international council on archives
conseil international des archives

Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique

Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique

AVANT-PROPOS

A LA TRADUCTION FRANÇAISE

Publié par le Conseil international des Archives. Ce module a été élaboré par une équipe mixte constituée de membres du Conseil international des Archives et de *l'Australasian Digital Recordkeeping Initiative.*La traduction française a été assurée par un groupe de jeunes professionnels français en 2010.

ISBN : 978-2-918004-00-4

En 2008, étaient présentés lors du congrès international des Archives tenu à Kuala Lumpur (Malaisie), les trois modules *des Principles and functional requirements for records in electronic office environments*, élaborés sous l'égide des Archives nationales d'Australie par un groupe de travail international, et publié sous les auspices du Conseil international des Archives (ICA).

La portée et la pertinence de ce texte ont contribué à attirer l'attention des professionnels de différentes régions du monde, et il est très vite apparu que des traductions s'imposaient, à commencer par celle en français, seconde langue de travail de l'ICA. Proposé par les Archives nationales d'Australie elles-mêmes, le projet de traduction en français a été organisé par le Secrétariat de l'ICA selon une procédure et une méthodologie ajustées à la nature et au contenu du texte. Un texte normatif tout d'abord, ou tout au moins énonçant des principes et des lignes directrices au niveau international, et par là, pouvant/devant être lu par n'importe quel professionnel dans le monde. En second lieu, un texte portant sur des aspects de l'exercice de la profession et des concepts plus ou moins bien connus, maîtrisés, développés, voire pris en compte dans un certain nombre de cultures ou de contextes professionnels. Enfin, il s'agissait d'assurer un contrôle de la qualité de la traduction, tant du point de vue de la langue que du respect des concepts et principes énoncés. Dès lors, cet exercice devenait un vrai défi.

Ce défi a été relevé non pas par un traducteur, mais par toute une équipe, composée de professionnels de l'archivage ayant à la fois une excellente maîtrise de la langue anglaise, et une bonne connaissance, par une approche pratique intelligente, des concepts présentés par la norme. Ce choix a permis de répondre au souci de produire un texte clair, écrit dans une langue compréhensible par les professionnels francophones. Par ailleurs, la sélection des membres de l'équipe a assuré une représentation large des différents environnements professionnels : secteur public, secteur privé ; administrations centrales de l'Etat, administrations territoriales ; institutions de conservation des archives ; entreprises, petites et grandes, nationales et multinationales. La coordination scientifique du projet a été confiée à Marie-Anne Chabin (Archive 17), consultante, experte à la fois pour le contenu et la traduction (elle est la traductrice en français, entre

autres, de la norme européenne MoReq, versions 1 et 2), et également enseignante au CNAM (Centre national des Arts et Métiers). Le Conseil international des Archives tient tout particulièrement à remercier, pour leur implication dans le projet à titre bénévole, les jeunes collègues qui ont répondu à l'appel lancé par le secrétariat de l'ICA:

Huguette BESSARD, Sanofi-Aventis
Alix CHARPENTIER, Archives départementales de la Haute-Marne
Alice CHATEAU, Ministère de l'Intérieur
Nathalie JUBIN, Debevoise & Plimpton
Isabelle LAKOMY, Archives départementales de l'Aisne
Nathalie MEVEL, Cour des Comptes
Vincent MOLLET, Service historique de la Défense
Myriam PAUILLAC, Anaphore
Clothilde ROULLIER, Archives nationales
Vanessa SZOLLOSI, Archives nationales
Fabrice YON, Stocomest.

La principale qualité de cette équipe est d'être composée de praticiens. On ne saurait trop souligner l'importance de cet aspect dans la conception, mais aussi la traduction d'une norme professionnelle, celle-ci étant – et c'est une évidence qu'on aurait parfois tendance à oublier – destinée à guider des professionnels dans leur travail quotidien. Ceci nous a permis d'opérer parfois plus facilement des choix délicats, en remplaçant le réflexe du dictionnaire par la question : « Quel est le mot/l'expression qui correspond le mieux à ce concept/pratique dans ma vie professionnelle ? Quel mot vais-je naturellement employer pour parler à mes interlocuteurs dans l'institution ou l'entreprise pour évoquer cet aspect des procédures, du traitement, des outils utilisés? Quels mots les utilisateurs vont-ils eux-mêmes utiliser plus volontiers ? ». L'identification et la compréhension des concepts évoqués dans le texte anglais, leur mise en relation avec une pratique existante, et leur « traduction » dans une langue simple et compréhensible par le commun des professionnels devenait ainsi plus aisée.

C'est ainsi que nous avons surmonté les débats sans fin autour de la traduction réputée difficile, sinon impossible, de concepts qui n'existeraient pas dans certaines cultures (dont la française, pour ne pas la citer). Comment traduire « records » ? « Records management » ? Comment prendre en compte le mot « business » accolé à nombre d'autres termes dans le texte anglais ? Est-on obligé de traduire toujours le même mot anglais par le même mot dans la langue de destination ? Il nous est apparu que non. Par exemple, il serait bien difficile d'imposer une traduction unique pour « records », tout au

moins dans ce texte, sans s'exposer à des faux sens, pour ne pas dire des non-sens. C'est ainsi que dans le seul module 1, au moins cinq traductions différentes ont été utilisées pour « records », sans dénaturer le sens du texte anglais et avec un résultat clair et intelligible pour le professionnel francophone.

Enfin le parti a été pris d'aller toujours vers la simplicité de la langue et de tendre vers l'épure. Le choix de supprimer des termes voire des expressions n'ajoutant pas de sens véritable au texte français a certes été pesé, mais on aboutit, là aussi, à plus de clarté dans le propos.

Il n'est pas inutile de préciser l'organisation du travail au sein de l'équipe : le texte ayant été découpé en courts extraits, chaque traducteur s'est vu confier environ une trentaine d'extraits pris dans les trois modules ; chacun était en outre chargé de revoir, en deux niveaux de relecture, les extraits traduits par ses co-équipiers. La coordination des opérations a été réalisée par Alice Chateau. Enfin, trois relectures finales du texte consolidé ont été effectuées par Marie-Anne Chabin, Alice Chateau, et Christine Martinez (secrétariat de l'ICA). Cette méthode de travail a permis, au cours des différentes réunions qui ont jalonné le projet, de débattre collectivement et d'opérer les choix les plus consensuels possibles pour une équipe riche de réalités professionnelles variées, exploitant les tendances et les évolutions de langue observées quotidiennement par les traducteurs dans leurs relations avec leurs interlocuteurs, clients, usagers, producteurs d'information.

Nous espérons avoir atteint l'objectif, et que vous aurez sinon du plaisir, tout du moins de l'intérêt à lire ce texte. D'autres communautés linguistiques ont entrepris de suivre ces pas, notamment nos collègues chinois et hispanophones, dont les expériences de traductions apporteront certainement beaucoup à cette réflexion sur la question délicate de la traduction des normes internationales.

Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique

Module 1

Contexte et déclaration de principes

Publié par le Conseil international des Archives. Ce module a été élaboré par une équipe mixte constituée de membres du Conseil international des Archives et de *l'Australasian Digital Recordkeeping Initiative.*

ISBN : 978-2-918004-00-4

SOMMAIRE

1. INTRODUCTION 4
1.1 Champ d'application et objectifs 4
1.2 Publics cibles 5
1.3 Autres normes du domaine 6
1.4 Structure et utilisation 6

2. BONNES PRATIQUES : L'ARCHIVAGE ELECTRONIQUE ET LE ROLE DES LOGICIELS 7

3. PRINCIPES DIRECTEURS 8
3.1 Principes liés aux documents 8
3.2 Principes liés aux systèmes 9

4. MISE EN ŒUVRE 10
4.1 Les clés d'une gestion réussie de l'information métier sous forme électronique 10
4.2 Maîtrise des risques 12
4.3 Aspects financiers et organisationnels de la maintenance des systèmes électroniques 14

5. LISTE CRITIQUE DES AUTRES EXIGENCES FONCTIONNELLES 16

6. GLOSSAIRE 19

1. INTRODUCTION

Diverses spécifications fonctionnelles pour les logiciels d'archivage électronique ont déjà été développées au sein de la communauté internationale. En 2006, le Conseil International des Archives a approuvé un projet global d'harmonisation des exigences fonctionnelles pour les logiciels, basé sur les spécifications des différents pays, en cohérence avec la norme internationale sur le records management, ISO 15489. Puisse cette série de recommandations et d'exigences aider les pays qui veulent développer ou adopter leurs propres spécifications fonctionnelles, mais aussi influencer la mise à jour et la révision des normes existantes. L'application de cette série d'exigences fonctionnelles ne vise pas seulement à influencer le développement de logiciels d'archivage électronique mais aussi à favoriser l'introduction de fonctionnalités d'archivage dans les systèmes d'information métier, tant génériques que spécifiques. Ces spécifications peuvent aussi être utilisées dans le secteur privé (par exemples, les groupes internationaux) comme un outil indépendant.

Le projet "Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique" a été parrainé par le Conseil International des Archives dans le cadre de l'axe prioritaire "Archives électroniques et informatisation" conduit par George Mackenzie, Directeur des Archives nationales d'Ecosse. Adrian Cunningham (Archives nationales d'Australie) a été le Coordinateur du projet. Les Archives de Nouvelle-Zélande (Stephen Clarke) ont tenu le secrétariat du projet. Les autres pays participants sont : les îles Caïmanes (Sonya Sherman), le Royaume-Uni– Angleterre et Pays de Galles (Richard Blake), l'Allemagne (Andrea Hänger et Frank Bischoff), la Malaisie (Mahfuzah Yusuf et Azimah Mohd Ali), les Pays-Bas (Hans Hofman), l'Écosse (Rob Mildren et Steve Bordwell), l'Afrique du Sud (Louisa Venter), la Suède (Göran Kristiansson), la France (Olivier de Solan) et les États-Unis (Mark Giguere). Le projet a également été soutenu par l'Australasian digital recordkeeping initiative (Initiative d'archivage électronique d'Australasie), un projet commun parrainé par le Council of Australasian Archives and Records Authorities (Conseil des Archives d'Australasie). Les Archives de l'Etat du Queensland (Rowena Loo et Anna Morris) ont contribué en tant que membres de l'ADRI à la rédaction du Module 3.

1.1 Champ d'application et objectifs

Le but du projet "Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique" est de produire des principes et des exigences fonctionnelles pour les logiciels dédiés à la production et à la gestion des documents archivés électroniquement. Il existe déjà des exigences fonctionnelles et des spécifications techniques dans un certain nombre de pays. L'objectif du projet est de synthétiser les travaux existants pour en faire un guide global qui réponde aux besoins de la communauté archivistique internationale et l'aide à avoir une position consolidée face à l'industrie du logiciel.

Les objectifs du projet sont :

- améliorer l'archivage dans les entreprises/organismes quels que soient leur niveau et leur statut juridique ;
- faciliter l'exécution du travail quotidien en y apportant une plus grande efficacité ;
- renforcer, au travers du déploiement de fonctionnalités d'archivage automatisées, la capacité à répondre aux audits ;
- améliorer la capacité de se conformer aux obligations réglementaires et législatives dans le domaine de l'information (par exemple pour la protection des données et de la vie privée) ;
- assurer une bonne gouvernance (par exemple : responsabilité, transparence et meilleure qualité de service) grâce à un bon archivage ;
- accroître la connaissance générale des possibilités de l'archivage automatisé en diffusant les principes clés; et
- renforcer la cohérence des exigences fonctionnelles d'archivage indépendamment du cadre réglementaire de tel ou tel pays et permettre à l'ensemble de la communauté archivistique de parler d'une seule voix à la communauté des éditeurs de logiciels.

Cette série de recommandations et d'exigences porte avant tout sur la production et la gestion des documents archivés électroniquement. Le processus de pérennisation des documents numériques proprement dit dépasse le cadre du projet même si celui-ci est abordé dans les modules. On suppose que l'application de ces exigences sera globale. C'est pourquoi il est impossible, compte tenu de l'éventail des applications potentielles, d'inclure ici des recommandations détaillées de mise en œuvre. De plus, dans la mesure où l'environnement des tests pour ces modules n'est pas encore défini, on a considéré que des tests spécifiques pour des logiciels dépassaient le cadre des modules.

1.2 Publics cibles

Il existe quatre publics cibles pour ces modules :

- les développeurs et vendeurs de logiciels, et pas seulement d'archivage, dans la mesure où ce document peut être utilisé comme un référentiel commun pour la conformité de l'archivage ;
- les organismes chargés d'établir des normes réglementaires et techniques car ces modules peuvent servir aussi bien de base pour le développement de nouvelles normes, que de référentiel d'évaluation pour les normes existantes sur l'archivage électronique ;
- les organismes gouvernementaux car toutes les fonctions peuvent être confrontées à l'archivage et se prêter à l'incorporation de fonctionnalités automatisées ; et
- les organismes du secteur privé qui peuvent introduire des fonctions d'archivage électronique automatisées dans leurs processus.

1.3 Autres normes du domaine

Les exigences présentées ici respectent les principes de la norme ISO 15489 – Information et documentation – Records management – Partie 1 – généralités, qui définit les exigences d'archivage, applicables également à l'électronique (capture et gestion dans un système d'archivage électronique).

La norme de métadonnées correspondante est ISO 23081 – 1: 2006, Information and Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles. Le jeu de métadonnées essentielles fourni par ISO 23081 – 2: 2007, Information and Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues est à la base de ces exigences.

Ces exigences sont fondamentales, primordiales et génériques pour l'archivage. Pour plus d'informations sur les fonctionnalités logicielles qui ne sont pas détaillées ici, on se reportera aux spécifications détaillées que sont DoD5015.2 ou MoReq2. Enfin, il conviendra de prendre en compte les autres normes, recommandations et spécifications d'ordre national ou local.

1.4 Structure et utilisation

L'ensemble des recommandations et des exigences fonctionnelles est organisé en trois modules :

- *Module 1 : Contexte et déclaration de principes* : contexte, organisation, principes fondamentaux et autres éléments contextuels ;
- *Module 2 : Recommandations et exigences fonctionnelles pour les systèmes d'archivage électronique* : une déclaration générale de haut niveau sur les exigences essentielles et optionnelles, comprenant des recommandations et une check-list de conformité ; et
- *Module 3 : Recommandations et exigences fonctionnelles pour l'archivage des documents dans les applications métier* : lignes directrices et exigences principales et optionnelles pour l'archivage dans les applications métier..

Le Module 2 s'adresse aux organismes qui envisagent de mettre en œuvre des systèmes d'archivage électronique. Il doit être lu conjointement avec le Module 1.

Le Module 3 s'adresse aux organismes qui souhaitent intégrer la fonction « archivage » dans des applications métier. Il doit être lu conjointement avec le Module 1.

Divers scénarios, compatibles entre eux, sont présentés ci-dessous pour illustrer comment ces modules peuvent être utilisés pour :

- Évaluer la fonction archivage dans les logiciels existants : un(e) entreprise/organisme peut utiliser ces modules comme check-list afin d'établir si les fonctionnalités d'archivage nécessaires et souhaitables sont présentes dans un outil non dédié à l'archivage.
- Intégrer un outil d'archivage électronique dans une application métier :

un(e) entreprise/organisme peut utiliser le Module 3 pour sélectionner les fonctionnalités d'archivage à intégrer dans les applications métier existantes.

- Utiliser des spécifications pour le développement de logiciels « maison » : le service informatique d'un(e) entreprise/organisme peut s'appuyer sur le Module 3 pendant les phases de conception et de test de la documentation d'un logiciel.
- Évaluer le logiciel dont on envisage l'achat : un(e) entreprise/organisme qui envisage l'acquisition d'un outil d'archivage électronique peut s'appuyer sur le Module 2 pour évaluer et comparer les fonctionnalités des logiciels d'archivage disponible sur le marché.
- Acquérir, déployer et configurer un outil d'archivage électronique : on peut utiliser le Module 2 pour établir les principes de base en termes d'exigences fonctionnelles pour une consultation du marché sur l'offre et la mise en œuvre d'un logiciel d'archivage électronique. Les exigences présentées dans ces modules pourront éventuellement être adaptées aux besoins de l'entreprise/organisme.
- Concevoir / re-concevoir des logiciels durant leur phase d'optimisation : les développeurs peuvent utiliser les Modules 2 et/ou 3 comme check-list des fonctionnalités qui seraient à réexaminer et/ou incluses dans les mises à jour de logiciels (dédiés à l'archivage électronique ou non).
- Développer des spécifications et des normes au plan national ou régional : un(e) entreprise/organisme peut s'appuyer sur ces trois modules à la fois pour établir ses propres spécifications d'archivage électronique, ou comme point de comparaison pour réviser les normes locales en la matière. D'autres exigences d'ordre national ou régional peuvent être ajoutées à celles qui sont présentées ici.

2. BONNES PRATIQUES : L'ARCHIVAGE ELECTRONIQUE ET LE ROLE DES LOGICIELS

Lorsque les entreprises/organismes introduisent de nouvelles technologies et de nouvelles méthodes de travail, il arrive que les anciennes méthodes et procédures d'archivage perdent en efficacité. Bien souvent, les documents engageants (à archiver) sont conservés dans des bases de données centralisées ou dans des répertoires partagés. D'autres fois, et l'un n'exclut pas l'autre, ils sont disséminés et stockés sur les disques durs locaux des collaborateurs. Pour compliquer les choses, dans tous les cas de figure, l'information stockée va bien au-delà des seuls documents engageants.

Dans bien des cas, les mesures de contrôle de l'intégrité et de l'authenticité sont ignorées et les documents électroniques archivés se retrouvent inaccessibles,

incompréhensibles et inexploitables pour l'entreprise/organisme ou pour l'institution archivistique.

Ceux qui s'appuient déjà sur des documents électroniques pour conduire et tracer leur activité, ou qui souhaiteraient supprimer les dossiers papier de leur système, recherchent des solutions aux questions d'authenticité, de gestion et de conservation des documents électroniques. Les décisions prises aujourd'hui concernant la capacité des systèmes d'information, l'organisation et la structure des ressources, et les politiques ou pratiques d'archivage dans l'environnement électronique vont avoir un impact significatif sur les stratégies et les méthodes que les institutions archivistiques déploieront pour garantir la pérennisation des documents qui présentent une valeur archivistique.

La gestion archivistique étant très proche, plus encore dans l'environnement électronique, de la conception des systèmes d'information et de l'élaboration de nouvelles politiques, les archivistes ont été conduits à analyser plus largement les problématiques d'archivage afin d'adapter les missions archivistiques à l'environnement électronique. Les logiciels fournissent aux administrateurs d'applications, aux responsables de l'archivage et aux archivistes d'importants moyens de pratiquer un bon archivage électronique.

3. PRINCIPES DIRECTEURS

Les entreprises/organismes qui réussissent ont besoin de systèmes d'information pour produire, conserver et utiliser, sous la forme de documents, la trace incontestable de leur activité, afin de répondre à leurs besoins et aux obligations légales. Dans l'environnement électronique, le développement et la mise en œuvre de ces systèmes devrait être guidés à la fois par les besoins métier et inspirés par les principes ci-après.

3.1 Principes liés aux documents

1. **L'information métier sous forme électronique doit être organisée et gérée de manière à constituer une trace fiable et probante de l'activité.**
   Les processus métier étant de plus en plus automatisés, l'information électronique qu'ils produisent peut se trouver être la seule preuve de certaines opérations ou décisions. Les besoins opérationnels et les exigences de responsabilité imposent donc de maintenir cette preuve en figeant et en archivant ces informations. Ce qui implique d'identifier les données électroniques qui constitueront les documents à archiver.
2. **L'information métier doit être reliée à son contexte au travers de métadonnées.**
   Pour que ces données puissent jouer le rôle de trace probante, il est nécessaire de les compléter avec d'autres données (les métadonnées) qui les replacent dans les contextes métier et informatique dans lesquels elles ont été créées.

Pour une application métier avec une production de type sériel, le contexte sera extrait du système et de sa documentation. Dans les autres cas, l'information contextuelle sera attachée à chaque document archivé afin de garantir l'interprétabilité du document dans le temps et d'optimiser sa valeur et son utilité comme trace probante de l'activité métier.

3. **L'information métier doit être conservée et rester accessible aux utilisateurs autorisés aussi longtemps que nécessaire.**
   La conception et la mise en œuvre des logiciels doivent garantir la recherche, le repérage et la restitution des documents engageants archivés dans des formats et des supports lisibles pendant la durée requise par les besoins métier et les exigences réglementaires. Dans ce contexte, les entreprises/organismes s'efforceront d'éviter un mauvais usage des technologies de gestion des droits numériques et de chiffrement.

4. **L'information métier doit pouvoir être détruite d'une manière organisée, systématique et auditable.**
   Un archivage pertinent se caractérise par une conservation et une destruction des documents issus des processus métier en fonction de règles prédéfinies. Les systèmes doivent pouvoir détruire les documents archivés selon un procédé systématique, tracé et auditable, en cohérence avec les besoins opérationnels et les obligations réglementaires.

3.2 Principes liés aux systèmes

5. **Tout système devrait intégrer la bonne gestion de l'information métier comme une brique du processus métier.**
   Bien que cela ne fasse pas l'unanimité, les bonnes pratiques archivistiques font partie intégrante des processus métier. L'automatisation d'un processus métier devrait toujours conduire à évaluer l'opportunité d'intégrer un logiciel d'archivage

6. **Les systèmes de capture et de gestion de l'information métier doivent s'appuyer sur des métadonnées normalisées[1] comme partie intégrante, active et dynamique du processus d'archivage.**
   Les solutions d'archivage offrent d'immenses capacités d'accès. A différentes étapes du cycle de vie du document, elles relient des informations contextuelles standardisées au contenu des documents grâce à des vocabulaires et des taxonomies contrôlés.

7 **Les systèmes doivent assurer une interopérabilité pérenne entre plateformes et domaines d'activités.**
   La valeur de preuve des documents électroniques est soumise à des exigences opérationnelles ou juridiques qui peuvent dépasser la durée de vie des matériels et logiciels ayant servi à sa production. C'est pourquoi, l'information archivée doit pouvoir être présentée de manière compréhensible et modifiable en cas de migration technologique.

---

1 « Normalisées » peut renvoyer à un schéma de métadonnées validé en interne ou à l'adoption/adaptation d'une norme réglementaire, nationale ou internationale, relative aux métadonnées.

8 Les systèmes doivent reposer autant que possible sur des standards ouverts et une neutralité technologique.
Bon nombre de logiciels générant ou gérant des documents à archiver sont développés avec des outils propriétaires. Cette dépendance matérielle et logicielle peuvent avoir des effets négatifs sur l'accès et la conservation des documents à long terme. L'utilisation des standards ouverts est une réponse à cette dépendance technologique.

9 Les systèmes devraient permettre des imports et des exports de masse en utilisant des formats ouverts.
Les documents électroniques engageants (ou à archiver) issus d'un processus et gérés par des logiciels d'archivage peuvent rester dépendants des logiciels et matériels. Idéalement les logiciels d'archivage devraient pallier ces contraintes par des procédures globales d'import ou d'export des données ou, au minimum, par un encodage non-propriétaire des métadonnées.

10 Les systèmes doivent maintenir l'information métier dans un environnement sécurisé.
Pour des raisons de sécurité, les systèmes d'automatisation de processus sont souvent dotés de sauvegardes qui limitent les actions d'utilisateurs sur les documents (par exemple, consultation, impression, publication, copie ou envoi). Les systèmes doivent interdire les modifications non autorisées sur des documents archivés (y compris les métadonnées) et tracer les modifications effectuées.

11 Les métadonnées devraient être principalement générées par le système.
Les utilisateurs sont souvent peu enclins à interrompre le déroulement de leur travail plus de trois fois lorsqu'ils exécutent des tâches annexes à leur activité principale. Attendre de l'utilisateur final qu'il renseigne les métadonnées peut s'avérer irréaliste et/ou inutile. Les systèmes devraient être conçus et mis en place de manière à renseigner automatiquement les métadonnées d'archivage.

12 La validation et la capture des documents traçant les activités devraient être aussi simples que possible pour les utilisateurs.
Il est nécessaire de concevoir des systèmes/logiciels d'archivage de telle sorte qu'ils rendent l'archivage largement transparent pour les utilisateurs finaux.

4. MISE EN ŒUVRE

4.1 Les clés d'une gestion réussie de l'information métier sous forme électronique

Un logiciel performant ne constitue qu'un des éléments d'un bon système d'information. Les autres éléments sont :

- **Principes directeurs d'une politique :** parallèlement au déploiement d'un logiciel d'archivage, il est nécessaire d'analyser les politiques de gestion de l'information et de sécurité existantes et la législation pour identifier les

lacunes à combler dans les fonctionnalités du logiciel. Ceci inclut l'identification des responsabilités de différents profils de collaborateurs pour la conservation et la destruction des documents engageants. Des outils tels que des plans de classement et des modèles de métadonnées peuvent être associés à la politique pour créer un cadre fondateur à un bon logiciel de gestion de l'information à archiver.

- **Analyse des processus métier :** Il est souhaitable de mener une analyse des processus avant tout déploiement technologique. Cette démarche inclut l'identification, l'articulation et potentiellement la réattribution des rôles et des responsabilités.
- **Gestion de projet** : tout déploiement de technologies de l'information nécessite une planification minutieuse et contrôlée des diverses étapes. Les techniques de gestion de projet sont des outils puissants pour une maîtrise du temps et des coûts de ce type de projet.
- **Conduite du changement :** l'automatisation des tâches dans un(e) entreprise/organisme change non seulement le mode de réalisation des processus métier mais aussi les rôles et responsabilités des utilisateurs du système. Des précautions doivent être prises pour bien préparer les utilisateurs aux changements engendrés par tout nouveau déploiement technologique. Les échecs dans ce domaine sont souvent davantage imputables à des lacunes dans la conduite du changement qu'à des erreurs technologiques.
- **Gestion du risque :** comme pour tout déploiement de systèmes d'information, la décision d'automatiser l'archivage devrait faire l'objet d'une analyse de risques avec des solutions alternatives incluses dans le dossier du projet. L'évaluation des risques liés au déploiement devrait être prise en compte dans la gestion globale des risques de l'entreprise/organisme.
- **Maintenance :** Le développement et la maintenance des systèmes informatisés couvrent plusieurs cycles budgétaires. Lors de l'automatisation du système d'archivage, il est important de prendre en compte, comme partie intégrante du projet d'informatisation, les coûts d'exploitation et de maintenance du système, si l'on veut assurer sa viabilité.
- **Développement des compétences :** l'automatisation exige d'étendre ou d'améliorer les compétences techniques des équipes directement concernées mais aussi d'autres personnes peu familières des technologies. Il est important de développer ces nouvelles compétences, individuelles et collectives, pour accompagner et maintenir les efforts d'informatisation.
- **Gestion de la qualité :** la mise en œuvre de solutions automatisées exige de développer des facultés d'évaluation et d'acceptation de performances de logiciels selon une liste de critères, sans oublier de mesurer l'impact du déploiement des logiciels sur les processus métier.
- **Configuration :** il ne suffit pas de s'assurer que le logiciel possède les fonctionnalités d'archivage nécessaires ; il faut également que celles-ci soient

configurées correctement et d'une manière qui permette d'opérer convenablement dans l'infrastructure technologique de l'entreprise/organisme.

- **Culture d'entreprise :** il est capital que la culture d'entreprise souligne la valeur et l'importance d'un bon archivage et que cela devienne la norme pour tous les collaborateurs. Ces exigences doivent être régulièrement exprimées par la direction générale par les différents canaux à sa disposition.

4.2 Maîtrise des risques[2]

Les risques habituellement associés aux déploiements de logiciels d'archivage peuvent se classer en plusieurs catégories :

- **La sélection de logiciels** : il s'agit à partir d'une variété de produits du marché, de décider du produit le mieux adapté à un déploiement dans un(e) entreprise/organisme.
- **Le développement de logiciels** : les problèmes de dépendance vis-à-vis d'éditeurs ou de développeurs de logiciels peuvent se manifester par des retards de livraison ou par une incapacité du fournisseur à diagnostiquer ou résoudre les bugs.
- **Compatibilité technique** : on rencontre des difficultés lors de l'intégration d'un logiciel d'archivage dans l'infrastructure informatique de l'organisation.
- **Communication** : incapacité à faire connaître aux utilisateurs ou à la hiérarchie les avancées et/ou les problèmes de déploiement.
- **Documentation** : incapacité à mettre en œuvre un programme d'archivage électronique approprié malgré les efforts de déploiement du logiciel ;
- **Gestion de projet** – la stabilité globale du projet peut être mise en danger par l'incapacité à respecter convenablement le calendrier ou les dépenses liées au projet.
- **Formation** : une formation inappropriée aux nouveaux logiciels peut provoquer un rejet des nouvelles technologies par certains utilisateurs.
- **Baisse de productivité au démarrage** : durant le temps d'adaptation des utilisateurs aux nouveaux processus automatisés, la productivité globale peut baisser en raison du caractère innovant des logiciels.
- **Rotation du personnel** : le déploiement d'un logiciel peut avoir un effet négatif sur le projet en général si les cadres supérieurs défenseurs du projet ou les responsables chargés de la mise en œuvre du logiciel changent.

---

2 Adapté de S. Asbury *How to Implement a Successful AM/FM Pilot Project* et Etat de Michigan, *Records Management Application Pilot Project : Final Report for National Historical Publications and Records Commission Grant #2000-05*, http ://www.archives.gov/records-mgmt/policy/pilot-guidance.html#3.1.6

- **Évolutivité** : la capacité d'un logiciel à pouvoir s'adapter à la dimension de l'entreprise/organisme doit être prise en compte et planifiée dès le début du projet.
- **Changements organisationnels** : les environnements métier changent souvent et de façon significative au cours de la vie d'une application ou d'un système d'archivage. Ces changements concernent la taille, la structure, les processus de travail, les fonctions et mandats de l'organisme lui-même.

Toute entreprise/organisme déployant un logiciel devrait savoir qu'il est nécessaire de prendre des risques contrôlés quand on veut adopter de nouvelles technologies ou changer les processus métier. Un moyen d'atténuer les risques liés à ces déploiements est d'organiser un pilote avant d'étendre l'utilisation du logiciel à l'ensemble des services.

Pour minimiser les risques associés au lancement d'un pilote, l'équipe projet doit :

- Établir des objectifs clairs de performance et des critères d'évaluation ;
- Impliquer et encourager continuellement les participants du projet pilote à l'utilisation du système ;
- Organiser des sessions de travail de prototypage du logiciel avant de le paramétrer ;
- Finaliser la conception du système ;
- Développer une méthodologie qualité afin qu'il soit facilement accepté ;
- Étendre le pilote progressivement à d'autres secteurs de l'entreprise/organisme en incluant d'autres formats de documents ;
- S'assurer que les exigences du pilote sont mesurables et bien comprises des participants.

Lister les problèmes que l'équipe projet peut rencontrer et identifier les solutions pour les éviter ou y répondre rapidement réduira les perturbations durant le pilote. Les actions préventives suivantes sont recommandées :

- Une revue de projets similaires aidera à identifier les problèmes qu'on peut rencontrer au cours d'un pilote de projet d'archivage électronique ; et
- Des réunions de réflexion avec l'équipe projet avant la mise en œuvre aideront à anticiper les défis à venir.

Développer un plan d'urgence pour chaque problème potentiel. Cette bonne pratique de gestion augmentera la confiance de l'organe de gouvernance dans la capacité de l'équipe à réussir la mise en place d'un SAE à l'échelle de l'entreprise/organisme. Voici quelques exemples de stratégies pour résoudre les problèmes récurrents :

- On constate souvent une résistance au changement lors de la mise en place d'un projet d'archivage électronique. Beaucoup estiment que la meilleure stratégie contre cette résistance au changement est de présenter l'importance d'un bon archivage aux nouveaux arrivants dans l'organisation.

- S'assurer qu'une version du logiciel sera opérationnelle pour l'équipe projet avant le déploiement au premier groupe participant au pilote. Désigner des personnes qui devront se former et travailler avec le logiciel avant la phase pilote permettra d'avoir un groupe d'utilisateurs relativement avertis qui pourra établir la liaison avec les participants du projet pilote. Quand on aura atteint une qualité satisfaisante dans cette phase préalable, on pourra lancer le pilote officiellement.
- Gérer les attentes des utilisateurs pendant le pilote réduira les risques d'échec. La formation des utilisateurs et la communication constante faite aux participants du pilote sont de bons vecteurs. Établir la communication dans le reste de l'organisme (par exemple, avec une page Web du projet pilote ou une lettre d'information en ligne), permet de tenir les collaborateurs informés de l'avancement du projet d'archivage électronique. Ceci facilitera le déploiement ultérieur dans leur secteur si la solution est adoptée à l'échelle de l'entreprise/organisme.

4.3 Aspects financiers et organisationnels de la maintenance des systèmes électroniques

La stabilité financière et organisationnelle de tout investissement important est normalement garantie par l'existence de processus propres à chaque environnement réglementaire. En simplifiant à l'extrême, on dira que dans le cas des technologies de l'information (logiciel d'archivage par exemple), l'ensemble des analyses d'un dossier d'opportunité (« business case ») peut être conçu comme le moyen collectif de garantit cette stabilité.

Dans sa forme la plus simple, un dossier d'opportunité regroupe diverses analyses qui valident un projet d'acquisition, et donc d'amputation du capital, en accord avec la stratégie de valorisation du capital et du contrôle des investissements. Pour l'acquisition d'un logiciel d'archivage, les éléments du dossier sont :

- **Stratégie d'acquisition** : état pluriannuel des besoins budgétaires pour les différentes tranches du projet ;
- **Gestion du programme** : présentation détaillée de la composition de l'équipe projet et répartition des responsabilités ;
- **Architecture technique** :– description des pré-requis techniques pour l'intégration du logiciel dans le schéma informatique global de l'entreprise/organisme ;
- **Analyses des alternatives possibles :** description des alternatives envisagées, avec les coûts cycliques et les retours sur investissement pour chacune.
- **Gestion des risques :** description des risques majeurs pour chaque alternative choisie, incluant la fréquence potentielle, les impacts et les stratégies de réduction des risques ;
- **Objectifs de performance** : voir comment le déploiement proposé répond aux objectifs stratégiques de l'entreprise/organisme, au travers notamment

des outils d'évaluation existants et des améliorations de performance tirées d'indicateurs spécifiques ;

- **Gestion de projet** – présentation détaillée des étapes de mise en œuvre, montrant les résultats attendus et les coûts associés à chacun des moments clés du projet, et
- **Gestion des changements** – pour les services dédiés à l'archivage et leur personnel.

5. LISTE CRITIQUE DES AUTRES EXIGENCES FONCTIONNELLES

L'objectif de ce projet est d'harmoniser les multiples considérations juridictionnelles propres aux spécifications attendues des logiciels d'archivage électronique de sorte qu'elles respectent les recommandations générales établies dans la norme internationale ISO 15489 sur le Record Management, Parties 1 et 2 (2001), et la norme internationale ISO 23081 (2006 et 2007) Records Management Processes – Metadata for Records, Part 1 – Principles et Part 2 – Conceptual and Implementation Issues. Les exigences nationales ou régionales suivantes ont été prises en compte dans la préparation des modules.

Archives New Zealand /
Electronic Recordkeeping Systems Standard, June 2005
http ://www.archives.govt.nz/continuum/dls/pdfs/ARC2529ElectronicRecordkeepingStandard.pdf

Bundesministerium des Innern, Germany
DOMEA Concept Requirement Catalogue 2.0, June 2005
http ://www.kbst.bund.de/cln_011/nn_838524/SharedDocs/Anlagen-kbst/Domea/domea-requirements-catalogue-2-0,templateId=raw,property=publicationFile.pdf/domea-requirements-catalogue-2-0.pdf

Cornwell Management Consultants plc
(for the European Commission Interchange of Documentation between Administrations Programme)
Model Requirements for the Management of Electronic Records, March 2001
http ://www.cornwell.co.uk/edrm/moreq.asp#moreqdownload

Department of Defense, United States
Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD, June 2002
http ://jitc.fhu.disa.mil/recmgt/p50152s2.pdf

Department of Defense, United States
Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD Version 3, exposure draft, August 2006
http ://jitc.fhu.disa.mil/recmgt/dod50152v3_13jun06.pdf

DLM Forum Working Group for the Development of MoReq
Scoping Report for the Development of the Model Requirements for the Management of Electronic Records, February 2006

European Commission
Model Requirements for the Management of Electronic Records Update and Extension, 2008, (MoReq2 Specification)
http ://ec.europa.eu/transparency/archival_policy/moreq/doc/calltender_ann9_en.pdf
http ://www.moreq2.eu/

Indiana University
Requirements for Electronic Records Management Systems, 2002
http ://www.indiana.edu/~libarch/ER/requirementsforrk.doc

International Council on Archives
Authenticity of Electronic Records, ICA Study 13-1, November 2002

International Council on Archives
Authenticity of Electronic Records, ICA Study 13-2, January 2004

National Archives and Records Administration, United States
Functional Requirements and Attributes for Records Management Services, December 2005
http ://www.archives.gov/era/pdf/frauml-sep0706.pdf

National Archives of Australia
Functional Specifications for Electronic Records Management Systems Software, February 2006
http ://www.naa.gov.au/records-management/publications/ERMS-specs.aspx

National Archives of Australia
Functional Specifications for business Information Systems Software, October 2006
http ://www.naa.gov.au/records-management/publications/BIS.aspx

Public Record Office Victoria
Standard for the Management of Electronic Records PROS 99/007 (Version 1), April 2000
http ://www.prov.vic.gov.au/vers/standard/ver1/99-7.pdf

Public Record Office Victoria
Standard for the Management of Electronic Records PROS 99/007 (Version 2), July 2003
http ://www.prov.vic.gov.au/vers/standard/pdf/99-7_ver2-0.pdf

Riksarkivet, National Archives of Norway
NOARK 4 Part 1 – Norwegian Recordkeeping System : Functional Description and Specification of Requirements, 1999
http ://www.riksarkivet.no/noark-4/Noark-eng.pdf

State Records of South Australia
Document and Records Systems Standard 2001, Version 1, January 2001
http ://www.archives.sa.gov.au/files/management_standard_documentrecordssystem.pdf

State Records of South Australia
South Australian Government EDRMS Functional Compliance Requirements 2002, Version 1.0, August 2002
http ://www.archives.sa.gov.au/files/management_EDRMS_functionalcompliance.pdf

State Records of South Australia
Across Government EDRMS Panel of Products Procurement and Pre-Implementation – Guideline, Version 1, October 2004
http ://www.archives.sa.gov.au/files/management_guidelines_EDRMS_pandp.pdf

The National Archives, United Kingdom
Requirements for Electronic Records Management Systems, 1 : Functional Requirements, *2002 Revision – Final Version*, 2002
http ://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/requirementsfinal.pdf

The National Archives, United Kingdom
Requirements for Electronic Records Management Systems, 2 : Metadata Standard,

2002 Revision – Final Version, 2002
http ://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/metadatafinal.pdf

The National Archives, United Kingdom
Requirements for Electronic Records Management Systems, 3 : Reference Document, 2002 Revision – Final Version, 2002
http ://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/referencefinal.pdf

The National Archives, United Kingdom
Requirements for Electronic Records Management Systems, 4 : Implementation Guidance, 2004
http ://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/implementation.pdf

The National Archives, United Kingdom
Rationale for the Functional Requirements for Electronic Records Management Systems, 2002
Link to various documents from :
http ://www.nationalarchives.gov.uk/electronicrecords/rat2002/

The National Archives, United Kingdom
Requirements to Sustain Electronic Information Over Time, March 2006
http ://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs1.pdf
http ://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs2.pdf
http ://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs3.pdf
http ://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs4.pdf

The National Archives, United Kingdom
Functional Requirements for the Sustainability of Electronic Records Management Systems, March 2006
http ://www.nationalarchives.gov.uk/electronicrecords/pdf/functional_requirements.pdf

6. GLOSSAIRE

Ce Glossaire constitue un sous-ensemble d'un glossaire plus complet et présent dans les Modules 2 et 3.

