية، من الضروري تحديد التطبيقات التي تساهم في معالجة البيانات.

يجري هذا التحديد انطلاقا من خريطة التطبيقات.

حسب أهمية الدور الذي تلعبه التطبيقات والوسائط في كل عملية، يُحدد فريق الرقابة العمليةَ أو العمليات التي يتعين تحليلها. تتضمن الخطوة الأولى استعراضا لمفهوم الإجراء (اختبار التصميم) الذي يسمح بفحص تماسك العملية مع تغطية المخاطر.

تبعا لاستعراض المفهوم، يمكن للمحتسب أن ينجز عمليات رقابة لحقيقة وفعالية تطبيق العملية.

النتيجة

يمكن للنتيجة أن تُرسّم على شكل الجدول التالي:

	التطبيق 1	التطبيق 2	التطبيق 3	التطبيق 4	التطبيق 5	التطبيق 6	التطبيق 7	التطبيق 8
العملية 1	X	X				X		
العملية 2			X	X	X			
العملية 3		X	X	X				
...						X		

الملحق 4. بطاقة تدقيق تفصيلية متعلقة بالأمن المعلوماتي

تدقيق نظام المعلومات	البطاقة رقم: 1
أخ البيئة المعلوماتية بعين الاعتبار	الطبعة: 0.1 مصادق عليه في: نوفمبر 2016 من طرف:

	سؤال حاسم

	الأجوبة	التأثير على موثوقية نظام المعلومات			التنقيط (على 3)	التعليقات
		ض	م	ع		
سياسة أمن المعلومات على مستوى الهيئة						
هل سياسة الأمن المعلوماتي (المادي أو المنطقي) مرسمة على مستوى المنظمة؟						
هل وضعت البنية المكلفة بالإعلام الآلي ونظم المعلومات وثيقة رسمية أو ميثاق حول الأمن يبرز هذه السياسة في شكل إجراءات ملموسة؟						
يتم توصيل الميثاق حول الأمن لكل المستعملين						
توجد مصلحة مخصصة لتسيير أمن المعلومات: لجنة، مسؤول أمن نظام المعلومات						
توجد إجراءات للترخيص لمعدات وبرامج معلوماتية جديدة						
الأمن المادي						
الدخول إلى قاعة المعلومات						
توجد قاعة معلومات مخصصة						
يتم إيقاء أبواب مباني الإعلام الآلي مقفلة						
هناك جهاز كشف عن عملية التسلل (أجهزة الإنذار، أجهزة الكاميرا)						
يدخل الأشخاص المرخص لهم فقط إلى المباني						
هناك تسيير للزائرين (أشخاص مرخص لهم مؤقتا للدخول لمباني الإعلام الآلي) يضمن إمكانية تتبع الدخول/ الخروج						
يتم تسجيل كل عمليات الدخول والخروج						
يتم تنظيم كل أوقات دخول كل الأشخاص						

جهاز مكافحة الحريق						
يوجد داخل المبنى نظام كشف الدخان						
يوجد داخل المبنى نظام استخراج الدخان						
يوجد جهاز إطفاء الحريق ساري الصلاحية في المبني						
يتم تدقيق جهاز القضاء على الحرائق الذي يعمل على الغاز من طرف شركات متخصصة وبفترات منتظمة						
أجهزة مضادة للتوتر الزائد والانقطاعات الكهربائية						
يوجد جهاز حماية (خوادم وأجهزة العمل) ضد التوتر الزائد والانقطاعات الكهربائية (العاكس)						
يتم إجراء اختبارات بانتظام						
أنظمة أمن أخرى						
يتم الاحتفاظ بالمباني نظيفة ، ولا يوجد ورق بالقرب من الخوادم						
مباني الخوادم مهواة ومكيفة الهواء						
يوجد جهاز التحكم في قياس الرطوبة						
الخوادم ليست موضوعة مباشرة على الأرض						
الخوادم غير موجودة في مباني الهيئة ولكن لدى مقدم خدمة خارجي معتمد						
لا تقع غرفة الاعلام الآلي في منطقة معرضة لخطر محتمل بالفيضان (الطابق السفلي، مبنى تحت السقف ، أنابيب المياه فوق الخوادم، إلخ.)						
يوجد نظام صرف المياه في أرضية غرفة الإعلام الآلي						
الأمن المنطقي						
أمن الشبكة						
هناك إجراء يحدد حماية الشبكة (البنية التقنية، تسيير البيانات الحساسة والملفات التعريفية للدخول، تسيير المستخدمين: إنشاء، تعمل، حذف)						
الإجراء مرسم (مكتوب)						
الوصول إلى الشبكة آمن ضد التسلل الخارجي: مثال: إنترنت عبر البروكسي، شبكة محلية بعد الجدار الناري						
الاتصالات عن بعد آمنة (VPN، MPLS ...)						
الوصول إلى الشبكة محمي بكلمة مرور						
لا يوجد حساب عام						
يتم تعيين كلمة المرور الأولى بشكل فردي لكل مستخدم (كلمة المرور غير معروفة)						

