GUIDE TECHNIQUE D'ACCREDITATION DEMATERIALISATION DES DONNEES DANS LES LABORATOIRES

Document LAB GTA 09

Révision 01 – Septembre 2008

cofrac

Section Laboratoires

SOMMAIRE

1

Objet du document

Les normes NF EN ISO/CEI 17025 et NF EN ISO 15189 définissent les exigences générales concernant la compétence respectivement des laboratoires d'étalonnages, d'essais et d'analyses, et des laboratoires d'analyses de biologie médicale.
Ces normes sont complétées par les documents Cofrac LAB REF 02, LAB CIL 02 et LAB LABM REF 02.
Les documents Cofrac LAB ML REF 02 et, LAB BPE REF 02 et 1022 rentrent également dans le champ d'application de ce guide.
Dans la suite du présent document, le terme « référentiel » s'applique aux normes et documents précités.
En cohérence avec l'annexe B « Lignes directrices pour l'établissement d'applications pour des domaines particuliers » de la norme NF EN ISO/CEI 17025, le présent Guide Technique d'Accréditation (GTA) définit les recommandations relatives à l'application de ces référentiels en matière de maîtrise des moyens informatiques et de dématérialisation des données au sein des Organismes d'Evaluation de la Conformité (OEC) concernés par les référentiels précités.

Après des premiers travaux dont le résultat a été la publication en 2005 du Guide Technique d'Accréditation intitulé « Dématérialisation des données – 1ere partie : Transmission électronique des rapports sur les résultats » (document Cofrac LAB GTA 09) il convenait naturellement de traiter les autres aspects de la dématérialisation des données, couvrant un champ très large depuis la maîtrise des données en amont des opérations techniques d'essais, d'analyses ou d'étalonnage, jusqu'au classement et à l'archivage en aval de ces opérations.

Il est alors apparu que le sujet traité comprend la **maîtrise des moyens informatiques** (matériels et logiciels) dans les OEC, moyens qu'il convient de considérer au même titre que tous les autres équipements de mesure, d'analyse ou d'essai, en transposant à leur utilisation les exigences du référentiel.

Il a donc été jugé préférable de produire un document unique, incluant le document LAB GTA 09 – Révision 00 – Novembre 2005, plutôt que de publier une deuxième partie à ce premier guide.
Les exigences du référentiel se rapportent notamment pour les moyens : à la réception, l'identification, la vérification, la validation et pour les données à l'intégrité, la confidentialité, l'archivage ainsi que l'authenticité des documents.
La finalité de ces exigences est que l'OEC s'engage de façon motivée et documentée sur l'aptitude à l'emploi de ses moyens, quelle qu'en soit leur nature.
Parmi ces exigences, applicables quelle que soit la nature du moyen, les normes NF EN ISO/CEI 17025 et NF EN ISO 15189 prévoient des clauses applicables aux équipements informatiques.

L'objectif de ce document est de présenter les points critiques à maîtriser et de donner à l'OEC des pistes de référence s'il souhaite approfondir une question et non pas de compiler les bonnes pratiques en matière de traitement de l'information. Les recommandations du présent guide, que l'OEC est libre d'appliquer ou non, sont celles reconnues par le Cofrac comme étant les plus appropriées pour répondre aux exigences du référentiel. Dans tous les cas, il revient à l'OEC de démontrer que les dispositions prises permettent de satisfaire pleinement ces exigences.

Comme toutes les organisations les OEC sont engagés dans la « révolution numérique » : le passage de l'information matérialisée à l'information dématérialisée. Celle-ci concerne bien évidemment le rapport émis par l'OEC mais également tout le processus du traitement de l'information mis en œuvre au sein de l'OEC. Cette révolution a de nombreuses conséquences dont la remise en cause des pratiques établies, jusqu'ici fondées sur des moyens techniques simples.
Par ailleurs, la législation jusqu'ici établie sur la notion de preuve par l'écrit papier a récemment évolué afin de prendre en compte la dématérialisation de l'information.
Le phénomène d'informatisation et de dématérialisation, favorisé par les évolutions technologiques, conduit à une évolution profonde des organisations et des modes de production. Les OEC sont, dans ce cadre, conduits à mettre en œuvre des méthodes et des outils nouveaux.

Si les exigences du référentiel ont été pour la plupart établies à partir de pratiques papiers, l'informatisation et la dématérialisation n'ont toutefois pas, en soi, conduit à une évolution du niveau des exigences. L'enjeu pour les OEC est donc de savoir quelles politiques et quelles pratiques mettre en œuvre en regard de ce mouvement d'informatisation. L'objectif est toujours de satisfaire aux exigences du référentiel, en tirant partie de l'informatisation et de la dématérialisation pour augmenter le niveau de performance de l'organisation.

2 Références bibliographiques et définitions

2.1 Références bibliographiques

Le présent document fait référence ou s'appuie sur les documents et textes de référence suivants :

- NF EN ISO/CEI 17025 (Septembre 2005) : Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais.
- LAB REF 02 (Révision 04 – Novembre 2007) : Exigences pour l'accréditation des laboratoires selon la norme NF EN ISO/CEI 17025.
- LAB ML REF 02 (Révision 01 – Décembre 2006) : Exigences pour l'accréditation des organismes procédant à la vérification d'instruments de mesure règlementés.
- LAB CIL REF 02 (Révision 02 – Septembre 2007) : Exigences pour l'accréditation des organisateurs de comparaisons interlaboratoires.
- NF EN ISO 15189 (Août 2007) : Laboratoires d'analyses de biologie médicale – Exigences particulières concernant la qualité et la compétence
- LAB LABM REF 02 (Révision 01 – Décembre 2007) : Exigences pour l'accréditation des laboratoires d'analyses de biologie médicale selon la norme NF EN ISO 15189.
- Document n°1022 (Révision 03 – Avril 1999) : Principe de bonnes pratiques de laboratoire pour les essais de produits chimiques.
- LAB BPE REF 02 (Révision 00 – Novembre 2004) : Référentiel des exigences de bonnes pratiques d'expérimentation (BPE) relatives à l'agrément pour la réalisation d'essais officiellement reconnus.
- Eurolab - Technical report n° 2/2006, d'octobre 2006 : Guidance for the management of computers and software in laboratories with reference to ISO/IEC 17025/2005.
- GBUI Guide de Bonne Utilisation de l'Informatique (produit par la SFIL, Société Française de l'Informatique des Laboratoires).

- NF Z42-013 (Décembre 2001) : Archivage électronique – Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.
- ISO 19005-1 (Octobre 2005) : Gestion de documents – Format de fichier des documents électroniques pour une conservation à long terme – Partie 1 : utilisation du PDF 1.4 (PDF/A-1).
- ISO/CEI 26300 (Décembre 2006) : Technologies de l'information – Format de document ouvert pour applications de bureau (OpenDocument) v1.0.
- ISO/CEI 13346 : Technologies de l'information – Structure de volume et de fichier de moyens d'écriture unique et de réécriture utilisant un enregistrement non séquentiel pour l'échange d'information.
- ISO/CEI 13490 (Décembre 1995) : Technologies de l'information. Structure de volume et de fichier de supports disque compact à lecture seule et à écriture unique pour l'échange d'information.
- Référentiel Général d'Interopérabilité (RGI) de la Direction Générale de la Modernisation de L'Etat (DGME).

Les textes réglementaires applicables sont consultables sur www.legifrance.gouv.fr.

2.2 Définitions

Pour les besoins du présent document, la définition ci-après s'applique :

- Organisme d'évaluation de la conformité (OEC) : laboratoire, organisme d'inspection, certificateur ou vérificateur individuel (cf. « Règlement d'accréditation » LAB REF 05).

3 Domaine d'application

Ce guide traite des activités techniques, d'analyses, d'essais et d'étalonnages de l'OEC. Toutefois, les principes généraux exposés dans ce guide peuvent être aussi appliqués à d'autres activités.

Le présent guide couvre le champ du processus de traitement et de transmission informatique depuis la production de la donnée jusqu'à son archivage, ainsi que la gestion des moyens informatiques mis en œuvre.
Il traite entre autres des questions d'authentification, d'intégrité, de validation, de traçabilité et d'archivage.

Ce guide, élaboré par un groupe de travail du Comité de Section Laboratoires, s'adresse :

- Aux OEC,
- Aux évaluateurs du Cofrac, à l'usage desquels il constitue une base d'harmonisation,
- Aux membres des instances du Cofrac (Comité de Section Laboratoires, Commissions Techniques d'Accréditation, Commission Interne d'Examen des Rapports pour l'Accréditation).

Ce guide correspond à l'état de la réglementation et de la normalisation au jour de sa publication. Il est de la responsabilité de l'OEC de prendre en compte les évolutions de la réglementation et de la normalisation lors de l'utilisation du présent guide.

4 Modalités d'application

Ce guide est applicable à compter du 01/11/2008.

5 Synthèse des modifications

Le document LAB GTA 09 - Révision 01 remplace la révision 00 intitulée "LAB GTA 09 - Révision 00 - Novembre 2005 - Dématérialisation des données - Première partie : Transmission électronique des rapports sur les résultats. Ce document a été profondément modifié afin d'étendre son champ d'application. En conséquence, aucune marque de modification n'y est apposée.

6 Recommandations pour la mise en place d'un système d'information

La richesse, voire la complexité de l'offre en matière d'outils informatiques, qu'il s'agisse d'acquisition, de traitement, de stockage, de dématérialisation ou de transmission électronique, ainsi que le besoin d'information des OEC comme de leurs clients, implique de disposer d'un modèle sur la base duquel l'OEC conduit une démarche débouchant sur la définition des pratiques et des outils à mettre en œuvre.

La démarche proposée ci-après vise à permettre à l'OEC d'identifier les points critiques à maîtriser en cas de dématérialisation de son activité de production d'essais, d'analyses ou d'étalonnages.