NB : l'ordre est l'ordre alphabétique des mots français, le terme anglais étant indiqué juste après.

Terme	***Définition***
Application métier / Business system	Dans le cadre de ce document : système automatisé qui crée ou gère les données d'un(e) entreprise/organisme. Ceci comprend les applications dont le rôle premier est de faciliter les transactions entre une unité organisationnelle et ses clients – par exemple, commerce électronique, gestion de la relation client, bases de données spécifiques ou personnalisées, systèmes relatifs aux finances ou aux ressources humaines.
Archivage / Recordkeeping	Organisation systématique de la production et capture, utilisation, maintenance et sort final des documents engageants (à archiver), en accord avec les besoins et responsabilités administratifs, réglementaires, financiers et sociétaux.
Archives / Archives	Documents produits ou reçus par une personne, une famille ou un organisme, public ou privé, dans le cadre de son activité, et conservés en raison de leur valeur de preuve des activités et responsabilités de leur producteur, particulièrement ceux qui sont gérés par les principes de provenance, de respect de l'ordre primitif et de contrôle collectif ; archives définitives. Note : en informatique, le terme « archives » revêt un autre sens ; il signifie « copie d'un ou plusieurs fichiers ou copie d'une base de données en vue d'assurer une sauvegarde à des fins de consultation ou une restauration si les données originales sont endommagées ou perdues. » Source: *IBM Dictionary of Computing*, McGraw Hill, New York, 1994, p. 30.
Autorité archivistique / Archival authority	Services et institutions archivistiques ou autres structures responsables des programmes de sélection, collecte, conservation, mise à disposition et contrôle de la destruction d'archives.
Convertir / Reformat	Créer une copie dans un format ou une structure différant de l'original, notamment pour le conserver ou le rendre accessible.
COTS / COTS	Logiciel commercial clé en main
Document électronique engageant / Electronic record	Document engageant sur support électronique, produit, transmis, conservé et/ou consulté via des outils électroniques.

Terme	***Définition***
Document engageant / Record (noun)	Toute information, sous tout format, produite, reçue ou conservée à titre de preuve et d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité. Source: ISO 15489, Part 1, Clause 3.15.
Dossier d'opportunité / Business case	Argumentaire pour l'amélioration de l'activité constituant une aide à la décision pour les dirigeants. Il est composé d'une analyse de performance des processus métier et des besoins ou problèmes afférents, de propositions de solutions alternatives, de prévisions et de contraintes, et d'une analyse de rentabilité ajustée au risque.
Facteurs humains / Human factors	Étude du comportement physique et psychologique des personnes en lien avec certains environnements, produits ou services. Une étude sur les facteurs humains ou l'ergonomie permet notamment de tester un prototype ou une version précoce d'un produit auprès d'un groupe représentatif de personnes, rémunérées ou bénévoles.
Information / Information	Connaissance transmise ou reçue. Résultat du traitement, de la collecte, de la manipulation et de l'organisation de données visant à transmettre un savoir au destinataire.
Logiciel d'archivage électronique / Electronic records management software	Logiciel spécialisé pour automatiser la gestion de l'archivage.
Logiciel propriétaire / Proprietary software	Logiciel qui est la propriété exclusive d'une seule société qui conserve soigneusement son savoir-faire technologique et la documentation de ses produits.
Métadonnées / Metadata	Informations structurées ou semi-structurées permettant de produire, gérer et utiliser les documents archivés dans le temps dans des domaines variés. Source: ISO 23081 – 1: 2006, Clause 4. Informations structurées qui décrivent et/ou permettent de retrouver, gérer, contrôler, interpréter ou conserver d'autres informations dans le temps. Source: Adapté de A. Cunningham, 'Six degrees of separation: Australian metadata initiatives and their relationships with international standards', *Archival Science*, vol. 1, no. 3, 2001, p. 274.
Migration / Migration	Action de transférer des documents archivés dans un système vers un autre, tout en préservant leur authenticité, leur intégrité, leur fiabilité et leur exploitabilité. La migration renvoie à des tâches précises visant à assurer le transfert périodique de données numériques d'un matériel ou logiciel informatique vers un autre, ou d'une génération technologique vers une autre. Source: Adapté de ISO 15489, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.

Terme	***Définition***
Projet pilote / Pilot project	Initiative expérimentale sur une durée limitée dont les résultats sont systématiquement évalués.
Retour sur investissement / Return on investment	Dans un(e) entreprise/organisme, le retour sur investissement équivaut aux bénéfices ou économies réalisés face à une dépense donnée. Son calcul permet, conjointement à d'autres démarches, d'établir un dossier d'opportunité pour un projet donné.
Sort final / Disposition	Destinations possibles des documents lors de la mise en œuvre des décisions de conservation, destruction ou transfert des documents archivés, selon les règles énoncées dans le référentiel de conservation ou dans d'autres outils. Source: ISO 15489, Part 1, Clause 3.9
Technologies de l'information / Information technology	Terme générique pour toutes formes de technologies de production, stockage, échange et utilisation de l'information sous toutes ses formes (données métier, conversations orales, images fixes, films, présentations multimédia et autres formes non encore inventées).
Utilisateur final / End-user	En informatique, le terme « utilisateur final » permet de différencier la personne à qui est destiné un logiciel ou un matériel, de celles qui le développent, l'installent et le réparent.

Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique

Module 2

Recommandations et exigences fonctionnelles pour les systèmes d'archivage électronique

Publié par le Conseil international des Archives. Ce module a été élaboré par une équipe mixte constituée de membres du Conseil international des Archives et de l'*Australasian Digital Recordkeeping Initiative*.

ISBN : 978-2-918004-00-4

Référence à citer: *Conseil international des Archives Principes et exigences fonctionnelles pour l'archivage électronique – Module 2: Recommandations et exigences fonctionnelles pour les systèmes d'archivage électronique,* 2008, publié sur www.ica.org

TABLE DES MATIÈRES

1.1 Champ d'application 5
1.2 Objectif 6
1.3 Publics cibles 7
1.4 Autres normes du domaine 7
1.5 Terminologie 8
1.6 Structure 10
2.1 Quels documents faut-il archiver et pourquoi ? 11
2.2 Caractéristiques des documents électroniques et des systèmes d'archivage électronique 13
2.2.1 Fonctions d'import, export et interopérabilité 15
2.2.2 Authentification, chiffrement et moyens technologiques de protection 16
2.3 Présentation des exigences fonctionnelles 16
2.3.1 Production et capture 17
Capture17
Agrégats 18
Identification (enregistrement) 19
Classement 19
Plans de classement métier 20
2.3.2 Maintenance 21
Authenticité et fiabilité des documents archivés 21
Contrôles et sécurité 21
L'archivage mixte 21
Conservation et destruction 21
2.3.3 Mise à disposition 22
2.3.4 Administration 22
2.4 Utilisation des exigences fonctionnelles 22
2.4.1 Éléments clés 22
2.4.2 Niveaux d'obligation 22
2.4.3 Risques et faisabilité face à la non-satisfaction de ces exigences 23
3.1 Capture 24
3.1.1 Processus de capture 24
3.1.2 Métadonnées de capture 25
3.1.3 Agrégats électroniques 26
3.1.4 Import de masse 27
3.1.5 Formats électroniques 28
3.1.6 Documents composites 29
3.1.7 Messagerie électronique 29
3.2 Identification 30
3.3 Classement 31
3.3.1 Élaboration d'un plan de classement 31
3.3.2 Niveaux de classement 32
3.3.3 Processus de classement 33
3.3.4 Volumes 35
3.4 Gestion de l'authenticité et de la fiabilité 36

3.4.1 Accès et sécurité 36
3.4.2 Contrôles d'accès 37
3.4.3 Mise en place de contrôles de sécurité 37
3.4.4 Attribution des niveaux de sécurité 37
3.4.5 Exécution des contrôles 38
3.4.6 Niveaux de sécurité 39
3.4.7 Métadonnées d'archivage 41
3.4.8 Traçabilité des mouvements 43
3.5 L'archivage mixte 43
3.5.1 Archivage des documents électroniques et non électroniques 43
Dossiers mixtes 44
Documents mixtes 44
3.6 Conservation et destruction 45
3.6.1 Référentiels de conservation 45
Élaboration des référentiels de conservation 45
Appliquer les référentiels de conservation 46
Mise en œuvre des règles de conservation/destruction 47
Tracer les actions de destruction 48
Révision du sort final 48
3.6.2 Migration, export et destruction 50
3.6.3 Conservation et destruction des documents électroniques et non électroniques 52
3.7 Recherche, repérage et restitution 52
3.7.1 Restitution: affichage 55
3.7.2 Restitution: impression 56
3.7.3 Restitution : extraits 57
3.7.4 Restitution: autres 57
3.7.5 Restitution: réutilisation des contenus 58
3.8 Administration 58
3.8.1 Rôle de l'administrateur 58
3.8.2 Gestion des métadonnées 59
3.8.3 Reporting 60
3.8.4 Sauvegarde et restauration 60
A Glossaire 62
B Lectures complémentaires 76
C Exemple de check-list pour l'évaluation d'un SAE 77

1 INTRODUCTION

Un bon archivage et une bonne gestion de l'information contribuent à rendre l'activité interne et externe de tout(e) entreprise/organisme plus performante ; ils deviennent dès alors essentiels à son bon fonctionnement. Ils assurent aussi, pour le secteur public ou privé, la justification de décisions et d'actions. Les archives fournissent aux citoyens les preuves leur permettant de confirmer ou revendiquer leurs droits et titres, et garantissent aux individus d'accéder aux traces des décisions gouvernementales et de vérifier la fiabilité des entreprises privées. Une bonne gestion de l'archivage est tout simplement une bonne pratique.

Les systèmes d'archivage favorisent :

- l'efficacité, en rendant l'information immédiatement disponible lorsqu'elle est nécessaire à la prise de décision et aux activités opérationnelles;
- le bon usage des ressources financières, en permettant, quand elle est opportune, la destruction des dossiers inutilisés ;
- la capacité à rendre compte, en permettant la constitution de traces complètes et probantes des activités officielles;
- la conformité, en prouvant que les exigences légales ont été remplies ; et
- la diminution du risque, en gérant les risques liés à la perte ou la destruction illégale d'archives, et à l'accès inapproprié ou non autorisé aux documents archivés.

1.1 Champ d'application

Différencier les systèmes d'information des entreprises/organismes des systèmes d'archivage électronique est un postulat de base essentiel. Les données des systèmes d'information sont généralement sujettes à des mises à jour constantes (données non figées) et des transformations (données manipulables) et elles sont exclusivement actives (non excédentaires), alors que, à l'inverse, les données des systèmes d'archivage électronique n'évoluent pas au rythme de l'activité métier (elles sont figées), ne peuvent pas être altérées (elles sont inviolables) et peuvent être inactives (excédentaires). Les applications métier ne rentrent donc pas dans le champ d'application de ce module (voir *Module 3 : Recommandations et exigences fonctionnelles pour l'archivage dans les applications métier*). Les documents au sein d'un système d'archivage électronique restent cependant dynamiques, au sens où ils peuvent être (ré)utilisés dans de nouvelles activités ou de nouveaux contextes métier, l'usage de leur contenu générant alors de nouvelles métadonnées. Il est plus approprié de parler d'un cadre pour la gestion systématique et structurée de l'archivage : les systèmes d'archivage lient les documents archivés aux activités métier, conservent les traces des actions passées et pérennisent le contenu et la structure des archives.

Le champ d'application de ce module est limité aux produits généralement appelés « systèmes d'archivage électronique » (SAE). Il ne cherche pas à établir des exigences pour les documents ou données utilisés au sein des applications métier.

Les objets numériques créés par la messagerie électronique, les outils bureautiques et l'imagerie (documents texte, images fixes et animées), dès lors que leur valeur pour l'activité métier est identifiée, devraient être gérés au sein de SAE répondant aux exigences fonctionnelles du présent module. Les documents gérés par un SAE peuvent être stockés sur différents formats, et peuvent être gérés au sein de dossiers mixtes comprenant à la fois des éléments électroniques et non électroniques.

Ce module ne cherche pas à inclure des exigences qui ne soient ni spécifiques ni nécessaires à la gestion de l'archivage, comme les exigences relatives à la gestion et à la conception générales du système. Il n'inclut pas non plus les exigences communes à toutes les applications informatiques, telles que la performance, l'extensibilité et la facilité d'utilisation de l'application. Ce document s'adressant à un public particulier, il requiert des connaissances sur les caractéristiques techniques liées à la conception, l'installation et l'évaluation des SAE, bien que ces questions ne soient pas traitées dans ce module.

Quoique les exigences fonctionnelles hors archivage ne soient pas incluses dans ce module, leur importance pour les systèmes d'archivage est reconnue par leur inclusion dans le modèle générique figurant en section 2.3 « Présentation des exigences fonctionnelles ».

Les spécifications pour la pérennisation des documents archivés électroniquement ne rentrent pas non plus dans le champ d'application de ce module : cette question devrait être traitée séparément, selon une stratégie particulière de conservation numérique ou « archivage électronique définitif ». Ces considérations sur l'archivage électronique définitif transcendent la durée de vie des systèmes et sont indépendantes desdits systèmes ; elles doivent être évaluées dans le cadre d'une stratégie de pérennisation. Cependant, le besoin de préserver les archives aussi longtemps que nécessaire doit être reconnu, et les questions de migration potentielle ou d'obsolescence des formats devraient aussi être prises en compte. Des politiques et procédures *ad hoc* devraient être développées pour favoriser la pérennité des documents archivés, en vue de leur conservation permanente ou à long terme.

1.2 Objectif

Ce module formule un ensemble d'exigences fonctionnelles pour les systèmes d'archivage électronique. Elles sont valables quel que soit le mode de création et de stockage des documents et visent à :

- expliquer les processus et les exigences pour identifier et gérer des documents dans un SAE ;
- développer des exigences afin d'inclure la fonction archivage dans les spécifications techniques lors de la conception, de la mise à jour ou de l'achat d'un logiciel d'archivage électronique ;
- faire en sorte que les exigences fonctionnelles relatives à l'archivage soient un critère de sélection des SAE disponibles sur le marché ; et
- réviser les fonctionnalités d'archivage ou évaluer la conformité des SAE existants.

Ce module a été développé comme une partie d'un projet du Conseil international des Archives destiné à :

- aider les entreprises/organismes à améliorer leurs pratiques d'archivage électronique ;
- réduire la multiplication des efforts et des coûts associés en identifiant un niveau minimal de fonctionnalités d'archivage pour un SAE ; et
- favoriser la standardisation des exigences nécessaires à la gestion des documents pour les fournisseurs de logiciels dans différents pays.

1.3 Publics cibles

Le premier public visé par ce document est le personnel responsable de la conception, de la révision et/ou de la mise en œuvre des SAE dans les entreprises/organismes – que ces systèmes soient des solutions du marché ou des applications développées en interne. Ce module aborde principalement les exigences propres aux archivistes, aux responsables de l'archivage ou aux acheteurs de solutions mais il s'adresse aussi aux organismes de normalisation nationaux et plus largement à la communauté des acteurs de l'archivage. Sont également visés les vendeurs et développeurs de logiciels, qui vendent et/ou développent des produits d'archivage électronique. Ce module cherche à éclairer leurs choix lors de la conception des fonctionnalités d'archivage de leurs produits.

Partant du principe que ce document s'adresse à un large public, les auteurs ont essayé de réduire l'emploi de termes purement archivistiques. Lorsqu'ils sont inévitables, le glossaire en annexe A en fournit la définition.

1.4 Autres normes du domaine

Suivant son axe prioritaire « archivage électronique et automatisation », le Conseil international des Archives a conçu un ensemble de recommandations et d'exigences fonctionnelles dans le cadre du projet relatif aux « Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique » :

Module 1 : Contexte et déclaration de principes

Module 2 : Recommandations et exigences fonctionnelles pour les systèmes d'archivage électronique

Module 3 : Principes et exigences fonctionnelles pour l'archivage dans les applications métier.

Le présent document constitue le Module 2 du projet. Il a été développé avec le soutien de l'*Australasian Digital Recordkeeping Initiative*.

Les lecteurs pourront se référer au Module 1 : « Contexte et déclaration de principes » pour avoir une vision plus large du contexte et des principes sur lesquels repose ce document, même si celui-ci peut être utilisé comme une ressource indépendante. Pour le détail des exigences fonctionnelles concernant les applications métier, les lecteurs se reporteront au Module 3 : « Recommandations et exigences fonctionnelles pour l'archivage des documents dans les systèmes métier ».

Les lecteurs de ce document doivent également prendre en compte toute spécification ou norme propres à chaque pays.

Note : ce module n'entend pas se substituer aux normes et exigences des législations nationales ou locales.

Les exigences de ce module sont basées sur les principes directeurs du Records management (gestion de l'archivage) énoncés dans première partie de la norme ISO 15489 et dont les exigences sont également applicables aux documents capturés et gérés sous forme électronique.

Pour ces exigences, la norme de référence relative aux métadonnées est ISO 23081 – 1: 2006, Information and Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles. Le jeu de métadonnées essentielles fourni par ISO 23081 – 2: 2007, Information and Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues est à la base de ces exigences.

Les exigences présentées dans ce module sont de trois types : fondamentales, essentielles et génériques. Les lecteurs à la recherche de conseils concernant d'autres fonctionnalités des logiciels, non traitées dans ce module, pourront se référer à d'autres spécifications plus détaillées, comme US DoD 5015.2 et Moreq2.

1.5 Terminologie

De nombreux termes utilisés dans ce document ont des définitions différentes selon la discipline. Par exemple, le terme « archives » peut désigner, dans le domaine informatique, le stockage de données peu utilisées dans une base de données, alors que dans le monde archivistique, il désigne la conservation d'une information sélectionnée et figée qui n'est plus conservée pour un usage métier courant. Il est donc important que le présent document soit lu en liaison avec le glossaire de l'appendice A. Certains concepts de base utilisés dans ce document sont toutefois présentés ci-dessous, pour éviter une mauvaise interprétation :

- **Documents engageants (à archiver) :** documents créés, reçus et conservés à titre de preuve et d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité[1]. Ils fournissent la preuve des activités et existent sous tous les formats.
- **Gestion de l'archivage** : contrôle de la création, de la réception, de la préservation, de l'utilisation et du sort final des documents, en accord avec les règles et les bonnes pratiques professionnelles et internationales. La gestion de l'archivage se distingue de la gestion des documents, laquelle concerne en priorité l'accès, le travail collaboratif et le contrôle des versions des documents, et non la gestion de l'authenticité, de la fiabilité, de l'intégrité et de l'exploitabilité dans le temps.
- **Systèmes d'archivage électronique (SAE)** : systèmes spécialement conçus pour gérer la conservation et le sort final des documents engageants archivés. Ils conservent le contenu, le contexte, la structure et les liens entre

[1] Norme internationale sur le Records Management, ISO 15489.

documents pour permettre d'y accéder et renforcer leur valeur de preuve. Dans le présent document, les SAE sont présentés séparément des applications métier dans la mesure où leur fonction première est la gestion des documents archivés.

- **Applications métier** : (dans ce document) systèmes automatisés qui créent ou gèrent des données issues des activités d'un(e) entreprise/organisme. Ceci comprend les applications dont l'objectif est d'abord de faciliter les transactions entre une entreprise et ses clients (système de commerce en ligne, système de gestion de la relation client, base de données *ad hoc* ou personnalisée, systèmes de gestion financière ou RH).
  Une application métier contient normalement des données dynamiques sujettes à des mises à jour constantes (pertinentes), modifiables (manipulables), et ce sont des données vivantes (non excédentaires). Dans ce document, les applications métier excluent les SAE.
- **Système** : le terme « système » désigne ici un système informatique. Il s'oppose au sens archivistique du terme qui couvre des aspects plus vastes : le personnel, les politiques, les procédures et les pratiques. Bien que le présent module soit avant tout centré sur les logiciels d'archivage électronique, les entreprises ou organisations devront veiller à ne pas perdre de vue les aspects précités afin de garantir une gestion optimale des documents archivés. Les outils essentiels à l'archivage comme les référentiels de conservation et les règles de classification pour la sécurité de l'information doivent être mis en place et fonctionner grâce à une culture de l'archivage établie au sein de l'entreprise/organisme. Un système peut comprendre plus d'une application, et inclure des logiciels complémentaires (plug-in).
- **Métadonnées d'archivage** : composante indissociable de la gestion de l'archivage, servant à diverses fonctions et objectifs. Dans un contexte d'archivage, les métadonnées se définissent comme des données décrivant le contexte, le contenu et la structure des documents ainsi que leur gestion dans le temps (ISO 15489 – 1: 2001, 3.12).

  Les métadonnées sont donc des informations structurées ou semi-structurées, qui permettent la création, l'enregistrement, le classement, l'accès, la conservation et la destruction des documents archivés dans le temps, dans différents domaines. Les métadonnées d'archivage servent à identifier, authentifier et contextualiser les documents engageants (à archiver) ainsi que les personnes, processus et systèmes qui les créent, les gèrent, les conservent et les utilisent, et les politiques qui les régissent. Initialement, les métadonnées définissent le document engageant au moment de sa capture, le figeant dans son contexte de production et établissant un contrôle sur sa gestion. Au cours de l'existence des documents ou des dossiers, de nouvelles couches de métadonnées s'ajouteront en raison de nouveaux rôles dans d'autres contextes ou d'autres usages. Ainsi les métadonnées continuent d'accroître l'information relative au contexte d'archivage, de production et d'utilisation des documents, ainsi qu'aux changements de fond et de forme des documents.

Les métadonnées peuvent alimenter de nombreux systèmes et être réutilisées à des fins diverses. Les métadonnées s'appliquant aux documents archivés pendant leur vie active peuvent aussi continuer de s'appliquer quand les documents, n'étant plus d'usage courant, sont conservés pour un besoin d'information ultérieur ou une autre raison. Le but des métadonnées d'archivage est de garantir l'authenticité, la fiabilité, l'exploitabilité et l'intégrité dans le temps, et de permettre la gestion et la compréhension des objets d'information, qu'ils soient physiques, analogiques ou électroniques. Ceci dit, les métadonnées doivent aussi être gérées comme des données engageantes, ou comme une composante d'un document archivé. L'archivage a toujours impliqué la gestion des métadonnées. Cependant, l'environnement électronique exige une interprétation différente des exigences traditionnelles, et des mécanismes différents pour identifier, capturer, attribuer et utiliser les métadonnées. Dans l'environnement électronique, les documents qui font autorité sont ceux accompagnés de métadonnées définissant leurs caractéristiques essentielles. Ces caractéristiques doivent être exprimées explicitement plutôt qu'être implicites, comme dans certains processus de l'environnement papier.

1.6 Structure

Ce document est divisé en quatre grandes parties :

- **Partie 1 : Introduction :** elle définit le champ, l'objectif, le public cible et la structure du document.
- **Partie 2 : Lignes directrices :** elles donnent une vue d'ensemble des bases conceptuelles du module et présente un modèle des fonctionnalités essentielles d'un système d'archivage électronique. Cette section explique pourquoi il est important d'archiver, définit les mots-clefs et les concepts et aborde dans les grandes lignes les exigences fonctionnelles plus largement explicitées dans la troisième partie du module. Elle souligne également les questions et processus à prendre en compte lors de la révision, la conception ou l'achat d'un SAE.
- **Partie 3 : Exigences fonctionnelles :** tableau des exigences fonctionnelles pour l'archivage, qui caractérisent et permettent d'évaluer tout SAE.
- **Partie 4 : Annexes :** glossaire des mots-clés, lectures complémentaires et exemple de check-list pour l'évaluation d'un SAE.

2 LIGNES DIRECTRICES

2.1 Quels documents faut-il archiver et pourquoi ?

Les documents engageants (à archiver) constituent un actif non négligeable de l'entreprise/organisme car c'est souvent par le biais de ces documents qui tracent les activités que les entreprises/organismes peuvent rendre des comptes. Les documents engageants sont ceux qui sont créés, reçus ou préservés à titre de preuve ou d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité[2]. Ils doivent être conservés pendant une durée conforme à un référentiel de conservation validé ou à une autorité de référence.

Un document engageant est plus qu'un ensemble de données ; il est la conséquence ou le produit d'une action et de ce fait est lié à une activité. Un trait distinctif des documents engageants est que leur contenu doit être formellement fixé, c'est-à-dire être une représentation figée d'une action donnée. La gestion de l'archivage dans des systèmes métier, qui contiennent des données dynamiques et fréquemment mises à jour, pose un problème sérieux et peut constituer un argument pour choisir un système d'archivage séparé. Les documents archivés ne se limitent pas à un contenu mais comprennent aussi des informations sur le contexte et la structure des documents. Les métadonnées d'archivage identifient, authentifient et contextualisent les documents ainsi que les personnes, les processus et les systèmes qui les créent, les gèrent, les conservent et les utilisent, avec la politique et les procédures associées[3.] Elles permettent de localiser, restituer et comprendre valablement les documents. ISO/TS 23081 – 2 fournit un modèle générique de métadonnées d'archivage. Il arrive aussi que les entreprises/organismes doivent tenir compte de contraintes réglementaires locales ou nationales.

Un document archivé et géré rigoureusement constituera :

- une aide à la décision (éclairage documenté et de qualité),
- une ressource documentaire pouvant prouver et justifier des activités de l'entreprise/organisme, et
- un élément de cohérence, de continuité et d'efficacité d'administration et de gestion.

La norme internationale sur le Records management, ISO 15489, constitue un guide pour bien archiver les documents engageants de sorte qu'ils soient authentiques, fiables, complets, intègres et exploitables. Les entreprises/organismes qui n'ont pas de SAE prennent le risque de perdre la trace de leur activité, ce qui se traduira par une perte de la mémoire institutionnelle, un manque d'efficacité, une incapacité à répondre aux audits et aux obligations réglementaires. Les risques à ne pas mettre en œuvre un SAE sont :

---

[2] Norme internationale sur le Records management, ISO 15489

[3] Norme ISO 23081 – 1: 2006, Information et documentation - Records management – Metadata for Records.

- le non respect des exigences législatives et réglementaires,
- la mise en difficulté des dirigeants, du gouvernement et/ou de personnes privées, surtout si les médias soulignent une incapacité flagrante à gérer l'information,
- la faiblesse de la planification et des décisions basées sur une information imprécise,
- l'inaccessibilité de l'information vitale pour la conduite des affaires, la résolution des conflits, les contraintes légales ou les besoins de preuve,
- la perte de crédibilité et de la confiance du public, des sanctions financières ou légales pour incapacité à produire les documents demandés ou la preuve de l'activité dans les délais requis,
- l'incapacité à produire la preuve des activités ou des relations avec d'autres organisations, les clients ou les fournisseurs,
- incohérence et inefficacité dans la conduite des affaires,
- l'incapacité à exploiter pleinement l'information et le savoir-faire internes,
- la destruction illégale de documents et incapacité à exploiter la connaissance et les données de l'entreprise/organisme,
- la dépense d'énergie pour une gestion médiocre des ressources et des actifs,
- la capacité réduite de prouver la bonne performance et les gains d'efficacité, ou d'améliorer la qualité des services,
- la mise en difficulté de l'entreprise/organisme et atteinte à son image.

Les bénéfices d'un bon archivage sont :

- la protection et l'aide en cas de contentieux, notamment la gestion des risques liés à l'existence ou à l'absence de traces de l'activité,
- la protection des intérêts de l'entreprise/organisme et des droits des salariés, clients, responsables présents et futurs,
- le renforcement de la sécurité des documents traçant l'activité et les relations commerciales stratégiques, de l'information sensible ou des données personnelles,
- la faculté de fournir des services d'une façon efficace et cohérente,
- la possibilité d'aider les activités de recherche et développement présentes et futures,
- une mémoire institutionnelle plus large et plus fiable,
- la disponibilité des documents traçant l'activité métier recherchés comme aide à la décision ou pour le développement d'une politique d'entreprise,
- la réduction du risque de perte de données ou de destruction accidentelle de documents archivés,
- la mesure fiable et performante des résultats,

- une augmentation de la confiance du public ou de la clientèle vis-à-vis de l'intégrité de l'entreprise/organisme et de ses activités,
- l'identification des documents vitaux pour le plan de continuité d'activité de sorte que l'entreprise/organisme puisse continuer à fonctionner en cas d'événement grave.

Un archivage efficient et crédible est un élément essentiel de bonne gouvernance et donne de la fiabilité et de la cohérence aux activités et aux services offerts par l'entreprise/organisme.

2.2 Caractéristiques des documents électroniques et des systèmes d'archivage électronique

Les documents engageants (à archiver) doivent être gérés dès leur validation et maintenus aussi longtemps que requis afin de leur assurer les caractéristiques suivantes[4] :

- **Authenticité** : le document peut prouver qu'il est bien ce qu'il prétend être, qu'il a bien été créé ou envoyé par la personne qui l'a créé ou envoyé et qu'il a bien été créé ou envoyé à la date indiquée.
- **Fiabilité** : le document archivé est bien la représentation complète et fidèle de la(des) opération(s) dont il atteste et on peut s'y fier dans le cadre d'opérations futures.
- **Intégrité :** le document est complet, non altéré et protégé contre toute modification non autorisée. Cette caractéristique est également appelée « inviolabilité ».
- **Exploitabilité :** le document peut être localisé, repéré, conservé et interprété.

En général, les SAE possèdent les fonctions suivantes pour garantir la maintenance de ces caractéristiques :

Production et capture des documents engageants dans leur contexte : les SAE permettent aux entreprises/organismes de capturer la preuve de leur activité. Cela nécessite d'identifier un ensemble d'informations électroniques constituant un document engageant, comprenant à la fois un contenu et un contexte. Ainsi, pour que ces informations puissent faire foi, il est nécessaire d'y ajouter des données complémentaires (les métadonnées) qui le replacent dans son contexte et son environnement informatique de production.

La gestion et la conservation des documents archivés – les documents électroniques, en tant que preuve d'une activité métier, doivent être activement gérés afin de maintenir leur authenticité, leur fiabilité, leur intégrité et leur exploitabilité. La maintenance de ces documents en tant que preuve est nécessaire au fonctionnement et à la responsabilité de l'entreprise/organisme.

La conservation des documents archivés aussi longtemps que nécessaire :

[4] Issues de la norme ISO 15489.1 sur le Records Management, section 7.2 « Caractéristiques des documents engageants (à archiver) »

les documents doivent être conservés pendant une durée répondant aux exigences législatives et réglementaires. Les durées de conservation des documents sont définies dans des référentiels de conservation/destruction. Certains doivent être conservés indéfiniment, tandis que d'autres sont soumis à des durées variables ou à une durée maximale (cas de protection de la vie privée et des données personnelles).

Le sort final des documents doit pouvoir être appliqué de manière ordonnée, systématique et auditable. La conservation et l'application respectueuse du sort final des documents conformément aux règles prédéterminées sont la garantie d'un bon archivage.

Les systèmes doivent pouvoir supprimer les documents de manière systématique, auditable et responsable, conformément aux exigences opérationnelles et juridiques. Il est nécessaire que les organismes respectent les politiques et procédures déterminées par leur environnement réglementaire pour l'identification, la conservation et la destruction des documents.

La configuration des métadonnées : pour être recevable en tant que trace probante d'un processus, les documents doivent être liés à leur contexte de production et d'utilisation. A cette fin, le document doit être associé à des métadonnées contextuelles dans un plan de classement. En plus de ces métadonnées de « classement », d'autres métadonnées devraient être capturées au moment de l'archivage du document, dont :

- un identifiant ;

- la date de création ;

- le créateur/auteur/responsable ; et

- l'intitulé de l'affaire en cours.

La plupart de ces informations peut être générée automatiquement. Dans ce module, l'intégration de métadonnées d'archivage est traitée à un niveau générique. Plutôt que de décrire de manière détaillée chaque métadonnée requise, ces exigences fonctionnelles fournissent des informations générales sur la nécessité d'une fonctionnalité permettant de créer, capturer et maintenir les métadonnées appropriées. Il est souhaitable que chaque entreprise/organisme capture les métadonnées d'archivage de manière normalisée, dans le respect des exigences réglementaires et/ou organisationnelles, et/ou conformément à l'ISO 23081 – 1: 2006, Information et documentation – Records management – Metadata for Records, Part 1 – Principles, et à l'ISO/TS 23081 – 2: 2007, Information et documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues.

Les documents archivés peuvent être réattribués ou reclassés, clos, et si nécessaire, copiés et extraits : l'identification des besoins de traçabilité des activités devrait établir à quelle étape de la procédure un document engageant devrait être produit. Toute action dont ce document ferait l'objet par la suite doit entraîner la production d'un nouveau document ou

l'enregistrement de nouvelles versions, plutôt que sa modification. Cela signifie que l'on ne peut réécrire le contenu ou les métadonnées d'un document archivé comme trace d'une décision ou d'un processus mais qu'un nouveau contenu ou de nouvelles métadonnées peuvent lui être ajoutés.

Il importe de s'assurer que le niveau de verrouillage du système n'empêche pas la correction de simples fautes (telles que la saisie erronée d'un nom), mais le droit de modifier les documents devrait être restreint à un administrateur système ou interdit par le système dans certains cas exceptionnels (contentieux en cours).

Des rapports peuvent être établis sur les documents archivés et leur gestion.

Les procédures de sécurité peuvent être mises en place : Les contrôles classiques des accès et de la sécurité du système contribuent au maintien de l'authenticité, de la fiabilité, de l'intégrité et de l'exploitabilité et devraient par conséquent être correctement définis.

Une évaluation des risques peut éclairer les prises de décisions sur le besoin et le niveau de ces contrôles. Par exemple, dans un environnement à haut risque, il peut être nécessaire de prouver exactement ce qui a été fait, quand et par qui. Ceci renvoie aux habilitations et aux journaux d'audit du système si on veut prouver que toutes les opérations listées ont été effectuées par des utilisateurs habilités.

Tableau 1 : niveaux d'accès

Utilisateur	Toute personne ayant un droit d'accès au SAE, c'est-à-dire toute personne qui produit et valide, reçoit et/ou utilise les documents conservés dans le système. Cela correspond au niveau d'accès élémentaire attribué à la plupart des employés d'un(e) entreprise/organisme.
Utilisateur habilité	Utilisateur ayant des droits d'accès particuliers lui permettant des accès et/ou contrôles supplémentaires sur les documents du SAE. En certaines circonstances, ces utilisateurs peuvent recevoir l'autorisation d'exécuter des tâches identiques à celles de l'administrateur système, telle que la possibilité de clore ou de rouvrir des documents, d'en créer des extraits et d'en modifier les métadonnées. Les droits attribués aux utilisateurs habilités dépendent de leur niveau de responsabilité et des besoins.
Administrateur de l'archivage (responsable de l'archivage, archiviste)	Un administrateur système, responsable de l'archivage ou archiviste, chargé de configurer, de contrôler et de gérer le contenu et l'utilisation du SAE.
Administrateur système *(*informaticien*)*	Personne chargée d'attribuer et de supprimer les droits des utilisateurs habilités ou non.

2.2.1 Fonctions d'import, export et interopérabilité

Les possibilités d'import et d'export des données et l'interopérabilité avec les autres

systèmes informatiques sont des fonctionnalités souvent nécessaires. On peut avoir besoin d'exporter des données archivées en cas de fusion ou réorganisation.

De nombreux documents archivés doivent être conservés pendant des durées qui excèdent la durée de vie du logiciel lui-même et, dans ce cas, il est essentiel de pouvoir exporter les données vers un nouveau SAE. On peut également avoir besoin d'importer des données à partir d'applications métier, et ce particulièrement dans les environnements de type collaboratif.

Les imports et exports seront facilités par l'utilisation de formats ouverts et de normes qui accroîtront le niveau d'interopérabilité tout en réduisant les coûts et les difficultés. Ces fonctionnalités doivent être prises en compte dès le début du projet.

2.2.2 Authentification, chiffrement et moyens technologiques de protection

Ces questions ont un impact sur la fiabilité des documents archivés. Les SAE doivent permettre de gérer efficacement les documents qui ont fait l'objet de mesures de protection technologique, telles que les signatures électroniques et tatouages numériques (gestion des droits numériques). Il est particulièrement important que ces systèmes assurent la permanence de l'intégrité des documents protégés par chiffrement ou signature électronique. Toutefois, si le chiffrement des données et la signature électronique jouent un rôle important pour garantir leur authenticité et leur intégrité lors de la transmission, ces moyens présentent aussi des risques pour la réutilisation des données lorsque les clés de déchiffrement et les clés publiques expirent avant l'échéance de la durée de conservation. C'est pourquoi il n'est pas recommandé d'archiver les documents sous forme chiffrée. Les métadonnées peuvent enregistrer les procédés de chiffrement et de déchiffrement et attester de la qualité du déchiffrement.