يجب تغيير كلمة المرور الأولى آليا عند تسجيل الدخول لأول مرة من قبل المستخدم						
تخضع كلمات المرور للتجديد المنتظم						
لا يُسمح للمستخدم باستخدام كلمة المرور نفسها عدة مرات متتالية						
تحتوي كلمات المرور على 8 أحرف أبجدية رقمية ورموز خاصة على الأقل						
بعد عدة محاولات غير ناجحة للدخول ، يتم حظر حساب المستخدم						
هناك ملفات تعريف لكل نوع من المستخدمين						
يتم إجراء مراجعة منتظمة لحقوق دخول المستخدمين						
بعد فترة معينة من عدم النشاط ، يدخل الجهاز في وضع السكون (تسجيل خروج تلقائي و / أو حماية بكلمة مرور)						
يتم تشفير الدخول وتبادل الويفي						
أمن التطبيقات مع تأثير مالي						
هناك إجراء لتسيير المستخدمين (الملفات التعريفية للمستخدمين، إنشاء، تعديل، حذف)						
الإجراء مرسم (مكتوب)						
يوجد ملف تعريفي لكل مستخدم						
فكرت الهيئة في فصل الوظائف واستنتجت ملفات تعريف المستخدمين مع تحديد الحقوق المصاحبة المرسمة في وثيقة معتمدة من الإدارة						
يتم إجراء مراجعة منتظمة لحقوق دخول المستخدمين						
الوصول إلى التطبيق محمي بكلمة مرور						
لا يوجد حساب عام						
يتم تعيين كلمة المرور الأولى بشكل فردي لكل مستخدم (كلمة المرور غير معروفة)						
يجب تغيير كلمة المرور الأولى آليا عند تسجيل الدخول لأول مرة من قبل المستخدم						
تخضع كلمات المرور للتجديد المنتظم						
لا يُسمح للمستخدم باستخدام كلمة المرور نفسها عدة مرات متتالية						
تحتوي كلمات المرور على 8 أحرف أبجدية رقمية على الأقل						
بعد عدة محاولات غير ناجحة للدخول ، يتم حظر حساب المستخدم						
أخرى						
الأجهزة والخوادم مجهزة ببرامج مكافحة الفيروسات						
برامج مكافحة الفيروسات موجودة ويتم تحديثها						

بانتظام						
نظام التشغيل تم تحديثه (ويندوز، غير ذلك،...)						
كشف الفيروسات يتم إنجازه على كل أنواع الملفات (البرامج، ملفات النظام والوثائق)						
يتم تفعيل برامج مكافحة الفيروسات على جميع الأجهزة ولا يمكن قطع اتصاله من قبل المستخدم						
تكون الرسائل والمرفقات أيضا موضوع تطهير من الفيروسات						
هناك نظام لمكافحة البريد المزعج						
تسيير عمليات الحفظ						
هناك إجراء يحدد تسيير عمليات الحفظ						
الإجراء مُرسم (كتابي)						
يشير الاجراء إلى نوع البيانات المحفوظة						
هل تسمح استراتيجة الحفظ بضمان ضياع محدد للبيانات قابلة التحمل من طرف الهيئة؟						
الخوادم مجهزة بأنظمة حفظ أو تستعمل وسيلة حفظ مشتركة						
تعمل عمليات الحفظ بنظام الإعلام الآلي (مرة واحدة كل 24 ساعة على الأقل)						
تتم رقابة التقارير تلقائيا						
يتم الاحتفاظ بعمليات الحفظ بشكل طويل كفاية، ويسمح ذلك بضياع محدود للمعلومات						
يوجد إجراء حفظ للحواسيب المحمولة						
يتم الاحتفاظ بمجموعة حفظ خارج الهيئة						
يتم فحص تآكل الأشرطة ويتم استبدال الأشرطة عند الاقتضاء						
يوجد تصنيف ووضع مراجع لوسائط الحفظ						
يتم إنجاز اختبارات استرجاع كاملة بانتظام						
تدمج اختبارات الاسترجاع مستعملي المهن						
يتم توثيق جميع حوادث الحفظ						
يتم الاحتفاظ بعمليات الحفظ في مكان محمي (نوع صندوق مانع للاحتراق)						
مكان تخزين عمليات الحفظ (الأشرطة، القرص الصلب، إلخ.) موجود خارج مبنى الخوادم						
في حالة الاستعانة بمصادر خارجية للحفظ، حدد العقد التزام مقدم الخدمة بكل نقطة من النقاط السابقة (خطة الحفظ، عدد ودورة حياة التوليدات، الأمن المادي للوسائط، إجراءات الاسترجاع، إجراءات تحديث خطة الحفظ، إجراء تقديم التقارير)						

خطة احتياطية						
توجد خطة احتياطية محددة ومرسمة						
تم التخطيط لمعدات احتياطية						
تم التخطيط لموقع احتياطي						
يتم إنجاز اختبار للخطة الاحتياطية مرة في السنة على الأقل						
يتم ترسيم عرض حال للاختبارات						
تتضمن الهيئة عقد صيانة حول الخوادم						
رقابة داخلية للوظيفة المعلوماتية						
يتم احترام مبادئ فصل الوظائف داخل مصلحة الإعلام الآلي (يتم الفصل بين وظائف Office Back (تطوير) و Front Office (استغلال))						
فصل مصلحة الإعلام الآلي عن العملياتيين						
يتم تبادل الخبرات وتوثيقها في قسم نظم المعلومات						
هناك خطة تكوين محددة لمصلحة الإعلام الآلي						
هناك إجراء لتسيير الحوادث						
الإجراء مرسم (مكتوب)						
يتم تتبع الحوادث وتحليلها وتصحيحها وتتبع حلها						
يوجد ميثاق معلوماتي موقّع من طرف المستخدِمين، مصادق عليه قانونيا وملحق بالقانون الداخلي						
يحدد الميثاق المعلوماتي قواعد استخدام نظم المعلومات (التطبيقات والبيانات) وأجهزة العمل و / أو الخوادم، والبريد الإلكتروني والإنترنت.						
تسيير التغييرات						
هناك إجراء لتسيير التغيير						
الإجراء مرسم (مكتوب)						
ينص الإجراء على الحالة الخاصة لترقية اصدار التطبيقات و / أو البرامج المعلوماتية القاعدية التي يجب تسييرها كمشروع						
يتم التصديق على طلبات التطورات الوظيفية من قبل المسير						
يتم توثيق الطلبات والتطورات						
هناك خطة اختبار عدم التراجع للتطورات (بما في ذلك ترقيات إصدار التطبيقات)						
يتم إجراء مجموعات وعروض حال الاختبار من قبل مقدم الطلب (مستخدم رئيسي)						

ويصادق عليه مقدم الطلب قبل بدء الإنتاج.						
هناك إجراء محدد للتغييرات الطارئة						
يتبعُ إنشاء الملفات الشخصية عملية تسيير التغييرات						
هناك فصل للوظائف بين بيئات الإنتاج والتطوير من حيث الدخول المنطقي						

Fiche audit - sécurité informatique.xlsx

الملحق 5. بطاقة تدقيق متعلقة بالمشروع المعلوماتي

	تدقيق نظام المعلومات	البطاقة رقم: 1
	تدقيق المشاريع المعلوماتية	الطبعة: 0.1 مصادق عليه في: نوفمبر 2016 من طرف:

		التعليقات
أهداف ورهانات المشروع		
دراسة الفرص والتعبير عن الحاجيات		
التخطيط		
هيئات التوجيه		
الطرق والأدوات		
التصميم		
التطوير، الإنجاز ووضع الاعدادات		
اختبارات وإيرادات		
قيادة التغيير والتنفيذ		
الوثائق		

الملحق 6. قاموس المصطلحات الخاصة

على هذه التعاريف السريعة أن تسمح للمدققين بأن يتقاسموا مع الخاضعين للتدقيق نفس الفهم لبعض المفاهيم الخاصة والمعقدة.