Etapes	Objectifs
1/ Définir les besoins et exigences	Mesurer les enjeux globaux (rester sur le marché, respecter des exigences, maintenir l'activité), identifier les besoins et exigences.
2/ Définir le champ d'application de la dématérialisation	Cibler les exigences des processus, définir les cahiers des charges
3/ Appréhender son propre système d'information	Connaître son environnement : pratiques, procédures et outils à mettre en œuvre.
4/ Vérifier l'influence des systèmes de dématérialisation	Evaluation de l'impact (risque) du choix d'un système de dématérialisation (modulaire ou global).
5/ Evaluer l'équilibre du système d'information	Mesurer la faisabilité de la dématérialisation et anticiper sur les actions à mener

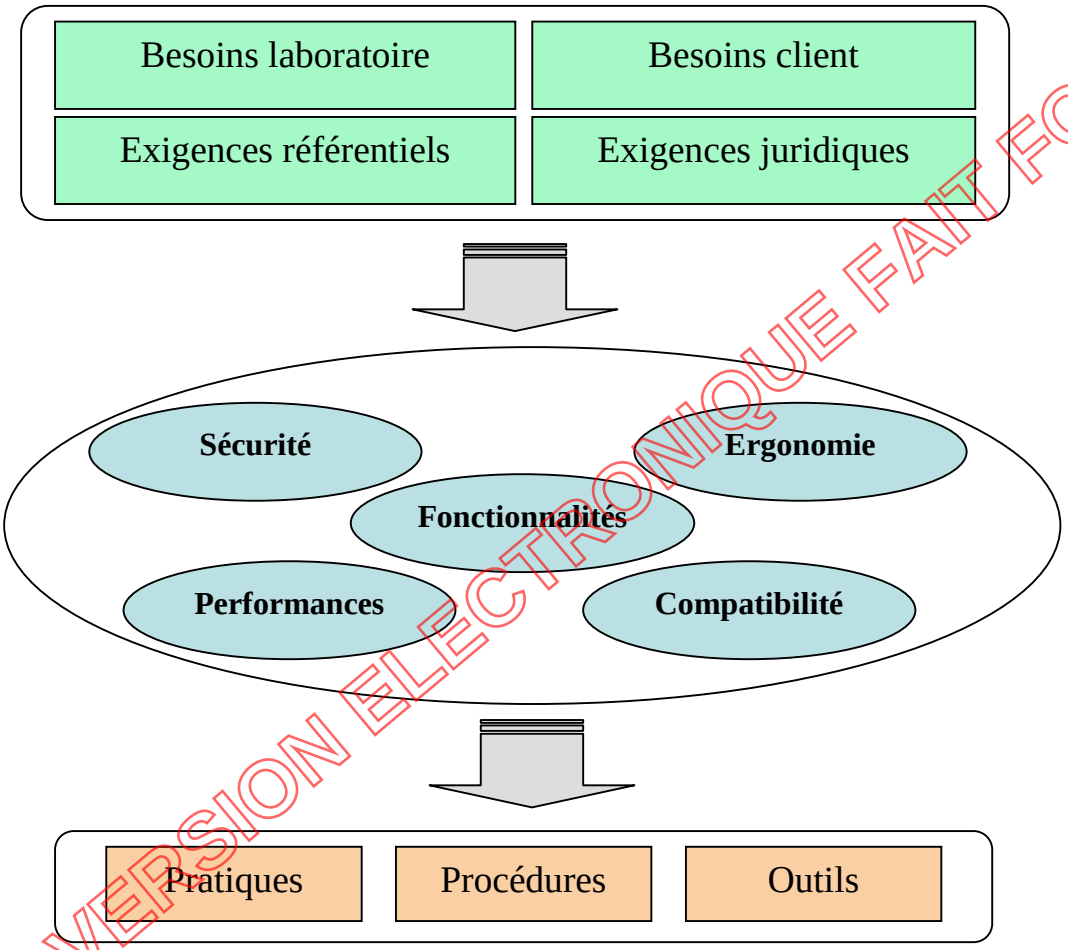
Pour chaque phase du processus de production et chaque moyen informatique, l'OEC doit s'interroger, en liaison avec ses clients et les éventuels tiers concernés (autorités réglementaires, autres utilisateurs des rapports,…) sur la criticité des données associées aux différentes phases du processus, des rapports sur les résultats émis et des risques encourus en cas de falsification, usurpation d'identité, répudiation, etc., afin de pouvoir identifier les pratiques, procédures et outils à mettre en œuvre.

6.1 Définir les besoins et exigences

Dans un premier temps, il est nécessaire de préciser les enjeux en termes de besoins clients et besoins de l'OEC ainsi que les exigences en matière juridique et de conformité à des référentiels.

☞EVITER DE S'ENGAGER SUR LA BASE DE MOTIVATIONS FAIBLES.

Ces enjeux constituent les données d'entrées du processus de dématérialisation.



6.2 Définir le champ d'application de la dématérialisation

Il est important de bien identifier les étapes du processus de manière à faciliter l'expression des besoins et, avant tout, d'anticiper sur les phases à risque, concernant :

- les niveaux de sécurité,
- les fonctionnalités,
- l'ergonomie,
- la performance (coûts, délais),
- la compatibilité des systèmes mis en œuvre.

☞EVITER DE GLOBALISER EN ASSURANT UNE DECOMPOSITION FINE DES ETAPES.

6.3 Appréhender son propre système d'information

Un système d'information se définit comme l'association :

- **De processus**

Les processus déterminent les enchaînements de travaux et tâches qu'il convient d'opérer pour obtenir un résultat à partir de la transformation d'informations initiales ou intermédiaires (savoir faire, procédures, pratiques).

- **D'utilisateurs**

Ils sont les acteurs du processus, ils opèrent les travaux éventuellement aux moyens d'outils et de méthodologies.

- **D'outils logiciels**

Les outils logiciels ou infrastructure logicielle permettent de faire réaliser certaines opérations par des matériels informatiques. On parle ici de logiciels, programmes, applications informatiques…

- **D'outils matériels**

Les outils matériels ou infrastructure matérielle permettent de faire fonctionner les outils logiciels et d'échanger les données. On désigne ici les infrastructures sous divers vocables adaptés : ordinateurs, serveurs, réseaux….

- **D'informations**

Il s'agit de la « matière » entrant dans le processus de transformation ou résultant de celui-ci qu'opère un système d'information. Une information est transformée en information ou action par un processus.

☞ PRENDRE EN COMPTE LE ROLE DES UTILISATEURS.

6.4 Vérifier l'influence des systèmes de dématérialisation

Le système de dématérialisation peut altérer les processus en terme de fiabilité des résultats ou de lisibilité. On recherchera avant tout la **cohérence** entre le système de dématérialisation et le processus de l'OEC.

Exemple :

Risques identifiés	Impact sur
Non intégration de conservation de données	La reproductibilité La traçabilité
Occultation des points de contrôles	L'exactitude La corruption des données

☞ RESISTER A LA TENTATION DU TOUT EN UN.

6.5 Evaluer l'équilibre du système d'information

Enfin, il s'agit d'évaluer les risques et enjeux liés aux thématiques suivantes :

- **Economiques**

Il s'agit d'évaluer les gains et les coûts d'exploitation.

- **Sociales**

Il s'agit d'évaluer l'amélioration des performances et les freins au changement.

- **Partenariales**

Il s'agit d'évaluer la demande externe et les risques de l'environnement (marché, etc.).

L'analyse débouche sur des modalités de déploiement intégrant les réponses apportées aux facteurs de risques ainsi qu'à la mise en œuvre des facteurs liés aux enjeux.

Exemple : Intégration d'un équipement de saisie mobile.

Facteur de risques :
- Changement des habitudes, suppression de postes d'opérateur de saisie → Accompagnement du changement, plan d'évolution de postes.
- Coût de développement des applications, du matériel.

Enjeux :
- Gain de productivité et marges
- Amélioration des délais → Communication client.

L'équilibre du système d'information résulte de cette analyse et se traduit souvent par un compromis entre le « tout manuel » et le « tout automatique ». Cette notion d'équilibre est fondamentale car elle permet d'optimiser les chances de succès de la mise en œuvre du dispositif.

☞ PRENDRE EN COMPTE LES FREINS AU CHANGEMENT ET L'ACCOMPAGNEMENT CORRESPONDANT : CHOISIR LE COMPROMIS.

Sous couvert de la mise en place de la démarche précédemment exposée, de nombreuses approches, dont quelques unes sont décrites dans ce guide, sont en accord avec le référentiel.
En tout état de cause, pour répondre aux exigences du référentiel d'accréditation, les pratiques et outils mis en œuvre doivent faire l'objet d'une revue.
En outre, la réglementation impose une relation contractuelle entre les parties (convention de preuve) pour certains aspects (signature électronique, archivage électronique, …).

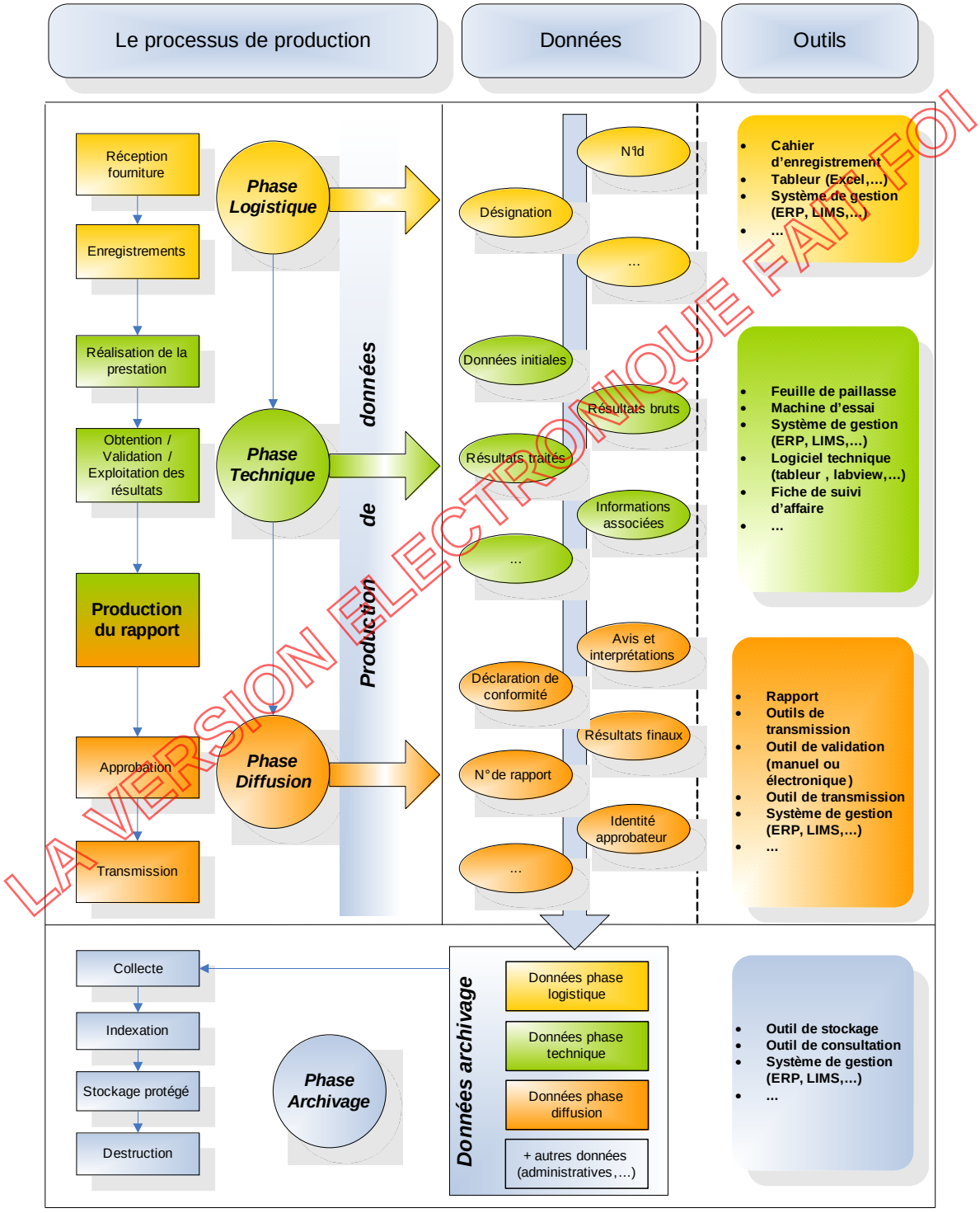
Il convient de porter une attention particulière à l'application des recommandations de ce guide dans un cadre international. Par exemple, dans les pays de l'Union européenne, les modalités de transposition de la directive 1999/93/CE relative à la signature électronique peuvent engendrer des différences d'application.