Quand la signature électronique est utilisée comme preuve de l'authenticité et de l'intégrité des documents archivés, on doit prendre en compte la gestion des clés. Les informations concernant la signature électronique et sa validation doivent être enregistrées dans les métadonnées.

2.3 Présentation des exigences fonctionnelles

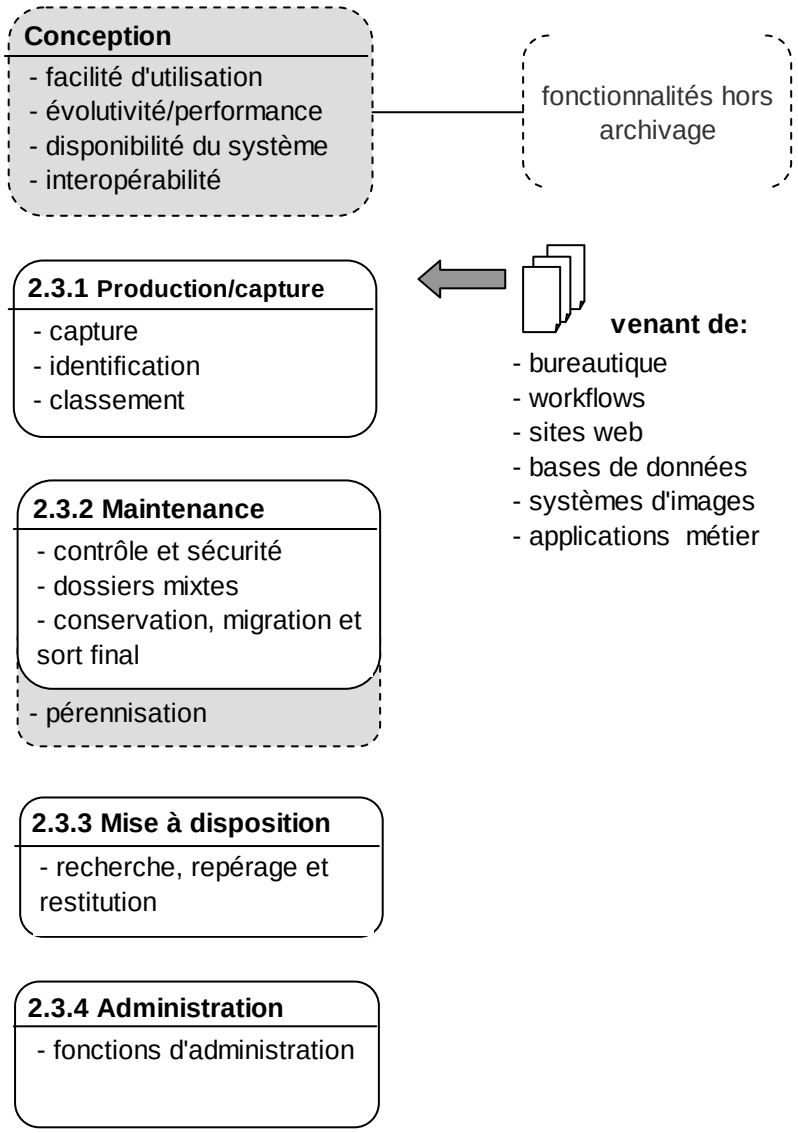
Cette section énumère et décrit sommairement les exigences fonctionnelles au travers d'un modèle conceptuel qui agrège les exigences pour faire ressortir leurs interrelations (figure 1). Le modèle vise d'abord à donner une vue globale aux lecteurs qui ne sont pas des professionnels de l'archivage.

Le module ne détaille pas les exigences pour la pérennisation des archives, les exigences communes à toutes les applications ni les fonctionnalités hors archivage, mais celles-ci sont indiquées dans le modèle conceptuel (en grisé). Les points d'intégration possible avec l'architecture informatique et les autres applications du système d'information apparaissent comme des sources d'alimentation du système.

Dans la partie 3, les exigences fonctionnelles sont regroupées en suivant le modèle conceptuel :

- production et capture
- maintenance
- mise à disposition
- administration

Figure 1 : Modèle conceptuel des exigences fonctionnelles pour un SAE



Notes:

- Les parties en grisé indiquent les fonctionnalités qui ne sont pas détaillées dans la partie 3 « Exigences fonctionnelles ».
- Ce modèle décrit les exigences fonctionnelles qui composent les SAE. Il ne décrit pas les étapes des processus gérés par un SAE.

2.3.1 Production et capture

Capture

En général, les SAE capturent, classent et identifient les documents engageants pour garantir que leur contenu, leur structure et leur contexte de production sont fixes dans le temps et l'espace. Ces processus d'archivage facilitent la constitution d'archives intègres, authentiques et exploitables. Une fonctionnalité permettant de créer un nouveau document en réutilisant contenu, structure et contexte des

documents déjà archivés est souhaitable. Le contrôle des versions et des documents dépasse les objectifs de ce module mais est toutefois abordé.

Agrégats

Ce sont des regroupements logiques de documents qui existent à un niveau supérieur à l'objet numérique simple (un fichier par exemple). Ils matérialisent le lien entre les documents et le système ou l'environnement au sein duquel ils ont été produits ; la notion d'agrégat est enregistrée dans les métadonnées ou au travers d'autres liens. Ces agrégats sont normalement contrôlés par le biais d'un plan de classement au sein du SAE.

Les SAE peuvent contenir des agrégats, des documents archivés individuellement ou les deux. Un agrégat structure un groupe de documents et facilite sa gestion et son utilisation. Les agrégats peuvent s'organiser sur plusieurs niveaux et posséder divers liens les uns avec les autres.

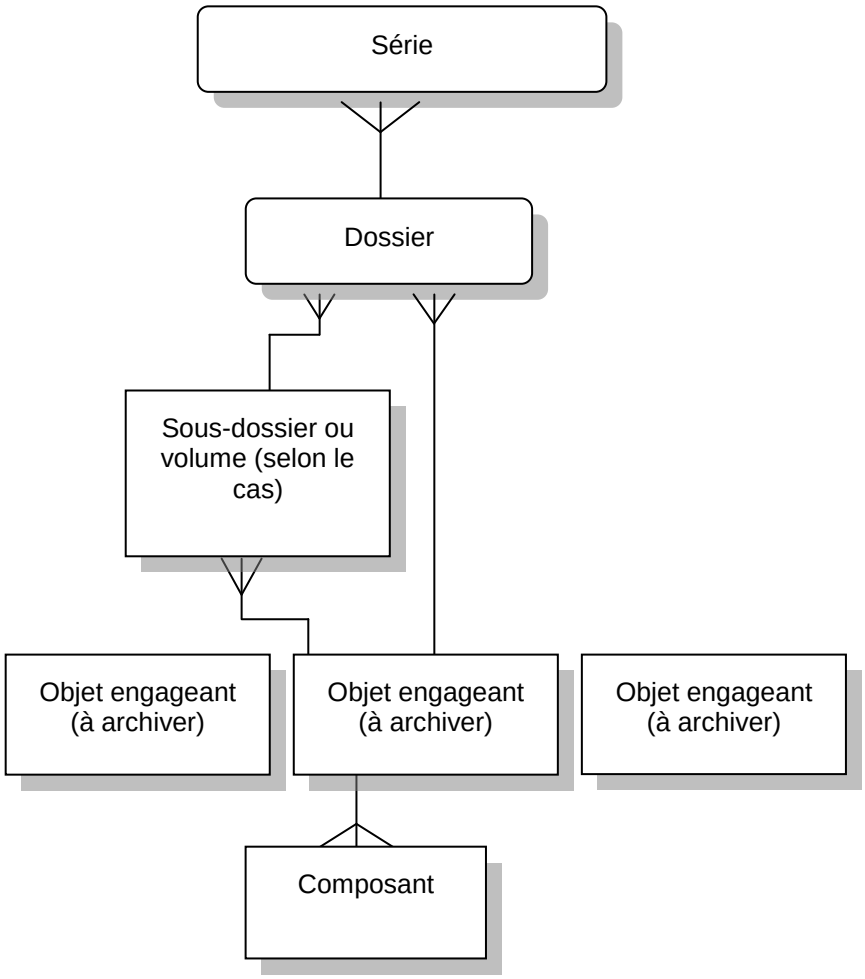
La nature du lien entre les documents électroniques d'un agrégat peut tenir à des caractéristiques ou des attributs communs, ou être d'ordre chronologique. Elle varie en fonction de facteurs tels que leur objet et leur structure, leur contenu et leur format.

Par exemple, un groupe de documents archivés électroniquement peut dans sa globalité constituer le récit d'événements (c'est-à-dire, une suite d'actions relevant du même processus) ; le lien est alors chronologique. Certains liens peuvent être définis par les métadonnées que sont le titre, la date, l'auteur, le numéro de dossier (s'il existe) ou d'autres données de ce type. Quand ces liens existent entre les documents importés ou extraits de systèmes métier externes, le SAE devrait être capable de les identifier, de les capturer, de les documenter et de les conserver.

Les agrégats peuvent matérialiser des liens formels ou structurels (par exemple, fichiers numériques rassemblant des documents numériques) ou peuvent être moins formalisés comme les relations de métadonnées établissant des liens entre les documents d'un agrégat.

Les agrégats doivent être fixés et conservés dans le temps. Tout changement dans un agrégat doit être enregistré et justifié. Ces agrégats ne devraient pas être confondus, ou remplacés par les regroupements documentaires, très différents, issus des réponses aux recherches ou des requêtes dans le système.

Figure 2 : les agrégats



Identification (enregistrement)

Pour contrôler son existence dans le système, tout document engageant, avec son agrégat doit être doté d'un identifiant unique et pérenne. Cela permet à l'utilisateur de localiser les documents archivés et facilite la distinction des versions.

Classement

Lors de la mise en œuvre des SAE, les agrégats sont souvent utilisés pour permettre l'héritage de caractéristiques par des documents produits ou associés à un niveau inférieur de l'agrégat. Dans les SAE, l'information est normalement gérée sous forme d'objets regroupés en séries ou en dossiers. Pour définir les agrégats les plus appropriés (par mission, par activité ou par action), les services devraient s'appuyer sur leurs propres besoins métier. Au sein d'un plan de classement métier, les caractéristiques contextuelles d'un document sont attribuées en les structurant en fonction de processus métier identifiables.

Les plans de classement thématiques permettront à des documents variés d'être regroupés si les activités et actions visent un même sujet (un immeuble, un client). Cependant, dans un classement thématique, le contenu du document est plus important que l'objectif ou l'activité pour lesquels il a été produit. Le contexte de l'activité métier peut se trouver ainsi être marginalisé rendant l'application du sort

final à des dossiers thématiques plus difficile si ces derniers regroupent des documents aux durées de conservation différentes.

Les plans de classement fonctionnels sont fondés sur l'analyse des missions et activités propres à l'entreprise/organisme et sont indépendants de sa structure administrative. Étant donné que les organisations et structures changent au cours du temps, cela rend le plan plus souple et pérenne. Ce système rompt avec l'organisation traditionnelle de l'information et facilite la conservation et l'application du sort final.

Plans de classement métier

Un plan de classement métier est un outil de classement hiérarchique qui peut faciliter la capture des documents engageants (à archiver), leur nommage, leur repérage, leur conservation et l'application du sort final. Il définit les modalités de regroupement des documents (agrégats) et leur lien au contexte de production ou de diffusion. Par exemple, dans un SAE à l'échelle de l'entreprise/organisme, les documents individuels peuvent être constitués en séries avec chacun leurs composantes et leurs métadonnées contextuelles ou peuvent faire l'objet de dossiers. (A noter que ces termes sont purement indicatifs, différents SAE utilisant différentes terminologies). Les documents sont souvent regroupés selon un plan de classement fonctionnel à trois niveaux, avec trois niveaux de granularité. Exemple :

Figure 3 : Plan de classement fonctionnel à trois niveaux

Niveau 1	Mission
Séries consistant en agrégats de dossiers qu'on peut appeler « classes » ou « catégories ».	
Niveau 2	Activité
Dossiers constitués par le regroupement de documents individuels et qu'on peut appeler « contenants ». Ils peuvent se diviser en volumes.	
Niveau 3	Action
Objets, appelés ici « document engageant » et pouvant être constitués de composants multiples.	

Note : Ceci est un modèle de base. Les plans de plus de trois niveaux peuvent être nécessaires en fonction des processus métier décrits ou pour une perception plus claire des sujets complexes.

Le document engageant (objet) se situe tout en bas de la hiérarchie. Certaines métadonnées peuvent être héritées d'un niveau supérieur de l'arborescence par tous les dossiers ou objets situés en dessous. Quel que soit le nombre de niveaux inférieurs dans l'arborescence, chaque niveau devrait répondre aux exigences de métadonnées du niveau supérieur.

2.3.2 Maintenance

Authenticité et fiabilité des documents archivés

Les documents capturés dans les SAE doivent faire l'objet d'une maintenance active pour garantir une accessibilité permanente. L'établissement de contrôles de sécurité appropriés, la préparation des destructions et la possibilité de gérer des dossiers mixtes facilitent la constitution d'archives exhaustives, authentiques, exploitables et inviolables et, le cas échéant, correctement détruites.

Contrôles et sécurité

Les documents capturés dans les SAE doivent être en permanence protégés contre toute modification intentionnelle ou accidentelle de leur contenu, structure et contexte, afin de préserver leur authenticité. Les SAE doivent contrôler l'accès aux métadonnées et leur modification. La traçabilité de la localisation, les contrôles des accès et des modifications apportées aux documents garantissent l'authenticité des documents archivés électroniquement.

L'archivage mixte

Les supports des documents engageants (à archiver) sont généralement très variés, électroniques ou non. Les SAE doivent être en mesure d'intégrer et de gérer les métadonnées des documents non électroniques aussi bien que celles des documents électroniques, ainsi que toutes les métadonnées associées. Qu'ils soient sous une forme électronique ou non, il est essentiel que les documents relevant d'un même contexte de production et appartenant au même agrégat obéissent aux mêmes processus d'archivage.

Afin de faciliter les fonctionnalités d'archivage mixte, le SAE doit pouvoir capturer et conserver les métadonnées des documents physiques. Cela nécessite la création de pointeurs, pour gérer les documents conservés physiquement hors de l'application métier. Les pointeurs contiennent les métadonnées nécessaires à la localisation et à la gestion des archives physiques et permettent ainsi un contrôle de gestion. Un pointeur peut renvoyer à un document physique, tel qu'un plan ou un dossier papier, ou à un document ou dossier électronique stocké sur un support amovible, tel qu'un CD-ROM ou une bande magnétique.

Conservation et destruction

Les référentiels de conservation sont des règles qui autorisent l'application du sort final, soit par une destruction, soit par un transfert, soit par l'attribution d'une nouvelle durée. Les référentiels de conservation définissent les durées de conservation et les actions de sort final des dossiers produits dans un contexte réglementaire ou métier. Les entreprises/organismes devraient réviser les sorts finaux à échéance des durées de conservation.

Les documents archivés sont souvent transférés d'un système d'archivage à un autre pour d'autres motifs que leur destruction, par exemple en cas de migration vers un nouveau système d'archivage à la suite d'un rafraîchissement technologique ou d'une réorganisation. Dans tous les cas de transfert (vers un autre SAE ou ailleurs) et/ou de destruction des documents dans le système d'archivage d'origine, toutes les métadonnées d'archivage et de capture doivent être prises en compte en même temps que les documents eux-mêmes.

2.3.3 Mise à disposition

Un SAE doit être en mesure de rechercher, repérer et restituer les documents archivés. Ces fonctionnalités facilitent l'exploitation des documents.

Le processus de recherche consiste à identifier les documents ou agrégats à partir de paramètres définis par l'utilisateur pour le repérage des documents, agrégats et métadonnées. La localisation des documents, agrégats et métadonnées d'archivage nécessite des outils de recherche et de navigation utilisant différentes techniques de requête pour répondre aux besoins des utilisateurs novices et confirmés. Le processus de repérage consiste à préparer les documents pour leur restitution et leur visualisation.

La restitution consiste à produire une représentation du document archivé lisible par l'homme, en général au moyen d'un affichage sur écran ou d'une impression papier. Les SAE conservent généralement des documents dans des formats variés. Une interface de restitution appropriée doit permettre à l'utilisateur de lire les documents, quel que soit leur format. Lorsque cela est pertinent, le SAE doit fournir des fonctionnalités permettant à tous les utilisateurs d'imprimer les documents ainsi que leurs métadonnées si nécessaire.

2.3.4 Administration

Comme pour la plupart des applications, un administrateur système est nécessaire pour assurer la maintenance du système et des autres fonctions supports, telles que la gestion des profils d'accès et la mise à jour du plan de classement métier. L'administration favorise l'exploitation des documents archivés, la fiabilité des systèmes, l'usage et l'application systématique des procédures d'archivage. Ce module traite uniquement de l'administration des documents archivés qui doit être contrôlée et auditable afin d'assurer leur intégrité, leur authenticité et leur fiabilité..

2.4 Utilisation des exigences fonctionnelles

La troisième partie énumère les exigences fonctionnelles pour l'archivage des documents engageants dans les systèmes électroniques. Elles sont regroupées en fonction des blocs modélisés en figure 1.

2.4.1 Éléments clés

Les exigences fonctionnelles insistent sur les éléments clés d'une gestion appropriée des documents engageants quel que soit le type de SAE utilisé. Dans la mesure où les exigences fonctionnelles décrivent sommairement plutôt qu'en détail les fonctionnalités d'archivage, il est évident que la technique et la stratégie pour atteindre les résultats dépendront du type de système utilisé. Chaque entreprise/organisme est censé(e) ajuster les exigences fonctionnelles à ses propres besoins.

2.4.2 Niveaux d'obligation

Les termes « doit », « devrait » et « peut » qui apparaissent dans les exigences de la troisième partie indiquent l'importance relative de chacune. Ils doivent être compris comme suit :

- « Doit » : exigence d'une nécessité absolue en termes de conformité.

- « Devrait» : exigence dont il est possible de ne pas tenir compte en cas de raison valable. Dans ce cas, les conséquences doivent être bien appréhendées et considérées avec attention.
- « Peut » : exigence optionnelle qui peut être prise en compte ou omise selon qu'elle s'avère opportune ou non.

Ce document reflète un consensus international ; exigences et niveaux d'obligation ne sont pas spécifiques à un État ou à une réglementation nationale. Les utilisateurs sont invités à prendre en compte leur propre environnement réglementaire, leurs exigences métier voire l'évaluation des risques.

2.4.3 Risques et faisabilité face à la non-satisfaction de ces exigences

Le risque est un facteur important qui devrait être pris en compte dans la gestion de l'archivage en appliquant ces niveaux d'obligation et d'exigence. Les risques peuvent consister en une mauvaise publicité, une désorganisation des activités, un affaiblissement de la production et une incapacité partielle de l'entreprise/organisme à engager des poursuites ou à se défendre.

Il existe une large gamme d'exigences pour assurer la traçabilité des activités. Si on estime que telle ou telle exigence n'est pas satisfaite, une analyse des risques et de la faisabilité peut aider à définir un plan d'action approprié et à décider en toute responsabilité.

Les entreprises/organismes peuvent avoir leur propre politique de gestion des risques avec différents niveaux de risques ; on peut les utiliser pour choisir les exigences prioritaires au regard de la preuve.

L'analyse de faisabilité peut aider à évaluer méthodiquement les possibilités financières, techniques, légales ou opérationnelles.

3 EXIGENCES FONCTIONNELLES

Cette partie présente l'ensemble des exigences fonctionnelles nécessaires dans un environnement électronique. Elles sont divisées en quatre sections selon les concepts et processus clés de la gestion de l'archivage présentés dans la partie 2 «Lignes directrices » :

- production et capture
- maintenance
- mise à disposition
- administration

Les exigences fonctionnelles se concentrent sur les éléments indispensables à un archivage approprié des documents engageants. Elles ne préconisent pas de processus particuliers, car il est évident que la technique et la stratégie pour atteindre l'objectif dépendront de l'organisation et du SAE utilisé. L'introduction de chaque section résume le concept d'archivage abordé et la finalité principale des exigences présentées.

Bien que les exigences communes de conception et de gestion des systèmes telles que l'interopérabilité, la capacité d'expansion et la performance ne soient pas abordées, il est clair qu'elles sont de nature à faciliter les fonctionnalités d'archivage du système. Les exigences fonctionnelles supposent qu'une structure basique de gestion de l'archivage existe, comme une politique, des procédures, des règles de conservation et un plan de classement métier.

PRODUCTION ET CAPTURE

3.1 Capture

Les documents engageants (à archiver) sont produits sous divers formats, pouvant comprendre plusieurs objets particuliers (documents composites), et sont transmis via des moyens de communication très variés (workflows, courrier électronique ou postal, etc.). Un SAE doit capturer le contenu, la structure et le contexte des documents engageants afin de garantir qu'ils sont des témoins fiables et authentiques des activités et des actions qui les ont créés ou transmis. Il s'agit des métadonnées de capture, qui devraient elles-mêmes être archivées ; il ne devrait pas être possible de modifier ces métadonnées sans que cela soit tracé et auditable.

3.1.1 Processus de capture

Un SAE **doit** :

1	Permettre une intégration avec les applications métier de manière à ce que les documents engageants produits par ces applications soient capturés dans le SAE (y compris les courriels, voir exigences 21-25).
2	Signaler quand un document engageant est capturé dans le SAE.

3	Empêcher la modification du contenu de tout document par tout utilisateur ou administrateur pendant le processus de capture. Voir aussi exigences 88 et 89.
4	Empêcher tout utilisateur, y compris l'administrateur, de détruire ou de supprimer tout document, sauf en cas de : • - destruction autorisée par un référentiel de conservation (voir section 3.6 « Conservation et destruction ») ; et • - suppression autorisée par un administrateur (voir section 3.8 « Administration »)
5	Permettre le nommage manuel de documents électroniques et accepter que ce nom soit différent du nom du fichier numérique (y compris les « objets » des courriels utilisés comme titre des documents). Si le nom du fichier est pris par défaut, le SAE doit autoriser la modification de ce nom au moment de la capture.
6	Autoriser l'administrateur à modifier si nécessaire les métadonnées d'un document afin de permettre la finalisation/correction du profil du document. Toute action de ce type doit être enregistrée dans les métadonnées d'archivage.
7	Toute révision ou modification d'une métadonnée d'archivage/de capture doit elle-même être enregistrée et ajoutée aux métadonnées.
8	Alerter l'utilisateur en cas d'échec de capture d'un document.
9	Pouvoir, à bon escient, produire une alerte si un utilisateur tente de capturer un document incomplet ou incohérent, dont l'authenticité pourrait être remise en cause.

3.1.2 Métadonnées de capture

Pour être une preuve valable d'un processus métier, les documents archivés doivent être replacés dans leur contexte de production et d'utilisation. C'est pourquoi, le document doit être associé à des métadonnées relatives à son contexte de production et au moment de sa capture.

La plupart de ces informations peuvent être générées automatiquement par le système. Chaque service ou entité capturera des métadonnées d'archivage selon une norme de métadonnées d'archivage (en conformité avec ISO 23081), et ses exigences organisationnelles ou réglementaires.

Le SAE **doit** :

10	Permettre l'utilisation de métadonnées pérennes.
11	Capturer des métadonnées pour chaque document archivé et maintenir un lien durable entre eux.
12	Garantir que les valeurs des métadonnées sont conformes aux schémas d'encodage définis.
13	Permettre à l'administrateur de prédéfinir (et redéfinir) les métadonnées associées à chaque document, en précisant le caractère obligatoire ou optionnel de chacune.

14	Permettre aux utilisateurs de voir toutes les métadonnées d'un document, sous réserve des droits d'accès alloués aux personnes et aux groupes.
15	Enregistrer automatiquement parmi les métadonnées la date et l'heure de capture de chaque document.
16	Permettre l'extraction automatique ou la migration des métadonnées à partir de : • l'application logicielle qui a créé le document, • un système d'exploitation ou un système métier, • un SAE, ou encore • l'en-tête du fichier, y compris le format de fichier, de chaque document et de ses composants capturés dans le système.
17	Empêcher la modification des métadonnées capturées selon l'exigence 16, sauf si l'administrateur système l'autorise.
18	Permettre l'ajout de métadonnées supplémentaires par les utilisateurs pendant la capture des documents et/ou à un stade ultérieur.
19	Garantir que seuls les utilisateurs habilités et les administrateurs peuvent modifier le contenu des métadonnées d'archivage.
20	Attribuer automatiquement à chaque document un identifiant, unique dans le système, au moment de la capture.

3.1.3 Agrégats électroniques

Les agrégats électroniques sont des regroupements logiques de documents électroniques dont la combinaison forme une entité à un niveau supérieur au simple document ou objet électronique ; les dossiers peuvent être regroupés eux-mêmes en série. Ces relations apparaissent dans les métadonnées de liens et dans les liens qui existent entre les documents électroniques ou entre les documents et le système. Par exemple, un groupe de documents archivés électroniquement peut dans sa globalité constituer le récit d'événements (c'est-à-dire, une suite d'actions relevant du même processus) ; le lien est alors chronologique. Certains liens peuvent être définis par les métadonnées que sont le titre, la date, l'auteur, le numéro de dossier (s'il existe) ou d'autres données de ce type. Quand ces relations entre les documents contrôlés par le SAE existent, le système devrait être capable de les identifier, de les capturer, de les documenter et de les maintenir ou de les détruire de manière systématique.

Le SAE **doit** :

21	Garantir que les documents capturés dans le SAE sont rattachés à au moins un agrégat.

22	Gérer l'intégrité de tous les pointeurs ou autres repères liés aux documents (s'il y en a) pour garantir que : • un pointeur permettra toujours de repérer correctement le document, quel que soit son agrégat de rattachement ; et • tout changement de localisation d'un document se traduit par la mise à jour systématique de son pointeur de référence.
23	Ne pas imposer de limites au nombre de documents pouvant être capturés dans un agrégat, ou au nombre de documents pouvant être stockés dans le SAE. Toutefois, le système peut permettre à l'administrateur de poser des limites à la quantité d'objets dans un agrégat si les besoins métier le justifient.
24	Permettre aux utilisateurs de sélectionner au moins l'un des choix suivants lorsqu'un objet électronique a plus d'une version : • enregistrer toutes les versions de l'objet comme un seul document ; • enregistrer une seule version de l'objet comme un document ; ou • enregistrer chaque version de l'objet comme un document distinct.

Le SAE **devrait** :

25	Donner la possibilité de rattacher des documents à plusieurs agrégats sans les dupliquer.[5]

3.1.4 Import de masse

Les documents engageants (à archiver) et leurs métadonnées peuvent être capturés en masse dans un SAE de plusieurs manières, par exemple, depuis un autre SAE ou par un transfert massif depuis un système de gestion électronique de documents ou d'un système de workflow. Le SAE doit être capable d'accepter ces imports et doit inclure des fonctionnalités pour gérer le processus d'import de masse.

Le SAE **doit** :

[5] Par exemple, une facture pourra, à l'aide d'un système de pointeurs, être ajoutée au dossier d'un fournisseur par un utilisateur, et au dossier d'un produit par un autre.

26	Pouvoir capturer en masse des documents provenant d'autres systèmes, y compris : • des documents électroniques dans leur format natif, sans dégradation de leur contenu ou de leur structure, ni perte des relations contextuelles entre les composants de chaque document ; • des documents électroniques avec leurs métadonnées d'archivage associées, en préservant les relations contextuelles entre chaque document et ses métadonnées ; • la structure des agrégats de documents, avec leurs métadonnées d'archivage en préservant les relations pertinentes entre les documents et les agrégats.[6]
27	Pouvoir importer toute métadonnée de l'historique des événements directement associée au document et/ou à l'agrégat, tout en la maintenant dans la structure d'origine.

3.1.5 Formats électroniques

Les SAE devront gérer plusieurs types de formats : ceux des applications courantes et, bien souvent, les formats spécifiques des outils métier. Un SAE doit être doté de capacités fonctionnelles prenant en charge les formats courants ou couramment utilisés dans tel environnement. Ces aspects varieront d'un système à l'autre et d'un(e) entreprise/organisme à l'autre.

Pour faciliter la migration des données et les procédures d'export, l'utilisation de formats ouverts ou de formats standard offrira un niveau plus élevé d'interopérabilité et réduira les coûts et les difficultés qu'implique une conservation efficace des documents engageants.

Le SAE **doit** :

28	Faciliter la capture des documents à archiver dans leur format natif à partir de logiciels d'usage courant tels que les : • outils bureautiques classiques (traitement de texte, tableur, présentation, base de données), • clients de messagerie, • outils de traitement d'images, • outils de conception de pages web.
29	Être en mesure d'élargir la gamme des formats gérés au fur et à mesure de l'apparition de nouveaux formats de production ou de conservation (par exemple, PDF/A).[7]

[6] Par exemple, en conservant durablement parmi les métadonnées une trace du plan de classement originel.

[7] Il peut arriver que la capture de certains documents ou des documents de certains systèmes spécialisés ne soit pas possible ; il faut tenter de réduire le risque, notamment par une démarche de normalisation des formats de capture ou une capture de l'ensemble

3.1.6 Documents composites

Les documents électroniques à archiver sont constitués d'au moins un composant. Un texte par exemple formera généralement un document individuel constitué d'un objet unique. Un document électronique composé de plus d'un composant ou de fichiers multiples, par exemple un rapport technique volumineux auquel seraient associés des liens dynamiques vers des diagrammes et des feuilles de calculs, peut être qualifié de « document composite ».

La nature des composants d'un document archivé électroniquement est variable. Un composant peut être un objet électronique, tel qu'un fichier électronique, ou une donnée, telle une entrée dans une base de données. A titre d'exemple, le composant d'un document archivé électroniquement dans un système de gestion documentaire peut consister en un simple fichier texte, alors que les composants d'un document électronique dans un système de gestion des ressources humaines correspondent à toute une série de données interconnectées dans une base de données (par exemple, toutes les informations concernant le profil personnel d'un employé). Il ne faut pas confondre ces composants avec les composants ou éléments associés à un document archivé, telles que les métadonnées d'un fichier électronique ou le pointeur d'un document physique.

Le SAE **doit :**

30	Capturer le document électronique composite dans son ensemble (s'il y a plus d'un élément) de façon à : • préserver les liens entre les composants constitutifs du document composite ; • préserver l'intégrité de la structure de chaque document composite ; et • restituer, présenter et gérer le document composite comme un tout.
31	Capturer de préférence le document électronique composite en une seule action, par exemple, en un seul clic.

3.1.7 Messagerie électronique

La messagerie électronique est utilisée pour envoyer de simples messages ou des documents (pièces jointes), au sein et entre les entreprises/organismes. Les caractéristiques mêmes du courriel rendent sa traçabilité et son enregistrement difficiles. Les entreprises/organismes doivent donner aux utilisateurs les moyens de sélectionner et de capturer certains messages avec leurs pièces jointes.

Le SAE **doit :**

32	Permettre aux utilisateurs de capturer les courriels (textes et pièces jointes) soit comme un seul objet, soit individuellement en les reliant par des métadonnées.

du système. A défaut, on verra à installer des fonctionnalités d'archivage dans le système métier.

33	Permettre à un utilisateur de capturer les messages (et leurs pièces jointes) à partir de son application de messagerie.
34	Permettre aux utilisateurs le choix de capturer : • le texte du message uniquement, • le texte et ses pièces jointes, ou • les pièces jointes uniquement.[8]
35	Garantir que les données de transmission sont capturées en tant que métadonnées et liées de façon pérenne au courriel archivé.
36	Rendre impossible, après capture, toute modification d'un courriel et de ses données de transmission. L'objet d'un courriel ne devrait pas non plus être modifiable, bien que le nom du document puisse être corrigé pour le rendre plus facilement accessible, par l'utilisation, par exemple, de mots-clés ou de règles de nommage de fichiers.
37	Garantir que la version « en clair » de l'adresse du courriel capturé, quand elle existe, est également capturée.[9]

3.2 Identification

Afin de vérifier leur existence dans le système, chaque document archivé et chaque agrégat doivent avoir un identifiant unique permanent. Cela permet à l'utilisateur de localiser les documents et l'aide à distinguer les différentes versions.

Le SAE **doit** :

38	Associer un identifiant unique à chacun des éléments suivants : • document, • extrait d'un document, et • agrégat.
39	Exiger que, au sein du SAE, les identifiants soient uniques et ne puissent être dupliqués.
40	Pouvoir stocker les identifiants uniques comme métadonnées des entités concernées.
41	*Soit*, générer automatiquement les identifiants uniques en empêchant les utilisateurs de saisir manuellement la référence ou de la modifier *a posteriori* (par exemple, un numéro séquentiel).
42	*Soit*, permettre aux utilisateurs de saisir un identifiant unique, mais en vérifier l'unicité avant validation (par exemple, un numéro de compte).
43	Permettre que le format de l'identifiant unique soit défini au moment de la configuration du système.[10]

[8] Il est essentiel que ces choix soient enregistrés et embarqués dans les métadonnées du document archivé. L'utilisateur doit être informé de l'existence des liens.

[9] Pour 'Samuel Johnson'<samjo@worldintnet.org>, par exemple, 'Samuel Johnson' est la version lisible et non ambiguë de l'adresse courriel samjo@worldintnet.org

Quand les identifiants sont générés automatiquement, le SAE **devrait** :

44	Permettre à l'administrateur de spécifier lors de la configuration, le numéro de base (par exemple : 1, 10, 100) et le type d'incrémentation (par exemple : 1, 10).

3.3 Classement

3.3.1 Élaboration d'un plan de classement

Un plan de classement est un outil de classification hiérarchique qui peut faciliter la capture, le nommage, le repérage, la maintenance et la destruction des documents engageants. Le plan de classement est au cœur de tout SAE puisqu'il définit la façon dont les documents archivés individuellement sont regroupés (agrégés) et liés à leur contexte de production ou de réception. En regroupant les documents, la plupart des processus d'archivage décrits ci-après peuvent être appliqués rapidement et efficacement.

Le SAE **doit** :

45	Permettre et être compatible avec le plan de classement de l'entreprise/organisme.
46	Pouvoir gérer un plan de classement reflétant les agrégats de documents dans une organisation hiérarchique d'au moins trois niveaux (mission, activité, action).
47	Permettre l'héritage des valeurs à partir du plan de classement.
48	Permettre que les règles de nommage ou les thésaurus soient définis au moment de la configuration du système.
49	Faciliter l'élaboration et la maintenance du plan de classement.
50	Permettre aux administrateurs de créer de nouveaux agrégats sous un agrégat déjà existant.
51	Ne pas limiter le nombre de niveaux hiérarchiques du plan de classement sauf décision de l'administrateur.
52	Permettre de définir les différents types de documents associés à un jeu de métadonnées applicable au moment de la capture.
53	Permettre l'attribution d'identifiants uniques aux documents archivés, selon la structure du plan de classement.

Lorsque les identifiants uniques sont basés sur une numérotation séquentielle, le SAE **devrait** :

[10] L'identifiant peut être numérique ou alphanumérique, ou reposer sur la concaténation des identifiants du volume et des agrégats dont l'entité concernée relève dans le plan de classement.

54	Pouvoir générer automatiquement le numéro séquentiel de tout nouveau document ajouté à un agrégat électronique au sein du plan de classement.[11]

Le SAE **peut :**

55	Offrir la possibilité d'un plan de classement partagé et maintenu par un réseau de centres d'archives électroniques.

Lorsque le SAE utilise une interface graphique, il **doit**

56	Fournir un outil de recherche et de navigation dans les agrégats et le plan de classement et permettre la sélection, le repérage et l'affichage des agrégats électroniques et de leurs contenus à l'aide de cet outil.

Le SAE **devrait** :

57	Permettre l'élaboration et l'utilisation simultanées de plusieurs plans de classement. Cela peut être nécessaire, par exemple, dans le cadre de la fusion de deux entreprises ou de la migration de systèmes existants. Cela n'est pas utile en temps normal.

3.3.2 Niveaux de classement

Le SAE **doit** :

58	Gérer les métadonnées des différents niveaux du plan de classement.
59	Fournir au moins deux mécanismes de nommage pour les documents du plan de classement : • un mécanisme d'attribution d'un code alphabétique, numérique ou alphanumérique (c'est-à-dire un identifiant unique au sein du plan de classement) pour chaque niveau du classement ; et • un mécanisme d'attribution d'un titre pour chaque agrégat électronique. Il doit être possible d'utiliser ces identifiants séparément ou conjointement.
60	Restreindre aux seuls utilisateurs habilités la possibilité de créer de nouvelles rubriques au sommet du plan de classement (par exemple pour le niveau « missions »).

[11] Par exemple, si le plan de classement comprend les agrégats suivants:

900 - 23 – 01 Fabrication : traitement des commandes : validation des bons de commande ;

900 - 23 – 02 Fabrication : traitement des commandes : facturation ;

900 - 23 – 03 Fabrication : traitement des commandes : traitement des avoirs ;

et si l'administrateur ajoute un nouvel agrégat à « traitement des commandes », le SAE devrait lui attribuer automatiquement la référence 900 - 23 – 04. De même, si l'administrateur ajoute une nouvelle série à « fabrication », le SAE devrait lui attribuer automatiquement la référence 900 – 24.

61	Enregistrer la date d'ouverture d'un nouvel agrégat dans ses métadonnées d'archivage.
62	Inclure automatiquement dans les métadonnées d'archivage d'un nouvel agrégat les attributs qui découlent de sa position dans le plan de classement (par exemple, l'intitulé et le code de classement).[12]
63	Permettre la création et la mise à jour automatiques d'une liste de niveaux de classement.

Le SAE **devrait** :

64	Permettre un mécanisme de nommage reposant sur les termes d'un vocabulaire contrôlé et leurs relations (le cas échéant) - issus d'un thésaurus conforme aux normes ISO 2788 ou ISO 5964 - et assurer l'articulation entre le thésaurus et le plan de classement.
65	Proposer un mécanisme de nommage optionnel intégrant les noms (par exemple, les noms de personnes) et/ou les dates (par exemple, les dates de naissance) dans les noms des fichiers avec la possibilité de valider les noms par rapport à une liste.
66	Proposer l'attribution d'un vocabulaire contrôlé - conforme aux normes ISO 2788 ou ISO 5964 - pour les métadonnées, venant s'ajouter aux autres recommandations de cette section.