أ) قاموس المصطلحات الخاصة لنظم المعلومات

أ. حوكمة نظام المعلومات

يشير مصطلح "حوكمة نظم المعلومات" أو "حوكمة الإعلام الآلي" إلى جهاز تضعه منظمة من أجل رقابة وضبط نظام المعلومات الخاص بها. بهذا العنوان، فحوكمة نظام المعلومات هي جزء لا يتجزأ من حوكمة المنظمة، ويتضمن أولا تحديد أهداف لنظام المعلومات تتأتى من استراتيجية المنظمة.

ب. المخطط التوجيهي والخطة الاستراتيجية للإعلام الآلي

المخطط التوجيهي هو خطة استراتيجية موجهة لتوجيه تطوير الإعلام الآلي في المنظمة، بما يتماشى مع استراتيجيتها العامة.

يصف المخطط التوجيهي للإعلام الآلي نظام المعلومات الحالي أو المستقبلي، ضمن منطق من الأهداف والخدمات المتوقعة. يوفر المخطط بالتالي رؤية شاملة للحالة الراهنة للنظام، وجرد ومواصفة الحاجيات ويحدد التوجيهات.

تتم المصادقة عليه من طرف أعلى مستوى في المنظمة. ينبغي أن يكون موضوع تحكيم واضح يمس الغايات المبتغاة، وتكييف العمليات العملية، والموارد البشرية والمالية المخصصة وخطوات ورزنامة الإنجاز.
تتراوح مدة حياة المخطط عادة بين سنتين وست سنوات.

ج. صاحب المشروع (MOA) والمشرف عن الإنجاز

صاحب المشروع هو الموصِي بمشروع الإعلام الآلي. يتعلق الأمر إما بالمديرية المهنية، التي تكون مصدر الحاجة الوظيفية والراعي للمشروع، أو (بوزارة الدفاع الوطني مثلا) بمديرية عامة متخصصة في التوجيه المشترك (مع المديريات الوظيفية) وتسيير المشاريع.

صاحب المشروع:

- يشكل فريق مشروع مكيف ويحوز على وسائل مالية وبشرية وتقنية ضرورية؛
- يحدد الحاجيات الوظيفية ويضع دفتر الشروط؛
- يحدد الوسائل والضغوط (المواعيد، التكاليف، النوعية، الخ)؛
- يحدد ويدعم حافظة مخاطر المشروع؛

- يحدد المشرف عن الإنجاز ويحرر، ويُخطِر بالصفقات المطابقة ويسيرها؛
- يوجه المشرف عن الإنجاز عبر نظام اللجان (comitologie) المكيف مع الرهانات والطرق المختارة (مثل طريقة أجيل) ؛
- يصادق على الحلول المقترحة من طرف المشرف عن الإنجاز ويتابع إنجازه؛
- يستقبل التطبيق طبقا للاحتياجات المعبر عنها؛
- يدير التطبيق لغاية سحبه.

يخفف مساعد صاحب المشروع (AMOA) من عبئ عمل صاحب المشروع من خلال إعفائه من مهام توجيهية ذات طبيعة تقنية (مساعدة في التخصيص، مساعدة على اختيار المشرف عن الإنجاز وعلى إجراء تعاقد الخدمة، أمانة نظام اللجان، إلخ. النقائص التي تمت ملاحظتها هي:

- مساعد صاحب المشروع الذي يخلف صاحب المشروع في الحقيقة، مما يؤدي إلى سريعا إلى نقص في التحكم في المشروع من طرف الموصِى، مع كل ما يترتب عن ذلك من انحرافات؛
- مساعد صاحب المشروع الذي يتدارك نقائص فريق المشروع عوض مساندته؛
- سوء اختيار مساعد صاحب المشروع ونقص الاستقلالية تجاه المشرف عن الإنجاز، مما يمكن أنه يكون له تأثير على محتوى المواصفة وإجراء المناقصة؛
- مساعد صاحب المشروع الذي لا يمكن إعادته للمنافسة بسبب قبضه على المشروع.

يلعب قسم "الدراسة" لدى مديرية الإعلام الآلي بشكل متكرر دور صاحب المشروع المفوض، إن هذا المخطط، الذي يسمح بتوجيه مساعد صاحب المشروع أو المشرف عن الإنجاز من طرف أخصائيين في مشاريع الإعلام الآلي، لا يعفي المديرية المهنية من مسؤولياتها الخاصة بصاحب المشروع.

يعتبر المشروف عن الإنجاز الضامن التقني للسير الحسن للمشروع.
المشرف عن الإنجاز:

- يقترح حلولا تقنية على أساس الحاجيات، الوسائل والضغوطات المحددة من طرف صاحب المشروع؛
- يضمن أو يشرف على تطوير التطبيق؛
- يراقب أو يجري اختبارا على النتائج (اختبارات الوحدة واختبارات التكامل)؛
- يسلم التطبيق ليخضع لاختبار القبول، ويعمل على استخدامه عند الاقتضاء.

د. مالك التطبيق أو البيانات

يُكلف مالك التطبيق بالسهر على مناسبة تطبيق أو حافظة تطبيقات للاحتياجات المهنية (مفهوم المواءمة الاستراتيجية) ولبيئة التطبيق أو حافظة التطبيقات من حيث البرنامج المعلوماتي والأجهزة.