En l'absence de réglementation (européenne, internationale, …), les règles sont définies dans un cadre contractuel.

7 Processus de production

7.1 Organisation générale

En amont de la dématérialisation, intervient la production de données. La donnée produite à l'issue d'une acquisition automatique ou d'une saisie manuelle est le point de départ de la dématérialisation. La figure ci-dessous met en avant les différentes étapes du processus de production du service rendu par l'OEC à son client.



Il apparaît que le processus de production se scinde en quatre phases, **trois phases intégrées au cycle de production (logistique, technique, diffusion)** et **une phase transversale (archivage).** Ces quatre phases existent implicitement au sein de l'OEC, quel que soit le modèle organisationnel utilisé :

- **Phase logistique**

C'est avant tout une **phase interne** au laboratoire. Sans être directement impliquée dans les autres phases, la phase logistique est le lieu où la fourniture (échantillon ou appareillage) est identifiée (N°, code barre, RFID,…). A ce stade, les données gérées permettent à l'OEC d'assurer la traçabilité des autres phases.

La phase logistique peut dans certains cas donner lieu à des enregistrements de données (cotations, références techniques, classification,…) pouvant ensuite faire l'objet de **traitements informatiques (§ 8.3)** en phase technique**.**

- **Phase technique**

C'est également une **phase interne** au processus de l'OEC. Elle comprend le management technique de la prestation, et est le lieu de production des **données initiales (§ 7.2)**.

Cette phase inclut la réalisation de la prestation technique et peut comprendre des **traitements informatiques (§ 7.3)**. Elle aboutit à la **production du rapport (§ 7.4)**.

- **Phase diffusion**

La diffusion, phase autant administrative que technique, concrétise la relation entre le client et l'OEC : elle relie **la production du rapport** aux étapes d'**approbation et de transmission (§ 7.5)**. Les modes de transmission et d'approbation du rapport sont fonction du **type de rapport (§ 7.4.2)** et de son **cycle de vie (§ 7.4.1)**.

- **Phase archivage**

Le schéma fait bien apparaître que chaque phase est productrice de données, ces données vont pouvoir, durant une période définie par le laboratoire, être retrouvées dans une phase commune : l'**archivage (§ 7.6)**.

7.2 Définition des données initiales

La donnée initiale est définie dans ce guide comme la première donnée qui n'a pas subi de transformation par l'utilisateur de l'équipement ou de la chaîne de mesure dans le cadre de la méthode d'analyse, d'essai ou d'étalonnage.

Ce peut être la donnée générée aussi bien par une chaîne de mesure complexe (intégrant des logiciels de pilotage ou de traitement) que par un simple mètre ruban (constat visuel). Dans le cas d'éléments informatiques associés ou intégrés aux équipements qui « produisent » la

donnée initiale, ceux-ci sont à gérer de préférence en tant qu'équipements de mesure ou d'essai et non en tant que moyens informatiques, conformément à leur fonction première.

Dans le cas d'un équipement « paramétrable » il convient que soient tracées les configurations de l'essai, de l'équipement, par exemple dans le cadre du mode opératoire ou des données de sortie liées à l'essai.

Exemple : la donnée initiale dans le cas d'une analyse microbiologique est le nombre de colonies présentes dans une boîte de Petri. Cette donnée est liée au temps d'incubation dans une étuve pour laquelle la température doit être enregistrée.

La température de l'étuve fait partie des enregistrements techniques associés à la donnée initiale. Par ailleurs, l'identité de la personne ayant réalisé l'analyse doit également être enregistrée au même titre que la température ou la donnée initiale.

La donnée initiale est aussi la première information enregistrable et conservable à des fins d'archivage et de traçabilité : cahier de paillasse, ticket d'imprimante, retranscription de la donnée dans un système informatique.

La donnée initiale peut être une information retranscrite sur un support (papier ou informatique) à des fins d'archivage. Le support peut être uniquement informatique, il n'existe pas nécessairement de support papier.

La retranscription est nécessaire dans le cas d'une lecture d'un afficheur ou lors d'un constat visuel, elle peut aussi être nécessaire dans d'autres cas incluant la retranscription de données imprimées.

D'ailleurs, la norme NF EN ISO/CEI 17025 évoque au paragraphe 4.13.2.2 un enregistrement des données au moment où elles sont produites.

Exemple : les résultats de mesure sont imprimés par l'imprimante intégrée à l'équipement de mesure sur un papier thermique, la retranscription de ces données sur un autre support (informatique ou non) permet de conserver la donnée initiale dans de meilleures conditions.

Il appartient à l'OEC de définir ce qu'il entend par donnée initiale dans le cadre de ses essais, analyses ou étalonnages en particulier en vue d'assurer une filière d'audit.

Les données initiales font partie des « observations originales » de la norme NF EN ISO/CEI 17025 (4.13.2.1) et des données brutes relatif au décret n°2006-1523 du 4 décembre 2006 relatif aux bonnes pratiques de laboratoire.

Elles sont donc soumises aux mêmes exigences en matière d'enregistrement et de traçabilité.

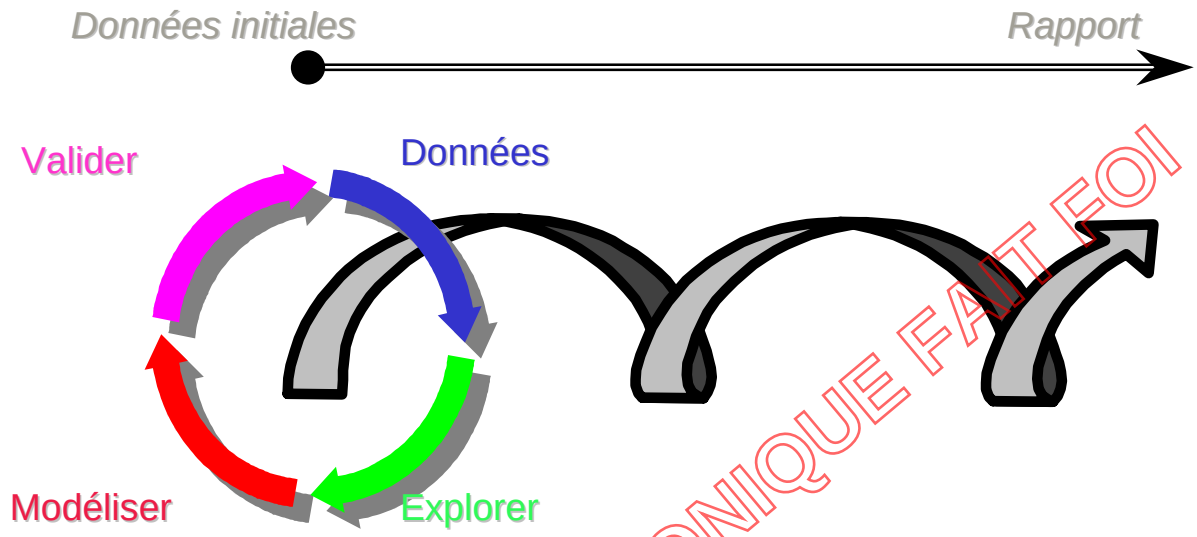
7.3 Traitements informatiques

La finalité d'un traitement informatique est de :

- transformer des données afin d'y ajouter de la valeur, cette valeur étant de nature informationnelle,
- stocker des données,
- restituer des données.

Les trois finalités peuvent être combinées.
Un modèle type de traitement est présenté ci-après. Les actions opérées sur les données, qu'il s'agisse de données initiales ou de données de sortie d'un traitement précédent, sont

fréquemment des actions d'exploration des données, de modélisation ou de transformation et enfin de validation du modèle ou du traitement. Ces actions ne sont pas toujours de nature informatique ; par exemple une validation peut être décidée par un expert et faire simplement l'objet d'un enregistrement.
Les traitements sont en général multiples et vont s'enchaîner de façon séquentielle ou itérative jusqu'à la production du rapport sur les résultats.



Modèle type de traitement

Un traitement informatique se déroule dans un environnement permettant d'assurer la maîtrise du traitement.
La qualité du traitement est garantie en particulier par la validation des logiciels utilisés, ainsi que par les procédures de maîtrise du traitement des données et des enregistrements.
La norme NF EN ISO/CEI 17025 demande dans son paragraphe 5.4.7 la mise en place de procédures et de vérifications systématiques concernant le traitement des données. Ces procédures se doivent d'assurer l'intégrité et la confidentialité des données et l'exactitude des résultats.

Les entrées du traitement sont d'une part des données (données d'entrée), d'autre part des paramètres spécifiant le traitement effectivement réalisé sur les données.
Les sorties du traitement, données de sortie, ou résultats, sont à valider avant toute utilisation, qu'il s'agisse d'un nouveau traitement ou d'une publication.
Le traitement s'accompagne d'enregistrements de diverses natures. Ces enregistrements doivent être définis par le laboratoire en fonction des risques associés aux conséquences d'un traitement défectueux ou d'une perte de traçabilité.
Les enregistrements peuvent être classés en quatre catégories principales :

- les enregistrements relatifs aux entrées du traitement,
- les enregistrements relatifs au traitement,
- les enregistrements relatifs aux modifications et corrections apportées en cours de traitement,
- les enregistrements relatifs aux sorties du traitement.