3.3.3 Processus de classement

Le SAE **doit** :

67	Permettre qu'un agrégat électronique (et ses volumes) soit déplacé vers une autre branche du plan de classement, tout en s'assurant que tous les documents électroniques associés restent associés aux agrégats et volumes déplacés.[13]
68	Permettre qu'un document électronique soit reclassé dans un autre volume du même agrégat.[14]
69	Réserver aux administrateurs du système, la possibilité de déplacer les agrégats (avec leurs volumes) et les documents.

[12] Par exemple, si un dossier se trouve au niveau hiérarchique : « Plan de développement régional : appel d'offres : offres reçues » et que l'administrateur ajoute un nouveau fichier intitulé « objections formelles » au même niveau que le fichier « offres reçues », ce fichier doit automatiquement hériter du préfixe « Plan de développement régional : appel d'offres ».

[13] Cette fonction est prévue lors de circonstances exceptionnelles telles que les fusions et les réorganisations, ou pour corriger des erreurs d'écriture. Cette exigence doit être lue conjointement avec les exigences 71, 72 et 80.

[14] Cette fonction est prévue lors de circonstances exceptionnelles : notamment pour corriger des erreurs d'écriture. Cette exigence doit être lue conjointement avec les exigences 71, 72 et 80.

70	Garder la trace de la localisation avant reclassement des agrégats déplacés (avec leurs volumes) de façon à pouvoir facilement en reconstituer l'historique.[15]
71	Ne jamais autoriser la suppression d'un agrégat électronique ou d'une partie de son contenu, à l'exception de : • la destruction conforme à un référentiel de conservation ; et • la suppression par un administrateur dans le cadre d'une procédure de contrôle.
72	Permettre la clôture d'un agrégat électronique par une procédure spécifique de l'administrateur, et restreindre cette fonction à un administrateur.
73	Enregistrer la date de clôture d'un volume dans les métadonnées de gestion des documents de ce volume.
74	Maintenir en permanence l'intégrité interne (intégrité relationnelle ou autre) du système, quels que soient : • les opérations de maintenance, • les autres actions des utilisateurs, et • la défaillance des composants du système.[16]
75	Ne pas permettre qu'un volume temporairement ré-ouvert par l'administrateur, reste ouvert après que celui-ci se soit déconnecté du système.
76	Permettre aux utilisateurs de créer des références croisées entre les agrégats interdépendants ou entre des agrégats et des documents indépendants.
77	Fournir des outils de reporting à l'administrateur pour qu'il puisse établir des statistiques sur l'activité du plan de classement : nombre d'agrégats (avec leurs volumes) et de documents créés, clos ou supprimés dans une période donnée, par un groupe d'utilisateurs ou un profil.
78	Permettre aux utilisateurs habilités de saisir le motif de reclassement des agrégats (avec leurs volumes) et des documents.

[15] *A minima*, cette information doit être stockée dans les métadonnées. On peut souhaiter l'enregistrer également ailleurs, par exemple dans les métadonnées des objets déplacés.

[16] C'est-à-dire qu'il doit être impossible que l'action d'un utilisateur ou une défaillance du logiciel puisse entraîner des anomalies dans le SAE ou ses bases de données.

79	Pouvoir clore automatiquement le volume d'un agrégat électronique en fonction de critères spécifiques définis lors de la configuration du système, soit au minimum : • les volumes délimités par une date de clôture annuelle (par exemple fin de l'année civile, année budgétaire ou autre cycle annuel) ; • le temps écoulé après un événement précis (par exemple, l'ajout du dernier document dans ce volume) ; et • le nombre de documents électroniques contenus dans un volume.[17]
80	Pouvoir ouvrir automatiquement un nouveau volume dans un agrégat électronique en fonction de critères définis lors de la configuration du système.
81	Permettre à l'administrateur de verrouiller ou de geler des agrégats pour éviter leur déplacement, leur suppression, leur clôture ou leur modification, lorsque les circonstances l'exigent, par exemple lors d'une action judiciaire.

3.3.4 Volumes

Cette section aborde les exigences relatives à l'utilisation des volumes qui servent à subdiviser les agrégats trop volumineux lesquels, sinon, seraient difficilement gérables. Ces exigences ne s'appliquent qu'aux agrégats de niveau « activité » [niveau 2]. Elles sont avant tout utiles pour les dossiers physiques dans les systèmes mixtes.

Lorsque le SAE utilise les volumes, il **doit**:

82	Autoriser les administrateurs à ajouter (ouvrir) un volume à n'importe quel agrégat électronique qui n'est pas clos.
83	Enregistrer la date d'ouverture d'un nouveau volume dans ses métadonnées d'archivage.
84	Inclure automatiquement dans les métadonnées des nouveaux volumes les métadonnées d'archivage des agrégats dont ils dépendent et qui en précisent le contexte (par exemple, intitulé, code de classement).
85	Respecter les principes suivants pour l'ouverture et la clôture des volumes dans les agrégats : • seul le volume le plus récent créé au sein d'un agrégat peut être ouvert ; et • tous les autres volumes dans cet ensemble doivent être clos (sauf exception temporaire conforme à l'exigence 68).[18]

[17] D'autres critères peuvent être retenus selon les circonstances, par exemple lorsque la taille du volume dépasse la capacité de stockage du support.

[18] A noter que l'on peut accéder aux documents d'un volume indépendamment du fait que celui-ci soit ouvert ou clos.

86	Empêcher les utilisateurs d'ajouter des documents électroniques à un volume clos (sauf exception temporaire conforme à l'exigence 68).
87	Permettre à un utilisateur habilité d'ajouter des documents électroniques à un dossier clos.[19]

MAINTENANCE

3.4 Gestion de l'authenticité et de la fiabilité

3.4.1 Accès et sécurité

Les entreprises/organismes ont besoin de contrôler l'accès à leurs archives. Normalement, l'accès aux documents et agrégats est limité à certains utilisateurs ou groupes d'utilisateurs. On peut avoir besoin d'aller plus loin et de mettre en place des classifications de sécurité. Cela se traduit par l'attribution de niveaux de sécurité aux agrégats et documents. Des habilitations permettant un accès sélectif aux agrégats et documents de niveaux de sécurité supérieurs peuvent alors être données aux utilisateurs.

Conserver les métadonnées retraçant toutes les actions effectuées par le SAE, ses utilisateurs et ses administrateurs est essentiel pour garantir la recevabilité juridique. Le volume de ces métadonnées peut devenir important si toutes les actions sont consignées. C'est pourquoi la direction peut considérer que certaines actions n'ont pas lieu d'être enregistrées. Le plus souvent, les métadonnées, d'abord conservées en ligne, sont périodiquement transférées sur support hors-ligne et détruites en même temps que les documents concernés, un enregistrement récapitulatif étant conservé. Ce processus est aussi appelé « traçabilité ».

Au fil du temps, les documents et agrégats peuvent être transférés d'un support ou d'un lieu de stockage à un autre (par exemple, lors d'une migration), lorsque leur usage et le besoin d'y accéder décroissent. Tout changement de localisation doit être tracé à la fois pour des questions d'accès et de respect des exigences réglementaires.

Le SAE **doit** :

88	Garantir que les documents archivés restent complets et intègres, sauf en cas de modification du contenu de documents ou de métadonnées ordonnée par une décision de justice. Dans ce cas, seuls les administrateurs du système dûment habilités peuvent procéder aux changements.
89	Enregistrer, dans les métadonnées appropriées, tout changement exceptionnel évoqué dans l'exigence 88.
90	Préserver l'intégrité technique et structurelle des documents et des métadonnées ainsi que leurs relations dans le système.

[19] Cette possibilité permet de rectifier une erreur d'utilisateur, par exemple si un volume a été clos par inadvertance.

3.4.2 Contrôles d'accès

Le SAE doit :

91	Restreindre l'accès aux fonctions du système conformément au profil de l'utilisateur et aux stricts contrôles de l'administration du système.[20]

3.4.3 Mise en place de contrôles de sécurité

Les systèmes standard de contrôle d'accès et de sécurité aident à préserver l'authenticité, la fiabilité, l'intégrité et l'exploitabilité et devraient donc être convenablement installés.

Une évaluation des risques peut éclairer les prises de décisions sur le besoin et le niveau de ces contrôles. Par exemple, dans un environnement à haut risque, il peut être nécessaire de prouver exactement ce qui a été fait, quand et par qui. Ceci renvoie aux habilitations et aux journaux d'audit du système si on veut prouver que toutes les opérations sont effectuées par des utilisateurs habilités.

Le SAE **doit :**

92	Permettre aux seuls administrateurs de configurer des profils utilisateurs et d'affilier les utilisateurs à des groupes.
93	Permettre à l'administrateur de réserver l'accès aux documents, aux agrégats, et aux métadonnées à certains utilisateurs ou groupes d'utilisateurs.
94	Permettre à l'administrateur de modifier les paramètres de sécurité de chaque document archivé. [21]
95	Permettre de réserver au seul l'administrateur le droit de changer les paramètres de sécurité pour les groupes ou les utilisateurs (droits d'accès, niveau de sécurité, privilèges, attribution et gestion de mots de passe).

3.4.4 Attribution des niveaux de sécurité

Le SAE **doit :**

[20] Par exemple, une tentative d'accès au système par un utilisateur non autorisé.

[21] Cette fonction est notamment utilisée pour dégrader le niveau de protection des documents quand leur confidentialité décroît au fil du temps.

96	Permettre au seul administrateur de paramétrer le profil de l'utilisateur selon les opérations, les métadonnées d'archivage, les documents ou les agrégats auxquels les utilisateurs ont accès. Ce paramétrage devra : • interdire l'accès au SAE sans un mécanisme d'authentification lié au profil de l'utilisateur ; • restreindre l'accès de l'utilisateur à certains documents ou agrégats ; • restreindre l'accès de l'utilisateur en fonction de son niveau d'habilitation ; • restreindre l'accès à certaines opérations (par exemple, lecture, mise à jour et/ou suppression de certaines métadonnées) ; • refuser l'accès après une date déterminée ; et • rattacher l'utilisateur à un ou plusieurs groupes.[22]
97	Pouvoir fournir les mêmes fonctions de contrôle pour les profils et les utilisateurs.[23]
98	Pouvoir constituer des groupes d'utilisateurs associés à un agrégat.[24]
99	Permettre à un utilisateur d'être membre de plusieurs groupes.

Si le SAE gère une liste des agrégats, il **doit** :

100	Pouvoir limiter l'accès de certains utilisateurs à certaines parties de la liste (à définir lors de la configuration).
101	Autoriser un utilisateur à spécifier quels autres utilisateurs ou groupes peuvent avoir accès aux documents dont il responsable.[25]

3.4.5 Exécution des contrôles

Le SAE **doit** :

102	Autoriser l'administrateur, conformément à la section 3.4.6 « Niveaux de sécurité », à modifier le niveau de sécurité de tous les documents d'un agrégat en une seule opération. Le SAE doit émettre une alerte si la classification d'un document est revue à la baisse et attendre une confirmation avant de terminer l'opération.[26]

[22] Le mot de passe est un bon exemple de mécanisme d'authentification.

[23] Cette fonction permet à l'administrateur de gérer et de maintenir un groupe limité de profils et de droits d'accès plutôt qu'un grand nombre d'utilisateurs individuels. Les exemples de profils types peuvent être : gestionnaire, responsable des litiges, analyste financier, administrateur de bases de données.

[24] Les groupes peuvent être par exemple les ressources humaines ou l'équipe de vente.

[25] L'accès à cette action doit être accordé à l'utilisateur par l'administrateur en fonction de la politique d'archivage de l'entreprise/organisme.

[26] Ce changement est régulièrement demandé pour réduire le niveau de protection affecté aux documents à mesure que leur caractère sensible décroît.

103	Autoriser l'administrateur à changer le niveau de sécurité des agrégats, conformément aux exigences de la section 3.4.6 « Niveaux de sécurité »
104	Enregistrer tous les détails relatifs aux changements de niveaux de sécurité dans les métadonnées d'archivage du document, volume ou agrégat concerné.
105	Produire une des réponses suivantes (à paramétrer lors de la configuration) lorsqu'un utilisateur cherche ou demande accès à un document, un volume ou un agrégat auquel il n'a pas le droit d'accéder : • afficher le titre et les métadonnées d'archivage ; • afficher l'existence d'un agrégat ou d'un document (c'est-à-dire son identifiant) mais ni son titre ni aucune autre métadonnée ; ou • ne rien afficher ni même indiquer l'existence du document.[27]
106	Ne jamais inclure, dans une liste de résultats en recherche plein texte ou autre, un document auquel l'utilisateur n'a pas le droit d'accéder.[28]

Si le SAE autorise les utilisateurs à faire des tentatives non autorisées d'accès aux agrégats (avec leurs volumes) ou aux documents, il **doit** :

107	Enregistrer toute tentative d'accès non autorisé aux agrégats (avec leurs volumes) ou aux documents dans leurs métadonnées respectives.[29]

3.4.6 Niveaux de sécurité

Les exigences fonctionnelles de cette section ne s'appliquent qu'aux entreprises/organismes qui gèrent des documents classifiés dans leur SAE (se référer aux exigences réglementaires nationales) et aux exigences de sécurité.

Le SAE **doit** :

108	Autoriser l'affectation de classes de sécurité aux documents.[30]

---

27 Ces options sont présentées dans l'ordre croissant de sécurité. Noter que l'exigence de la troisième option (la plus rigoureuse) implique que le SAE ne fasse pas apparaître ces documents dans les résultats de recherche.

28 Noter que si la première option de l'exigence 105 est choisie, l'exigence 106 peut sembler contradictoire. Ce conflit apparent est intentionnel, parce que si cette exigence n'est pas présente, les utilisateurs pourraient se servir de la recherche dans le texte pour trouver le contenu de documents auxquels ils n'ont pas accès.

29 Cette action pourra être paramétrée pour ne s'appliquer qu'aux niveaux de sécurité précisés par l'administrateur. Ceci dit, le système devrait capturer la localisation/interface et l'utilisateur ou le login qui a fait cette tentative

30 La classification de sécurité dépendra de la réglementation ou de l'organisation mais peut inclure des niveaux comme :
- non classifié
- personnel (relatif à la vie privée)
- sensible (relatif à la vie privée)
- diffusion restreinte (sécurité nationale)
- confidentiel (sécurité nationale)

109	Autoriser la sélection et l'affectation de classes de sécurité au niveau du système pour : • tous les niveaux d'agrégats archivés (avec leurs volumes) ; et • les documents individuels ou les objets engageants.
110	Autoriser l'affectation de classes de sécurité : • au niveau d'un groupe (pouvoir mettre en place un accès à certains dossiers, à un certain niveau de sécurité ou d'habilitation), • en lien avec une fonction dans l'entreprise/organisme, • au niveau de l'utilisateur, et • à une combinaison de ces trois critères.[31]
111	Autoriser l'affectation d'un niveau de sécurité : • à n'importe quel agrégat, • après une période ou un événement donné, • à un type de document.[32]
112	Permettre l'affectation automatique de la valeur par défaut « non classifié » à un agrégat ou un document dépourvu de niveau de sécurité.
113	Permettre au sous-système de sécurité de fonctionner véritablement en cohérence avec les outils généraux de sécurité.
114	Pouvoir déterminer le plus haut niveau de sécurité d'un document dans un agrégat par une simple requête.
115	Prendre en charge la révision régulière et programmée des classifications de sécurité.
116	Restreindre l'accès aux agrégats/documents électroniques d'un niveau de sécurité supérieur à l'habilitation de l'utilisateur.

Si les classes de sécurité sont attribuées aux agrégats aussi bien qu'aux documents individuels (voir l'exigence 109), alors le SAE **doit** :

117	Être capable d'éviter qu'un agrégat électronique ait un niveau de sécurité inférieur à l'un des documents qui le composent.

- secret (sécurité nationale)
- très secret (sécurité nationale)

D'autres avertissements peuvent être associés à tout niveau d'habilitation.

31 Ceci permettra à l'administrateur de gérer et maintenir un nombre limité de droits d'accès et de catégories basés sur les rôles au sein de l'entreprise/organisme plutôt qu'un grand nombre de profils individuels avec des droits d'accès différents.

32 A noter qu'une habilitation adéquate peut ne pas être suffisante pour être autorisé à accéder aux documents. Les recherches bloqueront l'accès en ne faisant pas apparaître les documents relevant d'une habilitation de niveau supérieur à celle du chercheur, voir les exigences 105 et 106.

3.4.7 Métadonnées d'archivage

Il est nécessaire de fournir des métadonnées sur les processus de gestion du document engageant archivé, y compris son sort final : toute altération, tout lien et toute utilisation du document doit être tracé(e) dans le temps de manière incontestable pour garantir l'intégrité et l'authenticité du document. Les documents existent à différents niveaux d'agrégation : pièce, article, dossier ou série. Les métadonnées d'archivage doivent être appliquées aux documents à tous ces niveaux. Même si le document engageant est figé et inviolable, les métadonnées d'archivage continueront à s'accroître durant toute sa vie administrative. Elles doivent être liées de manière permanente au document, pour garantir son authenticité, son intégrité et sa fiabilité.

Le SAE **doit** :

118	Être capable de créer des métadonnées inaltérables sur les opérations d'archivage effectuées sur les documents, les agrégats ou le plan de classement (opérations à préciser par l'administrateur). Ces métadonnées devraient comprendre notamment : • le type d'opération, • l'utilisateur ayant initié et/ou effectué l'opération, • les date et heure de l'opération.[33]
119	Tracer les événements (une fois que fonction « métadonnées » activée) sans intervention manuelle, et stocker les métadonnées.
120	Préserver les métadonnées aussi longtemps que nécessaire.
121	Ajouter les métadonnées de toute modification apportée : • aux agrégats électroniques (avec leurs volumes), • aux documents électroniques individuels, et • aux métadonnées d'archivage des uns et des autres.
122	Décrire toutes les modifications apportées aux paramètres d'administration (par exemple, les modifications apportées par l'administrateur aux droits d'accès d'un utilisateur).

[33] Le mot « inaltérable » signifie que les métadonnées ne peuvent être ni modifiées ni détruites, par quelqu'utilisateur que ce soit. Elles peuvent être soumises à réorganisation et à copie sur un support amovible, par exemple si le logiciel l'exige, dès lors que leur contenu reste inchangé et destiné à un but spécifique. Ce processus ne doit pas altérer les métadonnées initiales.

123	Être capable de capturer et stocker dans les métadonnées les informations suivantes : • date et heure de capture de tout document électronique, • reclassement d'un document électronique dans un autre volume électronique, • reclassement d'un agrégat électronique dans le plan de classement, • toute modification apportée à la règle de conservation d'un agrégat électronique, • toute modification apportée aux métadonnées d'archivage des agrégats ou documents électroniques, • date et heure de création, correction et suppression des métadonnées d'archivage, • modifications apportées aux droits d'accès se rapportant à un agrégat électronique, un document électronique ou un utilisateur, • actions d'export ou de transfert d'un agrégat électronique, • date et heure de restitution d'un document, et • actions de destruction d'un agrégat ou d'un document électronique.
124	Garantir que les métadonnées sont disponibles en cas de contrôle, de sorte que, pour un événement donné, toutes les données associées soient accessibles, et que cela soit à portée d'une personne extérieure, habilitée mais peu ou pas familière du système.
125	Être capable d'exporter les métadonnées de tels ou tels documents et de groupes de documents sélectionnés, sans affecter les métadonnées stockées par le SAE. [34]
126	Être capable de capturer et stocker les intrusions (c'est-à-dire les tentatives par un utilisateur d'accéder à un document ou un agrégat, avec ses volumes, dont l'accès lui est interdit), et (là où des intrusions sont possible) les tentatives de violation des mécanismes de contrôle d'accès.[35]
127	Être capable, au minimum, de produire des rapports sur les actions effectuées sur les documents et agrégats existants : • par document ou agrégat, • par utilisateur, et • par ordre chronologique.

[34] Cette fonctionnalité peut être utilisée par des auditeurs externes qui souhaitent examiner ou analyser l'activité du système.

[35] On peut admettre que ce contrôle d'action ne s'applique aux niveaux de sécurité précisés par l'administrateur.

128	Permettre à l'administrateur de configurer la fonctionnalité « métadonnées » et de sélectionner quelles métadonnées doivent être capturées et stockées automatiquement. Le SAE doit garantir que cette sélection et toutes ses modifications sont stockées parmi les métadonnées.
129	Être capable de produire des rapports sur les opérations effectuées sur les agrégats et documents, par poste de travail et, là où cela est techniquement approprié, par adresse réseau.
130	Permettre à l'administrateur de modifier toute métadonnée d'archivage saisie par un utilisateur. L'information sur tout changement de ce type doit être stockée dans les métadonnées.[36]

3.4.8 Traçabilité des mouvements

Le mot "localisation" peut signifier l'adresse physique d'archives mixtes, ou la localisation de documents électroniques dans un plan de classement ou une arborescence électronique. Le mot « mouvement » renvoie au changement de localisation de documents tant électroniques que physiques.

Le SAE **doit** :

131	Fournir une fonction de traçabilité pour contrôler et enregistrer la localisation et les mouvements des dossiers tant électroniques que physiques.
132	Enregistrer l'information sur les mouvements, notamment : • identifiant unique de l'agrégat ou du document, • localisation courante, ainsi qu'un certain nombre de localisations antérieures (à définir par l'utilisateur) ; • date d'envoi ou de transfert vers l'extérieur, • date d'arrivée (pour les transferts), et • utilisateur responsable du mouvement (le cas échéant).
133	Maintenir l'accès au contenu du document archivé. Ceci inclut les possibilités de restitution, et le maintien de sa structure et de son format, dans le temps et à travers les générations de logiciels bureautiques.[37]

3.5 L'archivage mixte

3.5.1 Archivage des documents électroniques et non électroniques

Les systèmes utilisés par les entreprises/organismes pour l'archivage des documents ne se limitent pas à la seule gestion des documents sous format électronique. Certains sont spécialement conçus pour pouvoir gérer à la fois

[36] Cette fonctionnalité doit permettre aux administrateurs de corriger les erreurs des utilisateurs (erreur de saisie, etc.) et de maintenir les accès des utilisateurs et des groupes.

[37] Cela peut se faire par le biais d'une application de visualisation multi-formats.

l'archivage des documents physiques et électroniques. C'est pourquoi, les exigences fonctionnelles doivent s'orienter vers des systèmes mixtes en prévoyant des fonctionnalités d'archivage à la fois électronique et papier.

Dossiers mixtes

La relation entre dossiers physiques et documents archivés électroniquement est assez délicate. Le système ne pouvant capturer et enregistrer directement les archives physiques (les dossiers papier), il doit créer et conserver des pointeurs – métadonnées de gestion des archives physiques – et maintenir ainsi les liens entre les dossiers physiques et électroniques.

Généralement, le pointeur identifie le titre et l'identifiant unique du document physique ; il donne des informations sur son contenu et sa localisation pour pouvoir le retrouver.

On entend par dossier mixte un ensemble cohérent constitué de dossiers physiques et d'agrégats électroniques (des fichiers électroniques par exemple) procédant de la même mission, activité ou action, et devant être géré comme un seul et même dossier. La gestion des dossiers mixtes implique de fusionner les processus d'archivage électronique et les processus d'archivage physique.

Documents mixtes

Les documents électroniques peuvent être liés à des documents physiques par le biais de métadonnées pour constituer un document mixte, de la même façon que les dossiers physiques et électroniques peuvent être reliés pour former des dossiers mixtes. La métadonnée qui relie les documents électroniques et physiques prend la forme d'un pointeur qui identifie le document physique et sa localisation. Le pointeur peut être attaché directement au composant électronique du document mixte.

Le SAE **doit** :

134	Être capable de définir au sein du plan de classement des agrégats et volumes physiques, et permettre l'existence de documents non électroniques dans ces volumes qui seront gérés de la même façon que les documents électroniques.
135	Permettre que ces deux types de documents (électroniques et physiques) soient archivés et gérés de façon intégrée.
136	Permettre à un agrégat non électronique associé à un agrégat électronique dans un dossier mixte de porter le même titre et le même identifiant numérique, avec la mention qu'il s'agit d'un dossier mixte.
137	Permettre de configurer un jeu de métadonnées d'archivage différent pour les dossiers électroniques et les dossiers physiques ; les métadonnées de documents physiques doivent indiquer leur localisation physique.
138	Assurer que, lorsqu'une recherche porte sur des agrégats non électroniques, le système affiche également les métadonnées des documents électroniques associés.
139	Inclure des fonctions de contrôle et d'accès aux dossiers non électroniques, comparable aux fonctions des agrégats électroniques, y compris des contrôles sur les niveaux de sécurité.

140	Assurer la traçabilité des dossiers non électroniques grâce aux éléments suivants : demandes de prêts, contrôles des emprunts et retours, localisation réelle des dossiers.

Le SAE **devrait** :

141	Permettre l'impression et la reconnaissance des codes-barres des objets non électroniques (documents, pochettes et autres contenants), ou permettre à d'autres systèmes d'automatiser la traçabilité des entrées et des mouvements de ces documents physiques.
142	Faciliter l'utilisation de règles de conservation et de destruction, et les appliquer régulièrement et de la même façon aux éléments électroniques et non électroniques des dossiers mixtes.

Quand les agrégats sont soumis à des niveaux de sécurité, le SAE **doit** :

143	Assurer que le niveau de sécurité d'un dossier mixte s'applique de la même façon à ses documents papier qu'à ses documents électroniques.

3.6 Conservation et destruction

3.6.1 Référentiels de conservation

L'expression « sort final » renvoie à l'ensemble des opérations de destruction, transfert, archivage définitif et révision de la durée de conservation, bien que le terme « destruction » soit souvent utilisé à la place de sort final, par commodité, notamment dans l'expression « règles de conservation et destruction » qui correspond en réalité à la durée de conservation et au sort final (Note).

> *NdT : Le texte anglais expose les nuances linguistiques entre « disposition » et « disposal » ; ces concepts n'ayant pas d'équivalents directs en français, la traduction complète du paragraphe a peu de sens. En revanche, les termes « destruction » et « sort final » utilisés communément en français méritaient un commentaire.*

La suppression est souvent considérée comme une destruction permanente, alors que l'information supprimée peut être encore accessible ou récupérable dans des sauvegardes, sur un disque dur personnel ou en utilisant des outils de recherche. Un examen sérieux de ces questions, à un niveau politique ou technique, peut s'avérer indispensable en cas de fortes exigences juridiques ou de sécurité.

Élaboration des référentiels de conservation

Le SAE **doit :**

144	Comprendre une fonction qui : • définit les référentiels de conservation ; • automatise les actions de reporting et de destruction ; • détruit les documents composites en une seule action ; et • fournit des outils intégrés pour l'export des documents et de leurs métadonnées d'archivage.
145	Pouvoir réserver la création et la modification des référentiels de conservation au seul administrateur.
146	Autoriser l'administrateur à définir et à stocker un jeu de règles de conservation/destruction personnalisées.
147	Prendre en charge des durées de conservation allant d'un minimum d'un mois à une période illimitée.

Appliquer les référentiels de conservation

Le SAE **doit** :

148	Pouvoir assigner une règle de conservation/destruction à tout type d'agrégat ou de document archivé.
149	Garantir que, par défaut, tout document d'un agrégat est régi par la ou les règles de conservation/destruction associée(s) à cet agrégat.
150	Indiquer pour chaque règle (et dans les métadonnées du document archivé) : un sort final, une durée de conservation et un événement déclencheur à partir duquel court cette durée.
151	Pour chaque agrégat : • garder automatiquement une trace de toutes les durées de conservation qui lui ont été affectées ; et • lancer le processus de destruction en rappelant à l'administrateur le sort final prévu à l'échéance de la durée de conservation afin que, le cas échéant, il l'approuve et l'exécute.
152	Permettre au moins une des décisions suivantes pour chaque règle de conservation/destruction : • conservation illimitée, • révision à une date ultérieure, • destruction à une date ultérieure, • transfert à une date ultérieure.

153	Permettre de différer le point de départ d'une durée de conservation de l'une des manières suivantes : • écoulement d'un laps de temps donné après l'ouverture du dossier ; • écoulement d'un laps de temps donné après la clôture du dossier ; • écoulement d'un laps de temps donné depuis l'ajout le plus récent d'un document au dossier ; • écoulement d'un laps de temps donné après un événement précis (à identifier dans la règle, avec notification au SAE par l'administrateur plutôt qu'une détection automatique par le système) ; et • mention « illimitée » pour indiquer la conservation à long terme du document.[38]
154	Permettre l'affectation à un agrégat d'une règle de conservation/destruction qui se substitue à la règle de l'agrégat « père ».[39]
155	Permettre à l'administrateur de modifier toute règle de conservation/destruction affectée à un agrégat, à tout moment de son cycle de vie.
156	Permettre à l'administrateur de changer la(s) règle(s) de conservation/destruction d'un agrégat à tout moment.
157	Permettre la définition du jeu de procédures comme outil d'alerte pour faciliter la gestion de certains agrégats avant de lancer le processus de destruction.[40]
158	Donner la possibilité, après le déplacement par l'administrateur de documents ou d'agrégats électroniques vers un autre agrégat, que la ou les règle(s) de conservation/destruction du nouvel agrégat remplace(nt) celle(s) qui s'appliquai(en)t précédemment.

Mise en œuvre des règles de conservation/destruction

Le SAE **doit** :

159	Autoriser l'administrateur à supprimer des agrégats, volumes et documents (conformément à la section 3.4.6 « Niveaux de sécurité »).[41]

[38] Bien que cette liste de cas suffise généralement, il est possible que certains documents aient d'autres exigences de conservation.

[39] Par exemple si un agrégat (« père ») contient un autre agrégat (« fils »), il doit être possible d'affecter une règle de conservation/destruction à l'agrégat « fils » à la place de celle du « père »..

[40] Par exemple, lors de la révision d'un agrégat et de son contenu par un responsable ou un administrateur, avertir l'administrateur si l'agrégat est soumis à un niveau de sécurité particulier.

[41] Cette fonctionnalité n'est prévue que pour les cas exceptionnels.

160	Lors de l'exécution des règles de conservation/destruction, le SAE doit pouvoir : • produire un rapport d'erreur pour l'administrateur ; • supprimer intégralement le contenu d'un agrégat ou d'un volume ; • rappeler à l'administrateur de justifier l'action ; • garantir qu'aucune pièce ne soit supprimée si cela a un impact sur un autre document (par exemple, si une pièce entre dans la composition de deux documents – voir section 3.1.3 « Agrégats électroniques » – dont un serait en cours de suppression) ; • informer l'administrateur de tout lien entre un agrégat ou un document et un autre agrégat ou volume sur le point d'être supprimé, et demander confirmation avant la suppression effective ; • alerter les administrateurs de tout conflit, par exemple lorsqu'une même pièce est liée, par des pointeurs, à plusieurs documents ou agrégats dotés de sorts finaux différents ; et • maintenir en permanence l'intégrité totale des métadonnées d'archivage.

Si un dossier est associé à plus d'une règle de conservation/destruction, le SAE **doit** :

161	Tracer automatiquement toutes les durées de conservation énoncées dans ces règles et ne lancer le processus de destruction qu'une fois toutes ces durées expirées.
162	Autoriser l'administrateur à bloquer ou geler les processus de destruction (gel pour cause de contentieux, procédures judiciaires, loi « Informatique et libertés »...), manuellement ou automatiquement.

Tracer les actions de destruction

Le SAE **doit** :

163	Enregistrer de manière détaillée toute action de suppression ou de destruction dans les métadonnées de gestion.
164	Enregistrer automatiquement et rapporter toute action de destruction à l'administrateur.

Révision du sort final

Le SAE **doit :**

165	Permettre la révision des agrégats électroniques en les présentant avec leurs métadonnées d'archivage et leur règle de conservation/destruction, de façon qu'on puisse parcourir efficacement le contenu de l'agrégat et/ou de ses métadonnées.

166	Autoriser, lors de la révision, au moins une des actions suivantes pour chaque agrégat : • marquer l'agrégat pour la destruction ; • marquer l'agrégat pour le transfert ; • marquer l'agrégat pour un gel indéfini, en raison par exemple d'un contentieux en cours ; et • changer la règle de conservation/destruction (ou affecter une autre règle) pour que l'agrégat soit conservé et révisé à nouveau à une date ultérieure, comme défini dans cette section.
167	Autoriser l'ajout de commentaires dans les métadonnées d'archivage de l'agrégat pour expliquer ses décisions.
168	Signaler à l'administrateur, avant toute opération de destruction, la liste des agrégats arrivés à échéance et, après confirmation de l'administrateur, lancer les actions de sort final définies dans cette section.
169	Stocker dans les métadonnées toutes les décisions prises au cours de la révision.
170	Produire pour l'administrateur un rapport recensant toutes les règles de conservation/destruction applicables à une date donnée et un rapport statistique sur la quantité et les types de documents concernés.
171	Pouvoir paramétrer la fréquence du rapport sur les règles de conservation/destruction, les types d'information qui y figurent et souligner les anomalies (par exemple, les destructions en retard).
172	Alerter l'administrateur si dans un agrégat électronique voué à la destruction existe un lien vers un autre agrégat et suspendre le processus de destruction pour permettre les actions suivantes : ▪ confirmation par l'administrateur de la destruction ou annulation ; et ▪ production d'un rapport détaillant l'agrégat ou le(s) document(s) concerné(s) et toutes les références ou liens correspondants.
173	Faciliter les outils de reporting et d'analyse permettant à l'administrateur de gérer les règles de conservation/destruction, notamment de : • faire la liste de toutes les règles de conservation/destruction ; • faire la liste de tous les agrégats électroniques rattachés à une règle de conservation/destruction donnée ; • faire la liste des règles de conservation/destruction associées à tous les agrégats à partir d'un certain point du plan de classement ; • identifier, comparer et réviser les règles de conservation/destruction pour l'ensemble du plan de classement ; et • identifier les contradictions formelles entre les règles de conservation/destruction pour l'ensemble du plan de classement.

174	Fournir un outil de workflow (ou à défaut permettre une interface avec un outil externe) pour tracer les processus liés à l'application du sort final, à la révision et à l'export / transfert, notamment : • le statut / l'avancement de la révision (« en attente » ou « en cours », par exemple), l'indication de l'auteur de la révision et de la date ; • les documents en attente de destruction après révision ; et • l'avancement du processus de transfert.

Le SAE **devrait** :

175	Être capable d'effectuer des statistiques sur les décisions de révision pour une période donnée et fournir un rapport d'activités sous forme de tableau et de graphique.

3.6.2 Migration, export et destruction

Le SAE **doit** :

176	Fournir un processus ergonomique pour le transfert des documents archivés vers un autre système ou vers un tiers, et assurer les processus de migration.
177	Lors d'un transfert d'agrégats ou de volumes par le SAE, inclure tous les agrégats, volumes, documents et métadonnées associées à l'entité transférée.
178	Être capable de transférer ou exporter un dossier (de quelque niveau qu'il soit) en une seule suite d'opérations, de sorte que : • le contenu et la structure des documents électroniques ne soient pas endommagés ; • tous les composants d'un document électronique (lorsqu'il en comprend plus d'un) soient exportés comme une seule unité, y compris les éventuelles mesures techniques de protection ; • tous les liens entre le document et ses métadonnées d'archivage soient préservés; et • tous les liens entre documents électroniques, volumes et agrégats soient préservés.
179	Être capable d'inclure une copie intégrale du jeu de métadonnées associé aux documents et agrégats transférés ou exportés depuis un SAE.
180	Produire un rapport détaillant les anomalies apparues au cours du transfert, de l'export ou de la destruction. Le rapport doit identifier les documents à transférer dont le traitement a provoqué une erreur, et tout ensemble ou document dont le transfert, l'export ou la destruction a échoué.

181	Garder une copie de tous les agrégats transférés et des documents qu'ils contiennent, au moins jusqu'à confirmation de la réussite du transfert.[42]
182	Être capable de continuer à gérer des documents et dossiers qui auront été exportés du SAE vers d'autres supports de stockage.
183	Avoir la possibilité de conserver les métadonnées d'archivage des documents et agrégats qui ont été détruits ou transférés.
184	Permettre à l'administrateur de définir un jeu de métadonnées d'archivage à conserver pour les dossiers détruits, transférés à l'extérieur ou mis hors ligne.[43]
185	Permettre la destruction totale des documents archivés (qu'ils soient identifiés par série ou individuellement) stockés sur un support réinscriptible, en les effaçant complètement de sorte qu'ils ne puissent être restaurés par des moyens spécialisés de restauration de données.

Le SAE **devrait** :

186	Fournir un utilitaire ou un outil de conversion pour permettre la conversion, dans tel ou tel format de transfert ou d'export, des documents archivés sélectionnés pour un transfert ou un export.
187	Offrir la possibilité d'ajouter des métadonnées, définies par les utilisateurs, aux agrégats électroniques sélectionnés pour un transfert vers les archives historiques.
188	Offrir la possibilité de trier les agrégats électroniques à transférer selon des listes de métadonnées sélectionnées par les utilisateurs.

Lorsque des dossiers mixtes doivent être transférés, exportés ou détruits, le SAE **devrait** :

189	Demander à l'administrateur de confirmer que la partie non électronique de ces agrégats a été transférée, exportée ou détruite avant que la partie électronique ne le soit.

[42] Il s'agit d'une mesure conservatoire, afin que les documents ne soient pas détruits avant confirmation de la réussite du transfert.

[43] Il est nécessaire que l'entreprise/organisme sache quels documents ont été archivés et à quelle date ils ont été détruits ou transférés, sans devoir pour autant financer la conservation de l'intégralité des métadonnées.