يعتبر مالك التطبيق، بهذا العنوان، المحاور لمسؤول العمليات المهنية المستخدِم للتطبيق، لمخطِط نظام الآلي، لمسير ميزانيات الإعلام الآلي (صيانة، تطور، مشاريع أخرى)، للمسؤول عن أمن الإعلام الآلي والمسؤول عن خطط استمرار واستئناف نشاط المنظمة.

هو مسؤول أمامهم عن مراعاة، بشكل صحيح، هذه الإشكاليات. ويسهر على أن يستفيد المستخدمون من تكوين ودعم مناسبين.

يجب عدم الخلط بين هذه الوظيفة ووظيفة مسؤول / مسؤولي التطبيق/ات، والتي تشير عموما إلى الشخص، ضمن مديرية الخدمات المعلوماتية، المكلف بتسيير حافظة التطبيقات الخاصة بالمنظمة.

يكون مالك البيانات مسؤولا أمام المديرية، عن العمليات العملية ومستخدِمي النوعية، وسلامته وأمن وتوافر مجموعة من البيانات. على وجه الخصوص، يُسند ويرصد حقوق إنشاء وتعديل وقراءة وحذف البيانات. كما أنه مسؤول، قدر الإمكان، عن فردية البيانات، أي عن عدم تكرارها، وخاصة المحلية منها، من قبل المستخدمين. تعد وظيفة مالك البيانات هذه أكثر أهمية لأن البيانات حساسة وتمس بمجالات كثيرة.

يعد مالك التطبيق أو البيانات مديرا عمليا.
داخل المنظمة، يجب أن يكون لكل تطبيق وبيانات مالك معين، بما في ذلك التطبيقات والعمليات التي يتم الاستعانة بها من الخارج.

هـ. قاعدة البيانات الرئيسية

عندما يتم تقاسم البيانات بين العديد من الجهات الفاعلة (الإدارات الوظيفية، وتطبيقات الإعلام الآلي، وما إلى ذلك) داخل منظمة ما، يجب وضع آلية تهدف لضمان وجود، لكل من هذه البيانات، مرجع لا جدال فيه.
قاعدة البيانات الرئيسية هي هذا المرجع. يمكن أن تتكرر في شكل قواعد بيانات موزعة، يتم إنشاؤها لتلبية حاجة جوارية جغرافية أو وظيفية. على سبيل المثال، تعتبر تفاصيل الزبائن أو قائمة الأعوان المحددين في نظام المعلومات معلومات حساسة تستخدمها العديد من التطبيقات: يجب ضمان دقتها، وتحديثها وخاصة فرديتها.
تتمثل إحدى المهام المهمة لمالك البيانات في السهر على نوعية عمليات النسخ المتماثل بين قاعدة البيانات الرئيسية والموزعة.

و. سياسة أمن المعلومات

تغطي مجمل التوجيهات التي تتبعها الهيئة فيما يخص الأمن. في ضوء نتائج تحليل المخاطر، تقوم هذه السياسة بـ:

- تحديد إطار استخدام موارد نظام المعلومات؛

- توضيح الأدوار والمسؤوليات في هذا المجال؛
- تحديد التقنيات الأمنية التي يتعين تنفيذها في مختلف مصالح المنظمة؛
- تحسيس المستخدِمين بأمن الإعلام الآلي.

ينتج أمان الإعلام الآلي عن تسوية بين حماية الأصول الرقمية والمعلوماتية وقدرة المستخدمين على تطوير الاستخدامات المشروعة التي يحتاجونها. سياسة أمن الإعلام الآلي هي، بهذا العنوان، من مسؤولية مديرية المنظمة المعنية.

ز. ميثاق الاستخدام

ميثاق الاستخدام هو عبارة عن وثيقة مصادق عليها من طرف المديرية العامة للمنظمة، وهو يعرض للمستخدمين سياسة أمن نظام المعلومات. يتم التوقيع عليه إجباريا من طرف كل مستخدِمي موارد الإعلام الآلي.

يمكن إعداد هذا الميثاق حسب النموذج التالي:

- كيفيات استخدام وسائل الإعلام الآلي والاتصالات السلكية واللاسلكية الموضوعة تحت التصرف.

على سبيل المثال:

- أجهزة العمل؛
- المعدات الثابتة؛
- مساحة التخزين الفردية؛
- الشبكة المحلية؛
- الإنترنت؛
- الرسائل الالكترونية؛
- الهاتف.

- قواعد الأمن التي يتعين مطابقتها، مما يمكن أن يضم على سبيل المثال:

- وسائل التسجيل؛
- كيفيات تدخل مصلحة الإعلام الآلي الداخلية؛
- الإبلاغ لمصلحة الإعلام الآلي الداخلية عن كل خرق أو محاولة خرق مشكوك فيها للحساب المعلوماتي للشخص، وعن كل خلل بصفة عامة؛
- عدم إعطاء إسم المستخدم / كلمة المرور الخاصة بالشخص للغير؛
- عدم تعديل إعدادات جهاز العمل؛

- عدم تثبيت أو نسخ أو تعديل أو إتلاف البرامج المعلوماتية دون ترخيص؛
- قفل جهاز الكمبيوتر الخاص بالشخص بمجرد ترك جهاز العمل الخاص به؛
- عدم الدخول، أو محاولة الدخول، إلى أو حذف المعلومات التي لا تندرج تحت المهام التي تقع على عاتق المستخدم؛
- كيفيات نسخ البيانات على واسطة خارجية.

– شروط إدارة نظام المعلومات ووجود، عند الاقتضاء، أنظمة آلية للتصفية أو التتبع؛
– المسؤوليات والعقوبات المتكبدة في حالة عدم الامتثال للميثاق.

ح. اختبار القبول

في الإعلام الآلي، اختبار القبول (recette) هي مرحلة للمشروع تهدف للضمان الرسمي أن المنتج مطابق للمواصفات.