Un enregistrement, ou un traitement, informatique nécessite une « validation ». Cela implique que tant que l'enregistrement, ou un traitement, n'est pas validé, il n'est pas utilisable. La validation peut se faire de nombreuses manières : simple déclaration par une personne compétente, mise en place de mécanismes de double saisie, règles de gestion et de contrôle informatisées.
Les modifications réalisées après validation peuvent être tracées dans l'enregistrement informatique lui-même (au moyen d'un commentaire), en conservant les versions successives de l'enregistrement, ou encore en s'appuyant sur un système de gestion de base de données qui conserve dans un journal toutes les modifications apportées au contenu de la base.
La définition d'une modification est un exercice délicat pour l'OEC et il convient qu'elle soit effectuée en gardant en perspective les risques encourus. Ainsi les erreurs de frappe lors de la saisie ou bien une manipulation de type glisser/déplacer aussitôt corrigée sont des opérations ne nécessitant en général pas de validation explicite.
Une politique basée sur la définition de « points de contrôle » dans le processus de traitement des données, qui définit les étapes critiques nécessitant une validation formelle peut être utilement mise en œuvre par le laboratoire.

En matière de gestion des erreurs et des corrections, dans le cas de supports informatiques, une façon de satisfaire à l'exigence du paragraphe 4.13.2.3 de la norme NF EN ISO/CEI 17025 est de conserver les différentes versions des fichiers contenant des enregistrements techniques corrigés ou modifiés, ceux-ci étant signés ou visés par la personne qui fait la correction.
Le besoin lié à cette exigence est de conserver une trace des modifications et de l'identité des personnes qui les ont réalisées. Cette exigence d'identification est réalisable dans un système informatisé à condition d'avoir défini au préalable quand une identification est nécessaire et quel moyen d'identification est à mettre en œuvre pour garantir un niveau d'authenticité suffisant compte tenu du risque.
Une solution simple est d'utiliser un identifiant de quelques caractères nommant la personne concernée. Cette solution présente l'inconvénient de ne pas garantir l'authentification (risque d'usurpation d'identité). Si l'identité doit être absolument garantie, il est alors possible d'utiliser une signature électronique.

7.4 Production du rapport

Historiquement, les rapports d'essais étaient émis exclusivement au format papier. L'évolution des moyens techniques mis à disposition des OEC, et la généralisation des outils informatiques dans le monde de l'entreprise ont permis à une nouvelle génération de rapport de voir le jour : le rapport électronique.

Aujourd'hui, il est possible pour un OEC d'émettre un rapport sous une forme papier ou « tout électronique ». Par « tout électronique » il faut comprendre document dématérialisé. La dématérialisation des données consiste à stocker et faire circuler des données sans support matériel autre que des équipements informatiques, tout en assurant la validation des flux de contenus. Les rapports dits « multimédia » appartiennent à cette dernière catégorie. Avant de se lancer dans le tout électronique, il est primordial que l'OEC prenne connaissance des dispositions légales en la matière. Le respect des textes réglementaires en vigueur implique cependant la mise en place d'outils spécifiques permettant à la fois d'assurer l'authenticité du rapport et sa validité dans la durée (indispensable en cas de litige).

Jusqu'à il y a encore peu de temps, la législation française ne reconnaissait qu'au seul écrit papier la valeur de preuve. Désormais, elle est en place pour les écrits purement électroniques à l'exception de ce qui concerne l'archivage électronique.
Le développement qui suit vise à comparer les formes papier et « tout électronique » et à réaliser un état des lieux des exigences juridiques à respecter pour chacune, et ce, afin de pouvoir leur conférer valeur probante en cas de litige. Avec l'informatisation grandissante, les documents émis ne se limitent pas à une forme ou à l'autre, mais présentent bien souvent les caractéristiques des deux. Par exemple, on peut envisager le cas de l'édition d'un rapport sur les résultats, numérisé pour faciliter sa conservation dans le temps, puis transmis au format papier au client. Dans ce cas, en cas de litige, l'OEC émetteur du rapport doit apporter devant la justice la preuve que le document numérisé est identique sur le fond à l'original papier envoyé au client, le but étant d'emporter la conviction du juge.
Si au contraire, l'OEC établit et conserve le rapport sur les résultats conformément au cadre juridique fixé par la loi, il ne lui appartient pas, en cas de litige, d'apporter la preuve de l'efficacité du système mis en place pour garantir l'intégrité et l'inaltérabilité du document dans la durée. Il est de la responsabilité de son détracteur d'apporter des éléments prouvant la non-fiabilité du système mis en place par le laboratoire : c'est ce que l'on appelle le renversement de la charge de la preuve. Cette notion de présomption de fiabilité apparaît notamment à l'article 2 du décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique qui stipule que *« la fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié ».*

Un moyen de se prémunir d'un éventuel litige peut consister à établir avec le client une convention relative à la preuve. Celle-ci est un contrat qui a pour objet de définir les modes de preuve admissibles entre les parties, la charge de la preuve et les modalités de règlement des conflits de preuve. La convention de preuve permet notamment de régir les modalités d'établissement, de signature (type d'outils pour signer électroniquement un document par exemple), de transmission et d'archivage des documents. Ce principe est celui de la liberté de la preuve tel qu'il est défini à l'article L110-3 du Code de Commerce : *A l'égard des commerçants, les actes de commerce peuvent se prouver par tous les moyens à moins qu'il en soit autrement disposé par la loi.*

Des conditions générales de vente (cf. article L441-6 du Code de commerce) peuvent compléter le processus de revue de contrat. Elles sont établies par l'OEC, conformément au principe de transparence qui préside aux relations entre fournisseurs et acheteurs. Elles visent à informer l'acheteur préalablement à toute transaction du barème de prix et des conditions de vente du vendeur et constituent le cadre de la négociation commerciale. Les conditions générales de vente peuvent inclure, en outre, la convention de preuve.

7.4.1 Cycle de vie d'un document

Le tableau suivant permet de faire un parallèle entre les cycles de vie d'un original papier et d'un document « tout électronique » depuis leur création jusqu'à leur conservation à des fins de preuve.

Papier	Tout électronique
1. Etablissement du document sous forme transitoire de « brouillon » *Exemple : rédaction d'un courrier sous traitement de texte*	1. Travail sur un fichier informatique *Exemple : rédaction d'un courrier sous traitement de texte*
2. Mise en forme sur support définitif papier : le document édité devient alors un original. *Exemple : courrier édité ou non sur papier entête et signé ≠ facture non signée* ***= original dans les deux cas***	2. Finalisation du document. Enregistrement du fichier sur support définitif électronique. *Exemple : enregistrement du fichier sur disque magnétique, optique, sur clé USB…*
3. L'original peut être signé au moyen d'une signature manuscrite ou non. Celle-ci n'est pas obligatoire, l'usage veut qu'elle permettre de distinguer plus nettement un original et d'établir les responsabilités au sein de l'entité émettrice du document en cas de litige.	3. Le document doit être signé électroniquement (= chiffrement du fichier) pour garantir son inaltérabilité dans le temps et lui conférer **le statut de document à valeur probante** (*). Dans le cas contraire, le document édité sur support papier est considéré comme l'original.
4. Archivage du document papier à des fins de preuves en cas de litige. L'important, c'est la fidélité, la durabilité et l'inaltérabilité du document qui lui confère sa vertu d'original. Le papier est considéré comme « fidèle et durable » au sens de l'article 1348 du Code Civil.	4. Archivage du document électronique selon un état de l'art pour conférer à ce dernier une valeur probante.

(*) « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.» (article 1316-1 du Code Civil)
« L'écrit sur support électronique a la même force probante que l'écrit sur support papier » (article 1316-3 du Code Civil).

Par ailleurs, « copie » et « duplicata » sont des mots utilisés pour désigner la reproduction manuscrite, mécanique ou électronique d'un contrat ou d'un document quelconque. En revanche, le « double », est un second original signé par le déclarant ou par les parties. Les notions de copie, de duplicata et de double ne s'appliquent qu'à un original papier. Au format électronique, les copies sont rigoureusement identiques au document source. Le terme d'original ne s'applique qu'à un écrit papier. Dès lors qu'il est signé électroniquement, le document informatique a force probante.
Sur le plan juridique, la copie (et par voie de conséquence le duplicata) est inférieure à l'original. L'article 1334 du Code Civil stipule en effet que *« les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée »*. De même, l'article 1348 dispose qu'en l'absence d'original, la copie doit être *« la reproduction non seulement fidèle mais durable [de l'original]. Est réputée*

durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support ».

7.4.2 Types de rapports

Un rapport peut être constitué d'un ensemble de données de natures différentes. Il peut s'agir par exemple de fichiers de formats différents mettant en jeu du texte, de la vidéo ou du son. Dans ce cas, on parlera de rapport multimédia. Ce type de rapport est nécessairement de par sa nature un rapport électronique. Celui-ci ne peut pas être édité en l'état sur un support papier puisque cela nécessite un certain nombre d'opérations pour rendre compatibles les informations avec les supports physiques choisis.

A titre d'exemple, on peut envisager que le texte soit imprimé sur support papier tandis que la vidéo ou l'audio soient transposées sur un support optique non réinscriptible (de type Write Once Read Many). Toutefois, sur le plan juridique, le rapport alors émis est une copie. On peut également envisager que l'ensemble du rapport soit contenu sur le support WORM. Dans ce cas, il a valeur de preuve.

Un support optique de ce type permet plus facilement qu'un support magnétique de garantir l'intégrité des données qui y sont inscrites, la réécriture étant impossible. On peut toutefois aussi trouver des offres à base de support numérique et de logiciel associé, apportant le même niveau de garantie.

Il appartient alors à l'OEC d'assurer l'intégrité de ce type de rapport (format garantissant l'intégrité lors de l'archivage). Pour une version texte (cas le plus courant), il existe plusieurs formats qui offrent des fonctionnalités similaires : on peut citer notamment les formats XPS (XML Paper Specification) et PDF. Ce dernier, en cours de normalisation pour la version 1.7, permet entre autre de préserver les polices, les images, les objets graphiques et la mise en forme de tout document source, quelles que soient l'application et la plate-forme utilisées pour le créer. En d'autres termes, ce format garantit l'intégrité du document, vis-à-vis des environnements techniques non nécessairement identiques de l'OEC et de son client. Toutefois, il ne garantit pas la non falsifiabilité du document ou l'identification de son auteur, sauf à mettre en œuvre des outils de signature électronique.