3.6.3 Conservation et destruction des documents électroniques et non électroniques

Le SAE **doit** :

190	Permettre l'attribution de règles de conservation/destruction à tout agrégat non électronique inclus dans le plan de classement. Les règles doivent fonctionner de manière cohérente pour les agrégats, électroniques ou non, avertissant l'administrateur lorsque la date du sort final est atteinte, tout en tenant compte des processus de destruction différents pour l'électronique et le papier.
191	Permettre l'application d'une même règle de conservation aux dossiers électroniques et papier qui constituent un dossier mixte.
192	Pouvoir appliquer la décision de révision de la partie électronique d'un dossier mixte à sa partie non électronique.
193	Alerter l'administrateur de l'existence et de la localisation de tout dossier papier associé, au sein d'un dossier mixte, à un agrégat électronique qui doit être exporté ou transféré.
194	Pouvoir enregistrer dans les métadonnées tout changement apporté aux métadonnées d'archivage des dossiers et documents papier ou mixtes.
195	Pouvoir offrir une traçabilité des emprunts et retours effectués sur les dossiers papier décrits dans le système. Permettre en particulier, lorsqu'un dossier papier est emprunté, d'enregistrer l'utilisateur ou la localisation des destinataires, et d'afficher cette information en cas de demande du même dossier par une autre personne.
196	Offrir la possibilité de rechercher des documents papier décrits dans le système, en permettant à l'utilisateur de saisir la date de la demande, tout en générant un message de demande de communication du dossier papier à la personne qui le gère ou à l'administrateur, selon la configuration.
197	Pouvoir exporter et transférer les métadonnées d'archivage des documents et dossiers non électroniques.

Le SAE **devrait** :

198	Faciliter l'application de la décision de révision d'un ensemble d'agrégats à toutes ses composantes non électroniques, en notifiant à l'administrateur les actions à leur appliquer.

MISE À DISPOSITION

3.7 Recherche, repérage et restitution

Un SAE ne doit jamais fournir d'information à un utilisateur non habilité à la recevoir. Toutes les notions et fonctionnalités décrites dans cette section sont soumises aux contrôles d'accès présentés dans la section 3.4 « Gestion de l'authenticité et de la fiabilité ». Par simplicité, ces contrôles sont sous-entendus et ne sont pas répétés dans les exigences ci-dessous.

Un SAE **doit** :

199	Fournir un éventail souple de fonctions s'appliquant aux métadonnées (à tous les niveaux de dossiers) et aux contenus des agrégats au travers de paramètres définis par les utilisateurs pour localiser, accéder et repérer les documents et/ou les métadonnées individuellement ou collectivement.
200	Permettre d'effectuer des recherches sur toutes les métadonnées des documents, volumes ou agrégats.
201	Permettre d'effectuer des recherches dans le texte des documents (le cas échéant).
202	Permettre à l'utilisateur d'effectuer une même requête en combinant métadonnées et/ou contenu du document.
203	Permettre aux administrateurs de configurer et modifier les critères d'interrogation afin de : • définir n'importe quelle métadonnée de document, volume ou agrégat, voire le contenu entier du document comme champ d'interrogation ; et • modifier la configuration des critères d'interrogation.
204	Fournir des outils de recherche pour : • effectuer une recherche en texte libre combinant les métadonnées des documents et des agrégats et le contenu des documents ; et • effectuer des recherches booléennes de métadonnées (voir aussi exigence 219)
205	Permettre des recherches de proximité de métadonnées en autorisant la saisie du début, de la fin, ou d'une partie d'un mot.[44]
206	Permettre une recherche à l'intérieur d'un seul agrégat ou sur plusieurs agrégats.
207	Pouvoir chercher, repérer et afficher tous les documents et toutes les métadonnées d'un agrégat ou d'un volume comme une seule et même unité.
208	Pouvoir rechercher, retrouver et restituer un agrégat électronique à l'aide de tout élément qui le caractérise, notamment : • son nom, et • son identifiant (code de classement).
209	Afficher le nombre des résultats de la recherche sur l'écran de l'utilisateur et autoriser l'utilisateur à en afficher la liste, ou à effectuer une nouvelle requête en affinant ses critères de recherche.

[44] Par exemple, la recherche du terme « proj* » peut conduire à retrouver le mot « projet » ou « PROJA » ; le terme « C*n » pourra conduire à retrouver le mot « Commission ».

210	Permettre de sélectionner des documents ou agrégats dans la liste des résultats de recherche, puis de les ouvrir (sous réserve des droits d'accès) à l'aide d'un simple clic ou d'une seule touche.
211	Autoriser les utilisateurs à retrouver des agrégats et des documents directement à l'aide d'un identifiant unique.
212	Interdire les fonctions de recherche ou de repérage susceptibles de révéler à un utilisateur des informations (métadonnées d'archivage ou contenu des documents) que les contrôles d'accès et de sécurité devraient lui cacher.
213	Posséder des outils de recherche intégrés pour tous les niveaux du plan de classement.[45]
214	Permettre de combiner efficacement des recherches en texte libre et des métadonnées.
215	Présenter une fonctionnalité continue pour les recherches d'agrégats électroniques, non électroniques et mixtes.
216	Permettre aux utilisateurs de sauvegarder et réutiliser leurs requêtes.
217	Autoriser un utilisateur qui consulte ou travaille sur un document ou sur un agrégat (à la suite d'une requête ou dans une autre circonstance) de voir la position du document dans la hiérarchie du plan de classement, sans avoir à quitter ou fermer le document.[46]
218	Autoriser les utilisateurs à préciser (affiner) leurs recherches [47]

Le SAE **devrait** :

219	Permettre des recherches basées sur la proximité des mots, en indiquant qu'un mot doit se trouver à telle ou telle distance d'un autre dans le document pour figurer dans le résultat de recherche (voir également les exigences 202, 203 et 204).
220	Permettre la recherche de n'importe quelle métadonnée (associée à un document, un volume ou un agrégat), que l'objet relié à la métadonnée soit sous forme électronique ou non, et qu'il soit stocké en ligne, en différé ou hors-ligne.

[45] En d'autres termes, l'utilisateur devrait avoir la même interface, la même fonction et le même choix, qu'il recherche une série, un dossier ou un document.

[46] Par exemple, l'utilisateur doit être en mesure de voir à quel volume ou agrégat le document qu'il est en train de consulter est lié. De même, quand il consulte les métadonnées d'archivage d'un agrégat, l'utilisateur devrait pouvoir trouver à quel agrégat il est relié.

[47] Par exemple, un utilisateur devrait être en mesure d'initier une nouvelle recherche à partir d'une liste de résultats d'une première recherche.

221	Permettre aux utilisateurs ou administrateurs de configurer l'affichage des résultats, rendant notamment possibles : • la sélection de l'ordre de présentation des résultats, • l'indication du nombre de résultats par page d'écran, • l'indication du nombre maximum de réponses, • la sauvegarde des résultats, et • le choix des métadonnées d'archivage à afficher dans la liste des résultats.
222	Fournir un classement pertinent des résultats de recherche.
223	Être en mesure de relier un extrait de document électronique à son document source, de sorte que le repérage de l'un permette de repérer l'autre, tout en conservant séparément les métadonnées d'archivage et d'accès de chacun des deux objets.
224	Permettre les recherches par concept grâce à l'utilisation d'un thésaurus intégré tel un index en ligne.[48]

Si une interface graphique est utilisée, le SAE doit :

225	Fournir un mécanisme de survol rapide des dossiers rendant possible à tous les niveaux du plan de classement l'application des techniques graphiques ou d'autres techniques de présentation.[49]

3.7.1 Restitution: affichage

Le SAE **doit** :

226	Afficher ou télécharger les documents résultant d'une recherche.[50]

Le SAE **devrait** :

227	Afficher les documents résultant d'une recherche sans chargement du logiciel applicatif associé.[51]

[48] Ceci permettra la recherche de documents à l'aide d'un terme élargi, spécifique ou associé au contenu ou aux métadonnées. Par exemple, une recherche « service ophtalmique » pourrait donner « services de santé », « soins oculaires » ou « ophtalmologie ».

[49] Ceci devra être utilisé avec les techniques de recherches décrites ci-dessus pour fournir un premier niveau de métadonnées pour un groupe d'agrégats ou de documents répondant à des critères de recherches définis.

[50] Si le système d'archivage stocke des documents dans un format propriétaire, on peut accepter de les restituer au travers d'une application informatique indépendante du système d'archivage.

[51] On intègre en général au SAE un visualiseur. Ceci est souvent souhaité pour augmenter la rapidité de restitution.

228	Pouvoir restituer certains types de documents électroniques en préservant leur contenu (par exemple, toutes les caractéristiques de présentation et de mise en page de l'application informatique d'origine) et en restituant tous les composants du document électronique dans leur configuration initiale.[52]

3.7.2 Restitution: impression

Cette section concerne les documents archivés et leurs métadonnées ainsi que les autres données imprimables au sein du SAE.

Le SAE **doit** :

229	Proposer à l'utilisateur différentes possibilités permettant d'imprimer facilement les documents et leurs métadonnées dont celle d'imprimer un document avec les métadonnées d'archivage définies par l'utilisateur lui-même.
230	Permettre d'imprimer les métadonnées d'archivage d'un agrégat.
231	Permettre à l'utilisateur d'imprimer la liste récapitulative d'une sélection de documents (par exemple les pièces d'un agrégat), constituée des métadonnées choisies par l'utilisateur (par exemple : titre, auteur, date de validation) pour chaque document.
232	Permettre à l'utilisateur d'imprimer la liste des résultats de toutes ses requêtes.
233	Pouvoir imprimer tous les types de documents électroniques définis par l'entreprise/organisme, en préservant la mise en page d'origine (de l'application de production) et la totalité des composants (imprimables) du document électronique.[53]
234	Permettre à l'administrateur de préciser que certaines métadonnées doivent être attachées à toutes les impressions de documents, par exemple : titre, numéro d'enregistrement, date et niveau de sécurité.
235	Permettre à l'administrateur d'imprimer le thésaurus, s'il existe dans le SAE.
236	Permettre à l'administrateur d'imprimer l'intégralité ou une partie des paramètres de gestion.
237	Permettre à l'administrateur d'imprimer les règles de conservation/destruction.
238	Permettre à l'administrateur d'imprimer le plan de classement.
239	Permettre à l'administrateur d'imprimer le modèle ou l'ensemble des métadonnées.

Le SAE **devrait** :

[52] L'entreprise/organisme doit définir les applications informatiques et les formats dont elle a besoin.

[53] L'entreprise/organisme doit définir les applications informatiques et les formats dont elle a besoin.

240	Permettre d'imprimer tous les documents d'un agrégat, en une seule opération et dans un ordre défini par l'utilisateur.

Si le SAE utilise des plans de classement et des thésaurus, il **doit** :

241	Permettre à l'administrateur de les imprimer.

3.7.3 Restitution : extraits

Un extrait ou document masqué est une copie d'un document électronique dont on a retiré ou masqué (anonymisé) des éléments de façon permanente. On parle d'extrait quand on ne peut accéder qu'à une partie du document et non à sa totalité.

Le SAE **doit** :

242	Permettre à l'administrateur de faire une copie d'un document pour les besoins de masquage.[54]
243	Enregistrer la création d'extraits dans les métadonnées d'archivage, soit au minimum : la date, l'heure, la raison de l'extrait et l'auteur.
244	Stocker dans les métadonnées toute modification effectuée en réponse aux besoins de cette section.

Le SAE **devrait** :

245	Fournir une fonctionnalité de masquage (voir le Glossaire en annexe A) pour gérer l'information sensible contenue dans l'extrait. Si le SAE ne la fournit pas directement, il doit autoriser d'autres logiciels à le faire.[55]
246	Inciter l'auteur d'un extrait à l'attribuer à un agrégat.
247	Stocker une référence croisée à l'extrait dans le même agrégat et volume que le document source, même si ce volume est clos.

3.7.4 Restitution: autres

Cette section s'applique uniquement aux documents archivés ne pouvant normalement pas être imprimés : fichiers audio, vidéo et bases de données.

Le SAE **doit** :

248	Intégrer des fonctions permettant via un périphérique approprié de restituer ces documents non imprimables.[56]

---

[54] Cette copie est appelée ici « extrait » du document (voir le Glossaire, annexe A).

[55] Il est essentiel que, quelles que soient les fonctionnalités de masquage utilisées, aucune des informations supprimées ou masquées ne puisse être visualisée dans l'extrait, ni sur l'écran, ni en l'imprimant, ni en le rejouant, quelle que soit l'utilisation qu'on puisse faire des techniques de rotation de page, de zoom ou autre manipulation.

[56] Exemples : fichiers audio, vidéo, sites Internet, etc.

3.7.5 Restitution: réutilisation des contenus

Le SAE **doit** :

249	Permettre la réutilisation ou le retraitement des contenus.[57]

ADMINISTRATION

3.8 Administration

Les documents archivés peuvent exceptionnellement être modifiés ou supprimés par les administrateurs système. Dans ce cas, il faut pouvoir en créer des copies ne comportant pas d'information sensible (copies masquées). Les administrateurs système doivent aussi pouvoir gérer les paramètres système, effectuer des sauvegardes, des restaurations et des statistiques. Cette section concerne les paramètres système, la sauvegarde et la restauration, l'administration du système et des utilisateurs. L'administration de la classification pour la sécurité, des contrôles, du classement, etc. est traitée dans les exigences relatives à la sécurité au point 3.4.4 « Gestion de l'authenticité et de la fiabilité ».

3.8.1 Rôle de l'administrateur

Le SAE **doit** :

250	Permettre à l'administrateur de retrouver, afficher et reconfigurer les paramètres système et de redistribuer les utilisateurs et les fonctionnalités selon les profils utilisateurs.
251	Fournir des fonctions de sauvegarde afin que les documents et leurs métadonnées d'archivage puissent être reconstitués par une combinaison des sauvegardes et des métadonnées.
252	Fournir des moyens de récupération et de retour en arrière en cas de panne du système ou d'erreur de mise à jour, et notifier à l'administrateur les résultats obtenus.[58]
253	Contrôler l'espace de stockage disponible et alerter l'administrateur lorsque l'espace disponible devient critique ou qu'il faut lui prêter une attention particulière.

[57] Par exemple, autoriser l'utilisateur à supprimer une partie du contenu d'un document texte ou lui permettre, dans un autre contexte, d'ajouter un lien dynamique vers un document sous forme d'image/graphique.

[58] C'est-à-dire que le SAE doit permettre aux administrateurs d'annuler une série d'opérations, jusqu'à revenir à un état intègre de la base de données. Ceci n'est nécessaire qu'en cas d'erreur.

254	Permettre à l'administrateur de faire des modifications en série dans le plan de classement en garantissant que toutes les métadonnées d'archivage sont en permanence traitées correctement et complètement, afin de gérer les changements organisationnels, par exemple: • division d'un service en deux, • regroupement de deux services en un, • nouveau rattachement ou nouvelle dénomination d'un service ; • réorganisation générale de l'entreprise/organisme en deux entités distinctes.[59]
255	Faciliter la mutation des utilisateurs entre les services.
256	Permettre la définition de profils utilisateurs, et pouvoir associer plusieurs utilisateurs à un profil.
257	Signaler toute erreur rencontrée lors de la sauvegarde des données sur les supports de stockage.

3.8.2 Gestion des métadonnées

Il est nécessaire de gérer des schémas de métadonnées, notamment pour la création, l'ajout, la suppression ou la modification de métadonnées, ainsi que les règles sémantiques et syntaxiques et leur caractère obligatoire ou non.

Le SAE **doit** :

258	Permettre à l'administrateur de créer, de définir et de supprimer des métadonnées, même pour les champs personnalisés.
259	Permettre à l'administrateur d'appliquer et de modifier les règles des schémas de métadonnées, y compris les règles sémantiques et syntaxiques, les schémas d'encodage et leur caractère obligatoire ou non.
260	Permettre à l'administrateur de configurer le système pour restreindre la consultation ou la modification des métadonnées en fonction des groupes, des fonctions ou des utilisateurs.
261	Décrire toutes les activités de gestion des métadonnées.

[59] Dans ce cas, les dossiers clos doivent rester tels quels, conservant leur référence au plan de classement d'avant la réorganisation. Les dossiers encore ouverts doivent être: soit clos, en gardant leur référence au plan de classement antérieur tout en étant rattachés à un dossier du nouveau plan de classement; soit référencés dans le nouveau plan de classement tout en conservant lisiblement leurs anciennes références de classement. Les changements organisationnels décrits ci-dessus peuvent induire des modifications équivalentes dans les plans de classement des services et des équipes. L'expression "modifications en série" signifie que tous agrégats et documents concernés peuvent être traités en un petit nombre d'opérations plutôt que un par un. Notons que ce procédé vise surtout les entreprises/organismes où les plans de classement suivent l'organigramme, et présente moins d'intérêt quand le plan de classement est organisé par fonction.

3.8.3 Reporting

Cette section se limite aux exigences minimales de reporting. Elle ne décrit pas les exigences d'un sous-système complet de reporting.

Le SAE **doit** :

262	Fournir à l'administrateur des outils de reporting modulaires capables de produire au minimum des données sur : • les nombres d'agrégats, volumes et documents archivés, • les statistiques d'opérations concernant les agrégats, volumes et documents archivés, et • les rapports d'activité par utilisateur.
263	Permettre à l'administrateur de faire des statistiques sur les métadonnées à partir d'une sélection de : • agrégats, • volumes, • documents ou objets archivés, • utilisateurs, • laps de temps, et • formats de fichiers et fichiers de tous formats.
264	Pouvoir produire une liste des agrégats, exhaustive ou partielle, structurée selon le plan de classement.
265	Permettre à l'administrateur d'éditer des rapports réguliers ou exceptionnels.
266	Permettre à l'administrateur de faire des statistiques sur les métadonnées à partir des : • niveaux de sécurité, • groupes d'utilisateurs, et • autres métadonnées d'archivage.
267	Inclure des fonctionnalités de tri et de sélection des données statistiques.
268	Inclure des fonctionnalités de consolidation et de synthèse des données statistiques.
269	Permettre à l'administrateur de limiter l'accès des utilisateurs à certains rapports.

3.8.4 Sauvegarde et restauration

Les SAE doivent avoir un contrôle exhaustif sur les documents archivés et leurs métadonnées d'archivage afin d'effectuer des sauvegardes régulières. Ces sauvegardes devraient permettre la restauration rapide des documents archivés qui auraient été perdus par suite de la défaillance du système, d'un accident ou d'une faille de sécurité. En pratique, les fonctions de sauvegarde et de restauration

peuvent être réparties entre les administrateurs du SAE et les équipes du SI (systèmes d'information).

Le SAE **doit** :

270	Fournir des procédures automatisées de sauvegarde et de restauration.
271	Permettre à l'administrateur de programmer des routines de sauvegarde en : • précisant la fréquence des sauvegardes ; et • en définissant le mode de sauvegarde ainsi que le support et le lieu de stockage (stockage hors ligne, système séparé, site distant, etc.).
272	Réserver au seul administrateur le droit de restaurer les données à partir des sauvegardes du SAE. L'intégrité des données doit être assurée après restauration.
273	Réserver au seul administrateur le droit de procéder à une mise à jour de la base restaurée (« roll-forward »). L'intégrité des données doit être maintenue.
274	Permettre aux utilisateurs de signaler les documents considérés comme vitaux.[60]
275	Pour les utilisateurs dont les dernières mises à jour n'ont peut-être pas été complètement restaurées, pouvoir les avertir, quand ils se reconnectent au système, que la restauration effectuée est potentiellement incomplète.

[60] Les documents vitaux sont les documents absolument indispensables à la poursuite des activités d'un organisme ou d'une entreprise, aussi bien en termes de capacité à réagir de façon adéquate en cas d'urgence ou de sinistre, que de capacité à protéger ses intérêts financiers et juridiques. C'est pourquoi l'identification et la protection de ces documents sont cruciales pour toute entreprise/organisme.

4 ANNEXES

A Glossaire

Ce Glossaire constitue un sous-ensemble d'un glossaire plus complet et présent dans les Modules 2 et 3.

NB : l'ordre est l'ordre alphabétique des mots français, le terme anglais étant indiqué juste après.

Terme	***Définition***
Accès / Access	Droit, modalités et moyens de recherche, d'exploitation ou de repérage de l'information. Source: ISO 15489, Part 3, Clause 3.1.
Action / Transaction	La plus petite unité de l'activité métier. L'exploitation d'un document archivé est elle-même une action. Troisième niveau du plan de classement métier. Voir aussi **Activité, Plan de classement métier et Mission.** Sources : Adapté de AS 4390, Part 1, Clause 4.27; AS ISO 15489, Part 2, Clause 4.2.2.2.
Activité métier / Business activity	Terme générique pour l'ensemble des missions, processus, activités et actions d'un(e) entreprise/organisme (i.e. l'administration comme le secteur marchand) et de ses employés.
Activité / Activity	Second niveau d'un plan de classement métier. Les activités sont les tâches principales mises en œuvre par un(e) entreprise/organisme pour mener à bien ses missions. Les activités sont nommées et décrites. La description inclut toutes les actions qui s'y rapportent. Selon la nature des actions, une activité peut être mise en œuvre en relation avec une ou plusieurs missions. Voir aussi **Plan de classement métier, Mission,** et **Action.**
Administrateur système / System administrator	Rôle utilisateur avec la responsabilité de configurer, contrôler et gérer le système métier et son utilisation. Il peut exister avec différents degrés d'ancienneté et une variété de permissions pour la prise en charge des missions de l'administration du système et des processus d'archivage.
Administrateur / Administrator	Rôle responsable de la gestion quotidienne de la politique d'archivage dans un(e) entreprise/organisme. Il peut aussi désigner la responsabilité de gestion du SAE de l'entreprise/organisme.
Agrégat / Aggregation	Tout regroupement organique d'entités documentaires élémentaires (document, objet numérique), par exemple un dossier numérique, une série. Les documents peuvent être regroupés en dossiers et les dossiers (avec leurs documents constitutifs) peuvent être regroupés eux-mêmes en dossiers (cela dépend de la terminologie utilisée par le SAE). Voir aussi **Dossier** et **Catégorie de documents**.
Ajusté / Adequate	La granularité des documents archivés devrait être ajustée aux objectifs de la conservation. Ainsi, une décision essentielle sera décrite de manière détaillée alors qu'une action administrative de routine sera décrite plus légèrement, avec quelques données minimales d'identification. La granularité des documents devrait refléter le niveau de preuve et de traçabilité requis par l'activité.

Terme	***Définition***
Application du sort final / Disposition action (et Disposal action)	Destination d'un document archivé notée dans le référentiel de conservation avec la durée minimale de conservation et l'événement déclencheur de calcul du sort final. Voir aussi **Événement déclencheur du sort final** et **Durée de conservation.**
Application métier / Business system	Dans le cadre de ce document : système automatisé qui crée ou gère les données d'un(e) entreprise/organisme. Ceci comprend les applications dont le rôle premier est de faciliter les transactions entre une unité organisationnelle et ses clients – par exemple, commerce électronique, gestion de la relation client, bases de données spécifiques ou personnalisées, systèmes relatifs aux finances ou aux ressources humaines. Voir aussi **Système de gestion des documents et d'archivage électronique,** et **SAE** (**EDRMS**).
Archives / Archives	Documents produits ou reçus par une personne, une famille ou un organisme, public ou privé, dans le cadre de son activité, et conservés en raison de leur valeur de preuve des activités et responsabilités de leur producteur, particulièrement ceux qui sont gérés par les principes de provenance, de respect de l'ordre primitif et de contrôle collectif ; archives définitives. Note : en informatique, le terme « archives » revêt un autre sens ; il signifie « copie d'un ou plusieurs fichiers ou copie d'une base de données en vue d'assurer une sauvegarde à des fins de consultation ou une restauration si les données originales sont endommagées ou perdues. » Source: IBM Dictionary of Computing, McGraw Hill, New York, 1994, p. 30.
Authentification / Authentication	Processus par lequel l'expéditeur d'un message est identifié comme celui qu'il prétend être. Source: National Archives of Australia, *Recordkeeping and Online Security Processes : Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Autorisation d'accès / User permissions	Droits attribués aux employés précisant dans quelle mesure ils sont habilités à créer/initier, ajouter, modifier et supprimer des documents dans le système d'archivage.
Autorité archivistique / Archival authority	Services et institutions archivistiques ou autres structures responsables des programmes de sélection, collecte, conservation, mise à disposition et contrôle de la destruction d'archives.
Autorité de certification / Certification authority	Organisme qui produit, signe et délivre des certificats de clé publique reliant les signataires à leur clé publique. Source: National Archives of Australia, *Recordkeeping and Online Security Processes : Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Base de données / Database	Collection organisée de données. Les bases de données sont souvent structurées et indexées pour améliorer l'accès des utilisateurs et le repérage d'informations. Elles peuvent exister dans un format physique ou numérique.

Terme	***Définition***
Capture / Capture	1. Processus consistant à faire passer un document ou un objet numérique dans un système d'archivage, à lui attribuer des métadonnées pour le décrire et à le contextualiser, permettant ainsi de le gérer dans le temps. Pour certaines activités métier, cette fonctionnalité peut être native dans l'application métier, de sorte que la capture des documents à archiver et leurs métadonnées est concomitante à la validation des documents. Voir aussi **Enregistrement.** Source: National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004. Adapté de AS 4390, Part 1, Clause 4.7. 2. Processus de fixation du contenu, de la structure et du contexte d'un document pour garantir une représentation fiable et authentique des activités et actions métier pour lesquelles il a été produit ou transmis. Une fois le document capturé dans un SAE, les utilisateurs ne seront plus en mesure d'en altérer le contenu, la structure ou le contexte
Catégorie de conservation / Disposition class (et Disposal class)	Description des caractéristiques d'un groupe de documents traçant des activités similaires et auquel on peut appliquer le même sort final. La description comprend mission et activité commentées, description du document et sort final. Composant du référentiel de conservation intégré à l'application métier comme série de règles applicables à toute entité archivée et comprenant : événement déclencheur du sort final, durée de conservation et action de sort final.
Catégorie de documents / Record category	Subdivision du plan de classement pour l'archivage qui peut elle même être subdivisée en une ou plusieurs catégories sur un ou plusieurs niveaux. Une catégorie de document est constituée par des métadonnées qui peuvent être héritées d'un parent (catégorie de documents) et transmises aux enfants (dossier ou agrégat de documents numériques). La somme des catégories, tous niveaux confondus, constitue le plan de classement pour l'archivage. Voir aussi **Plan de classement pour l'archivage**. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 1.
Certificat numérique / Digital certificate	Document électronique signé par une autorité de certification identifiant un propriétaire de clé et l'entité qu'il représente, associant ce propriétaire à une paire de clés en spécifiant laquelle est la clé publique, et devant contenir toute autre information exigée par le profil du certificat. Source: National Archives of Australia, *Recordkeeping and Online Security Processes : Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Champ / Field	Lot d'une ou plusieurs données représentant une catégorie d'informations au sein d'une base de données. Voir aussi **Base de données.**

Terme	***Définition***
Chiffrement / Encryption	Processus de conversion des données dans un code sécurisé à l'aide d'un algorithme de chiffrement, pour la transmission dans un réseau public. La clé mathématique de l'algorithme de chiffrement est encodée et transmise avec les données fournissant ainsi les moyens de déchiffrement à l'arrivée et de restauration des données originales. Source: National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004. Adapté de The Australian Government Information Management Office, *Trusting the Interne: A Small business Guide to E-security, 2002, p. 43.*
Classement / Classification	1. Identification systématique et organisation des activités métier et/ou des documents en catégories selon des conventions logiques, des méthodes et des règles articulées dans un plan de classement. 2. Le classement inclut des conventions de nommage des documents et des fichiers, les habilitations des utilisateurs et les restrictions d'accès. Voir aussi **Plan de classement métier, Plan de classement pour l'archivage et Taxonomie**. Source: Adapté de la norme ISO 15489, Part 1, Clause 3.5 ; AS 4390, Part 1, Clause 4.8.
Classer / File (verb)	Action de localiser les documents selon un plan de contrôle.
Clé cryptographique / Cryptographic key	Données utilisées pour le chiffrement ou le déchiffrement de messages électroniques. Elle consiste en une séquence de symboles qui contrôle l'opération de transformation cryptographique, comme le chiffrement. Source: National Archives of Australia, *Recordkeeping and Online Security Processes : Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Composant / Component	Les composants sont les parties constitutives d'un document numérique (ex : les composants multimédias d'une page web). Il est nécessaire de capturer les métadonnées des composants si on veut gérer le document dans le temps, par exemple pour une migration. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 1.
Continuum / Records continuum	Cycle complet de vie d'un document engageant (à archiver). Cela renvoie à une série régulière et cohérente de processus de gestion depuis la production et la capture des documents (voire avant avec la conception des systèmes d'archivage) jusqu'à la conservation et l'utilisation des documents archivés comme archives historiques.
Contrôle d'accès / Access controls	Ensemble de mécanismes non hiérarchiques applicables aux documents électroniques pour empêcher l'accès à des utilisateurs non habilités. Il peut inclure la définition de groupes utilisateurs et de listes nominatives d'utilisateurs. Voir aussi **Contrôles de sécurité**, **Règles d'accès, Groupes d'utilisateurs**. Source: Adapté de *The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference*

Terme	***Définition***
	Document, 2002, p. 28.
Contrôle d'accès / System access control	Tout mécanisme utilisé pour empêcher l'accès à l'application métier par des utilisateurs non habilités, pouvant inclure des profils utilisateurs, ou des identifiants utilisateurs et des mots de passe. Voir aussi **Contrôle d'accès** et **Contrôle de sécurité**
Contrôle de sécurité / Security controls	Niveau de protection pouvant être attribué aux utilisateurs, aux documents numériques et aux entités du plan d'archivage pour restreindre les accès. Il peut inclure un niveau hiérarchique de sécurité parallèlement à un qualificatif non hiérarchique. Voir aussi **Contrôle d'accès et Descripteur**
Contrôle / Control	1. Gestion physique et/ou intellectuelle des documents s'appuyant sur une description de leur état physique et logique, de leur contenu, de leur provenance et de leurs relations. Les systèmes et procédures de contrôle sont notamment l'enregistrement, le classement, l'indexation et la traçabilité. Voir aussi **Classement** et **Enregistrement.** 2. Terme informatique pour l'élimination d'un document d'une façon qui permet cependant de le récupérer si nécessaire (forme de « destruction douce »). Voir aussi **Destruction.**
Conversion de fichier / Rendition	Instance d'un document numérique rendu disponible dans un autre format ou sur un autre support par un processus entièrement contrôlé par l'application métier et sans perte de contenu. Un fichier converti devrait présenter les mêmes métadonnées et être géré en étroite relation avec le document natif. Le besoin de conversion est lié à la conservation, à l'accès ou à la consultation. Voir aussi **Conversion**
Conversion / Conversion	Processus de changement de support ou de format appliqué aux documents. La conversion implique un changement de format du document mais garantit que celui-ci conserve à l'identique l'information primaire (le contenu). Voir aussi **Migration.** Source: Adapté de la norme ISO 15489, Part 1, Clause 3.7 et Part 2, Clause 4.3.9.2.
Descripteur / Descriptor	Dans ce document, qualificatif non hiérarchisé (par exemple « personnel ») attribué à un niveau de sécurité dans le but de limiter l'accès à certains documents. Informatif ou consultatif, il ne peut véritablement contrôler les accès. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, pp. 27–8.
Destruction / Destruction	1. Processus d'élimination ou de suppression des documents sans aucune possibilité de restitution. 2. Dans ce document, la destruction renvoie au processus d'élimination où les documents numériques, les entités du plan de classement et leurs métadonnées sont retirées, effacées ou oblitérées selon les règles du référentiel de conservation. Voir aussi **Suppression.** Source: Adapté de la norme ISO 15489, Part 1, Clause 3.8.

Terme	***Définition***
Document composite / Compound record	Un document archivé composé de plusieurs objets numériques élémentaires (ex : des pages web avec des graphiques et des feuilles de style embarquées).
Document engageant / Record (noun)	Toute information, sous tout format, produite, reçue ou conservée à titre de preuve et d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité. Voir aussi **Document hybride** et **Document physique**. Source: ISO 15489, Part 1, Clause 3.15.
Document mixte / Hybrid record	1. Série de composants numériques et physiques étroitement liés au travers de métadonnées et gérés comme un document unique. Voir aussi **Document physique** et **Document engageant.** 2. Document engageant constitué de composants électroniques et non électroniques. Le document électronique et ses métadonnées d'archivage sont conservés dans le SAE avec les métadonnées d'archivage du document non électronique.
Document physique / Physical record	Document engageant sous la forme d'un objet matériel (page, dossier papier, liasse, photographie, microfilm, enregistrement audio ou film). Voir aussi **Pointeur**, **Dossier physique** et **Document engageant**.
Document (nom) / Document (noun)	Information enregistrée sur un support ou objet pouvant être traité comme une entité. Voir aussi **Document engageant.** Source: ISO 15489, Part 1, Clause 3.10.
Dossier / File (noun)	Unité organisée de documents accumulés pendant leur utilisation courante et conservés ensemble parce qu'ils traitent du même sujet, de la même activité ou action. *Note des traducteurs : en anglais le mot « file » désigne également un fichier informatique (groupe d'informations doté d'un nom, stocké sur un ordinateur et traité comme une entité basique).* Source: Adapté de J -Ellis (ed.), *Keeping Archives, 2nd edition, Australian Society of Archivists and Thorpe, Melbourne 1993, p. 470.*
Dossier mixte / Hybrid file	Groupe logique de dossiers numériques et physiques. Les deux dossiers ont une étroite relation à l'intérieur de l'application métier et sont gérés comme un objet unique. Les documents gérés à l'intérieur d'un dossier mixte traitent des mêmes sujets, activités ou actions. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 4.
Dossier numérique / Digital file	Ensemble de documents numériques reliés logiquement, maintenus en relation étroite dans l'application métier et gérés comme un objet unique. Type d'agrégat de documents numériques. Peut également être dénommé « contenant ». Voir aussi **Agrégat** et **Dossier.**

Terme	***Définition***
Dossier physique / Physical file	Entrée du plan de classement pour un dossier matériel (souvent papier). Le dossier proprement dit est stocké hors du système mais ses métadonnées de localisation et de gestion sont conservées dans l'application. Un dossier physique peut être autonome dans le plan de classement ou participer d'un dossier mixte matérialisant un lien étroit entre objets numériques et physiques. Voir aussi **Dossier** et **Pointeur.** Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 5.
Durée de conservation / Retention period	Période de temps, après l'événement déclencheur, pendant laquelle un document engageant doit être conservé et accessible. A l'expiration de cette durée, on peut appliquer le sort final. Voir aussi **Application du sort final et Événement déclencheur du sort final.**
Enregistrement / Registration	Action de donner à un document ou à un dossier engageant un identifiant unique dans un système d'archivage pour constituer une trace de sa validation ou de sa capture. L'enregistrement suppose une brève description du contexte du document et ses relations avec les autres documents archivés. Archivistiquement parlant, on peut enregistrer aussi bien des agrégats (par exemple les séries) que des documents individuels. Voir aussi **Capture et Identifier.** Source : Adapté de la norme ISO 15489, Part 1, Clause 3.18 ; AS 4390, Part 1, Clause 4.24.
Enregistrements qualité / Quality records	Documents utilisés pour assurer la conformité aux exigences spécifiques et le fonctionnement effectif des systèmes qualité selon la série des normes ISO-9000.
Évaluation / Appraisal	Processus de sélection des activités métier pour déterminer quels documents doivent être capturés et combien de temps il faut les conserver pour répondre aux besoins métier, aux exigences de responsabilité et aux attentes de la communauté.
Événement déclencheur du sort final / Disposition trigger (also Disposal trigger)	Événement à partir duquel on peut calculer la date du sort final. Ce peut être la date d'achèvement d'une action ou la date de survenance d'un fait. Voir aussi **Durée de conservation**
Export / Export	Processus de sort final consistant à transférer des copies de documents numériques (ou de groupes de documents) avec leurs métadonnées, d'un système vers un autre, en interne ou à l'extérieur. Avec l'export, les documents ne sont pas supprimés dans le système d'origine. Voir aussi **Transfert.** Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 3.
Extrait / Extract	Copie d'un document numérique engageant dont on a retiré ou masqué durablement certains éléments. On réalise un extrait quand seule une partie du document peut être communiquée, et non sa totalité. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference*

Terme	***Définition***
	Document, 2002, p. 3.
Filigrane numérique / Digital watermark	Dessin complexe visible ou invisible contenant la provenance ou la propriété de l'information. Un filigrane peut être surimposé sur une image numérique et ne peut être enlevé qu'à l'aide d'un algorithme et d'une clé sécurisée. Sons et films numérisés peuvent se voir appliquer des technologies similaires. Source: Cornwell Management Consultants (for the European Commission's Interchange of Documentation between Administrations Programme), *Model Requirements for the Management of Electronic Records* (MoReq Specification), 2001, p. 70.
Fonds d'archives historiques / Archive	Ensemble des documents constituant la mémoire d'une personne physique ou morale, conservé sans limitation de durée.
Format natif / Native format	Format dans lequel un document engageant est produit ou dans lequel l'application source le conserve. Voir aussi **Conversion**. Source: Adapté de NSW Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B : Specifications*, 2001, p. 13.
Format / Format	Forme physique (papier, microfilm) ou format de fichier informatique dans laquelle (lequel) un document est conservé. Voir aussi **Format natif.** Source: Adapté de Department of Defense (US), *Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD*, 2002, p. 14.
Gestion de l'archivage (archivage) / Records management (Recordkeeping)	Organisation de la production et de la conservation d'une trace complète, exacte et fiable des activités sous la forme de documents engageants. L'archivage englobe la production et la capture des documents engageants issus des activités (y compris la vérification de la qualité de ces documents), la conception, la mise en place et le fonctionnement des systèmes d'archivage ; et la gestion des documents archivés pour les besoins des producteurs (partie assimilée traditionnellement à l'archivage) et en tant qu'archives historiques (partie vue traditionnellement comme le domaine spécifique de l'Administration des Archives). Source: Adapté de AS 4390, Part 1, Clause 4.19 and Part 3, Foreword.
Groupe d'utilisateurs / User access group	Liste nominative de personnes (utilisateurs connus du système métier) qui fonde un groupe stable et identifié. L'accès à certains documents ou à certaines entités du plan de classement peut être restreint aux membres de certains groupes. Voir aussi **Contrôle d'accès**. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 28.
Hériter / Inherit	Recevoir une métadonnée d'une entité de niveau supérieur. Source: Adapté de *The National Archives (UK), Requirements for Electronic Records Management Systems, 3 : Reference Document, 2002, p. 4.*

Terme	***Définition***
Identification / Identify (Identification)	Processus de liaison permanente entre un document ou un agrégat et son identifiant unique. Voir aussi **Enregistrement.**
Import / Import	Réception dans un système des documents numériques archivés avec leurs métadonnées, en provenance d'un autre système, interne ou extérieur.
Indexation / Indexing	Processus d'établissement de points d'accès pour faciliter le repérage de documents et/ou d'informations.
Instance / Instance	Occurrence d'un document numérique dans un format donné ou un moment donné. Par exemple, un document dans son format natif est une instance tandis que le fichier converti en est une autre. Les instances peuvent être le produit des processus de migration ou de conversion.
Interface de programmation / Application program interface (API)	Il s'agit de la méthode spécifique prescrite par un système d'exploitation d'ordinateur ou une application de manière à ce que l'application puisse faire des requêtes sur le système d'exploitation ou sur une autre application.
Interface utilisateurs graphique / Graphical user interface (GUI)	Interface utilisateurs utilisant le graphisme plutôt que le texte (par exemple, une interface à fenêtres).
Pointeur / Marker	Type de métadonnée pour un document stocké physiquement hors de l'application métier. Un pointeur renvoie à un document physique (une liasse volumineuse ou un plan) ou à un document électronique stocké sur un support amovible (un CD-Rom ou une vidéo). Formalisation d'un lien vers un document archivé dans le SAE et défini comme devant être accessible depuis plusieurs points d'entrée ; il sert à alerter les utilisateurs de son existence. Note: un dossier papier sera généralement représenté et géré dans l'application comme un dossier physique. Il n'est pas envisagé qu'un dossier physique contienne des pointeurs pour chacun des documents d'un dossier d'archives papier, sauf en cas de recommandations particulières pour répondre à des exigences métier. Le pointeur peut aussi être considéré comme un terme spécifique au SAE.
Masquage / Redaction	Processus d'occultation ou de suppression d'informations dans un document engageant.
Messages électroniques / Electronic messages	Tout système de communication utilisant l'électronique dans la conduite des activités, en interne, entre les entreprises/organismes ou avec le reste du monde. Les exemples les plus connus sont le courriel, la messagerie instantanée et les SMS (service de messagerie courte). Source: National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004.
Métadonnées / Metadata	Informations structurées ou semi-structurées permettant de produire, gérer et utiliser les documents archivés dans le temps dans des domaines variés. Source: ISO 23081 – 1: 2006, Clause 4. Informations structurées qui décrivent et/ou permettent de

Terme	***Définition***
	retrouver, gérer, contrôler, interpréter ou conserver d'autres informations dans le temps. Source: Adapté de A Cunningham, 'Six degrees of separation: Australian metadata initiatives and their relationships with international standards', *Archival Science*, vol. 1, no. 3, 2001, p. 274.
Métadonnées d'archivage / Records management metadata	Métadonnées qui identifient, authentifient et contextualisent les documents engageants ainsi que les personnes, processus et systèmes de création, gestion, conservation et utilisation afférents, et les règles associées. Voir aussi **Métadonnées** Source: ISO 23081, Part 1, Clause 4.
Migration / Migration	Action de transférer des documents archivés d'un système vers un autre, tout en préservant leur authenticité, leur intégrité, leur fiabilité et leur exploitabilité. La migration renvoie à des tâches précises visant à assurer le transfert périodique de données numériques d'un matériel ou logiciel informatique vers un autre, ou d'une génération technologique vers une autre. Source: Adapté de ISO 15489, Part 1, Clause 3.13 et Part 2, Clause 4.3.9.2.
Mission / Function	1. Premier niveau d'un plan de classement métier. Les missions sont les principales responsabilités de l'entreprise/organisme pour atteindre ses objectifs. Source: Adapté de AS 4390, Part 4, Clause 7.2. 2. Unité la plus grande de l'activité métier dans un(e) entreprise/organisme ou un État.
Niveau de sécurité / Security category	Désignation hiérarchisée (« très secret », « protégé », etc.) attribuée à un utilisateur, à un rôle utilisateur, à un document numérique ou autre entité du plan d'archivage pour indiquer le niveau d'accès autorisé. Le niveau de sécurité reflète le niveau de protection qui doit être appliqué pendant l'utilisation, le stockage, la transmission, le transfert et la conservation du document. Voir aussi **Contrôle de sécurité** Source: Adapté de Cornwell Management Consultants (for the European Commission Interchange of Documentation between Administrations Programme), *Model Requirements for the Management of Electronic Records* (MoReq Specification), 2001, p. 107.
Objet numérique / Digital object	Objet pouvant être représenté par un ordinateur tel un type de fichier généré par un système particulier ou un logiciel (par exemple, un document en traitement de texte, un tableau, une image). Un document numérique peut comprendre un ou plusieurs objets numériques. Voir aussi **Composant.**
Outil de classement / Records classification tool	Dispositif ou méthode d'aide au classement, au nommage, à l'accès, au contrôle et au repérage des documents engageants, comprenant un plan de classement pour l'archivage, un thésaurus, un plan d'indexation ou un vocabulaire contrôlé.
PCM / BCS	voir **Plan de classement métier**
Plan de classement métier / Business classification scheme	1- Représentation conceptuelle des missions et des activités de l'entreprise/organisme. Le plan est une taxinomie dérivée de l'analyse de l'activité métier.