يندرج هذا الاختبار ضمن النشاطات الأكثر عمومية للتأهيل. تنطوي هذه الخطوة على السير الصارم لإجراءات الاختبارات الموصوفة سابقا، وتحديد كل فارق وظيفي أو تقني. في هذه الخطوات الخاصة بالاختبارات الوظيفية، يستوجب اختبار القبول توافرا قويا للمستخدِمين (المديريات المهنية).

يشير هذا المصطلح إلى مفاهيم مختلفة في الصفقات: فحص السير الحسن، فحص السير المنتظم، الخدمة المنجزة. وفي حالة صفقة للإعلام الآلي، على الأطراف أن تتفق على نطاق هذه التعبيرات، مما يمكن أن يتطلب توضيحها.

ط. اتفاق أو عقد خدمة (SLA / OLA)

عقد الخدمة، الذي يسمى أيضا اتفاق الخدمة، والذي يعبر عنه غالبا بالاختصار الإنجليزي SLA (service level agreement)، هو وثيقة تحدد المتطلبات بين مقدم خدمة إعلام آلي ومستعملي الخدمة أو "الزبائن".

عقد الخدمة هو الترسيم لعقد تم التفاوض عليه بين طرفين. هو يضع بالتالي، كتابيا، مستوى من الخدمة، يتم التعبير عنه بتوقعات الطرفين حول محتوى الخدمات، كيفيات تنفيذها، ومسؤوليات الأطراف، والضمانات، لاسيما من حيث استمرارية الخدمة أو إعادة القيام بها.

على سبيل المثال، يمكن لعقد الخدمة أن يحدد بشكل خاص مستويات توافر أو أداء خدمة إعلام آلي (الأجهزة، بما في ذلك الشبكة، البرامج المعلوماتية، دعم المستخدمين، أجال التدخل، الخ).

على كل التزام كمي أن يكون قابلا للقياس، ويتم قياسه بفعالية، وأن يكون موضوع حوار للتسيير.

ي. خطة استمرار النشاط وخطة استئناف النشاط

هذان المفهومان متميزان.

– خطة استئناف النشاطات (PRA) هي مجموعة من التدابير التي من شأنها أن تسمح لمنظمة باستئناف نشاطها بعد وقوع كارثة، على سبيل المثال: عطل من شأنه أن يشل نظام معلوماتها خارج نطاق تحملها.

– خطة استمرار النشاط (PCA) هي مجموعة من التدابير التي من شأنها أن تسمح لمنظمة بمواصلة نشاطها خلال كارثة ما. الفرق ملحوظ لأنه في الحالة الأخيرة لا يتوقف النشاط. ولذلك فإن المنظمة مجبرة، لكل نشاطها أو جزء منه، على العمل بشكل مختلف عن عملها المعتاد.

تذهب كل من خطة استئناف النشاط وخطة استمرار النشاط إلى أبعد من الإعلام الآلي مجردا. ولذلك فهما جهازان رئيسيان للمنظمة، يضعان شروط قدرتها على التصرف في حالة أزمة داخلية او خارجية، ويجب، بهذا العنوان، أن يكون الجهازان جزءا من استراتيجيتها الأمنية. ويجب أن يكونا دائما في ظروف عملية، مما ينطوي على وضع سياسة اختبارات منتظمة.

نظرا للاعتماد القوي للمنظمات على نظام معلوماتها، يجب أن تتطور كل من خطة استمرار النشاط وخطة استئناف النشاط سوية مع نظام المعلومات. يمكن للخطتين أن تتنوعا في مفهوم ذي صلة، مقتصر على الإعلام الآلي: خطط استئناف الإعلام الآلي (PCI) أو استمرار الإعلام الآلي (PRI).

ك. الإدارة الخارجية للمعلوماتية (Infogérance) والاستعانة بالمصادر الخارجية (Outsourcing)

تتضمن الاستعانة الخارجية للمعلوماتية أن نفوض لمقدم خدمات أو مقدمي خدمات إعلام آلي كل أو جزءا من تسيير نظام المعلومات. يتم ترسيم الخدمات الموافقة ومستوى الخدمة المتوقعة في إطار تعاقدي أو عن طريق صفقة.

يمكن لهذا أن يعني عناصر للبنية التحتية (وضع واستغلال الخوادم أو نظم الحفظ، الإشراف على الخدمات الشبكية أو الهاتفية...) و/أو جوانب للبرامج المعلوماتية (التطوير، الصيانة...).

في الإدارة الخارجية للمعلوماتية التي تطلق عليها صفة "الكلية"، تعهد المنظمة كل تسيير نظام معلوماتها إلى مؤسسة للغير، مرورا بالاستغلال.

تعد الحساسية الاستراتيجية لنظام المعلومات والأصول الرقمية ونوعية الخدمة وانعكاسها عناصر أساسية في القرار.

تشهد آليات الإدارة الخارجية للمعلوماتية، والاستعانة بمصادر خارجية رجوعا كبيرا للساحة، والذي له صلة بظهور مفهوم الحوسبة السحابية (cloud computing).

ل. الحوسبة السحابية (Informatique en nuage أو Cloud computing)

الحوسبة السحابية هي تقنية تعتمد على قدرات الشبكات على تزويد المستخدمين النهائيين بخدمة، مقدمة من قبل البرامج المعلوماتية والبنية التحتية المعلوماتية البعيدين عادة.

في معظم الحالات، لا يدرك هؤلاء المستخدمون التموقع الدقيق للأجهزة والبرامج المعلوماتية والبيانات التي يدخلون إليها من خلال شبكة عامة أو خاصة. يمكن تقديم الخدمة نفسها من قبل هيئة عمومية، حتى الدولة (يشار إليها أحيانا باسم "السحاب السيادي") أو بواسطة متعامل خاص.

تتيح الحوسبة السحابية تركيز المعدات والبرامج المعلوماتية التقنية في منشآت ("مراكز بيانات") أكبر حجما بعدد محدود، مما يُجنبُ تكاثر المنشآت المحلية، ذات الحجم الصغير ومعايير الأجهزة أو البرامج المعلوماتية المتفرقة. وهذا يسمح بتركيز الموارد البشرية المختصة اقتصاد الحجم، ويسهل الصيانة ويحسن الأمن المادي والمنطقي.