7.5 Approbation et transmission du rapport

7.5.1 Contexte juridique : imputabilité de l'acte juridique

Aux termes de l'article 1316-4 alinéa 1 du Code Civil, il faut, en premier lieu, que la personne auteur de l'acte soit dûment identifiée. L'article considéré stipule en effet que : *« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose »*. Cette exigence renvoie à la notion d'imputabilité de l'acte, c'est-à-dire l'identification de l'auteur de l'acte et de son lien avec lui. D'un point de vue juridique, l'imputabilité parfaite d'un acte à son auteur se matérialise par la signature de l'acte.
La preuve de l'approbation du rapport sur les résultats est donc apportée par l'autorisation de la (ou des) personne(s) autorisée(s) à signer ce rapport. Chacun des signataires engage sa responsabilité pour un périmètre donné qui doit par ailleurs être défini.

7.5.2 Types d'approbation en fonction du format choisi

7.5.2.1 Approbation d'un rapport sur les résultats émis au format papier

Pour un rapport émis au format papier, l'usage veut que cette approbation se traduise par l'apposition sur l'original de la signature manuscrite du (ou des) signataire(s). Un rapport émis au format papier sans signature manuscrite peut également être recevable au titre d'original selon l'article 1316-2 du Code Civil qui stipule que « *Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.* »

7.5.2.2 Approbation d'un rapport électronique

L'article 1316-4 alinéa 2 du Code Civil relatif à la signature électronique précise « *lorsqu'elle est électronique, elle (la signature) consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État.* ».
Actuellement, les exigences d'identification et de lien avec l'acte telles que définies par le législateur sont remplies techniquement par le procédé de signature électronique basé sur la cryptologie à clé publique et reposant sur des certificats électroniques, que la signature soit simple ou sécurisée au sens du décret n° 2001-272 du 30 mars 2001.
Pour un rapport électronique, cette validation va donc se traduire par le chiffrement du document, chiffrement réalisé à l'aide de la clef privée du signataire (= signature électronique). Il faut alors utiliser la clef publique correspondante pour déchiffrer et lire le rapport.

La signature électronique permet également de valider les rapports multimédia. Le recours à une signature manuscrite numérisée ne garantit nullement que le rapport électronique a été validé. Pour que ce dernier puisse l'être, il faut utiliser un mécanisme permettant d'associer de façon certaine la signature au signataire par des dispositions appropriées définies par l'OEC ou un procédé de signature électronique.

7.5.3 Transmission du rapport

Le tableau qui suit présente un comparatif des usages postaux et des nouvelles pratiques en matière de dématérialisation des échanges. Il n'a pas la prétention d'être exhaustif ni de

donner de valeur absolue dans les niveaux de fiabilité évalués mais il permet de positionner de façon relative les procédés les plus courants.

Par ordre croissant de fiabilité pour le critère évalué (de + à +++)

Critère évalué	Papier	Electronique
Confidentialité (prise de connaissance par un tiers non autorisé)	+ Envoi postal banalisé. ++ Envoi RAR. +++ Remise en main propre.	++ Chiffrage du document avec certificat du destinataire. +++ Avec signature présumée fiable ou convention de preuve entre émetteur et destinataire
Intégrité	+ Papier ordinaire ++ Papier filigrané, non photocopiable.	++ Signature électronique +++ Signature électronique présumée fiable ou convention de preuve entre émetteur et destinataire
Authenticité	+ Marque distinctive imprimée ou pré imprimée. + Signature manuscrite	++ Signature électronique +++ Signature électronique présumée fiable ou convention de preuve entre émetteur et destinataire
Horodatage: Datage de l'émission Datage de la réception	+ Cachet de la poste ++ Envoi avec AR	++ Utilisation d'une signature électronique de la date (système d'horodatage)
Non répudiation (assurance du caractère définitif de l'acte)	+++ Acte réalisé devant un officier public (notaire,...)	+++ Signature électronique présumée fiable avec système d'horodatage garanti par un tiers de confiance

Les pratiques suivantes sont données à titre d'exemple :

Le mél (e-mail ou courriel) avec pièce jointe

Cette pratique permet en principe d'assurer la confidentialité, le message n'étant délivré qu'au destinataire nommé. Il est toutefois recommandé d'utiliser une adresse électronique nominative.
Comme dans le cas de l'envoi postal, des risques d'interception du message existent.
L'intégrité du document joint, copie d'un document original de référence, n'est assurée qu'en utilisant des formats de fichier protégés autorisant uniquement la lecture et l'impression (par exemple un format de type PDF).

A cet égard il convient de ne jamais oublier qu'aucune protection n'est parfaite et que dans l'absolu, en y allouant les ressources nécessaires, toutes les protections peuvent être franchies.
L'archivage d'une copie (fidèle et durable) du rapport transmis est un des éléments essentiels permettant de garantir l'intégrité du document transmis par voie électronique. Si cette copie est conservée sous format électronique uniquement, il faut pouvoir démontrer les garanties prises en terme de conservation des données dans le temps (intégrité et permanence de l'accès).
L'authenticité du message est assurée par l'adresse électronique de l'émetteur. Cependant, il est admis que des risques d'usurpation d'identité existent.
Les accusés de réception retournés automatiquement par la messagerie du destinataire présentent un intérêt pratique mais ne présentent pas nécessairement toutes les garanties attendues en matière de fiabilité des informations transmises (date de réception, de lecture,…).
La messagerie électronique présente globalement un niveau de sécurité comparable au courrier postal simple.
Les atouts de la messagerie électronique en matière d'efficacité et de rapidité sont à rapprocher des dangers d'une diffusion immédiate à grande échelle en cas d'erreur.
L'utilisation de ce type d'outil nécessite la mise en place d'un contrat (ou convention de preuve) entre l'émetteur et le destinataire préalablement à toute transmission électronique.

L'extranet

Cette pratique consiste à mettre à disposition des documents sur un site Internet à accès restreint.
La confidentialité est assurée par une politique adaptée de gestion des profils des utilisateurs.
Un des risques potentiels est l'usurpation de l'identité des utilisateurs.
L'intégrité des données ou des documents extraits est assurée par l'existence d'originaux qui sont le contenu même de l'extranet.
La sauvegarde et l'accessibilité du site (disponibilité de service) doivent être assurés.
Comme dans le cas précédent, il est admis que l'usurpation de l'identité du site constitue un risque potentiel.
Le site peut être conçu pour garder trace des accès des utilisateurs.
Un extranet développé et administré selon les règles de l'art présente, en principe, un niveau de sécurité supérieur au courrier postal avec des fonctionnalités supplémentaires en terme de traçabilité.
L'utilisation de ce type d'outil nécessite la mise en place d'un contrat (ou convention de preuve) entre l'émetteur et le destinataire préalablement à toute transmission électronique.

Les supports d'enregistrement numérique

S'agissant de medias physiques, le niveau de confidentialité de la transmission est a priori de même nature que pour un document papier : courrier postal, remise en main propre,…
La confidentialité et l'intégrité du contenu sont assurées de la même façon que par une pièce jointe à un mél.
De même, ici, l'archivage d'une copie fidèle et durable (sous forme papier ou électronique) du rapport transmis est un des éléments essentiels permettant de garantir l'intégrité du document transmis sur le support d'enregistrement numérique (CD, DVD, Blu-ray disc, disques optiques rigides UDO (Ultra Density Optical), …).

A condition qu'il soit non réinscriptible, un support d'enregistrement numérique permet d'assurer l'authenticité de l'émetteur de la même façon que pour un document papier, par exemple en y apposant un logo et en le signant de façon indélébile.
L'accusé de réception est assuré de la même façon que pour un document papier.
Comme dans le cas de l'utilisation d'une messagerie électronique, ce type de support nécessite la mise en place d'un contrat (ou convention de preuve) entre l'émetteur et le destinataire préalablement à tout échange d'information.

La signature électronique

La signature électronique présumée fiable permet de répondre sans autre disposition à toutes les exigences, hormis celles relatives à la datation de l'envoi ou de la réception du document (sauf dispositions relatives à l'horodatage).
La présomption de fiabilité est garantie par l'existence d'un certificat qualifié délivré par un tiers de confiance ou prestataire de service de certification électronique (PSCE) qualifié par un organisme de certification accrédité par le Cofrac.
La signature électronique « simple » permet de répondre aux mêmes exigences pour autant qu'un contrat (ou convention de preuve) ait été établi entre l'émetteur et le destinataire du rapport sur les résultats.
En effet, en cas de contestation, l'OEC devra démontrer la fiabilité du procédé de signature électronique employé. Dans ce cas, le fait de signer, en amont, une convention de preuve avec ses clients constitue juridiquement une force probante pour l'OEC.
Ce contrat doit préciser les outils utilisés pour la transmission par voie électronique, les modes de preuve admissibles entre les parties et les modalités de règlement des conflits en cas de problème.
Par ailleurs, si la convention de preuve ne porte pas sur l'archivage électronique, une copie fidèle et durable du rapport sur les résultats transmis par voie électronique doit être conservée sous forme papier ou électronique.
Dans le cas d'une version électronique, il faut pouvoir démontrer les garanties prises en terme de conservation des données dans le temps (intégrité et permanence de l'accès).

7.6 Archivage

7.6.1 Conservation des données et des enregistrements

L'OEC peut définir une durée de conservation des données initiales différente de celle des rapports sur les résultats. Par exemple, on peut envisager que l'OEC conserve les données initiales pour pouvoir rééditer éventuellement son rapport en cas de réclamation du client dans des délais impartis, délais qui seraient précisés à l'avance dans le contrat avec le client.
La ré exécution des traitements à partir des données brutes ne serait effectuée alors qu'en cas de contestation du rapport émis. Au-delà du délai prescrit dans le contrat, la non manifestation du client (oral/écrit) pourrait valoir approbation définitive du rapport. Il n'y aurait dès lors plus aucun intérêt pour l'OEC (à moins d'y être tenu par la réglementation) de conserver plus longtemps les données brutes. L'archivage du rapport final seul suffirait. Bien évidemment, la durée d'archivage des rapports définie par l'OEC doit permettre d'assurer une filière d'audit entre deux évaluations d'accréditation successives conformément au § 4.13.2.1 de la norme NF EN ISO/CEI 17025 et au document d'application LAB REF 02 du Cofrac. La durée d'archivage doit aussi être compatible avec les réglementations sectorielles en vigueur.