Terme	***Définition***
(BCS)	2- Document qui sert de base à l'élaboration des outils de classement comme les thésaurus fonctionnels et les plans de classement pour l'archivage. Voir aussi **Référentiel de conservation, Outils de classement** et **Taxonomie.**
Plan de classement pour l'archivage / Records classification scheme	Outil de classement hiérarchique qui, intégré à une application métier, peut faciliter la capture, le nommage, le repérage, la conservation et la destruction des documents. Un plan de classement pour l'archivage découle du plan de classement métier de l'organisation.
Profil utilisateur / User profile	Résumé de tous les attributs d'un utilisateur d'une application métier, c'est-à-dire toutes les données connues du système : nom d'utilisateur, identifiant et mot de passe, droits de sécurité et d'accès et droits d'accès fonctionnels. Voir aussi **Contrôle d'accès**
Référentiel de conservation / Disposition authority (et Disposal authority)	Outil méthodologique qui décrit les différentes séries de documents et définit pour chacune les durées de conservation et les sorts finaux associés. Voir aussi **Application du sort final, Catégorie de conservation** et **Durée de conservation.** Source: Adapté de AS 4390, Part 1, Clause 4.10.
Règles système / System rules	Politiques internes au logiciel qui peuvent être établies et/ou configurées par un administrateur pour gouverner les fonctionnalités d'un système donné et déterminer la nature des processus opérationnels qui s'y rapportent.
Responsabilité / Accountability	Principe selon lequel les individus, les entreprises/organismes et la collectivité doivent répondre de leurs actes. Les entreprises/organismes et leurs employés doivent pouvoir rendre compte aux autorités de contrôle, aux actionnaires ou à leurs membres et au public de la façon dont ils répondent aux obligations statutaires, aux exigences de l'audit, aux normes en vigueur, aux codes de bonnes pratiques et aux attentes de la collectivité.
Restitution / Render	Production d'une représentation d'un document lisible par l'homme, en général via un écran ou un tirage papier.
Rôle utilisateur / User role	Compilation ou liste normalisée de permissions fonctionnelles de l'application métier pouvant être accordées à un groupe déterminé d'utilisateurs. Source : Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 6.
Signature électronique / Digital signature	Mécanisme de sécurité inclus dans un document numérique rendant possible l'identification du producteur de l'objet numérique et pouvant aussi être utilisé pour détecter et tracer tout changement subi par lui. Source : National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004*. Adapté de *The Australian Government Information Management Office, Trusting the Internet: A Small business Guide to E-security, 2002, p. 43*.

Terme	***Définition***
Sort final / Disposition	Destinations possibles des documents lors de la mise en œuvre des décisions de conservation, de destruction ou de transfert des documents archivés, selon les règles énoncées dans le référentiel de conservation ou dans d'autres outils. Source: ISO 15489, Part 1, Clause 3.9
Spécification de conception / Design specification	Document détaillant les exigences relatives aux fonctionnalités, à la performance et à la conception à prendre en compte pour la construction d'un système. Ces spécifications détaillent ce qui est à bâtir, comment le construire et comment cela fonctionnera.
Suppression / Deletion	Processus qui enlève, efface ou oblitère des informations archivées sur un support, en dehors du processus de destruction. La suppression, au sein des systèmes électroniques, correspond au retrait du pointeur (l'information de localisation) qui permet au système d'identifier où une donnée particulière est stockée sur le support. Voir aussi **Destruction** et **Sort final.**
Système d'archivage électronique (SAE) / Electronic records management system	Système automatisé de gestion pour la production, l'utilisation, la maintenance et le sort final des documents produits et validés sous forme numérique et constituant une trace probante des activités. Ces systèmes conservent l'information contextuelle (métadonnées) et les liens entre les documents archivés afin de consolider leur valeur probante. L'objectif premier d'un système d'archivage électronique est la capture et la gestion des documents numériques. Ces systèmes sont communément appelés, en anglais, EDRMS. Voir aussi **Système de gestion documentaire et d'archivage électroniques**. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004.*
Système d'archivage mixte / Hybrid recordkeeping system	Système d'archivage gérant une combinaison de formats papier, électronique ou autre. Source: National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004.
Système d'archivage / Records management system	Dispositif visant à capturer, conserver et fournir un accès aux traces de l'activité au fil du temps, conformément aux exigences réglementaires et aux pratiques métier. Les systèmes d'archivage comprennent : les professionnels de l'archivage et les utilisateurs, une politique, des responsabilités et des délégations d'autorité, des procédures et des pratiques, des guides utilisateurs et d'autres documents utilisés pour appuyer et diffuser les politiques, les documents eux-mêmes, les systèmes spécifiques utilisés pour contrôler les documents, les logiciels, matériels et autres équipements et les fournitures diverses. Source: Adapté de AS 4390, Part 3, Clause 6.2.1.
Système de classification pour la sécurité / Security classification system	Série de procédures pour l'identification et la protection de l'information officielle dont la divulgation pourrait avoir des conséquences néfastes. Le système de classification pour la sécurité est mis en œuvre par des marqueurs qui montrent la valeur de l'information et indiquent le niveau minimum de protection à appliquer. Voir aussi **Classement et Niveau de sécurité**.

Terme	***Définition***
	Source: Adapté de Attorney-General's Department, *Commonwealth Protective Security Manual*, 2000.
Système de gestion des documents et d'archivage électronique / Electronic document and records management system (EDRMS)	SAE possédant des fonctionnalités de gestion documentaire.
Systèmes de messagerie électronique / Electronic messaging systems	Applications utilisées par les entreprises/organismes ou les individus pour envoyer, recevoir, stocker et retrouver des messages électroniques. Ces systèmes ne possèdent généralement pas de fonctionnalités d'archivage. Source: National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004.*
Taxonomie / Taxonomy	1. Classement des entités dans un système ordonné qui indiquant les relations naturelles. 2. Science, lois et principes de classement. Voir aussi **Classement**
Thésaurus / Thesaurus	1. Dans un thésaurus, le sens d'un terme est précisé et montre les relations avec les autres termes. Un thésaurus devrait fournir suffisamment de points d'entrée pour permettre aux utilisateurs de naviguer facilement des termes non préférentiels aux termes recommandés. 2. Outil de classement des documents comprenant une liste alphabétique et contrôlée de termes liés les uns aux autres par des liens sémantiques, hiérarchiques, d'association ou d'équivalence. Source: Adapté de AS 4390, Part 4, Clause 7.3.2.2; AS ISO 15489, Part 2, Clause 4.2.3.2.
Traçabilité / Tracking	Production, capture et conservation de l'information relative aux mouvements et à l'utilisation des documents archivés. Source: ISO 15489, Part 1, Clause 3.19.
Traçabilité / Action tracking	Processus par lequel les actions sont programmées et contrôlées en fonction des échéances des activités.
Trace probante / Evidence	Preuve d'une action (au-delà du sens juridique du mot preuve).
Transfert / Transfer	Processus de sort final consistant en un export effectif de documents électroniques (avec leurs métadonnées) ou ld'agrégats électroniques, suivi de leur destruction dans l'application d'origine. Les transferts peuvent s'effectuer d'un(e) entreprise/organisme vers une autre avec un changement de responsabilité, d'un(e) entreprise/organisme vers un service d'archives historiques, d'un(e) entreprise/organisme vers un tiers archiveur, d'une administration vers le secteur privé ou d'une administration à une autre. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 6.*

Terme	***Définition***
Transfert (garde) / Transfer (custody)	Changement de la propriété et/ou de la responsabilité de la garde des documents engageants.
Transfert (mouvement) / Transfer (movement)	Changement de localisation des documents.
Type de document / Record type	Définition d'un objet engageant doté d'exigences de gestion, de métadonnées et de règles. Les types de documents sont en principe normalisés ; des types de documents spécifiques sont des variantes de la norme qui permettent à un(e) entreprise/organisme de faire face aux exigences réglementaires (données personnelles ou concordance de données) pour certains groupes de documents. Source: Adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 5.
Vocabulaire contrôlé / Controlled vocabulary	Liste alphabétique contenant des termes ou des titres autorisés ou contrôlés de façon à ce qu'un seul et même titre ou une seule et même forme de titre désigne un concept ou un nom donné. Voir aussi **Thésaurus**. Source: Adapté de J Kennedy and C Schauder, *Records Management : A Guide to Corporate Recordkeeping*, 2nd edition, Longmans, Melbourne, 1988, p. 291.
Volume / Volume	Subdivision ou « partie » d'un agrégat, électronique ou non. Il s'agit souvent d'une partie de dossier close en raison de contraintes de taille et de durée. Par exemple, « formulaires de déclaration de dépense 2007-2008 ». Voir aussi **Agrégat**

B Lectures complémentaires

Australian Standard for Work Process Analysis for Recordkeeping, AS 5090 – 2003, http: //www.standards.com.au.

Cornwell Management Consultants (Programme de la Commission européenne relatif aux échanges de documentation entre administrations Programme de la Commission européenne relatif aux échanges de documentation entre administrations), *Modèle d'exigence pour l'organisation de l'archivage électronique*, mars 2001.
www.cornwell.co.uk/moreq.

Université d'Indiana, *Electronic Records Project,*
http: //www.libraries.iub.edu/index.php?pageId=3313.

Conseil international des Archives, *Authenticité des archives électroniques*, étude 13-1, novembre 2002 et 13-2, janvier 2004.

Norme internationale pour le Records Management, ISO 15489 – 2001 (inclus également la série de normes ISO 23081)

Archives nationales d'Australie, *Functional Specifications for Electronic Records Management Systems Software*, première mouture, février 2006.
http: //www.naa.gov.au/records-management/publications/ERMS-specs.aspx.

Archives nationales d'Australie, *Guidelines for Implementing the Functional Specifications for Records Management Systems Software, février 2006.*
http: //www.naa.gov.au/records-management/publications/ERMS-guidelines.aspx.

Université de Pittsburgh, *Functional specifications for Evidence in Recordkeeping: The Pittsburgh Project*. 1996,
http: //www.archimuse.com/papers/nhprc/BACartic.html.

C Exemple de check-list pour l'évaluation d'un SAE

Cet outil suppose que le SAE en question gère des documents engageants et que les documents traçant les activités ont été identifiés. On suppose également que les outils essentiels de l'archivage tels que le référentiel de conservation, le plan de classement des activités, la classification en matière de sécurité et les droits d'accès existent dans l'entreprise/organisme.

N°	**Élément à contrôler**	**État d'avancement/ commentaires**	**Niveau d'achèvement (1–5):** 5 = Satisfait 3 = Partiellement satisfait 1 = Non satisfait
GENERALITES			
	Est-ce que le personnel a été formé correctement à l'exercice de ses responsabilités en matière d'archivage ?		
ARCHIVER DES DOCUMENTS LIES A LEUR CONTEXTE			
	Le système peut-il figer/rendre statiques les documents engageants (à archiver) ?		
	Le système peut-il archiver les documents engageants en lien avec leur contexte métier ?		
	Le système peut-il capturer les métadonnées d'archivage exigées par les contraintes réglementaires et les besoins métier ?		
	Les liens entre les métadonnées d'archivage et les documents archivés sont-ils créés et maintenus dans le temps ?		
GERER ET CONSERVER LES DOCUMENTS ARCHIVES			
	Existe-t-il une politique et des procédures détaillées pour la gestion de l'archivage ?		
	Les documents archivés peuvent-ils prouver ce qu'ils prétendent être ; ont-ils bien été produits ou envoyés par les personnes indiquées ; et ont-ils bien été produits ou envoyés à la date indiquée ?		
	Les contrôles sont-ils suffisants pour protéger les documents archivés contre un accès, une modification, une suppression ou un usage non autorisé ?		
	Peut-on rechercher, afficher et consulter les documents archivés de manière explicite ?		

	Existe-t-il une politique et des procédures pour effectuer des audits réguliers du système d'archivage ?		
	Existe-t-il des sauvegardes et un plan de reprise d'activité pour le système ?		
	Existe-t-il une documentation complète et à jour du système (spécifications, manuels, conception, intégration, etc.) ?		
	Les documents signés électroniquement peuvent-ils être lus si besoin ?		
IMPORT/EXPORT ET INTEROPERABILITE			
	Si les documents sont stockés dans une entité, mais que la responsabilité de gestion et de contrôle appartient à une autre, les responsabilités respectives sont-elles bien définies, comprises et tracées ?		
	Les processus et mécanismes gérant l'accès aux documents archivés sont-ils bien conformes aux exigences de conservation, au-delà de la durée de vie du système ?		
	Les documents archivés peuvent-ils être transférés du système vers une institution archivistique ?		
CONSERVATION ET DESTRUCTION			
	Peut-on mettre en œuvre les sorts finaux recommandés par le référentiel de conservation ?		
	Les documents sont-ils bien conservés conformément au référentiel de conservation et non supprimés ou réécrits ?		
ARCHIVAGE MIXTE			
	Si le système d'archivage gère à la fois des documents papier et des documents électroniques, dispose-t-il d'une fonctionnalité d'archivage mixte ?		

`

Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique

Module 3

Recommandations et exigences fonctionnelles pour l'archivage des documents dans les applications métier

Publié par le Conseil international des Archives. Ce module a été élaboré par une équipe mixte constituée de membres du Conseil international des Archives et de l'*Australasian Digital Recordkeeping Initiative*.

ISBN : 978-2-918004-00-8

Référence à citer: Conseil international des Archives - Principes et exigences fonctionnelles pour l'archivage électronique – Module 3 : Recommandations et exigences fonctionnelles pour l'archivage des documents dans les applications métier, 2008, publié sur www.ica.org

TABLE DES MATIÈRES

1.1 Champ d'application et objectif 5
1.2 Publics cibles 7
1.3 Normes du domaine 7
1.4 Terminologie 7
1.5 Structure 8
2.1 Pourquoi est-il important de tracer les processus et activités métier ? 9
2.2 Panorama des applications métier et archivage 10
2.3 Définir les besoins de traçabilité des événements, actions et décisions dans les applications métier 11
2.3.1 Analyser les processus métier 11
2.3.2 Identifier les exigences de traçabilité des activités 13
Étape 1 – déterminer globalement les fonctions métier ainsi que les activités et actions particulières effectuées en totalité ou en partie par l'application 13
Étape 2 – considérer, pour chaque mission, activité, action ou processus gérés par le système, les traces que l'entreprise/organisme doit absolument conserver 13
2.3.3 Identifier le contenu et l'information de traçabilité qui constitue la preuve 14
Étape 3 – pour chaque exigence de preuve, identifier le contenu ou les données qui constituent la preuve 14
Étape 4 – identifier les informations additionnelles nécessaires pour que le contenu ait une valeur de preuve pérenne 17
2.3.4 Identifier les liens avec le système 18
2.3.5 Définir la meilleure stratégie d'archivage à partir d'une évaluation des différents scénarios 19
2.3.6 Évaluation des risques et des scénarios 23
2.3.7 Mise en œuvre 24
2.4 Utilisation des exigences fonctionnelles 26
2.4.1 Éléments-clés 27
2.4.2 Développer des spécifications conceptuelles pour une application métier avec des fonctionnalités d'archivage 28
Étape 1 – Évaluer les exigences fonctionnelles 28
Étape 2 – Vérifier la pertinence des exigences 29
Étape 3 – Vérifier la pertinence du niveau d'obligation 29
Étape 4 – Identifier les lacunes dans les exigences fonctionnelles 29
2.4.3 Analyser, évaluer et auditer les applications métier existantes 30
2.4.4 Lancer un processus d'évaluation 30
Préparation et recherche préliminaire 30
Identifier le besoin de traçabilité 31
Créer une check-list d'exigences 31
Évaluer l'application métier avec la check-list 31
Exploiter les résultats de l'évaluation et prioriser les améliorations 32

2.5 Modèles de relations entre entités 32
2.5.1 Catégories de documents et plan de classement pour l'archivage 33
2.5.2 Agrégats électroniques 34
2.5.3 Documents archivés électroniquement 35
2.5.4 Extraits 35
2.5.5 Composants 35
Intégration à d'autres systèmes 36
Exclusions 36
Types d'exigences 37
Niveaux d'obligation 37
3.1 Production et capture des documents engageants dans leur contexte 38
3.1.1 Production et fixation du document 39
3.1.2 Métadonnées d'archivage 42
3.1.3 Gérer les agrégats électroniques 44
3.1.4 Classement des documents archivés 44
3.2 Gestion et maintenance des documents archivés 45
3.2.1 Paramétrage des métadonnées 46
3.2.2 Réaffectation, reclassement, duplication et extraction des documents archivés 48
3.2.3 Reporting sur les documents engageants archivés 49
3.2.4 Processus de sécurité en ligne 50
Chiffrement 50
Signatures électroniques 52
Authentification 53
3.3 Import, export et interopérabilité 54
3.3.1 Import 54
3.3.2 Export 55
3.4 Conservation et destruction selon les règles 56
3.4.1 Conformité avec les référentiels de conservation applicables 57
3.4.2 Application du sort final 59
3.4.3 Révision 62
3.4.4 Destruction 62
3.4.5 Métadonnées de sort final 63
3.4.6 Reporting de sort final 64
A Glossaire 66
B Intégration des exigences d'archivage dans le cycle de vie des applications 76
1 Initialisation du projet 76
2 Planification 77
3 Analyse des exigences 77
4 Conception 77
5 Mise en œuvre 78
6 Maintenance 78
7 Revue du projet et évaluation 78
C Lectures complémentaires 80

1 INTRODUCTION

Les entreprises/organismes mettent en œuvre des systèmes pour automatiser leurs activités et leurs processus. Dès lors, le système métier, bien qu'il n'ait pas été conçu dans ce but, produit une information électronique qui se trouve souvent être la seule preuve ou trace du processus. Sans cette trace, les entreprises/organismes risquent de ne pas pouvoir répondre aux exigences de légalité et de responsabilité, aux besoins des métiers ou aux attentes de la collectivité.

Les systèmes métier étant par essence dynamiques et manipulables, la capture de documents engageants figés et la gestion de leur authenticité, fiabilité, exploitabilité et intégrité dans le temps représentent un véritable enjeu. Les entreprises/organismes courent alors un véritable risque de mauvaise gestion, d'inefficacité et de dépenses superflues.

Bien que certain(e)s entreprises/organismes possèdent un système d'archivage électronique (SAE),[1] celui-ci ne capture par forcément la totalité des documents engageants à archiver. L'objectif de ce document est d'aborder les lacunes en matière d'archivage du fait d'un recours croissant aux systèmes métier.

Ce document établit les lignes directrices pour identifier les besoins en archivage et y répondre au travers d'un jeu d'exigences fonctionnelles et génériques à introduire dans les logiciels métier. Ses objectifs sont :

- d'aider les entreprises/organismes à améliorer leurs pratiques d'archivage électronique ;
- de réduire les investissements et les coûts excessifs, en identifiant un minimum de fonctionnalités d'archivage à introduire dans les systèmes métier ; et
- de renforcer la normalisation des exigences d'archivage à destination des éditeurs de logiciels.

Le document ne préconise pas une démarche de mise en œuvre particulière. Ces spécifications peuvent être réalisées par le biais d'une interface ou par l'intégration de l'application au SAE, ou par l'ajout de fonctionnalités d'archivage au système métier.

1.1 Champ d'application et objectif

Ce document aidera les entreprises/organismes à s'assurer que les preuves (traces) de leurs activités produites par leurs applications métier sont correctement identifiées et gérées. Plus particulièrement, il aidera à :

- comprendre les procédures et exigences d'identification et de gestion des documents engageants dans les applications métiers ;

---

1 Un système d'archivage électronique est un type de système métier spécialement conçu pour gérer les documents engageants. Cependant, dans un souci de clarté et de concision, et pour les besoins de ce document, l'expression « système métier » devrait être comprise comme excluant les systèmes d'archivage électronique.

- formuler des exigences pour la prise en compte des fonctionnalités d'archivage dans les spécifications lors de la conception, de l'amélioration ou de l'acquisition d'un logiciel métier ;
- évaluer la capacité de gestion de l'archivage des logiciels internes ou des logiciels du marché intégrés ;
- réviser les fonctionnalités d'archivage ou évaluer la conformité de l'application existante.

Ce document ne fournit pas toutes les spécifications d'archivage mais il met l'accent sur un certain nombre d'exigences-clés, avec leur niveau d'obligation, peuvant servir de point de départ pour un développement ultérieur. Il faut insister sur le fait que les entreprises/organismes devront évaluer, amender et sélectionner les exigences en fonction de leurs environnements et contraintes tant métier que techniques et réglementaires.

Ce module se limite aux exigences de gestion de l'archivage et ne traite pas de la gestion du système en général. Les exigences conceptuelles telles que l'exploitabilité, les statistiques, la recherche, l'administration du système et sa performance dépassent le cadre de ce document. Le module suppose un certain niveau de connaissances en matière de développement de spécifications conceptuelles, de processus d'achat et d'évaluation, mais ces points seront moins détaillés.

La conservation à long terme des archives électroniques ne sera pas abordée explicitement dans ce document ; toutefois, les exigences relatives à l'export vont dans ce sens en permettant l'export des documents archivés vers un système de pérennisation, ou la migration régulière des documents vers de nouveaux systèmes.

Les conseils présentés dans ce module devraient être applicables pour l'archivage dans des environnements logiciels complètement intégrés et reposant sur des architectures orientés « services », mais ces scénarios ne sont pas présentés en tant que tels. Dans ces environnements, les principes et procédures applicables seront les mêmes mais une analyse complémentaire sera nécessaire pour définir quels processus et quelles données, dans l'ensemble des systèmes, constituent la preuve ou la trace de telle ou telle action.

L'utilisation du terme « système » dans ce document renvoie à un ordinateur ou à une application informatique, alors que, dans le monde de l'archivage, « système » inclut également les personnes, les politiques, les procédures et les pratiques. Les entreprises/organismes devront prendre en compte tous ces aspects, et s'assurer que les outils fondamentaux de la gestion de l'archivage, comme les référentiels de conservation[2], les règles de classification pour la sécurité de l'information et la familiarité avec le concept d'archivage existent, de sorte que les documents métier soient correctement gérés.

---

2 Outil méthodologique qui décrit les différentes séries de documents et définit pour chacune les durées de conservation et les sorts finaux associés.

1.2 Publics cibles

Ce document s'adresse en premier lieu aux équipes chargées de la conception, de la révision et/ou de la mise en œuvre de systèmes métier, tels que les analystes métier, les acheteurs et les responsables investissement des directions informatiques.

Sont également visés les professionnels de l'archivage impliqués ou associés à de tels processus ainsi que les éditeurs et développeurs de logiciels qui souhaitent intégrer des fonctionnalités d'archivage à leurs produits.

Partant du principe que ce document s'adresse à un large public, l'emploi de termes purement archivistiques a été réduit au minimum. Lorsqu'ils sont inévitables, le glossaire en annexe A en fournit des définitions. Certains termes essentiels sont également définis dans la section 1.4 « Terminologie ».

1.3 Normes du domaine

Suivant son axe prioritaire « archivage électronique et automatisation », le Conseil international des Archives a conçu un ensemble de recommandations et d'exigences fonctionnelles dans le cadre du projet relatif aux « Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique » :

Module 1 : Contexte et déclaration de principes

Module 2 : Recommandations et exigences fonctionnelles pour les systèmes d'archivage électronique

Module 3 : Principes et exigences fonctionnelles pour l'archivage dans les applications métier.

Le présent document constitue le Module 3 du projet. Il a été développé avec le soutien de l'*Australasian Digital Recordkeeping Initiative*.

Bien qu'il puisse être utilisé de façon autonome, les lecteurs auront avantage, pour une meilleure compréhension du contexte et des principes qui ont présidé à son développement, à se référer également au Module 1.

Les exigences fonctionnelles identifiées dans la partie 2 ont été établies à partir des exigences minimales d'archivage définies par la norme internationale sur le Records management, ISO 15489.

La norme de référence pour les métadonnées est ISO 23081 – 1: 2006, Information and Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles, et ISO 23081 – 2: 2007, Information and Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues.

1.4 Terminologie

Étant donné que ce document contient de nombreux termes dont le sens diffère selon la discipline, il est important de lire en parallèle le glossaire de l'annexe A. Certains des concepts-clés utilisés dans ce document sont également détaillés ci-dessous :

- Les **documents engageants** (à archiver) sont des informations produites, reçues et conservées à titre de preuve ou d'information par une personne physique ou morale, conformément aux obligations légales ou dans l'exercice

de ses activités.[3] Elles fournissent la preuve des activités et se présentent sous tous les formats.

- Les applications **métier,** dans le cadre de ce document, sont des systèmes automatisés qui créent ou gèrent des données relatives à l'activité d'un(e) entreprise/organisme. Ce sont les applications dont l'objectif est d'abord de faciliter les transactions entre un service et ses clients (système de commerce en ligne, système de gestion de la relation client, base de données *ad hoc* ou personnalisée, et systèmes de gestion financière ou des ressources humaines). Une application métier contient normalement des données dynamiques sujettes à des mises à jour constantes (données pertinentes), modifiables (manipulables), et ce sont des données vivantes (utilisées). Dans ce document, les applications métier excluent les systèmes d'archivage électronique.
- **Systèmes d'archivage électronique** (SAE) – systèmes spécialement conçus pour gérer la conservation et le sort final des documents engageants. Ils conservent le contenu, le contexte, la structure et les liens entre documents pour permettre d'y accéder et renforcer leur valeur de preuve. Dans ce document, les SAE sont distingués des applications métier dans la mesure où leur fonction première est la gestion des documents engageants (à archiver).

1.5 Structure

Ce document est divisé en quatre parties :

- **1ère partie : introduction** – qui décrit le champ d'application, l'objectif, le public visé et la structure de l'ensemble du document.

- **2e partie : lignes directrices** – qui contextualise l'importance de la gestion de l'archivage, définit les termes-clés et les concepts, et décrit le processus de définition des besoins d'archivage et d'identification des documents engageants dans les applications métier. Il souligne également quelques points et processus à prendre en compte lors de l'examen, de la conception, de l'achat ou du développement d'une application afin d'y inclure des fonctionnalités d'archivage.

- **3e partie : exigences fonctionnelles** – qui donne une vue d'ensemble des principales exigences fonctionnelles d'archivage à incorporer dans une application métier (appelées « exigences fonctionnelles ») et insiste sur le caractère obligatoire ou optionnel de ces exigences pour les applications métier.

- **4e partie : annexes** – qui fournit un glossaire des termes-clés et une liste de lectures complémentaires.

---

3 Norme internationale sur le Records management, ISO 15489.

2 LIGNES DIRECTRICES

2.1 Pourquoi est-il important de tracer les processus et activités métier ?

C'est souvent grâce aux documents qui tracent leurs engagements que les entreprises/organismes peuvent rendre compte de leurs activités. Les documents engageants constituent un actif non négligeable qui permet de se défendre, de mieux décider, de prouver la propriété immobilière ou intellectuelle, et de conforter les processus métier.

Les documents engageants sont ceux qui sont créés, reçus ou conservés à titre de preuve ou d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de ses activités[4]. Ils doivent être conservés pendant une durée préconisée par un référentiel de conservation.

Le défaut de fonctionnalités d'archivage dans les applications métiers peut entraîner une perte de traçabilité, des dysfonctionnements et l'incapacité de satisfaire aux exigences de responsabilité et aux obligations légales, ou encore une perte de mémoire institutionnelle.

Un document engageant est plus qu'un ensemble de données ; il est la conséquence ou le produit d'une action[5]. Un trait caractéristique des documents engageants est que leur contenu doit être fixé, c'est-à-dire qu'il doit être une représentation figée de l'action. Ce peut être un véritable défi pour les applications qui, par nature, contiennent des données dynamiques et fréquemment mises à jour.

Les documents engageants sont plus qu'un contenu ; ils comprennent aussi des informations sur le contexte de production et la structure des documents, formalisées en métadonnées. Les métadonnées figent le document dans son contexte métier et définissent les règles de gestion de son cycle de vie. Les métadonnées d'archivage servent donc à identifier, à authentifier et à placer les documents dans leur contexte, au moment de leur production mais aussi tout au long de leur vie.[6] Elles permettent de localiser, restituer et interpréter correctement les documents. La norme internationale ISO 23081 : Information and Documentation – Records Management Processes – Metadata for Records, Part 2 fournit un modèle générique de métadonnées d'archivage. Il arrive aussi que les entreprises/organismes doivent tenir compte de contraintes réglementaires locales ou nationales.

Un document engageant géré rigoureusement constituera :

- une aide à la décision claire, documentée et de qualité ;

---

4 Norme internationale sur le Records management, ISO 15489

5 Philip C Bantin, *Strategies for Managing Electronic Records: Lessons Learned from the Indiana University Electronic Records Project,* disponible à : http: //www.indiana.edu/~libarch/ER/ecure2000.pdf , 2003.

6 Norme ISO 23081 : Information et la Documentation – Records management – Metadata for Records, Part 2,

- une ressource documentaire pouvant prouver et justifier des activités de l'entreprise/organisme ;
- un élément de cohérence, de continuité et d'efficacité d'administration et de gestion.

La norme internationale sur le Records management, ISO 15489, constitue un guide pour bien archiver afin que les documents engageants soient et demeurent authentiques, fiables, complets, intègres et exploitables.

2.2 Panorama des applications métier et archivage

Les applications métier sont ordinairement conçues pour répondre à un certain type de processus métier. Les documents engageants (à archiver) étant le produit d'actions dont l'ensemble forme un processus métier (par exemple, les actions composant le processus d'une demande d'autorisation), il s'ensuit que l'intégration des fonctionnalités d'archivage dans les systèmes doit être entreprise du point de vue du processus métier.

Les processus métier qui offrent le plus de potentiel pour un bon archivage sont les processus fortement structurés, avec des actions bien définies où il est dit relativement clairement à quel moment des documents doivent être produits, voire sous quelle forme (formulaires...). En effet, l'archivage a plus de chance d'être intégré avec succès dans des systèmes gérant ce type de processus, parce que, par nécessité, leur conception tient compte des actions des processus métier. En outre, le développement de systèmes gérant ces processus métier passe normalement par une série d'étapes structurées, basées sur des outils et des techniques de développement de systèmes qui traitent généralement l'ensemble des phases du développement, depuis la planification et la conception jusqu'à la mise en œuvre et la révision. Enfin, dans un projet de développement de système bien géré, toutes les communautés qui au sein de l'entreprise/organisme exercent une responsabilité dans le système (depuis les utilisateurs des applications jusqu'aux spécialistes chargés de les développer) doivent se partager clairement les responsabilités de l'intégrité de la conception, du développement et de la maintenance du système (y compris l'intégrité des données elles-mêmes). Tous ces facteurs accroissent les chances d'une bonne intégration de l'archivage dans la conception des systèmes de gestion de processus métier structurés.

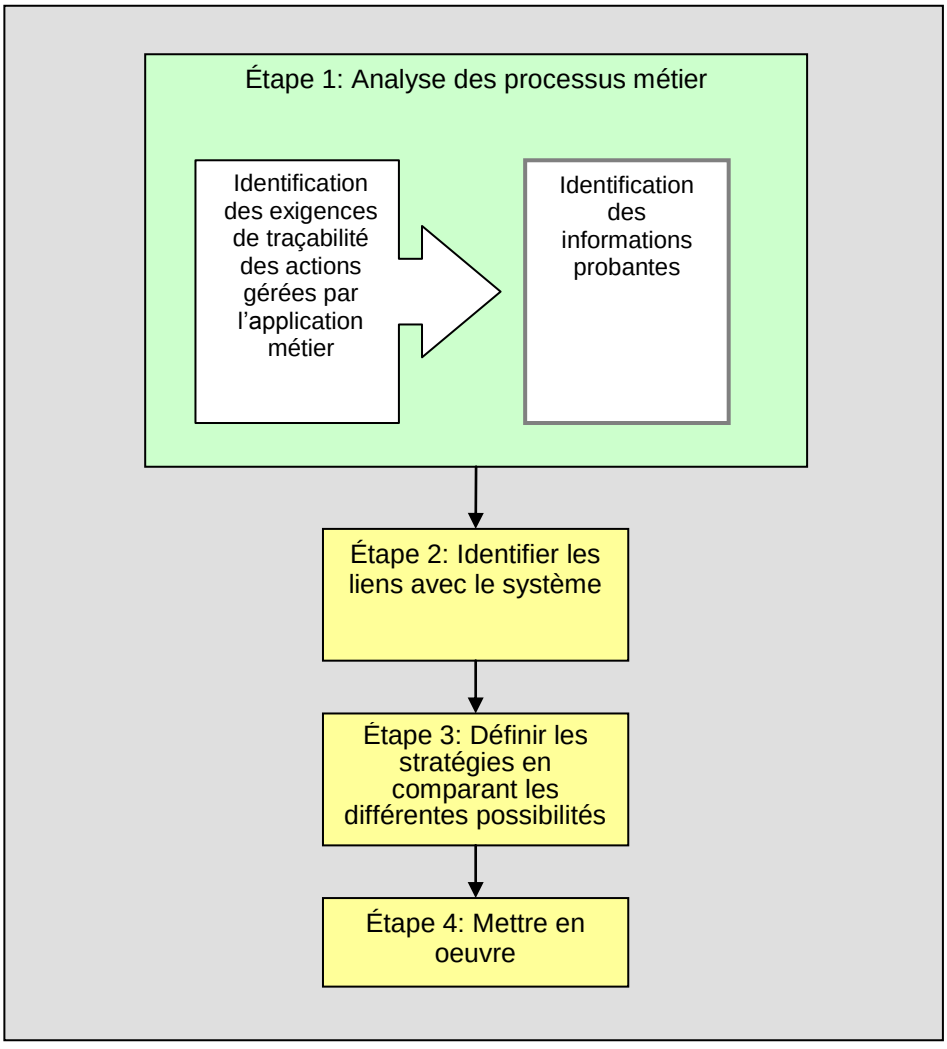
L'intégration de l'archivage est autrement problématique dans un environnement où les processus ne sont pas précisément définis, où l'on manque d'outils et de techniques pour une conception et un développement systématiques, et où la responsabilité des technologies utilisées (et plus encore de l'information générée dans cet environnement) n'a pas été clairement répartie. Dans ce contexte, les individus (tous types d'employés) sont largement autonomes pour décider quelles informations ils créent et partagent, comment ils les partagent, où ils les rangent, comment ils les organisent, les décrivent, les conservent, et quel est leur sort final. On constate souvent une prédominance des courriels et de leurs pièces jointes, avec peu de règles métier pour guider leur création, leur transmission et leur gestion. L'intégration de l'archivage dans un tel environnement est extrêmement difficile, car il manque les bases de processus métier précis (de workflow, pour employer le jargon

des bureaux modernes), une approche structurée du développement des systèmes, et une répartition des responsabilités (pour plus de détail, voir annexe B).