ولذلك، يتعلق الأمر بترتيب تقني وعملي، والذي ينبغي النظر في نتائجه القانونية والعملية بأخذ كل حالة على حدة من جانب المسؤولين العمليين. على وجه الخصوص، قد توجد البنى التحتية للإعلامي الآلي (خوادم التطبيقات وقواعد البيانات) في الخارج، مما يثير تساؤلات حول حماية المعلومات الحساسة والقانون المعمول به، مثل البيانات الشخصية.

يمكن للمستخدم عادة الاستفادة من مستويات الخدمة التالية:

– مستوى IaaS (البنية التحتية كخدمة). تتضمن هذه الخدمة توفير الدخول إلى حظيرة إعلام آلي مجمعة. ولذلك فهي تسمح بالدخول إلى البنية الأساسية للأجهزة التي يمكن للمستخدم أن يثبت عليها أجهزته الافتراضية وبيئتها المعلوماتية للاستغلال. إنها خدمة استضافة تسمح بمشاركة المعدات؛

– مستوى PaaS (منصة كخدمة). تضع هذه الخدمة في تصرف المستخدم الأجهزة الافتراضية وبيئتها المعلوماتية للاستغلال التي لم يعد على المستخدم ضمان عملها. يقوم المستخدم بتثبيت التطبيقات والأدوات الخاصة به على هذه الأجهزة الافتراضية. إنها خدمة تسمح بمشاركة أنظمة الإعلام الآلي؛

– مستوى SaaS (البرامج المعلوماتية كخدمة). في هذا النوع من الخدمات، توضع التطبيقات تحت تصرف المستخدمين الذين لا يكون عليهم أن يقلقوا بشأن تثبيتها، وإجراء التحديثات عليها، وإضافة تصحيحات الأمان

وضمان توفر الخدمة. لم تعد المؤسسة التي تلجأ إلى هذه الخدمة تشتري ترخيصا للبرنامج المعلوماتي ولكنها تشترك في هذا البرنامج المعلوماتي. التطبيق قابل للاستخدام مباشرة عبر متصفح الويب؛

– يمكن أن تنطلق الحوسبة السحابية بالتالي من الأمور القاعدية إلى الكاملة تماما (IaaS، PaaS، SaaS، إلخ، ويبقى المحتوى الدقيق لكل من هذه المفاهيم قيد المناقشة). تستهدف عروض IaaS وPaaS خدمات الإعلام الآلي بينما تستهدف عروض SaaS مستخدمي التطبيق مباشرة.

م. مركز البيانات

مركز البيانات، أو "مركز معالجة البيانات"، هو مكان متخصص يحتوي على خوادم تسيير قاعدة البيانات (SGBD)، وخوادم الملفات، وخوادم التطبيقات. يمكن أن يكون خاصا بمنظمة ما، أو، على العكس من ذلك، تمت الاستعانة به من مصدر خارجي، أو تمت مشاركته (منطق الحوسبة السحابية).

يقدم مركز البيانات عادة مستويات الخدمات التدريجية، وهي تتراوح بين توفير البيئة وحسب (يجلب المستفيد خوادمه الخاصة به) والإدارة الكاملة لمجموعة تطبيقية. يستضيف مركز البيانات عموما، وعلى نحو متزايد، الأصول الأكثر قيمة لمنظمة ما.

تتميز هذه المراكز عادة ببيئة (الطاقة، وتكييف الهواء، والحماية المادية والمنطقية، والمحاكاة الافتراضية، والدخول إلى الشبكات، وأدوات الإدارة والإشراف) بكونها مصممة بعناية فائقة، لضمان مستوى عال جدا من التوافر والسلامة والموثوقية. تُمثل هذه، مع المشاركة بين جميع المستخدمين للتكلفة المالية والبشرية لمثل هذه البيئة، الورقة الرابحة الرئيسية لهم.

إن إدخال مثل هذا المركز في سلسلة طاقوية جيدة يجب أن يعزز أيضا تحقيق الأهداف البيئية للمؤسسة (مفهوم الحوسبة الخضراء).

إن الرهانين الرئيسيين حاليا هما موقع هذه المراكز، لأسباب تتعلق بالسرية والنظام القانوني، ومطاردة مراكز البيانات الصغيرة والمتعددة "التاريخية" (في بعض الأحيان مجرد كمبيوتر مكتبي)، وهو ما يوفر، بشكل عام، بيئة بعيدة عن أفضل الممارسات.

ن. صيانة تطبيقية أو تصحيحية

تعد صيانة تطبيق ما نشاطا لا غنى عنه، ويتضمن باستمرار تكييف تطبيق ما لتطور بيئته التقنية والبرمجية والأمنية. يتطلب تجديد الأجهزة، في الواقع، اللجوء إلى برامج تشغيل جديدة، وينبغي أخذ تعديل حزمة برامج المعلوماتية (مجموعة أدوات الإعلام الآلي التي تسمح بعمل التطبيق، نظام التشغيل مثلا) بعين الاعتبار من طرف التطبيقات ويستلزم الكشف عن خلل أمني وضع نظام حماية.

بصفة عامة، تكلف هذه الصيانة سنويا خُمس السعر الأساسي للتطبيق. إن التنفيذ الحسن لها هو من مسؤولية مالك التطبيق. يتم تكليف مديرية نظم المعلومات في كثير من الأحيان بمتابعة هذه الصيانة، من طرف قسم " الدراسات" عموما.

تتم الإشارة إلى الصيانة التطبيقية أحيانا بالاختصار MCO (maintien en condition opérationnelle) و MCS (maintien en condition de sécurité).

تختلف الصيانة التطبيقية عن الصيانة التطويرية بحيث أن الأولى لا تحدث أي تطور وظيفي، بينما تضيف الثانية وظائف ضعيفة الحجم عادة. بالنسبة للتطويرات الوظيفية الأكثر عمقا، يكون الحديث أكثر عن نسخة تطبيقية جديدة، بل حتى مشروع جديد.

تنطوي الصيانة التطبيقية من طرف الغير (TMA) على الاستعانة خارجيا بالغير للصيانة التطبيقية و/أو التطويرية.