Une liste non exhaustive de documents pour lesquels la réglementation impose une durée minimale de conservation figure ci-dessous à titre informatif.

Documents à conserver	Délais de conservation	Textes applicables
Statuts de la société et pièces modificatives	30 ans à compter de la date à laquelle l'acte cesse de produire ses effets (dissolution, cessation des relations contractuelles,…)	Article 2262 du Code Civil
Factures clients et fournisseurs	10 ans à compter de la clôture de l'exercice comptable	Article L123-22 du Code de Commerce
Bons de commande, de livraison et de réception	10 ans à compter de la clôture de l'exercice comptable	Article L123-22 du Code de Commerce
Correspondances commerciales (lettres reçues et copies des lettres envoyées)	10 ans	Article L123-22 du Code de Commerce
Contrats commerciaux entre commerçants	10 ans à compter de leur terme	Article L110-4 du Code de Commerce
Contrats entre commerçants et non commerçants	10 ans à compter de leur terme	Article L110-4 du Code de Commerce

Dans ses aspects juridiques, l'archivage est lié à la question de la preuve. En effet, en cas de litige, le but est de pouvoir justifier de certains droits par la conservation d'informations nécessaires jusqu'à expiration des délais prévus.

7.6.2 Archivage électronique de documents

Légalement, le papier est considéré comme un support *« fidèle »* et *« durable »* (cf. article 1348 du Code Civil). Le législateur n'a pas eu besoin de légiférer sur la conservation des archives papiers, car elles ne font pas l'objet de controverses juridiques.

Seules des durées de conservation de certains documents, qu'ils soient papiers ou électroniques, sont définies en fonction de la législation applicable au type de document (code du travail, code du commerce, code fiscal…).
En cas de litige, c'est le titre original papier qui sera ressorti des archives pour être produit à titre de preuve. La certitude qu'un écrit papier demeure intact dans le temps correspond à une notion juridique fondamentale, que l'on retrouve inscrite dans différentes dispositions du Code Civil (cf. article 1348 déjà cité plus haut). En effet, un tel écrit peut traverser les siècles s'il est correctement conservé.
En matière numérique, la qualité d'original ne tient pas, comme en matière d'écrit papier, à une absence de modification du support matériel d'origine, mais plutôt à ce qu'aucune modification ne puisse être apportée à un document sans que l'on puisse en détecter l'origine et la nature. C'est ce qu'établit l'article 1316-1 du Code Civil puisqu'il conditionne la recevabilité d'un écrit électronique au fait *« …qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*. La conservation de ce type de document nécessite donc la mise en place d'infrastructures et de processus dédiés. En particulier, la conservation d'un écrit électronique ne se limite pas à la conservation de l'écrit en lui-même, mais elle inclut aussi tous les éléments à même de garantir les exigences juridiques qu'il remplissait lors de son établissement, à savoir pour l'imputabilité, la validité de la signature électronique, et donc celle du certificat afférent au document signé. Il est par conséquent indispensable que l'OEC qui a fait le choix du numérique mette en place un système d'archivage dédié.
A l'heure actuelle, bien que la problématique de la conservation des documents électroniques se pose, celle-ci n'est pas traitée dans la loi du 13 mars 2000 sur la preuve électronique ni dans la directive européenne 1999/93/CE sur la signature électronique. Il n'existe pas, pour le moment, de loi en France sur l'archivage électronique. Cette situation conduit les organismes souhaitant mettre en place un archivage électronique de leurs documents à s'appuyer sur le cadre de référence que constituent les normes et les guides existants.
En conséquence, plutôt que d'archivage à valeur légale, il est préférable d'utiliser l'expression d'archivage à valeur probante, la finalité de ce dernier étant de pouvoir restituer des informations fidèles permettant d'apporter des éléments de preuve en cas de litige.

7.6.3 Valeur probante de l'archivage électronique

L'archivage électronique à valeur probante est un ensemble de modalités de conservation et de gestion des archives électroniques ayant une valeur juridique lors de leur établissement et jusqu'au terme du délai durant lequel des droits y afférent peuvent exister.
Dans cette optique, il est nécessaire de distinguer très clairement le cas d'un document papier dématérialisé de celui d'un document d'origine électronique. S'agissant du document papier dématérialisé, numérisé en l'occurrence, seul l'original papier aura valeur probante. A contrario, pour un document produit directement sous format électronique, seule la version électronique fera foi. Une impression papier de ce document électronique n'aura, quant à elle, pas de valeur probante. Il appartiendra à l'OEC d'apporter des éléments de nature à emporter la conviction du juge quant à la fidélité de l'impression. Un rapport sur les résultats émis au format papier devra être archivé de préférence tel quel. Un rapport tout électronique, adressé par voie électronique par exemple, aura intérêt à être archivé au format électronique.
Il convient que l'archivage électronique à valeur probante soit en cohérence avec la politique de sécurité des systèmes d'information, le contexte législatif et réglementaire, le standard d'échange de données pour l'archivage. La valeur probante d'un document électronique se traduit par son intégrité, son authenticité, sa lisibilité ou intelligibilité, son accessibilité durant

les délais de conservation définis. L'authenticité et l'intégrité peuvent être assurées en utilisant une signature électronique.
L'accessibilité du document peut être garantie par des logiciels de gestion de documents (de type RSD Folders, Docubase…) au travers de techniques d'indexation et d'horodatage.
La lisibilité peut être apportée par la pérennité des supports, des formats de documents utilisés et l'interopérabilité des différents outils.
Il est admis qu'une archive électronique doit être gérée dynamiquement et considérée comme vivante. En fonction de la durée de conservation des données/documents/enregistrements ; il faut périodiquement prévoir de changer de support, de changer de format, de durcir la signature… Des migrations de support et de format des documents électroniques sont nécessaires tout au long de la durée de conservation définie.
Il convient que la mise en œuvre d'un archivage électronique à valeur probante s'appuie sur un état de l'art normalisé lorsque celui-ci existe.

7.6.3.1 Formats de fichiers normalisés

Le format PDF/A-1 (PDF Archive), basé sur la version 1.4 de PDF a été normalisé par l'Organisation internationale de normalisation pour l'archivage électronique des documents bureautiques statiques. Cette norme ISO 19005-1 a pour objectif d'assurer la conservation à long terme des fichiers archivés au format PDF/A-1. Elle comprend la définition de ce dernier ainsi que la façon de développer un outil de visualisation de fichiers conforme audit format : ceci garantit la possibilité d'accéder à ces fichiers dans le futur. La version 1.7 est la version la plus récente de PDF. Elle sert de base à l'élaboration de la norme ISO 32000, encore au stade de projet à l'heure actuelle.
Le format de document ouvert pour applications de bureau ODF (Open Document Format for Office Applications), basé sur le langage XML 1.0, a également été normalisé par l'Organisation internationale de normalisation. La norme ISO/CEI 26300 vise à garantir l'interopérabilité entre les applications bureautiques et la pérennité des données, c'est-à-dire que ces dernières puissent rester disponibles et utilisables au-delà de la durée de vie du système qui les a générées.
Par ailleurs, l'Organisation internationale de normalisation a approuvé récemment le format de fichier « Office Open XML » utilisé dans la fameuse suite bureautique Office 2007, et lui a conféré le statut de norme internationale sous la référence ISO/CEI DIS 29500.

7.6.3.2 Normalisation et archivage à valeur probante

La norme française NF Z42-013 « *Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes* » fournit des règles concernant les dispositions organisationnelles et techniques à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer la conservation et l'intégrité de ceux-ci. Pour répondre à l'objectif d'intégrité des documents électroniques archivés, la norme préconise d'utiliser des supports non réinscriptibles de type WORM (Write Once Read Many) ou équivalents qui répondent à des spécifications normalisées, telles que décrites dans les normes ISO/CEI 13446 et ISO/CEI 13490 par exemple.

Il apparaît évidemment que mettre en place un archivage électronique sécurisé est une compétence à part entière. Il est indispensable de penser à la question de l'archivage électronique dès la phase de conception des données informatisées.
Afin de conférer une valeur probante à une archive électronique, il est possible de s'appuyer sur la normalisation, ou sur des documents de référence publiés par des organismes de renom. Cette tâche peut être externalisée et confiée à un prestataire de services appelé tiers archiveur qui assure par ailleurs l'indépendance nécessaire.
De plus, pour suivre les technologies et assurer que les migrations de support permettront de garantir l'intégrité des données, il est nécessaire d'assurer une veille juridique et technologique permanente.
Dans le cas où un tiers archiveur est choisi, la rédaction du contrat de prestation est un point critique. Un contrat type de ce genre doit prévoir des clauses de sécurité, d'information ou conseil, de reprise et de continuité, de confidentialité et de respect de l'état de l'art.

8 Gestion des moyens informatiques

La gestion des moyens informatiques vise à la maîtrise des dispositifs techniques informatiques mis en œuvre par l'OEC. Cette gestion couvre un ensemble de domaines permettant d'assurer :

- Le choix, l'acquisition et la mise en service des systèmes informatiques de mesures et de traitements.
- Le maintien en conditions opérationnelles des systèmes informatiques.
- La gestion de la documentation des systèmes informatiques.
- La protection des accès aux moyens et données ainsi que leur conservation.
- L'adaptation permanente des moyens aux évolutions ainsi que la mise en conformité réglementaire des dispositifs.

Les moyens informatiques se distribuent en moyens matériels (ordinateurs, imprimantes, matériels de mesures, réseaux,…) et immatériels (logiciels). Les moyens matériels sont au service des moyens immatériels. Cette distinction est importante en ce sens que la gestion des moyens est souvent concurrente. A titre d'exemple, l'évolution d'un logiciel peut nécessiter le changement de matériel. La gestion des moyens informatiques se distingue selon la typologie des moyens. Elle doit toutefois prendre en compte l'aspect concurrent.

La gestion des moyens informatiques est décrite par un ensemble de processus qui concourent à sa réalisation. Quelle que soit l'étendue du système informatique considéré, chaque processus exposé ci-après contribue à sa gestion. A cet égard, l'exigence de management que pose le chapitre 4 de la norme NF EN ISO/CEI 17025 engage le laboratoire à mettre en place et piloter l'organisation permettant les vérifications appropriées en tous les points des processus notamment relatifs aux moyens informatiques. Plus précisément sont visés aux § 5.4.7, 5.5 et 5.6.1, de la norme, différentes dispositions qui relèvent de la gestion des moyens informatiques. Par ailleurs, l'annexe B de l'ISO 15189 précise différentes dispositions de gestion des moyens informatiques dans le but d'assurer la sécurisation des données et des traitements.