2.3 Définir les besoins de traçabilité des événements, actions et décisions dans les applications métier

Il n'est pas forcément nécessaire d'archiver à titre de preuve toutes les informations contenues dans un système métier. Avant toute révision, conception, construction ou achat de logiciels, il convient de définir ce que l'entreprise/organisme a réellement besoin d'archiver, de façon à développer et à mettre en œuvre les stratégies adéquates. La figure 1 présente ce processus, expliqué dans les pages suivantes.

Figure 1: Étapes pour définir les exigences d'archivage



2.3.1 Analyser les processus métier

En général, les applications métier stockent de grands volumes de données fréquemment mises à jour. C'est pourquoi, il est difficile de savoir quelle information dans le système nécessite d'être gérée comme un document engageant, preuve d'un processus ou d'une affaire.

Les applications métier peuvent contenir :

- une collection de données (ou données structurées) liées et contrôlées par le système, par exemple des données dans une base de données[7] ;
- des objets numériques individuels, contrôlés par le système et ayant un format de données clairement défini (informations non structurées ou semi-structurées), par exemple des textes, des courriels ou des feuilles de calcul ; ou
- une combinaison des deux.

L'identification des documents doit démarrer par une prise de recul vis-à-vis du système, c'est-à-dire par une analyse des processus de travail en lien avec les exigences règlementaires et les usages internes à l'entreprise/organisme afin de déterminer ce qui doit être conservé à titre de preuve.[8]

Les documents étant directement liés aux processus métier, l'identification de ceux qui doivent être archivés passe par des techniques et des outils standard d'analyse des processus, comme les schémas d'activité, les décompositions de processus et les organigrammes. [9]

Ce faisant, il importe de collaborer étroitement avec les professionnels de l'archivage au sein de l'entreprise/organisme, car il se peut que ce travail ait été largement entrepris lors de l'élaboration d'un référentiel de conservation.[10]

Ce processus d'identification des documents implique deux tâches principales :

1. identification des exigences de traçabilité et de preuve dans les affaires gérées par l'application métier ;
2. identification des éléments de traçabilité et de preuve qui constitue « le document engageant à archiver ».

---

[7] Ce document traite de la gestion des documents engageants constitués de données structurées plutôt que de données non structurées.

[8] Se référer à : National Archives of Australia, *DIRKS Manual: A Strategic Approach to Managing business Information*, disponible sur le site http: //www.naa.gov.au/records-management/publications/DIRKS-manual.aspx pour de plus amples informations.

[9] Pour plus d'informations sur la modélisation des processus métier, consulter le site de Process Modelling Notation : http: //www.bpmn.org/.

[10] A titre d'exemple d'un environnement réglementaire particulier, consulter : Queensland State Archives, *Guideline for the Development of Retention and Disposal Schedules*, à l'adresse http: //www.archives.qld.gov.au/downloads/rdschedule.pdf pour les recommandations concernant la mise en place d'un référentiel de conservation.

2.3.2 Identifier les exigences de traçabilité des activités[11]

Étape 1 – déterminer globalement les fonctions métier ainsi que les activités et actions particulières effectuées en totalité ou en partie par l'application

Cette analyse tiendra compte de la documentation relative au processus métier, les informations en entrée et en sortie et les politiques et procédures associées[12]. Dans les environnements fortement intégrés, une analyse des différents systèmes est nécessaire pour obtenir une vision complète des processus et des activités.
C'est notamment le cas du secteur public où plusieurs organisations peuvent partager leurs systèmes.

Étape 2 – considérer, pour chaque mission, activité, action ou processus gérés par le système, les traces que l'entreprise/organisme doit absolument conserver

Ces exigences peuvent avoir diverses origines. Il s'agit de se poser les questions suivantes :

- existe-t-il des obligations légales de tracer et d'archiver certaines informations ? Certaines législations peuvent implicitement ou explicitement affirmer la nécessité de formaliser certains documents et de les archiver.
- existe-t-il des outils réglementaires qui doivent être appliqués et qui exigent des traces pour prouver la conformité : normes obligatoires, codes de bonnes pratiques, etc. ?
- existe-t-il des règles d'organisation exigeant la production de documents probants : politiques, code de bonne conduite, rapports, etc. ?
- quelle traçabilité est requise pour les décisions qui jalonnent le processus métier lui-même ou pour éclairer la prise de décision future ?
- existe-t-il dans l'entreprise/organisme des missions ou des activités à haut risque ou susceptibles de litiges graves, qui exigeraient un niveau plus grand de traçabilité ?
- quelles sont les différentes parties concernées et quelles sont leurs attentes concernant la production de documents probants ?
- quelles sont les attentes de la collectivité en termes de traçabilité des activités des entreprises/organismes ?

Ce processus peut impliquer toute une série de consultations et de validations avec la direction générale. La norme internationale ISO/TR 26122-2008 sur l'analyse des

---

[11] Le terme de trace traduit ici le terme anglais « evidence » utilisé au sens de documentation formelle et probante d'une action (et non au sens restrictif de preuve juridique).

[12] Cette analyse peut déjà avoir été menée pour des objectifs de gestion de l'archivage comme la destruction ou le classement, ou lors du développement du système lui-même par l'analyse du processus métier.

processus d'archivage et le manuel australien DIRKS sont des ressources utiles pour atteindre ces objectifs.[13]

2.3.3 Identifier le contenu et l'information de traçabilité qui constitue la preuve

Il n'est pas forcément nécessaire d'archiver à titre de preuve toutes les informations contenues dans une application.

Étape 3 – pour chaque exigence de preuve, identifier le contenu ou les données qui constituent la preuve

Dans les systèmes qui gèrent des objets numériques individualisés, par exemple des documents en traitement de texte, les données sont déjà assemblées dans une structure logique. Il peut donc être relativement facile d'identifier les documents ou rapports dont le contenu peut servir de preuve de telle activité ou action.

Pour d'autres, il sera nécessaire d'analyser la structure des données, les modèles de données et les modèles de classement qui sous-tendent le système, pour identifier, parmi toutes les données, celles dont l'agrégation constitue le contenu à archiver et fournit la preuve nécessaire (voir à titre d'exemple les figures 2 et 3 ci-dessous).

Il est important de remarquer que le contenu ou les données qui constituent la preuve peuvent se trouver pour partie en dehors du système, par exemple dans d'autres systèmes, dans la documentation du système, dans des procédures, des documents sur papier, etc. Dans des environnements fortement intégrés, la preuve exigée peut être répartie entre divers systèmes, et certains systèmes ou composants peuvent être partagés avec d'autres organisations.

Les éléments susceptibles de constituer la preuve peuvent être nombreux et variés. On décidera alors quel contenu est le plus à même de former la preuve exigée, en se basant sur une évaluation des besoins et des risques métier. Les documents à archiver doivent être pertinents, c'est-à-dire qu'ils doivent être suffisamment probants pour rendre compte de la conduite des activités ou des actions effectuées. Une décision majeure sera donc largement documentée, tandis qu'une action de routine peu risquée pourra être tracée par un nombre restreint d'informations.

La figure 2 représente le contenu d'une base de données contrôlée par un système métier.[14] Dans cet exemple, le document à archiver[15] est constitué par l'agrégation

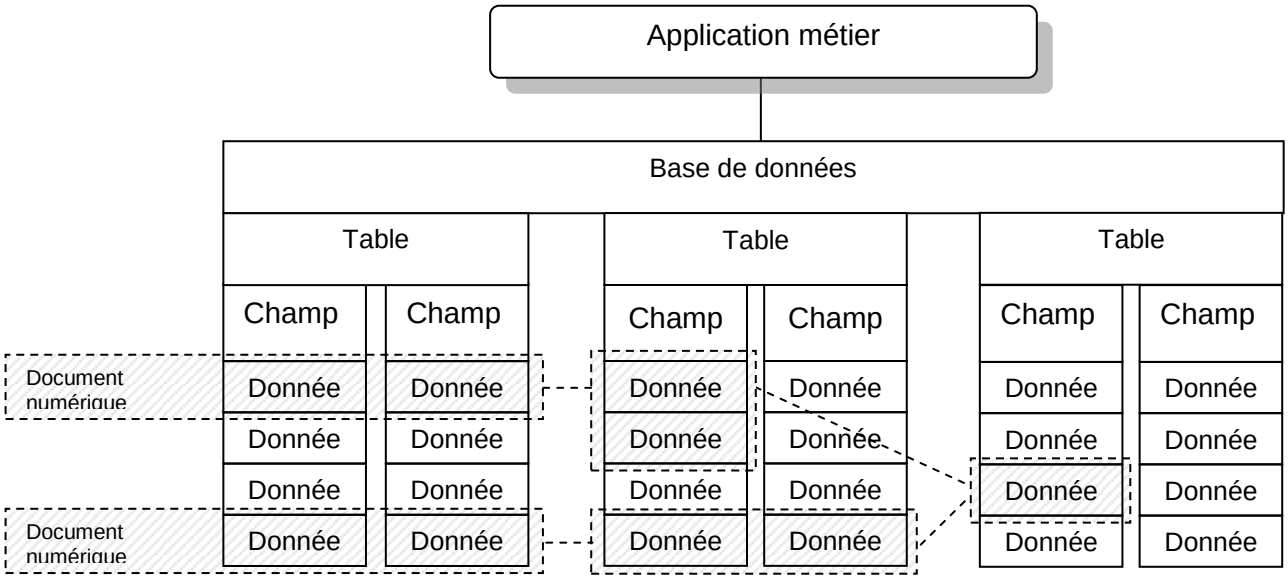
---

[13] DIRKS signifie Designing and Implementing Recordkeeping Systems (conception et développement de systèmes d'archivage). Les étapes A-C traitent de ce processus d'analyse. Pour plus d'information, se référer au manuel DIRKS sur le site des Archives nationales d'Australie concernant les stratégies de gestion de l'information métier et disponible à l'adresse suivante : http: //www.naa.gov.au/records-management/publications/DIRKS-manual.aspx. On peut aussi consulter, sur le site du State Records NSW (Archives d'État du New South Wales), *The DIRKS Manual: Strategies for Documenting Government business*, à l'adresse suivante : http: //www.records.nsw.gov.au/recordkeeping/dirks-manual_4226.asp.

[14] La figure 2 montre une base de données normalisée. Il est conseillé d'utiliser les concepts de base de données relationnelle et les techniques standard de modélisation de données et de normalisation, pour fournir la structure et le contexte nécessaires à la traçabilité du document à archiver.

de données provenant de différents champs. Un document est composé des données identifiées dans la base et des métadonnées exigées pour lier les éléments entre eux et fournir la structure et le contexte nécessaires à l'archivage.

Figure 2: Identification des composants d'information (ou données) constituant un document électronique engageant dans une base de données



A noter qu'un même document peut comprendre plusieurs données extraites d'un même champ ou d'une même table, et aussi qu'une même donnée peut faire partie de plusieurs documents.

La figure 3 montre un exemple très simple de tables au sein d'une base de données relationnelle dans un système de gestion des ressources humaines. Chaque table représente une partie de la base contenant des informations étroitement liées. Les tables A, B et C fournissent des données relatives, respectivement, au personnel, aux salaires et aux centres de coût. Les tables D et E fournissent les liens entre les données des autres tables. La table D relie les membres du personnel au montant de leur salaire, et la table E les relie à leur centre de coût.

Chaque table consiste en un certain nombre de colonnes qui représentent des champs contenant des données. Au sein de chaque table, les lignes établissent des liens entre des données des différents champs. Dans la littérature sur les bases de données, ces lignes sont quelquefois appelées « enregistrements ». *[Note des traducteurs : voir la note 15]*

Si l'on analyse le processus métier, il y a de nombreux documents potentiels dans la figure 3. Ces documents sont représentés sous forme d'un certain nombre de données qui peuvent être liées entre elles au sein d'une ou de plusieurs tables, et provenir d'un ou de plusieurs champs.

---

[15] Note du traducteur: la version anglaise introduit ici une note sur le double sens de record : document engageant (à archiver) et enregistrement informatique.

Figure 3: autre exemple de l'identification des éléments ou données constituant un document engageant électronique dans une base de données

Table A: Personnel				
Matricule	**Nom**	**Prénom**	**Adresse**	**Ville**
0078652	Lecomte	Michel	78 rue des Archives	Paris
0078653	Duval	Jeannie	55 rue de la Paix	Paris
0078654	Baldi	Enrico	7 corso Garibaldi	Turin
0078655	Lopez	Diego	1 calle San Clemente	Sevilla
0078656	Diouf	Fatou	67 rue du Port	Dakar

Table B: Salaires			
Code salaire	**Niveau**	**Année**	**Montant**
A41	APS4	Année 1	€45,000
A42	APS4	Année 2	€46,000
A43	APS4	Année 3	€47,000
A44	APS4	Année 4	€48,000
A51	APS5	Année 1	€54,000
A52	APS5	Année 2	€55,000
A53	APS5	Année 3	€56,000

Table C: Centres de coût	
Matricule	**Code salaire**
0078652	A53
0078653	A42
0078654	A42
0078655	A41
0078656	A51

Table D: Responsable de la paie		
Code service	**Cost centre**	**Directeur**
M001	Bureau de Paris	Jean Fontaine
S001	Bureau de Milan	Marco Siffredi
P001	Bureau de Dakar	Vital N'Gosso
C001	Bureau de Naples	Francesca Scotto

Table E: Relation Personnel - Centres de coût	
Matricule	**Code service**
0078652	M001
0078653	M001
0078654	C001
0078655	S001
0078656	P001

Légende	
	données constituant un document sur l'individu Fatou Diouf
	données constituant un document sur l'adresse d'Enrico Baldi
	données constituant un document sur le personnel du bureau de Paris

On distingue dans le système trois types de documents à archiver :

- Les lignes en jaune correspondent aux données constituant un document sur un employé. Ce document rassemble des données des cinq tables et contient des informations sur l'employé, son nom, son adresse, son salaire et son centre de coût.
- Les lignes en bleu correspondent aux données constituant un document d'identification d'un employé: nom, adresse et numéro matricule. Ces seules données pourraient constituer un document à archiver, mais le document créé par les lignes en jaune est plus complet et est préférable.
- Les lignes en rouge correspondent aux données constituant la liste de tous les employés relevant d'un centre de coût particulier. Ces lignes peuvent présenter une méthode alternative pour interroger les données contenues dans les tables.

A noter que dans ce scénario, l'information contenue dans la table B ne constitue pas un document mais seulement une partie du document sur le salaire du personnel. En effet, la table B ne contient que des données supplémentaires qui ne valent qu'en tant que composants d'un document, c'est-à-dire une fois rattachées à un employé figurant dans la table A. Les données de la table B proviennent vraisemblablement d'un document externe, par exemple une convention collective.

On remarquera aussi que dans certains cas, il peut y avoir chevauchement des documents issus d'une même base de données. Les données d'un document dans une base relationnelle peuvent aussi appartenir à d'autres documents générés par la même base de données. Par exemple, le document sur l'employée « Jeannie Duval » et le document sur le personnel du bureau de Paris contiendront les mêmes données extraites de la table A.

Lorsqu'il y a chevauchement des données formant deux documents, le système métier doit pouvoir garantir qu'il ne détruira pas les données partagées avant que les deux documents électroniques n'aient atteint leur durée de conservation minimale.

Étape 4 – identifier les informations additionnelles nécessaires pour que le contenu ait une valeur de preuve pérenne

Il s'agit des métadonnées d'archivage qui font partie intégrante du document engageant (à archiver). Les métadonnées d'archivage peuvent servir à contrôler la durée de conservation d'un document, à établir ses droits et restrictions d'accès, et à faciliter sa recherche et son repérage.

La production, la capture et la gestion des métadonnées sont essentielles pour que les documents puissent être identifiés, compris et repérés, et pour préserver leur authenticité, leur fiabilité et leur intégrité. Les métadonnées devraient être capturées en ligne à l'aide d'un modèle de métadonnées d'archivage, en accord avec les exigences réglementaires et/ou organisationnelles.

Il n'est pas nécessaire de conserver les métadonnées au même endroit que le contenu, du moment qu'elles sont liées ou associées aux données. Les métadonnées peuvent être conservées dans des systèmes externes au système métier en question, ou se présenter sous la forme de documents ou d'outils tels que des schémas XML, des modèles de données, des modèles de classement, qui

permettent aux documents de rester compréhensibles et significatifs de façon pérenne.

Il peut être difficile, particulièrement dans les bases de données, de distinguer le contenu du document de ses métadonnées. Par exemple, les métadonnées qui tracent le fait que telle personne a consulté tel document à telle date constituent elles-mêmes un document. Souvent, dans un système métier, les métadonnées se rapportent à tout le système ; elles visent globalement tous les documents du système, et non un document en particulier. Elles peuvent se trouver dans les règles ou la documentation du système, et non dans chacun des documents.

2.3.4 Identifier les liens avec le système

Une caractéristique essentielle des documents archivés est qu'ils ne peuvent pas être compris isolément. La nécessaire restitution des documents dans leur contexte peut exiger des informations supplémentaires relatives au processus ou au système métier, pour renforcer et fiabiliser les éléments de preuve, ou s'il s'avère nécessaire un jour de déplacer les documents d'un système vers un autre.

Ce sont notamment :

la localisation,

les pannes du système,

la taille,

les règles métier,

les formats de fichier,

la sécurité,

la gestion des données personnelles,

la structure des données,

le modèle des données et le plan de classement,

les règles de workflow,

l'historique des événements.

L'information relative au processus métier peut inclure des procédures ou des instructions qui montrent que les décisions sont prises dans le respect de la réglementation.

De plus, en accord avec la section 2.3.1 « Analyser les processus métier », de nombreux processus dépassent le cadre d'une seule application métier. Avant de développer une stratégie d'archivage dans les systèmes métiers, il convient donc de prendre en compte les liens qui seraient nécessaires avec les autres systèmes ou avec les dossiers papier.

Les durées de conservation constituent un élément-clé. Les documents engageants qui sont archivés doivent être conservés pendant un laps de temps commandé par la législation et la réglementation ou les besoins métier.

Les décisions relatives aux durées de conservation sont consignées dans un référentiel de conservation. Les entreprises/organismes devront prendre en compte les exigences de leur environnement réglementaire spécifique en matière de conservation et de destruction de documents.[16]

Les documents visés par des durées de conservation longues devront normalement être contrôlés de manière plus stricte afin de s'assurer qu'ils restent accessibles tout au long de la période requise par le référentiel de conservation. Si les demandes d'accès aux documents les plus âgés sont faibles, on peut décider de ne pas tout stocker dans le système vivant. Mais il est indispensable que les documents soient identifiés et repérables en accord avec les niveaux de service définis.

Archivage *versus* conservation et destruction de documents

Le terme « archivage » a des acceptions différentes selon les approches archivistique ou informatique (voir le glossaire à l'annexe A).

On aurait tort de croire que l'archivage des données sur des supports secondaires ou hors-ligne répond aux exigences d'archivage car cela ne satisfait pas aux exigences de conservation/destruction des documents. Les sauvegardes des applications pour des besoins de continuité ou de reprise d'activité ne satisfont pas non plus à ces exigences.

Pour plus de détail, voir Section 3.4 « Conservation et destruction selon les règles ».

2.3.5 Définir la meilleure stratégie d'archivage à partir d'une évaluation des différents scénarios

Après l'identification des documents à produire pour assurer la traçabilité des activités, avec les liens hiérarchiques et associatifs afférents, on peut définir la bonne stratégie de gestion de l'archivage, en se basant sur une évaluation des risques liés aux documents.

Pour être considéré comme une trace authentique et fiable, le contenu doit être fixé à un moment donné et être non modifiable. Les applications métier contenant généralement des données actives et dynamiques régulièrement mises à jour, il faut mettre en œuvre une stratégie de fixation des documents, qui dépendra du choix du système qui gérera l'archivage et de l'évaluation des différents scénarios.

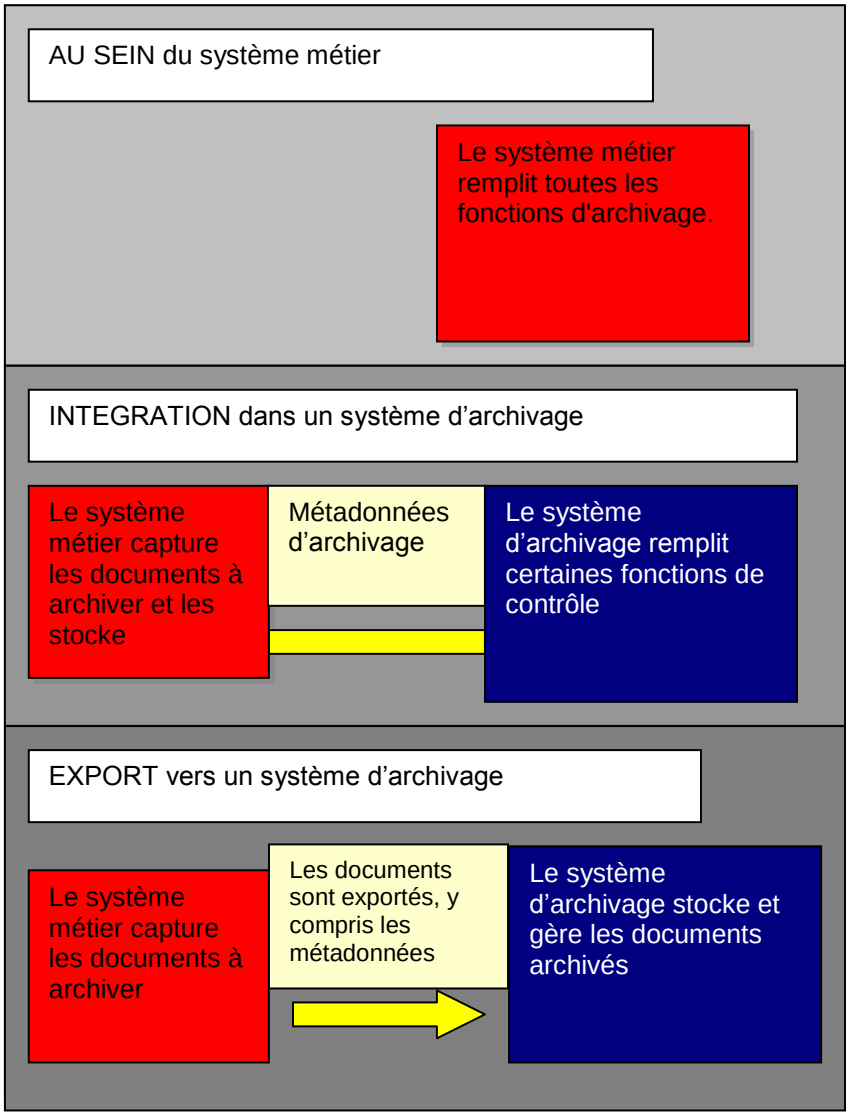
Avant toute utilisation des exigences fonctionnelles, il conviendra d'étudier quelles fonctionnalités d'archivage seront fournies par les mécanismes propres des applications métier, et quelles exigences seront satisfaites par une interaction avec des applications externes au système et capables de fournir les fonctions nécessaires à la gestion de l'archivage.

16 Pour plus de détail sur les exigences de destruction, se rapprocher, le cas échéant, de l'autorité compétente ou voir ISO 15489.

Les exigences fonctionnelles obligatoires présentées ici correspondent au noyau dur des processus d'archivage. Il existe différents scénarios de mise en œuvre de ces exigences, présentés dans la figure 4, notamment :

- conception du système métier de sorte qu'il possède les fonctions d'archivage en interne ;
- intégration dans un système d'archivage, par exemple un système d'archivage électronique ; ou
- conception d'une fonctionnalité d'export au sein du système métier afin d'exporter directement les documents engageants à archiver et leurs métadonnées dans tel système d'archivage.

Figure 4 : les différentes possibilités de système pour gérer les documents créés dans des systèmes métier.



Il existe d'autres possibilités, à explorer par les entreprises/organismes selon une démarche appropriée.

Pour les systèmes métier qui gèrent des objets numériques individualisés, la fixation des documents peut se faire par l'activation de l'attribut « lecture seule » et l'ajout de métadonnées d'archivage qui définissent les règles d'archivage et tracent l'utilisation du document dans le temps (métadonnées d'historique).

En revanche, les systèmes de bases de données contiennent en principe des données fréquemment mises à jour, manipulables et actives, ce qui présente un vrai défi pour assurer la fixité d'un document archivé. Les stratégies de réponse sont notamment :

- la conception de contrôles qui empêchent la réécriture ou la suppression de certaines données dans le système. Cela peut se traduire par l'autorisation de mettre à jour les champs mais en historisant les valeurs précédentes. Le document archivé est formé par la combinaison de certains champs avec les données historisées correspondantes. Cela ne veut pas dire que toutes les modifications de données doivent être conservées. Seules sont concernées les données identifiées comme correspondant aux exigences de traçabilité.

Exemple :

Un employé saisit les coordonnées d'un nouveau client dans le système. Plus tard, le client change de nom ; l'employé met à jour le système avec ces nouvelles données mais le nom originel reste dans le système et est géré et conservé comme un élément constitutif du document engageant.

Exemple :

Chaque année la valeur du capital d'une police d'assurance est automatiquement indexée et le champ « valeur du capital » est automatiquement mis à jour. Afin de tracer la valeur du capital au moment d'une demande d'indemnisation, quand le champ est mis à jour, l'information « valeur du capital » est transférée vers le champ « valeur précédente ». Le système conserve les valeurs précédentes pendant trois ans (mettons que la demande d'indemnisation doit être faite dans les trois ans) ainsi que les valeurs des années ou une demande a été faite, conformément au référentiel de conservation applicable. Le système déclenche la suppression des données périmées, en incluant les validations appropriées.

- l'agrégation des données sélectionnées (issues de la même table ou sélectionnées dans différentes tables) et création d'un objet numérique individualisé, fixe et non modifiable. Cela peut se traduire par la production d'un état ou d'une version « historisée » en lecture seule de la base de données.

Exemple :

Un(e) entreprise/organisme utilise un système métier avec workflow pour gérer un processus de demande de prêt. Quand une demande est finalisée, le système génère automatiquement un rapport détaillant les étapes de gestion du dossier, rapport qui est ensuite stocké comme un document engageant dans le SAE. Les métadonnées décrivant le contexte du processus, rassemblées tout au long du workflow, sont exportées avec le rapport vers le SAE.

Quelle que soit la stratégie retenue, il est essentiel que tous les processus fondamentaux d'archivage soient pris en compte, de sorte que les documents engageants soient non seulement archivés mais qu'ils puissent aussi être détruits correctement.

Exemple :

Les commandes clients sont enregistrées dans une base de données. Conformément au référentiel de conservation, les données de la commande doivent être conservées pendant deux ans après la clôture de la commande. Une fois par an, on réalise une requête pour identifier toutes les commandes clôturées depuis plus de deux ans. Un responsable vérifie les résultats et s'assure qu'aucune donnée ne se rapporte à des affaires encore en cours et, après validation, les champs concernés sont supprimés. Le résultat de cette requête, la validation, et la confirmation de la suppression sont conservés pour tracer le processus.

Le processus a été soigneusement conçu pour que seuls les champs relatifs à la commande soient supprimés, et que les coordonnées du client (qu'il convient de conserver plus longtemps) ne soient pas touchées.

La partie 3 « Exigences fonctionnelles » traite de ces exigences fondamentales, soulignées par ailleurs dans la section 2.4.1 « Éléments-clés ».

Plusieurs facteurs entrent en jeu pour décider de retenir telle ou telle démarche pour tel ou tel système :

- les besoins du métier incluant le niveau de risque pour une fonction donnée ; les fonctions à haut risque nécessitent une documentation et des contrôles d'archivage plus rigoureux ;
- le contexte général de l'archivage, précisant la préférence pour une approche distribuée ou centralisée de l'archivage ; et
- la faisabilité technique, en fonction des systèmes concernés ; il s'agit de savoir si l'entreprise/organisme possède un SAE et si le système métier peut lui être facilement intégré, quelles sont les fonctionnalités propres de l'application et quelles modifications on peut y apporter, quelle est la durée de vie espérée du système existant et s'il est pertinent d'y ajouter les fonctionnalités nécessaires.

Le tableau 1 présente les principales difficultés et avantages de chacune de ces possibilités.

Tableau 1 : Points d'attention pour le choix d'une démarche de gestion des documents engageants produits par les applications métier

Scénario	Avantages	Enjeux
Conception de l'application métier de sorte qu'il possède les fonctions d'archivage en interne	• L'archivage des documents engageants et leur gestion fait partie du processus métier • Si l'architecture technique est orientée composants, le composant archivage peut être réutilisé pour d'autres systèmes • Procure une plus grande possibilité d'historisation des données	• Les problèmes de stockage • Les coûts de développement accrus • Assurer une gestion cohérente des documents engageants à l'échelle de toute l'entreprise/organisme
Intégration dans un système d'archivage identifié, par exemple un SAE (archivage fédéré)	• Les documents engageants issus des applications métier peuvent être gérés collectivement avec des documents issus d'autres systèmes • Possibilité de réutiliser un système d'archivage externe	• La continuité du processus peut être affectée par la capacité du système d'archivage concerné • Difficultés au moment de la mise à jour de l'un des deux systèmes • Difficultés pour la restauration des données et la conservation d'un historique des événements • Une interface personnalisée peut s'avérer nécessaire
Conception d'une fonctionnalité d'export au sein du système métier afin d'exporter directement les documents à archiver et leurs métadonnées dans le système d'archivage	• Les documents engageants issus des applications métier peuvent être gérés collectivement avec des documents issus d'autres systèmes • Est sans doute plus adapté à des systèmes existants	• La duplication des documents dans l'application métier et dans le système d'archivage • Les défauts éventuels dans le processus d'import-export • Les utilisateurs doivent connaître deux systèmes (l'application métier pour les données actives et le système d'archivage pour l'information plus ancienne) à moins qu'une interface continue ne soit fournie.

2.3.6 Évaluation des risques et des scénarios

Le risque est un élément-clé pour la définition d'une bonne stratégie. Les risques sont variés : des documents engageants ni validés ni archivés, des archives détruites trop tôt, une accessibilité et une lisibilité non garantie dans le temps. Diverses conséquences peuvent en découler : mauvaise publicité, manque d'efficacité dans

les processus métier, handicap de l'entreprise/organisme dans la défense de ses droits.

Une solide évaluation des risques indiquera le niveau de traçabilité requis et le degré de rigueur avec laquelle l'archivage doit être contrôlé. Les entreprises/organismes qui relèvent de contextes réglementaires spécifiques avec différents niveaux de risque peuvent s'en servir pour prioriser les exigences.

L'évaluation des risques est d'autant plus indispensable si les éléments de preuve ou les documents archivés eux-mêmes sont en partie gérés par un tiers, ou si l'information se trouve dans des systèmes partagés entre plusieurs entités. Il convient d'établir si ce tiers ou ce système partagé est fiable et en mesure de maintenir l'intégrité et la traçabilité nécessaires pendant la durée requise. La stratégie de réduction de ce risque suggère de vérifier que la traçabilité requise est assurée par le système sous contrôle de l'entité responsable ou que les accords de partage des systèmes prévoient cette traçabilité.

Une étude de faisabilité peut aider les entreprises/organismes à évaluer de manière organisée leur capacité financière, technique, juridique ou opérationnelle à répondre aux exigences. Elle facilitera la prise de décision argumentée et transparente aux moments-clés du processus.

La faisabilité opérationnelle peut intégrer des questions telles que la nature et le niveau d'implication des utilisateurs dans le développement et la mise en œuvre du système, et le soutien apporté par la direction au nouveau système. La faisabilité technique peut inclure la connaissance des solutions technologiques existantes ou émergentes et la disponibilité d'une équipe technique qualifiée pour la durée du projet et la phase de maintenance ultérieure[17].

2.3.7 Mise en œuvre

La démarche de mise en œuvre étant propre à chaque stratégie, elle dépasse le champ d'application du présent document ; les exigences liées à la mise en œuvre de l'ensemble du système (par exemple la conduite du changement) également.

Cependant, un des aspects-clés de la mise en œuvre est de s'assurer que les rôles et responsabilités sont bien définis et approuvés. Le tableau 2 offre un aperçu d'une répartition possible de ces rôles. Dans la pratique, les entreprises/organismes devront définir d'autres rôles. Là où les systèmes sont partagés entre plusieurs entités, les rôles et les responsabilités de tous devraient être analysés, clairement compris et décrits.

[17] Pour en savoir plus sur l'analyse de faisabilité, voir les Archives nationales d'Australie, Manuel DIRKS : Une approche stratégique pour la gestion de l'information métier disponible (en anglais) http: //www.naa.gov.au/Images/dirks_A12_feasibility_tcm2-940.pdf.

Tableau 2: Rôles utilisateurs

Utilisateur	Toute personne ayant un droit d'accès l'application métier. C'est-à-dire quiconque qui produit et valide, reçoit, révise et/ou utilise les documents archivés dans ce système. C'est le niveau d'accès standard que possède la plupart des employés.
Administrateur de l'archivage	Utilisateur doté d'une habilitation particulière lui donnant un droit d'accès et de contrôle plus large sur les documents conservés dans l'application. Les administrateurs de l'archivage peuvent dans certains cas posséder des droits leur permettant d'effectuer les mêmes tâches que l'administrateur système, comme la possibilité de fermer et de rouvrir un dossier, de créer des extraits de documents et d'éditer des métadonnées. Les pouvoirs attribués aux administrateurs de l'archivage varieront en fonction des besoins de l'entreprise/organisme et du niveau de responsabilité des intéressés.
Administrateur système	Personne ou rôle ayant la responsabilité d'intervenir sur le système lui-même, par exemple, les fonctions de configuration et d'administration. L'administrateur système aura la responsabilité d'attribuer ou de retirer les droits d'accès aux utilisateurs et aux administrateurs de l'archivage.

Le tableau 3 présente un exemple de matrice de rôles et quelques exemples des fonctions qu'on peut attribuer à des utilisateurs (à développer). « Oui » indique que le système doit permettre d'associer le rôle à la fonction. « Non » signifie que le système doit empêcher d'associer le rôle à la fonction). « Optionnel » indique que le système peut permettre ou empêcher d'associer le rôle à la fonction et que l'entreprise/organisme doit préciser si ses politiques internes et ses procédures permettront ou interdiront cette association.

Tableau 3: Rôles et fonctions

Fonction	**Utilisateur**	**Administrateur de l'archivage**	**Administrateur système**
Produire et valider de nouveaux documents	Oui	Oui	Oui
Ajouter/éditer des métadonnées lors de l'identification des documents [18]	Oui	Oui	Optionnel
Accorder des autorisations de détruire un document ou, le cas échéant, un dossier	Non	Optionnel	Oui
Voir l'historique des événements	Optionnel[19]	Optionnel	Oui
Éditer les données de l'historique [20]	Non	Non	Non

[18] L'administrateur système peut déterminer quelles métadonnées les utilisateurs, ordinaires ou habilités peuvent ajouter lors de l'identification du document à archiver, y compris les métadonnées héritées automatiquement qui peuvent être modifiées ou écrasées.

[19] L'entreprise/organisme devra préciser s'il y a des raisons opérationnelles valables pour autoriser des utilisateurs à voir l'historique des événements.

2.4 Utilisation des exigences fonctionnelles

Les exigences fonctionnelles peuvent être utilisées de diverses façons, notamment :

- développer des exigences d'archivage à inclure dans les spécifications conceptuelles ou dans l'évaluation lors de la conception, la mise à jour ou l'achat d'un logiciel métier ;

- réviser les fonctionnalités d'archivage ou évaluer la conformité d'un système métier existant.