تنطوي الصيانة الاستغلالية من طرف الغير (TME)، كتكملة، على الاستعانة خارجيا بكل أو جزء من البنية التحتية (بما في ذلك تطورها) ووظائف الإدارة والدعم للمستخدمين.

هناك سلسلة متصلة بين الاستعانة خارجيا للصيانة التطبيقية والاستعانة خارجيا بعملية كاملة، حيث تشكل كل وضعية حالة محددة تحكمها أحكام تعاقدية محددة.

الملحق 7. أنواع عمليات الرقابة المتصلة بالتطبيقات

نميز أنواع عمليات الرقابة التطبيقية التالية:

1. إنشاء وترخيص
2. إدخال البيانات وتسجيلها
3. معالجة المعلومات
4. مخرج البيانات (Output)
5. الوسائط

1. <u>إنشاء وترخيص</u>

الأهداف الرئيسية المتعلقة بالإنشاء والترخيص هي التالية:

- التقليل من الأخطاء والسهو؛
- تحديد وتوثيق وتوصيل وتصحيح الأخطاء والمخالفات بمجرد ظهورها؛
- فحص دقة تصحيح الأخطاء بواسطة خدمة مستقلة / شخص مستقل؛
- لا يتم تنفيذ العمليات التجارية (المعاملات) إلا من قبل الأشخاص المخولين و/أو وفقا للإجراءات المرخص بها؛
- يتم تحديد الأشخاص المسؤولين عن إدخال المعاملات التجارية في النظام؛
- الأدلة التبريرية لإدخال المعلومات، التي يتم إصدارها شاملة ودقيقة ويتم إرسالها في الوقت المناسب؛
- يتم الاحتفاظ بالوثائق التبريرية لإدخال المعلومات خلال الفترة القانونية وفي الشكل الموصوف أو يمكن إعادة تشكيلها من قبل المنظمة.

عمليات الرقابة النموذجية التي تتعلق بالإنشاء والترخيص هي التالية:

- ملفات تعريف الاختصاصات لإنشاء المستندات المحاسبية (مثل القانون حول التوقيعات) والتنفيذ من خلال رقابة التراخيص بواسطة أنظمة تسيير الدخول؛
- الفصل بين وظائف إنشاء والتصديق على المستندات المحاسبية؛
- التأشير أو التوقيع على الوثائق التبريرية لإدخال المعلومات؛
- استمارات الإدخال مفهومة ومفيدة (على سبيل المثال: مع حقول مطبوعة مسبقا)؛
- عملية التحديد المبكر ومعالجة الأخطاء والمخالفات؛

- جمع تلقائي للمستندات المحاسبية (على سبيل المثال، حسب الترتيب الزمني باستخدام ختم زمني أو بالتتابع باستخدام نظام ترقيم مستمر)؛
- التسجيل الميكروفلمي أو رقمنة الوثائق التبريرية وحفظها على واسطة تسمح بإعادة تشكيل المعلومات الأصلية في الآجال المطلوبة.

2. <u>إدخال وتسجيل البيانات</u>

الأهداف الرئيسية لإدخال وتسجيل البيانات هي التالية:

- وحدهم الأشخاص المخولون (أو العمليات المرخص بها) يمكنهم تسجيل البيانات؛
- تتم رقابة دقة وشمولية وصحة الحقول المهمة (مثل أرقام الحساب، والمبالغ، ورمز المادة) في الشاشات أو البرامج قبل عملية الإدخال؛
- يتم تحديدُ الأخطاء والمفارقات في الإدخال/ التسجيل وتوثيقُها وتوصيلُها وتصحيحُها في الوقت المناسب؛
- يتم فحص دقة تصحيح الخطأ بواسطة خدمة مستقلة / شخص مستقل؛

عمليات الرقابة النموذجية لإدخال وتسجيل البيانات هي التالية:

- ملفات تعريف الاختصاصات لإدخال/ تسجيل المعاملات والتنفيذ من خلال رقابة التراخيص بواسطة أنظمة تسيير الدخول؛
- أقنعة الإدخال المفهومة وسهلة الاستعمال مع عناصر تحكم في تنسيق البيانات المدمجة (مثل حقول التاريخ، والبيانات الرقمية، والحقول الإجبارية، إلخ.، وقائمة القيم المحددة مسبقا والمتكررة)؛
- التحكم الآلي المعمق للقيم المدخلة (على سبيل المثال، تجاوز القيم الحدية، التحكم في معقولية المحتويات، المزامنة مع البيانات المسجلة)؛
- عرض الثوابت الحرفية للرموز كاملة بعد إدخال الرمز (على سبيل المثال، يتم عرض تسمية المادة عند إدخال رقم المادة)؛
- مقارنة البيانات المدخلة، أي مقارنة البيانات المراد إدخالها مع البيانات المرئية على الشاشة أو مع سجلات إدخال البيانات (مع مراعاة التكلفة، تكون هذه مناسبة فقط للمعاملات الحرجة مثل نقل البيانات القاعدية بالخصوص)؛

- مجاميع عمليات الرقابة حسب الدفعات: عدد الوثائق (مثل عدد الفواتير)، مجموع مناطق القيم التي تظهر على الوثائق أو المجاميع الرقمية (المبالغ، الكميات)، مجموع الرقابة (ناتج التكثيف، التجزئة، الإضافة الرياضية لأرقام الوثائق، أرقام الحساب)؛

- رقابة ترتيب ظهور المستندات المحاسبية المرقمة بالتتابع داخل دفعة ما لتحديد الأرقام الناقصة أو الإدخالات المزدوجة؛

- مقارنة البيانات التي تم إدخالها مع القيم المسجلة (مثل الأجهزة المفتوحة مع عمليات محاسبية منشأة حديثا)؛

- الإدخال الرقابي (يسمى أيضا الإدخال المزدوج، الرقابة بـ 4 عيون)؛ الإدخال المزدوج للقيم المهمة من قبل أشخاص مختلفين (مسير من طرف نظام تسيير الدخول) أو، إذا لزم الأمر، من قبل الشخص واحد نفسه (على سبيل المثال: عند إدخال مخفي لكلمة مرور جديدة)؛

- الرقابة البصرية للقيم التي يدخلها شخص آخر عادة؛ مناسبة للحالات الحرجة وعدد صغير من المعاملات؛

- عملية تحديد مبكر ومعالجة الأخطاء والانحرافات، والتحقق من المعاملات التي تم التحقق منها بشكل كامل مرة أخرى.