La dématérialisation des mesures, données et rapports sur les résultats pousse à regarder la gestion des moyens informatiques sous l'angle de sa capacité à assurer la pérennité et la disponibilité des données d'une part, la pertinence et l'exactitude des données d'autre part.

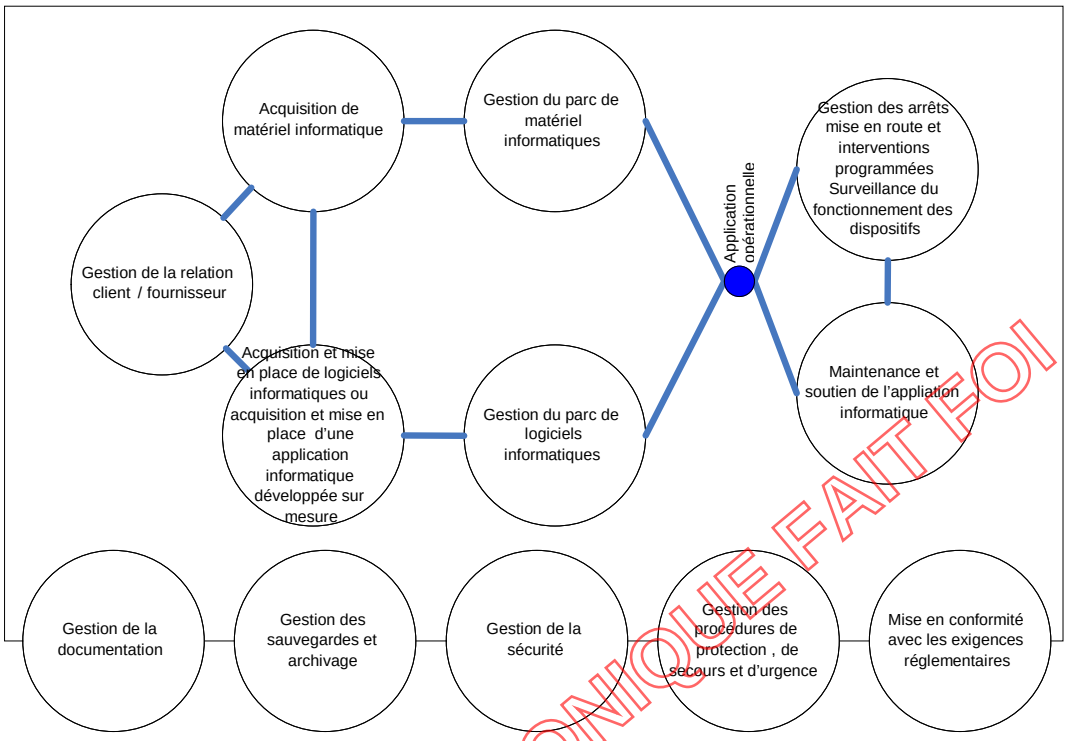
Dans la mise en place des dispositions de management, il appartient à chacun d'apprécier l'importance qu'il doit donner à un processus et donc la pertinence que revêt tel ou tel sous processus dans l'objectif poursuivi de disponibilité, de traçabilité et de sécurisation.

Nous considérons au titre de la gestion des moyens informatiques, les processus suivants :

- L'acquisition de matériels informatiques. Il s'agit des activités recouvrant l'acquisition des moyens de traitements informatiques depuis la définition des besoins jusqu'à l'acquisition des matériels.
- La gestion du parc de matériels informatiques. Ce processus recouvre le suivi de la vie des outils matériels de traitements depuis leur mise en service jusqu'à leur mise au rebus. Bien souvent, ce processus recouvre la maintenance des matériels.
- L'acquisition de logiciels informatiques et la mise en place d'applications informatiques développées ou paramétrées sur mesure.
- La gestion du parc de logiciels informatiques. Ce processus recouvre le suivi de la vie des outils logiciels depuis leur mise en service jusqu'à leur réforme en passant par les différentes étapes du cycle de vie du parc logiciel (notamment la gestion de versions).
- La maintenance et le soutien des applications informatiques (dont étalonnage, vérification périodique). Ce processus recouvre les activités de correction, d'évolution et d'adaptation des applications informatiques ainsi que les activités de support aux utilisateurs.
- La gestion de la documentation (notamment manuel de procédure au sens ISO 15189)
- La gestion des dispositifs en exploitation. Il s'agit ici de gérer les matériels informatiques et logiciels mis en service.
- La gestion des sauvegardes et archivages.
- La gestion de la sécurité (dont sécurité d'accès aux données, matériels et programmes, sécurisation des réseaux et des matériels eux mêmes).
- La gestion des procédures de protection, de secours et d'urgences.
- La mise en conformité avec les exigences réglementaires et obligations contractuelles.

La couverture proposée ici est vaste. Les différents points de la norme ISO/CEI 17025 cités ci-dessus sont couverts. D'autres points sont formulés qui n'apparaissent pas en citation directe de la norme. Ils contribuent, de manière générale, à l'amélioration de la traçabilité et plus globalement aux exigences de management de la qualité que présente la norme.

Le schéma suivant présente les relations entre les principaux processus de la gestion des moyens informatiques



Le tableau suivant en reprend les éléments a l'exception de la relation client / fournisseur qui ne présente pas de spécificité dans le domaine de la gestion des moyens informatiques

Processus	Méthode ou actions de gestion
Acquisition et mise en service de matériels et applications informatiques	**Définition des besoins** : élaboration d'un cahier des charges ou d'une expression de besoin. **Identification des outils** : analyse des offres des fournisseurs. **Choix d'un fournisseur et acquisition** : directement ou par le biais d'un appel d'offres. Attention : l'application informatique peut être l'objet d'un développement ou d'un paramétrage spécifique. Il est alors indispensable de suivre le processus de fabrication de l'application. A ce titre il est recommandé de disposer des différents dossiers appropriés à ce type de démarche notamment dossier de spécifications, dossiers techniques d'architecture, dossier de paramétrage, dossier d'installation, manuel utilisateur. **Installation, étalonnages** (inscription des valeurs dans des documents d'enregistrement appropriés). **Réception technique** : vérification d'aptitude et de bon fonctionnement (consignation des tests opérés, moyens de tests et des résultats obtenus, inscription des matériels, logiciels dotés de leurs versions en inventaire). Formulation de la réception par procès verbal. **Mise en exploitation** : Installation du dispositif étalonné (soit matériel, soit logiciel soit les deux), dans le dispositif global de l'OEC.
Gestion du parc de matériel et applications informatiques	**Consignation du matériel dans un registre inventaire** identifiant la date, le n° affecté ou le n° de référence du matériel. **Consignation de la sortie de matériels pour la maintenance** ou consignation du changement d'une pièce ou d'un ensemble de pièces. **Consignation de la sortie de matériel pour mise au rebus.** La mise au rebus doit être consignée à plusieurs titres : - afin de conserver à jour la liste des immobilisations comptables, - afin d'acquitter de l'écotaxe. Attention, la loi interdit la mise en décharge des matériels informatiques. Ils doivent être recyclés. **Inventaire périodique du parc.** **Mise en place de la gestion des versions** : définition d'une politique de version décrivant les principes retenus pour les versions mineures, les versions majeures. Etablissement du planning des versions prévues. Intégration via les versions des événements subis par l'application (corrections, adaptations,

Processus	Méthode ou actions de gestion
	évolutions,…). **Vérification périodique de bon fonctionnement** : élaboration d'un planning de vérification, mise en place de campagne de vérification, consignation des résultats dans le registre du logiciel en service. **Reforme de l'application par retrait** : consignation de l'opération dans un registre inventaire du logiciel en service identifiant la date, le n° de version.
Maintenance et soutien du dispositif informatique en service (matériels et applications)	**Mise en place du dispositif de maintenance** (maintenance corrective, maintenance évolutive, maintenance préventive, maintenance légale, maintenance adaptative). Il s'agit ici d'exprimer un cahier des charges de la maintenance, une convention de service décrivant les engagements pris par l'entité assurant la maintenance et de mettre en place l'organisation et les moyens qui opéreront la maintenance (par ex. accord avec prestataire, fournisseur de matériel,…) **Mise en place du soutien** (téléphonique, fax ou mél). Le soutien est mis en place selon trois niveaux qui - Niveau un : prise en compte des problèmes techniques simples et connus. - Niveau deux : prise en compte des problèmes de mise en œuvre (ex interprétations de valeurs.) - Niveau trois : accès au fabricant technique pour signalement d'un problème a traiter. Il est important de préciser que la mise en place du soutien nécessite que soient consignés les éléments de réponses aux principales questions que posent les utilisateurs. Ces éléments seront eux mêmes enrichis progressivement des réponses apportées aux nouvelles questions.
Gestion de la documentation	**Gestion du référentiel documentaire** : recensement des documents, classification des documents, validation de l'inscription dans le référentiel, codification éventuelle des documents, copie des documents, rangement des documents et des copies, archivage et réforme des documents.
Surveillance du fonctionnement des dispositifs	**Surveillance du fonctionnement des systèmes** : définition des opérations de surveillance (surveillance des espaces disques, du fonctionnement des dispositifs d'échanges de données, de la durée de fonctionnement de tel ou tel logiciel…), des exigences de fonctionnement (ex : 24/24 – 7/7), du planning d'interventions programmées, des protocoles d'arrêts et de redémarrages programmés. Consignation dans le cahier d'exploitation des événements prévisionnels. Nomination d'un responsable de l'exploitation et de son suppléant. La surveillance des systèmes est fondamentale dès lors que les systèmes sont critiques ou que l'interopérabilité des systèmes est une caractéristique majeure de leur bon fonctionnement. Faute de surveillance, une chaîne peut être bloquée arrêtant tout ou partie de la production de l'OEC.
Gestion des sauvegardes et archivage	**Mise en place et mise en œuvre des sauvegardes.** La mise en place et la mise en œuvre des sauvegardes nécessitent que soient déterminés pour chaque dispositif sauvegardé, la fréquence de sauvegarde, l'acteur de la sauvegarde, les principes de sauvegarde et de restauration. Ces éléments sont consignés dans un cahier approprié de sorte à être exploitables. **Vérification périodique des sauvegardes**. Les sauvegardes doivent être testées de manière a vérifier périodiquement leur capacité a être restaurée. **Mise en archives.** Les sauvegardes sont en générales limitées dans le temps. Au delà d'une certaine durée, les éléments sauvegardés sont versés dans les archives. Il convient lors de la constitution du fond d'archive de bien déterminer les éléments qui y figureront. **Tests des restaurations d'archives.** **Accès aux archives, restaurations.** L'accès au archives est une disposition a prévoir en même temps que la constitution du fond. En général les archives ne sont pas situées au même endroit que les sauvegardes. L'accès est donc un aspect à prendre en compte.
Gestion de la sécurité	**Description de la politique de sécurité** : périmètre technique sécurisé matériels et logiciels, moyens de sécurisation, processus d'inscription et de radiation des autorisations. **Définition et mise en place de procédures de sécurisation** : tests des procédures, publication de la procédure, nomination d'un responsable de la sécurité et de son suppléant **Mise en place et gestion des dispositifs de sécurité :** habilitation des utilisateurs aux outils informatiques, mise à jour des accès, radiation des habilitations, suivi des droits d'accès.
Gestion des procédures de protection, de secours et d'urgence	**Définition et mise en place d'un plan de secours et de reprise d'activité** ainsi que d'un plan de retour (une fois incident clos), Nomination d'un responsable des moyens de secours. Vérification périodique de l'opérabilité du plan de secours. Publication d'une organisation (rôles, responsabilités). Il est important de préciser qu'il existe différents types de plans de secours. Ils se différencient par la criticité du dispositif secouru. A minima on définira un plan de reprise d'activité (PRA) (reprendre l'activité après un arrêt), a maxima, un plan de continuité d'activité (PCA), sera envisagé de sorte a ce que l'activité ne soit pas arrêtée.
Mise en conformité avec les exigences réglementaires	**Déclarations à la CNIL**. **Définition et mise en place d'un processus de demande**, d'instruction des demandes et de publication des réponses. **Inscription dans un registre des demandes instruites** et des réponses apportées.