3. معالجة البيانات

الأهداف الرئيسية لمعالجة البيانات هي كالآتي:

- يتم فحص شمولية، دقة وصحة المعالجات المنجزة حسب إجراء روتيني، وتحديد أخطاء المعالجة في وقت مبكر، وتوثيقها وتصحيحها في الوقت المناسب؛

- يجري تصحيح المعاملات الخاطئة دون الإعاقة التي لا طائل منها للمعاملات الأخرى؛

- يتم إنجاز الحسابات والتجميعات والتوطيدات والتحليلات والتخصيصات بشكل صحيح من طرف البرنامج؛

- يتم ضمان فصل الوظائف بما في ذلك أثناء معالجة البيانات؛

- تكون المعاملات التي يولدها التطبيق آليا (مثل فوائد دورية على اعتماد، طلبيات في حالة تجاوز عتبة أمن المخزون) موضوع نفس عمليات رقابة الشمولية والدقة والصحة التي تكون على المعاملات المنعزلة؛

- يأخذ الأشخاص ويفحصون القرارات المهمة التي تعتمد على الحسابات الآلية.

عمليات الرقابة النموذجية لمعالجة البيانات هي كالآتي:

- يمكن أن يُطبق على المعالجة العديدُ من عمليات الرقابة الموضحة سابقا لإدخال البيانات وإنشاءها (م على سبيل المثال، مقارنة الحقول الفردية، مجاميع الرقابة حسب الدفعات، رقابة ترتيب ظهور البيانات ومقارنتها، مزامنة الدفتر الكبير والدفاتر المساعدة). ومع ذلك، فمن المهم أن تكون الوثائق والمجاميع المستخدمة لعمليات الرقابة مطابقة لنتائج نهاية المعالجة؛

- مقاربة البيانات المعالجة في النظام مع تأكيدات خارجية (على سبيل المثال، عمليات الجرد، تأكيدات الأرصدة البنكية وأرصدة الحسابات)؛

- ضمان سلامة المعالجة بفضل الأهداف الأربعة للعمليات الأعلى: الذرية (Atomocité) (وحدة العمل غير القابلة للتجزئة، جميع الإجراءات ذات الصلة يتم تنفيذها بنجاح أو لا ينجح أي منها)، التماسك (عندما لا تصل المعاملة إلى أي وضع نهائي ثابت، يجب إعادة تمهيدها في النظام)، والعزل (سلوك معاملة ما لا يتأثر بالمعاملات الأخرى التي تتم في وقت واحد) والاستدامة (في نهاية المعاملات، تبقى عواقبها مستديمة، بما في ذلك التغييرات في حالة أعطال في النظام). غالبا ما يتم تنفيذ عمليات الرقابة هذه خارج التطبيقات (على سبيل المثال، في أنظمة قاعدة البيانات). ومع ذلك يجب التحقق من ذلك بأخذ كل حالة على حدة.

4. مخرج البيانات (Output)

الأهداف الرئيسية لمخرج البيانات هي كالآتي:

- يتم إخراج البيانات في الوقت المناسب، في المكان المناسب ووفقا للإجراءات المحددة؛

- يتم ضمان شمولية، دقة وصحة المعلومات، التي يتم إصدارها، من خلال إجراءات منجزة بشكل تلقائي على المجاميع الرقابية ومقاربة مع المجاميع الرقابية الموافقة للمعالجة؛

- تتطابق معالجة والاحتفاظ بالمخرجات وتدميرها مع متطلبات حماية وأمن البيانات (قبل وبعد نشرها للمستخدمين)؛

- يتم الاحتفاظ بالمعلومات المطبوعة وفقا للأحكام القانونية.

عمليات الرقابة النموذجية لإخراج البيانات هي كالآتي:

- تضبط عمليات رقابة الإرسال والاستقبال كيفيات توصيل القوائم والمخرجات الأخرى(من، متى، ماذا، كيف وعدد النسخ)؛

- تضمن أنظمة تسيير الدخول إمكانية تتبع دخول المستخدمين أثناء تصفح القوائم على الشاشة أو طلب القوائم عبر الإنترنت؛

- عمليات رقابة الترقيم والشمولية التي تضمن كون تسيير، وإصدار، واسترجاع، واستلام وتدمير (في حالة نسخة للرقابة مثلا) المخرجات الحرجة (مثل الصكوك والايصالات، والسندات النقدية، وما إلى ذلك) يتم وفقا للإجراءات؛

- تتم رقابة دقة وشمولية المطبوعات الدورية (مثل المعالجة السداسية والسنوية) عن طريق عمليات الرقابة بأخذ العينات.

5. **الوسائط**

الأهداف الرئيسية المتعلقة بالوسائط هي التالية:

- يتم فحص صحة وسلامة المعلومات الواردة من مصادر خارج المنظمة بعناية قبل اتخاذ أي إجراء محتمل، بغض النظر عن وسيلة الاستقبال (الهاتف أو البريد الصوتي أو الورق أو الفاكس أو البريد الإلكتروني أو الملف)؛

- المعلومات الحساسة محمية خلال إرسالها من خلال تدابير مناسبة ضد الدخول غير المرخص به، التعديلات أو العنونة الخاطئة.

عمليات الرقابة النموذجية للوسائط هي التالية:

- يمكن أيضا استعمال عدد كبير من عمليات الرقابة، التي تم عرضها سابقا لإدخال وتسجيل البينات، من أجل رقابة الوسائط (مثال: مقارنة الوضعيات الفردية، مجاميع رقابة الدفعات، رقابة ترقيم ومقارنة البيانات)؛

- تشفير كل رسالة (مهمة) من أجل ضمان:
  - سرية المحتوى؛
  - سلامة محتوى الرسالة؛
  - هوية المستخدم.