9 Eléments d'explication concernant la signature électronique

9.1 Contexte réglementaire

Le texte de base en la matière est la directive européenne 1999/93/CE du 13 décembre 1999 qui fixe un cadre communautaire pour les signatures électroniques.
Cette directive a été transposée en droit français par une loi et deux décrets d'application.

9.1.1 La loi n°2000-230 du 13 mars 2000

Cette loi portant sur la preuve en matière de technologies électroniques de l'information a inséré de nouveaux articles dans le code civil qui stipule :

- à l'**article 1316** : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ».

- à l'**article 1316-3** : « L'écrit sur support électronique a la même force probante que l'écrit sur support papier ».

Ces deux articles signifient donc qu'un document sur support électronique et transmis électroniquement constitue une preuve.

La loi prévoit cependant des conditions définies à l'**article 1316-1** : *« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*.
L'émetteur doit donc être identifiable de façon certaine et le support utilisé doit permettre la conservation du document dans son intégralité sans que le contenu n'en soit altéré.

- à l'**article 1316-4** : « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.
Lorsqu'elle est électronique, la signature consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque, dans des conditions fixées par décret en Conseil d'Etat :
- la signature électronique est créée,
- l'identité du signataire assurée,
- l'intégrité de l'acte garantie ».

Un procédé de signature électronique peut donc bénéficier d'une présomption de fiabilité s'il satisfait aux exigences ci-dessus.

La signature électronique doit permettre d'identifier de façon fiable la personne dont elle émane.

- à l'**article 1316-2** : « Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. ».

C'est-à-dire que le juge se base sur la loi ou sur une convention (aussi appelée convention de preuve) établie entre les parties.

9.1.2 Le décret n°2001-272 du 30 mars 2001

L'article 1316-4 de la loi du 13 mars 2000 est complété par le décret n°2001-272 du 30 mars 2001 relatif à la mise en place d'une signature sécurisée. Ce texte définit ainsi la signature électronique :

« Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase de l'article 1316-4 du code civil. »

« Signature électronique sécurisée : une signature qui satisfait, en outre, aux exigences suivantes :
- être propre au signataire,
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif,
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ».

Le décret du 30 mars 2001 fixe également, à l'article 2, les conditions dans lesquelles une présomption de fiabilité doit être attachée au procédé utilisé dans le cas de signatures sécurisées :

« La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque :
- ce procédé met en œuvre une signature électronique sécurisée (voir plus haut),
- [cette signature est] établie grâce à un dispositif sécurisé de création de signature électronique et que
- la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié ».

9.1.3 Le décret n°2002-535 du 18 avril 2002

Les notions de dispositif sécurisé de création de signature électronique et d'utilisation d'un certificat électronique qualifié sont définies aux articles 3 à 9 du décret n°2001-272 du 30 mars 2001 complété par le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes de la technologie de l'information.

9.1.4 L'arrêté du 31 mai 2002

Ce texte traite de l'organisation du schéma national volontaire de reconnaissance de la qualification des prestataires.
Les certificats qualifiés délivrés par des prestataires certifiés dans le cadre de ce schéma sont présumés remplir les conditions énoncées à l'article 6 du décret du 30 mars 2001 - ce schéma vise donc à développer la confiance.
Il traite aussi de la responsabilité des prestataires de services de certification électronique (PSCE).
En attente de précisions du droit relatif aux relations entre les prestataires délivrant des certificats qualifiés et ceux qui se fient à de tels certificats, les premiers peuvent être présumés responsables (transposition de l'article 6 de la directive 1999/93/CE) sauf dans certains cas d'imprudence de la part de la personne qui se fie au certificat.

9.1.5 L'arrêté du 26 juillet 2004

Ce texte est relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
L'évaluation des prestataires de certification électronique est réalisée par des organismes indépendants, eux-mêmes accrédités par le Cofrac, sur la base de critères comme les ressources cryptographiques utilisées, les procédures d'audit interne, la gestion des secrets et la politique de sécurité des prestataires de certification électronique.

9.1.6 L'ordonnance 2005-674 du 16 juin 2005

Ce texte modifie les articles 1369-1 à 1369-11 du Code Civil.
L'article 1369-2 permet de transmettre par courrier électronique les éléments relatifs à l'exécution d'un contrat si le destinataire accepte l'usage de ce moyen.
L'article 1369-8 concerne la transmission par voie électronique de courriers recommandés avec accusé de réception. Le procédé utilisé doit permettre « *d'identifier le tiers, de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si la lettre a été remise ou non au destinataire* ». Ces informations sont présumées fiables si le procédé satisfait à des exigences fixées par un décret en Conseil d'Etat (non paru à la date de publication du présent guide).

9.2 Signature électronique et signature électronique présumée fiable

9.2.1 Signature électronique

Dans un premier temps, il est important de souligner que la signature électronique, au sens de la directive européenne et des textes réglementaires français n'est pas la numérisation (« scannerisation ») d'une signature manuscrite.
En effet, la pratique qui consiste à numériser des signatures manuscrites pour insérer dans un document des images de cette signature ne répond pas à la définition et aux exigences des textes réglementaires sur la signature électronique.

La signature électronique est un moyen d'authentifier un document en garantissant à la fois l'identité du signataire et l'intégrité du document transmis.
Elle est propre au signataire, est créée par des moyens que le signataire puisse garder sous son contrôle exclusif et garantit avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

Une signature électronique utilise un certificat électronique de type ICP (infrastructure de clés publiques) ou, en anglais, PKI (Public Key Infrastructures).
Un certificat est un ensemble de deux clés (publique et privée) propriété du signataire.

Ce certificat repose sur deux principes :

- un principe technique selon lequel un certificat est mis en œuvre à l'aide d'un dispositif de création de signature électronique (au moyen de clés de cryptage),
- un principe organisationnel selon lequel le lien entre l'identité du signataire, le certificat électronique et sa période de validité est garanti par une autorité de confiance qui, en quelque sorte, joue le rôle de notaire.

Un dispositif de création de signature électronique peut être uniquement logiciel ou intégrer un dispositif matériel.
Il peut s'agir :

- d'une carte à puce (avec ou sans code secret),
- d'un dispositif de reconnaissance biométrique (empreinte digitale, de l'œil, de la voix,…),
- d'un appareil d'enregistrement de la « dynamique » de la signature manuscrite,
- d'un logiciel installé sur un ordinateur.

Ce dispositif protège la clé secrète, permet sa mise en œuvre par le seul utilisateur légitime sans qu'il soit possible de la falsifier et sans qu'il soit possible d'altérer le message.

Il existe trois modes (combinables) d'identification du signataire par le dispositif de création de signature électronique :

- par code secret (PIN : Personnal Identification Number),
- par caractéristique biométrique (empreinte digitale,…),
- par objet personnel (carte à puce,…).

Un module d'autoformation à la signature numérique est accessible sur le site de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) à l'URL suivante : http://www.formation.ssi.gouv.fr/autoformation/signature.html.

9.2.2 Signature électronique présumée fiable

L'autorité de confiance délivrant le certificat peut être l'organisme d'appartenance du signataire ou un organisme tiers appelé tiers de confiance ou PSCE (prestataire de services de certification électronique).
Cet organisme peut être qualifié, au sens de la réglementation française. Il délivre alors des certificats qualifiés.
La qualification de ces organismes est évaluée par des organismes de certification indépendants accrédités par le Cofrac.

Si la signature électronique s'appuie sur un certificat qualifié comprenant un dispositif de création de la signature certifié, il s'agit alors d'un procédé présumé fiable, sans exigence de démonstration complémentaire.

La signature électronique est définie comme signature électronique « simple » dans les autres cas.
Cependant, un procédé de signature électronique « simple » n'est pas pour autant sans valeur juridique. Toutefois, dans ce cas, en cas de contestation, c'est à l'utilisateur de ce procédé de signature électronique qu'il revient d'apporter la preuve de sa fiabilité ou de lui donner, en amont, force probante en vertu de la signature d'une convention sur la preuve.

9.3 Références bibliographiques relatives à la signature électronique

Le présent chapitre fait référence ou s'appuie sur les documents et textes de références suivants :

- Directive européenne 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
- Loi n° 2000-230 du 13 mars 2000 portant sur la preuve en matière de technologies électroniques de l'information.
- Décret n° 2001-272 du 30 mars 2001 relatif à la mise en place d'une signature sécurisée.
- Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes de la technologie de l'information.
- Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.
- Arrêté du 28 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
- Ordonnance 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique.

Une liste de sites Internet relatifs à cette thématique est consultable sur www.ssi.gouv.fr.