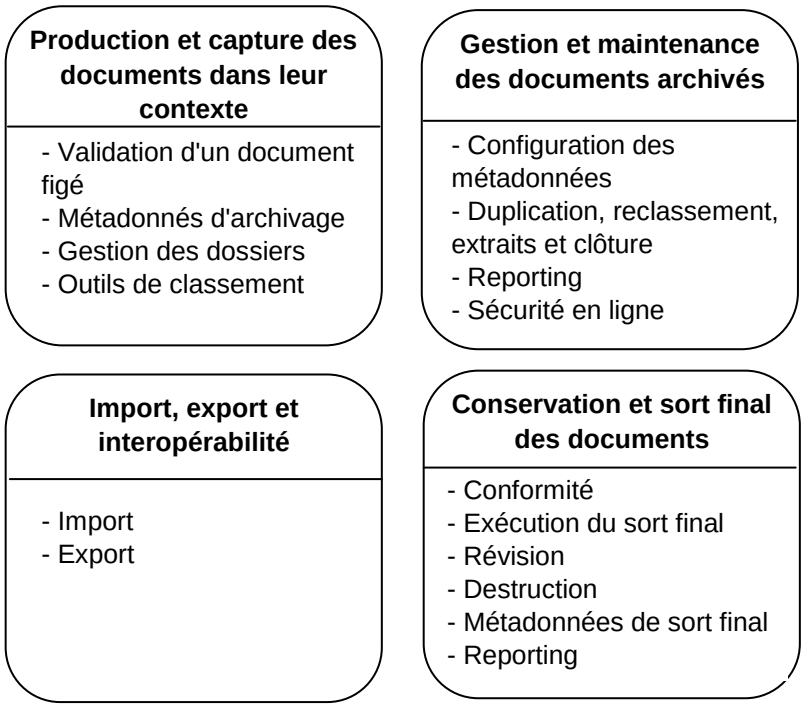
Avant d'utiliser ces exigences fonctionnelles, les entreprises/organismes devront clairement identifier leurs besoins en termes de documents engageants et d'archivage (voir la section 2.3).

20 Le système devrait empêcher toute modification de l'historique des événements y compris les modifications effectuées par l'administrateur système.

2.4.1 Éléments-clés

Les exigences fonctionnelles sont réparties en quatre secteurs-clés.

Figure 5: Secteurs-clés



- **Production et capture des documents dans leur contexte –** Les systèmes d'information qui supportent l'activité des entreprise/organismes doivent capturer la trace de cette activité. Cela suppose d'identifier dans le système un jeu de données électroniques qui constitue le document engageant à archiver. Les documents engageants doivent être reliés à leur contexte de production.
- **Gestion et maintenance des documents archivés –** Les documents archivés électroniquement doivent être gérés efficacement et conservés comme trace des activités de l'entreprise/organisme, en préservant leur authenticité, leur fiabilité, leur intégrité et leur exploitabilité. Les fonctionnalités qui garantissent l'authenticité, la fiabilité et l'exploitabilité des documents engageants relèvent de la conception des systèmes et dépassent donc le champ d'application de ce document mais leur importance est connue. L'aspect « gestion et maintenance des documents archivés » des exigences fonctionnelles traitera donc de fonctionnalités plus pointues.
- **Import, export et interopérabilité –** Les systèmes doivent garantir dans le temps l'interopérabilité entre les plateformes et les usages. L'information archivée doit donc être encodée de façon à rester compréhensible et apte à être modifiée si nécessaire, pour une migration vers de nouvelles plateformes technologiques.

- **Conservation et sort final des documents archivés –** Les documents archivés doivent être conservés et rester accessibles aux utilisateurs habilités aussi longtemps que la réglementation, la collectivité et les besoins métier l'exigent, avant d'être détruits ou de subir un autre sort, de manière raisonnée, systématique et auditable. Un archivage cohérent se caractérise par la conservation et la destruction des dossiers selon des règles précises.

Tout ceci est expliqué plus longuement dans la partie 3 « Exigences fonctionnelles ».

L'importance des métadonnées d'archivage

Les métadonnées d'archivage sont des informations structurées qui identifient, authentifient et contextualisent les documents archivés les personnes, les processus et les systèmes qui les produisent, les gèrent, les conservent et les utilisent ainsi que les politiques qui les régissent. Tandis que certaines métadonnées sont capturées au moment de la validation des documents, d'autres s'ajoutent tout au long de la vie du document. En fait, elles sous-tendent tout le processus d'archivage. C'est pourquoi, les exigences fonctionnelles pour les métadonnées d'archivage sont réparties dans toutes les parties-clés de ce document.

2.4.2 Développer des spécifications conceptuelles pour une application métier avec des fonctionnalités d'archivage

Les exigences fonctionnelles peuvent être utilisées pour préciser les fonctionnalités d'archivage dans les spécifications conceptuelles. Au cours du processus d'acquisition ou de conception, le logiciel métier devra être évalué en fonction des exigences énoncées dans ces spécifications, incluant les exigences d'archivage. [21] Les exigences fonctionnelles étant par nature génériques, un(e) entreprise/organisme devra les revisiter à la lumière de ses propres besoins et contraintes métier, ainsi que de ses obligations en matière d'archivage. Cette analyse aidera à identifier les fonctionnalités que l'application métier devra proposer.

Il est important que l'équipe projet s'appuie sur un panel d'experts : experts métier, experts en évaluation des risques, professionnels de l'archivage/records management, afin de garantir que les systèmes sont bien dimensionnés et adaptés aux risques identifiés.

Étape 1 – Évaluer les exigences fonctionnelles

Établir jusqu'où les documents engageants seront gérés par l'application métier. Par exemple, si l'application métier se limite à la production et à la validation des documents qui seront ensuite exportés puis gérés par un SAE, les exigences fonctionnelles serviront à identifier les exigences correspondantes à inclure dans les spécifications, ainsi que toutes les exigences relatives à l'intégration du système et à l'export des données.

Il faudra également évaluer la pertinence du caractère obligatoire ou optionnel des exigences pour voir si elles répondent bien aux besoins des métiers et aux besoins

[21] Le processus d'évaluation peut inclure la consultation de sites de référence offrant la possibilité d'étudier les fonctionnalités d'archivage d'une application métier.

d'archivage.

Parmi les questions à prendre en compte :

- telle exigence répond-elle bien aux besoins des métiers et aux besoins d'archivage ?
- les utilisateurs feront-ils usage des fonctionnalités définies dans cette exigence ?
- est-il moins coûteux et plus efficace de répondre au besoin par une solution extérieure à l'application métier ?

Étudier la mise en œuvre de fonctionnalités supplémentaires offrant une valeur ajoutée à l'application métier, et accompagner cette mise en œuvre. Supprimer toute fonctionnalité superflue.

Étape 2 – Vérifier la pertinence des exigences

Vérifier si la formulation des exigences fonctionnelles, telles que définies à l'étape 1, répond bien aux besoins de l'entreprise/organisme. La formulation de certaines exigences peut être affinée pour mieux coller à ces besoins.

Si les exigences retenues correspondent aux exigences fonctionnelles décrites ici, les entreprises/organismes sont invité(e)s à adopter les définitions du glossaire de l'annexe A. Les exigences utilisent en effet une terminologie très structurée, qui doit être conservée dans son contexte pour leur garder tout son sens.

Étape 3 – Vérifier la pertinence du niveau d'obligation

Évaluer le niveau d'obligation des exigences afin de faire les bons choix correspondant aux besoins métier.

Le niveau d'obligation des exigences fournit un guide d'utilisation pour le développement des spécifications conceptuelles d'un logiciel en interne. Suivant l'option choisie – gestion de l'archivage partiellement ou complètement développée dans l'application métier ou intégration avec un SAE – certaines exigences (même celles considérées comme obligatoires) peuvent ne pas être pertinentes.

Les entreprises/organismes devraient être très prudents avant de supprimer une exigence obligatoire ou d'en changer le niveau d'obligation. Cela suppose au moins d'identifier une solution alternative à la fonctionnalité décrite dans l'exigence. Par exemple, certaines exigences peuvent viser des fonctionnalités qui peuvent être mises en œuvre par une règle métier appropriée plutôt que par une solution logicielle.

Étape 4 – Identifier les lacunes dans les exigences fonctionnelles

Évaluer globalement l'ensemble des exigences fonctionnelles retenues afin de voir s'il y aurait d'autres besoins fonctionnels non couverts par ces exigences. Ajouter toute exigence nécessaire à combler les lacunes correspondantes.

2.4.3 Analyser, évaluer et auditer les applications métier existantes

Les entreprises/organismes peuvent utiliser les exigences fonctionnelles pour analyser et évaluer les fonctionnalités d'archivage dans les applications métier. Cela leur permettra d'avoir :

- une compréhension des forces et faiblesses des applications métier existantes pour une bonne gestion de l'archivage ;
- une appréciation réelle des risques liés à l'archivage (conséquence des faiblesses identifiées dans les applications métier) en termes d'activité et de responsabilité ; et
- une base d'information pour développer une stratégie d'amélioration des fonctionnalités d'archivage.

2.4.4 Lancer un processus d'évaluation

Le processus d'évaluation consiste à comparer formellement une application métier donnée avec les exigences fonctionnelles, et à en analyser les différences.

Lors de l'évaluation, il importe de considérer non seulement les fonctionnalités du logiciel, mais aussi l'environnement du système au sens large, y compris les règles et processus métier et les systèmes physiques ou électroniques associés. En effet, certaines exigences d'archivage peuvent être satisfaites par l'infrastructure supportant le système, plutôt que par le logiciel lui-même.

Lorsque des documents engageants sont gérés par un système extérieur à l'application métier, on devrait, pour évaluer la conformité avec les éléments obligatoires des spécifications, considérer le niveau de conformité des deux systèmes comme un tout.

Le but du processus d'évaluation variera selon la nature de l'analyse. Dans le cadre d'un audit, on se concentrera sur l'identification du niveau de conformité aux normes existantes, et des domaines où le système métier ne répond pas de manière adéquate aux exigences de l'entreprise/organisme en matière d'archivage. En revanche, une révision préliminaire à la mise à jour d'une application existante se concentrera sur l'identification des forces et faiblesses du logiciel en l'état, et des fonctionnalités qui pourraient être ajoutées pour mieux répondre aux besoins métier.

L'évaluation d'une application métier peut comprendre les tâches suivantes[22] :

Préparation et recherche préliminaire

Identifier la ou les applications informatiques qui feront l'objet de l'évaluation, ainsi que leurs composantes (bases de données intégrées, etc.), l'infrastructure qui les supporte et leur documentation. Effectuer une recherche préliminaire pour que le personnel chargé de la révision puisse se familiariser avec les processus métier

[22] On trouvera plus d'informations sur l'évaluation des systèmes existants dans National Archives of Australia, *DIRKS Manual: A Strategic Response to Managing business Information*, Step D, disponible sur http: //www.naa.gov.au/records-management/publications/DIRKS-manual.aspx

gérés ou contrôlés par cette application, avec le logiciel lui-même et avec les objectifs de l'évaluation.

Identifier le besoin de traçabilité

Avant d'évaluer la capacité du système à archiver correctement les documents, commencer par analyser et comprendre les processus métier, en identifiant les cas où l'activité ou l'action, parce qu'elle engage l'entreprise/organisme, doit être tracée formellement dans un document (voir la section 2.3).

Créer une check-list d'exigences

Rassembler toutes les exigences relatives aux besoins métier et d'archivage de l'entreprise/organisme, dans une check-list, avec le niveau d'obligation correspondant.

La check-list peut simplement reprendre les exigences, ou être rédigée sous forme d'une série de questions. Selon le but recherché, on proposera une réponse binaire (« oui » ou « non ») pour déterminer si telle ou telle exigence est remplie ou non, et on utilisera un système de notation du niveau de conformité (par exemple une échelle de 1 à 5). La méthode employée devrait permettre de déterminer clairement si l'application métier répond de manière adéquate à chaque exigence.

La check-list devrait comporter un espace pour les commentaires, de façon à détailler le cas échéant la façon dont chaque exigence est satisfaite. Il est particulièrement utile de s'informer sur les « solutions de contournement » adoptées par le personnel pour pallier les carences qu'il a pu percevoir dans le logiciel.

Évaluer l'application métier avec la check-list

Pour pouvoir utiliser la check-list de façon pertinente, on devra bien comprendre comment l'application gère les documents issus des processus métier. La norme ISO/IEC 15504 : « Technologies de l'information – Évaluation des processus » peut servir utilement de base à une évaluation.

Cette opération peut mêler des démonstrations participatives du logiciel et des entretiens avec les responsables métier, les administrateurs de l'application et ses utilisateurs. Ceci permet de comprendre l'interaction des fonctionnalités du logiciel avec les processus et procédures associés, afin d'avoir une vision complète de la façon dont chaque fonctionnalité d'archivage est ou n'est pas satisfaite. [23]

S'il s'avère que l'application métier ne satisfait pas à une exigence fonctionnelle donnée, il sera nécessaire de déterminer si cela est dû à une insuffisance conceptuelle du système, ou au simple fait que le système n'a pas été configuré pour répondre à cette fonctionnalité.

[23] Par exemple, telle exigence peut être satisfaite par un mécanisme de l'infrastructure qui supporte le système métier, comme une application informatique intégrée ou des processus manuels effectués selon les politiques et procédures de gestion de l'information en vigueur dans l'entreprise/organisme, plutôt que par le logiciel lui-même.

Exploiter les résultats de l'évaluation et prioriser les améliorations

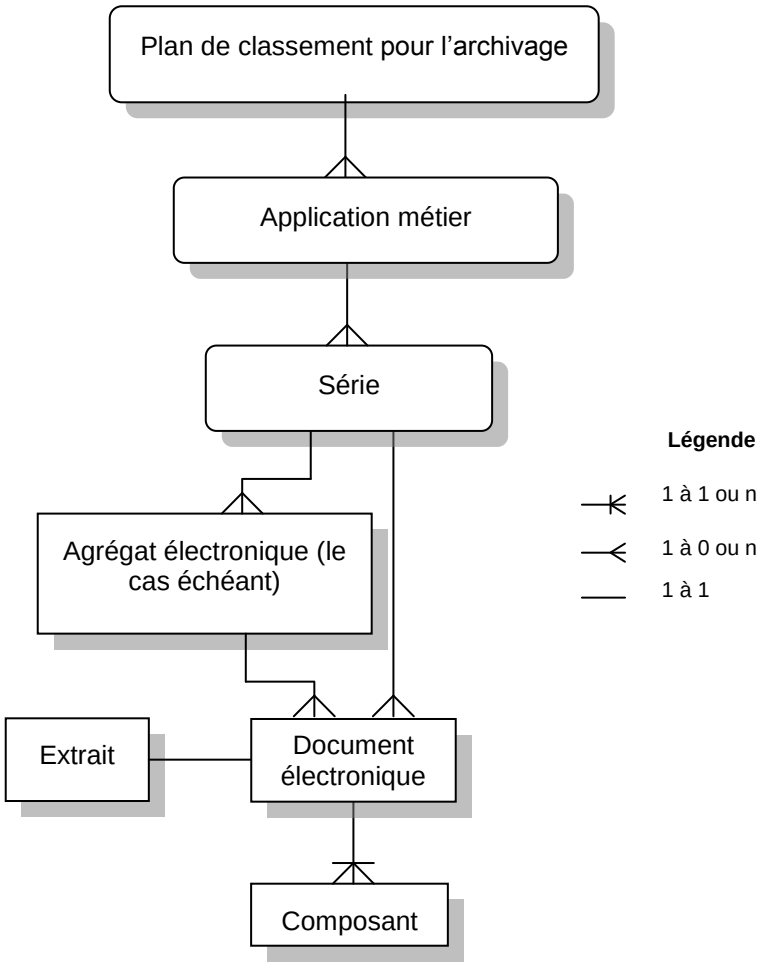
Exploiter les conclusions de l'évaluation, identifier les faiblesses et forces, et formuler des recommandations d'amélioration des fonctionnalités d'archivage. Les recommandations peuvent être priorisées selon le risque, l'importance et la faisabilité. Par exemple, si le développement du système n'est pas prévu dans un futur proche, on se concentrera sur l'amélioration du contrôle de l'archivage en révisant les processus ou les règles métier. En revanche, si l'évaluation est lancée préalablement à un redéveloppement du système, on pourrait donner la priorité à des mécanismes automatisés pour améliorer la gestion de l'archivage.

2.5 Modèles de relations entre entités

Les exigences fonctionnelles ont été développées à l'aide de la modélisation des relations entre entités.[24] La figure 6 présente le modèle conceptuel des relations nécessaires à l'archivage électronique dans une application métier. Chaque entité liée à l'application est décrite et expliquée ci-dessous.

Figure 6: Modèle des relations entre entités pour l'archivage électronique dans une application métier

24 Modèle conceptuel utilisé pour concevoir les systèmes d'information.



2.5.1 Catégories de documents et plan de classement pour l'archivage

Un plan de classement pour l'archivage est un outil de classement hiérarchique qui peut faciliter la capture, le nommage et le repérage, la maintenance et la destruction des documents archivés. Il définit la manière dont ces documents sont regroupés (agrégés) et reliés à leur contexte de production et de diffusion. Ce type de classement des documents archivés permet d'effectuer rapidement et efficacement la majeure partie des processus d'archivage.

Le plus souvent, les applications métier ne comportent pas nativement de plan de classement pour l'archivage ; ces documents engageants devront donc être rattachés à la catégorie appropriée du plan.[25]

Quoi qu'il en soit, pour certaines applications, on peut souhaiter inclure dans le système un plan de classement pour l'archivage, ou au moins un extrait du plan. Pour ce faire, on pourra utiliser les exigences fonctionnelles du plan de classement

25 Une catégorie est une subdivision du plan de classement qui peut elle-même être subdivisée en une ou plusieurs sous- catégories. Voir le glossaire à l'annexe A pour une définition plus détaillée.

exposées dans le module 2 « Lignes directrices et exigences fonctionnelles pour l'archivage électronique ».

La figure n°6 présente un modèle où des extraits de plan de classement pour l'archivage sont intégrés à l'application métier ; on peut aussi convenir de rattacher les documents archivés à des catégories extérieures au système. La définition préalable de règles par l'administrateur système peut fournir un mécanisme permettant le rattachement automatique des métadonnées associées à une catégorie extérieure aux documents engageants correspondants (ou aux agrégats de documents engageants, voir chapitre 2.5.2) dans le système métier. La définition de ces règles permet de garantir que, lorsque certains types de documents sont validés ou reçus dans le système, le jeu de métadonnées correspondant leur est attribué automatiquement.

2.5.2 Agrégats électroniques

Un agrégat électronique, par exemple un dossier, est un assemblage organique d'entités archivées électroniquement, dont le regroupement constitue une entité supérieure à l'objet électronique élémentaire. Les agrégats traduisent les liens qui unissent les documents engageants au sein d'une application métier. Ces relations se retrouvent dans les liens (via les métadonnées) et les associations existant entre les documents électroniques ou entre les documents électroniques et le système.

Une application métier peut contenir des agrégats, des documents archivés hors agrégat ou les deux. L'agrégation des documents archivés électroniquement peut améliorer la capacité du système dans la mise en œuvre des processus d'archivage. Ceci dit, dans les systèmes métier qui permettent ce type d'agrégations, il n'est pas forcément nécessaire de rattacher tous les documents archivés électroniquement à un agrégat dès leur validation. L'agrégat peut intervenir à plusieurs niveaux, selon les besoins du métier.

Le lien qui unit les documents d'un agrégat électronique peut être des caractéristiques ou attributs communs, ou un lien séquentiel entre les documents. La nature de la relation entre les documents électroniques d'un agrégat dépendra de critères tels que la finalité et la structure de l'application métier, ou le contenu et le format des documents eux-mêmes.

Par exemple, un agrégat électronique peut représenter un récit d'événements (un enchaînement logique d'opérations) au sein duquel les documents peuvent être reliés entre eux par un critère chronologique. Toute relation séquentielle de ce type entre les documents archivés électroniquement doit se traduire dans les métadonnées des documents : intitulés, dates, auteur, identifiant physique (le cas échéant) ou autres attributs. Lorsque de telles relations existent entre des documents engageants gérés par le système métier, ce dernier devrait être en mesure de les identifier, de les capturer, de les décrire et de les conserver.

Ces agrégats peuvent reposer sur des relations formellement structurées dans le cadre du système métier (par exemple des dossiers numériques contenant des documents numériques), ou peuvent simplement reposer sur des métadonnées reconnues par le système comme créant un lien entre les documents qui composent l'agrégat.

Les agrégats doivent être figés et pérennisés. Tout changement apporté à un agrégat doit être enregistré et expliqué. A noter que ces agrégats créés à des fins d'archivage ne devraient pas être confondus ni remplacés par les dossiers documentaires résultant de diverses recherches ou requêtes dans le système.

2.5.3 Documents archivés électroniquement

Le système doit être en mesure d'archiver et de gérer de multiples documents électroniques ainsi que leurs métadonnées. L'archivage des documents électroniques au sein de l'application métier dépend en grande partie des règles prédéfinies par l'administrateur système. Ces règles système fournissent le lien nécessaire entre l'application métier et les documents qu'elle gère. Elles permettent l'application des procédures d'archivage aux documents et déterminent pour l'essentiel le fonctionnement du système.

2.5.4 Extraits

Un extrait est une copie d'un document archivé électroniquement, dont une partie a été supprimée ou masquée de façon permanente. On crée un extrait lorsque le document n'est pas communicable dans son ensemble mais qu'une partie l'est.

Une application métier peut générer et conserver un ou plusieurs extraits d'un document électronique. Ces extraits doivent pouvoir être créés, conservés et gérés par l'application d'origine ou par une intégration ou une interface avec un autre logiciel.

2.5.5 Composants

Les composants sont des éléments constitutifs des documents numériques, par exemple, les composants multimédia d'une page Web. Les documents archivés électroniquement comprennent au minimum un composant. Ceux qui comprennent plusieurs composants sont appelés « documents composites ».

La nature des composants d'un document électronique donné variera suivant le système utilisé. Le composant peut être un objet numérique, comme un document numérique, ou une donnée, telle une entrée dans une base de données. Par exemple, le composant d'un document électronique dans un système de gestion documentaire peut consister en un simple fichier texte, alors que les composants d'un document électronique dans un logiciel de gestion des ressources humaines comprendront plusieurs entrées de la base de données liées étroitement entre elles (toutes les données relatives à un employé).

3 EXIGENCES FONCTIONNELLES

Cette section énumère les exigences fonctionnelles pour l'archivage des documents engageants dans les applications métier. Elle est divisée en quatre sections selon les concepts et processus-clés de l'archivage.

Les exigences fonctionnelles insistent sur les éléments-clés qui peuvent garantir une gestion pertinente de l'archivage sans entrer dans le détail de processus particuliers, dans la mesure où les techniques et stratégies utilisées pour atteindre les objectifs dépendent du type de système utilisé.

Chaque exigence détaille un aspect fonctionnel spécifique de l'archivage. Les sections et sous-sections correspondent à la figure 5 de la section 2.4.1 « Éléments-clés ». L'introduction de chaque section donne un résumé du concept d'archivage et de l'objectif global des exigences correspondantes.

Métadonnées d'archivage

Les métadonnées sont essentielles à une gestion pertinente de l'archivage. Contrairement aux métadonnées de recherche de contenu, les métadonnées d'archivage ne sont pas statiques mais s'enrichissent au fil du temps, en traçant les modifications et l'utilisation des documents archivés. Ce qui explique qu'elles soient réparties dans toutes les sections.

Intégration à d'autres systèmes

On admet (voir la partie 2) que l'entreprise/organisme choisisse de gérer l'archivage à l'extérieur de l'application métier. Cette option peut être mise en œuvre soit par l'export direct des documents à archiver, soit par l'intégration à un système d'archivage externe comme le montre la figure 4, section 2.3.5.

Le choix de la façon d'archiver les documents engageants influencera la sélection des exigences présentées ici ou leur modification pour les inclure dans l'application métier. Bien que les exigences soient exprimées en termes de fonctionnalités que l'application métier « doit » ou « devrait » avoir, on considère que, selon le modèle retenu, l'exigence ne sera pas forcément gérée directement par l'application métier en cause mais pourra l'être au travers d'autres outils, logiciels d'exploitation ou solution d'intégration ou d'export de données vers un système d'archivage externe.

Exclusions

Ces exigences fonctionnelles ne couvrent pas toutes les fonctionnalités traditionnelles des systèmes de gestion de l'information (par exemple : la facilité d'utilisation, la recherche, le reporting, l'accès, la sécurité et la sauvegarde), mais on sait bien que ces processus facilitent les fonctions d'archivage au sein du système. Par exemple, les contrôles d'accès et de sécurité contribuent à garantir l'authenticité et l'intégrité des documents engageants, et le reporting peut être utilisé pour identifier les documents à détruire.

Les exigences fonctionnelles supposent que les cas où l'action qui engage l'entreprise/organisme doit être tracée formellement dans un document ont déjà été identifiés (voir section 2.3).

Types d'exigences

Les spécifications contiennent deux types d'exigences :

- **Les exigences non conditionnelles** – exigences autonomes, indépendantes de toute autre.

Exemple:

L'application métier doit être en mesure de capturer et conserver les métadonnées d'un plan de classement métier ou du plan de classement pour l'archivage, en respectant les normes sur les métadonnées.

- **Les exigences conditionnelles –** exigences dont la mise en œuvre présuppose que l'application métier gère ou non telle exigence non-conditionnelle. L'exigence conditionnelle commence par : « Quand l'application métier [gère ou ne gère pas telle exigence particulière] elle doit/devrait/pourrait, etc. »

Exemple:

Si l'application métier gère des liens entre les fonctions de mise en œuvre du sort final et d'autres mécanismes de gestion de l'archivage, elle doit alerter l'administrateur en cas de révision des mécanismes de gestion des règles de conservation, et empêcher toute modification des catégories concernées jusqu'à la fin de la révision.

Les exigences conditionnelles suivent l'exigence non conditionnelle dont elles relèvent, quel que soit le niveau d'obligation ou la fonctionnalité d'archivage concernée. Ainsi, les exigences de destruction, conditionnées par le plan de classement, apparaissent à la section 3.1.4 « Classement des documents ».

Un numéro séquentiel a été attribué à chaque exigence non conditionnelle (de 1 à 125). Les exigences conditionnelles sont identifiées par l'ajout d'un numéro à celui de l'exigence non conditionnelle correspondante (par exemple, 3.1, 3.2).

Niveaux d'obligation

Le niveau d'obligation indique l'importance relative de chaque exigence fonctionnelle. Les mots tels que « doit », « devrait » ou « pourrait » doivent être interprétés comme suit :

- « Doit » - exigence dont le respect est indispensable pour la conformité à ces spécifications.
- « Devrait » - exigence qui peut être abandonnée s'il y a une raison valable, mais les conséquences de cet abandon devront être bien comprises et sérieusement pesées avant toute décision.
- « Pourrait » - exigence optionnelle.

Les niveaux d'obligation doivent être compris à la lumière de la réflexion précédente sur l'intégration à d'autres systèmes.

3.1 Production et capture des documents engageants dans leur contexte

La liste des exigences fonctionnelles ci-après est destinée à garantir:

La fixation des documents engageants – Les systèmes génèrent de l'information à toutes les étapes d'un processus métier. L'identification du besoin d'archiver des documents engageants devrait conduire à préciser à quel moment du processus les documents doivent être figés. Tout processus ultérieur doit entraîner la production d'un nouveau document ou un ajout à celui qui existe, plutôt que son altération. Les données à conserver pour tracer les décisions ou processus ne peuvent donc pas être écrasées, mais on peut en ajouter de nouvelles. L'évaluation des besoins d'archivage montrera parfois qu'il n'est pas nécessaire de conserver certaines données qui pourront donc être écrasées.[26] Il est important de garantir, si possible, que le système ne soit pas « verrouillé » au point que de simples erreurs (comme une faute de frappe dans un nom) ne puissent pas être corrigées, même si l'autorisation de modification est réservée à un administrateur système.

Lorsque l'on a déterminé quels documents l'entreprise/organisme a besoin d'archiver pour tracer un processus, on doit s'assurer que l'application métier est capable de les produire et de les capturer.

Le type et le volume des documents engageants qu'une application métier peut produire varieront selon la nature de l'activité traitée et les exigences d'archivage associées. Certaines applications métier pourront produire et capturer une large gamme de documents électroniques, utilisant des formats de données complexes (par exemple, les systèmes d'information géographique) ; d'autres systèmes ne pourront archiver que des documents électroniques simples d'un type unique.

Les documents engageants (à archiver) produits par une application informatique sont des objets numériques – documents bureautiques (textes, tableaux, etc.), sites internet, documents audio et vidéo – ou des formats de fichiers spécialisés et/ou d'autres données avec leurs métadonnées.

La production des documents engageants renvoie à l'identification d'objets numériques existants qu'il faut archiver, à la configuration du système pour garantir que telles actions sont bien enregistrées et non écrasées, ou à l'identification des champs (et des relations entre champs) qui peuvent être « extraits » comme trace d'un événement donné.

La capture des métadonnées d'archivage - Pour constituer une preuve significative d'un processus métier, les documents engageants (à archiver) doivent être liés au contexte de leur production et de leur usage. Pour cela, le document doit être associé à des métadonnées relatives au contexte métier.

Une grande partie de ces informations peut être générée automatiquement par le système. Les métadonnées figurent dans les exigences fonctionnelles à un niveau assez général. Plutôt que de détailler spécifiquement toutes les métadonnées requises, les exigences donnent les grandes orientations pour que certains types d'outils métiers puissent produire, capturer et préserver les bonnes métadonnées. Il revient à chaque entreprise/organisme de capturer ses

26 La décision de permettre l'écrasement des données peut être considérée comme une action de destruction : en fonction des exigences réglementaires, elle peut nécessiter d'être explicitement autorisée par un référentiel de conservation.

métadonnées en respectant une norme sur les métadonnées, conformément aux exigences organisationnelles et/ou réglementaires.

La gestion des agrégats et les mécanismes d'aide au classement (le cas échéant) – Les métadonnées sur l'activité peuvent se présenter sous forme de valeurs sélectionnées dans un plan de classement des activités ou un plan de classement pour l'archivage. En général, une application métier ne comporte pas de plan de classement ; c'est pourquoi cet aspect n'est pas détaillé dans ce module.[27] Pour les systèmes ne traitant qu'un nombre limité d'opérations, ces métadonnées pourront se trouver dans la documentation de l'application[28], plutôt que d'être directement associées à chaque document archivé.

3.1.1 Production et fixation du document

L'application métier doit pouvoir, seule ou en relation avec d'autres :

1	Assurer que les documents électroniques validés ou reçus par le système peuvent être capturés et stockés avec leurs métadonnées, quels que soient leur format et leurs caractéristiques techniques.[29]
2	Comporter des mécanismes de capture des documents numériques reçus par le système : • automatisés ou • semi automatisés.
3	Comporter des mécanismes garantissant sa capacité à capturer tous types de documents numériques, y compris ceux qui proviennent systèmes de gestion documentaire externes.[30] En voici quelques exemples : • applications bureautiques classiques, • logiciels de workflow, • systèmes de messagerie électronique, • systèmes de commerce en ligne, • systèmes de gestion de contenu sur Internet, • systèmes de conception et d'art graphique, • logiciels multimédia, • systèmes d'information d'entreprise, • systèmes de sécurité, • autres systèmes d'information métier. Les documents archivés peuvent comporter plusieurs composants.

27 Sur les exigences fonctionnelles relatives au plan de classement, voir *Module 2 : Principes et exigences fonctionnelles pour l'archivage électronique*

28 La documentation des applications peut comprendre: schémas, dictionnaires de données, modèles de données et de classement.

29 Les formats de fichier et les types de documents devraient être définis en fonction des besoins métier.

30 Ces systèmes devraient être choisis en fonction des besoins métier. A noter que chaque système métier ne recevra des documents à archiver que d'un nombre limité d'applications. Du reste, tous les systèmes ne sont pas capables de recevoir des documents d'autres applications.

	3.1 Quand l'application métier capture un document électronique composite, elle doit préserver le lien entre tous les composants et leurs métadonnées, de sorte qu'il soit géré comme un document unique et que son intégrité structurelle soit préservée. 3.2 Quand l'application métier valide ou reçoit des documents numériques provenant de systèmes de messagerie électronique, elle devrait pouvoir capturer les pièces jointes et les objets embarqués avec les messages comme s'il s'agissait de documents associés ou d'un document composite unique. 3.3 Quand l'application métier valide ou reçoit des documents numériques générés par des systèmes de messagerie électronique, elle devrait pouvoir effectuer une capture groupée de messages électroniques relevant de la même affaire. 3.4 Quand l'application métier valide ou reçoit des documents numériques issus d'Internet comme une page dynamique par exemple, elle devrait être en mesure de capturer le document comme : • un document composite unique, • un agrégat de composants reliés entre eux, • un instantané – à l'instant « t », • une série de composants que l'on peut reconstituer ou reproduire à la demande, ou • une combinaison de ces éléments. 3.5 Quand l'application métier valide ou reçoit des documents numériques générés par des systèmes de messagerie électronique, elle peut permettre la capture des messages et de leurs pièces jointes directement à partir d'une messagerie externe comme un client de messagerie. 3.6 Quand l'application métier valide ou reçoit des documents numériques générés par des systèmes de messagerie électronique, elle devrait pouvoir indiquer[31] si un message électronique a une pièce jointe dans le système, voir l'exigence 3.5. 3.7 Quand l'application métier valide ou reçoit des documents numériques générés par des systèmes de messagerie électronique[32], elle doit pouvoir capturer et identifier tous les messages entrant et sortant avec leurs pièces jointes.
4	Garantir que chaque document archivé ait un identifiant unique et stocker cet identifiant comme métadonnée du document.[33]

L'application métier devrait pouvoir, seule ou en relation avec d'autres :

31 Par exemple au moyen d'un symbole ou d'une icône spécifique.

32 Certaines applications (commerce en ligne par exemple), offrent la possibilité de créer et d'envoyer des messages électroniques à partir de leurs fonctions propres.

33 L'identifiant doit être unique au sein de l'application. Dans le cas où le document doit être exporté en dehors de l'application, l'identifiant doit même être unique au sein de l'entreprise/organisme, par exemple par ajout d'un préfixe.

5	Fournir une interface de programmation (API) ou l'équivalent permettant l'intégration à d'autres systèmes (notamment un système d'archivage électronique) de façon à : • permettre aux documents numériques validés ou reçus par l'application métier d'être exportés vers un système externe ; • permettre, au besoin, au SAE de s'interfacer avec l'application métier afin de pouvoir effectuer les contrôles d'archivage nécessaires sur les documents électroniques archivés ; et • fournir un mécanisme permettant à l'application métier d'importer des documents numériques directement d'un système externe[34], si les fonctions métier principales l'exigent.
6	Autoriser les utilisateurs à capturer et stocker dans leur format natif tous les documents numériques reçus par le système.
7	Ne pas limiter le nombre de documents pouvant être capturés et conservés par le système.[35]

L'application métier doit pouvoir, seule ou en relation avec d'autres :

8	Permettre à l'entreprise/organisme de définir le format ou la syntaxe de l'identifiant unique, lors de la configuration ou via des exigences *ad hoc*.
9	Être sollicité, au moment de la capture, pour convertir un document électronique de son format d'origine, propre à l'application initiale, dans un format compatible avec l'application métier.[36] 9.1 Quand l'application métier intègre la conversion des formats numériques dans le processus de capture[37], elle doit garantir que le contexte, la structure et le contenu du format d'origine sont conservés et que les exigences relatives à la conversion ont été respectées[38].
10	Faciliter le nommage des documents numériques : • soit par la saisie manuelle des noms par les utilisateurs ; • soit par un processus de nommage automatique défini par l'administrateur du système métier ou au travers d'exigences particulières.

34 Il est assez fréquent qu'une ou plusieurs applications soient suffisamment intégrées pour que le partage d'informations devienne une pratique opérationnelle normale. Cela implique souvent que les documents numériques soient transférés d'un système à l'autre dans un processus de workflow.

35 Les limites ne sont acceptables que pour répondre à une exigence métier du système. Si elles résultent d'incapacités techniques, elles sont inacceptables.

36 Il arrive que la conversion des formats soit une fonction propre de l'application métier. Il peut arriver aussi qu'un document se présente dans un format propriétaire non assimilable par l'application mais qui peut être converti dans un autre format lisible.

37 Cette exigence s'applique aussi à la conversion de format prise en charge par le processus d'import de masse, voir l'exigence 54.

38 Le terme « structure » est utilisé ici dans le sens archivistique de lien entre les composants du document archivé, par opposition aux structures de stockage de données à l'intérieur d'un système donné.

	10.1	Quand l'application métier permet le nommage des documents numériques, elle devrait fournir des outils de nommage comme : • un vérificateur orthographique, ou • une alerte quand un utilisateur tente de produire et valider un document en utilisant un nom existant déjà dans le système.
	10.2	Quand l'application métier permet le nommage des documents numériques, elle devrait être capable de limiter la possibilité de changer le nom du document à l'administrateur du système ou à un utilisateur dûment habilité.
11	Fournir des mécanismes pour garantir qu'un document électronique reçu par l'application peut être capturé même si l'application initiale n'est pas reconnue par le système d'exploitation.[39]	

3.1.2 Métadonnées d'archivage

L'application métier **doit** pouvoir, seule ou en relation avec d'autres :

12	Gérer la variété de métadonnées décrites dans les normes de référence sur les métadonnées et toutes les autres métadonnées nécessaires à la gestion des affaires.
13	Être capable de capturer automatiquement les métadonnées créées par une application de référence[40], un système d'exploitation, un système d'archivage électronique[41] ou produites par l'application elle-même.[42]
14	Capturer toutes les métadonnées définies lors de la configuration du système, et les conserver en relation étroite[43] et permanente avec les documents concernés.
15	Restreindre la possibilité de modifier les métadonnées d'archivage, de sorte que : • lors de la production/capture, un utilisateur ne puisse corriger que certaines métadonnées; • lors de la production/capture, d'autres métadonnées ne puissent être corrigées que par un utilisateur habilité ; et • les métadonnées ne puissent être corrigées par la suite que par un utilisateur habilité.

39 Cette exigence s'applique particulièrement aux systèmes transactionnels qui reçoivent une grande variété de formats à capturer.

40 Cas où le document à archiver est reçu par l'application métier et non produit par elle. L'application de référence peut être une autre application métier qui envoie directement les documents à archiver dans le système.

41 Cas où l'application métier exporte les documents engageants qu'elle a produits ou reçus vers un SAE pour y être stockés et gérés : les métadonnées d'archivage générées par le SAE doivent être capturées et attachées au document. Les modalités de gestion des métadonnées dépendront du niveau d'intégration entre l'application et le SAE.

42 L'application métier génère les métadonnées d'archivage des documents engageants qu'elle produit, ainsi que celles des documents qu'elle reçoit en provenance d'applications logicielles externes.

43 Le lien entre les métadonnées et les documents numériques auxquels elles se rapportent doit être solide et indéfectible.

	Les restrictions peuvent être précisées dans les exigences ou lors de la configuration par l'administrateur système.
16	Donner la possibilité à un administrateur système ou à un utilisateur habilité de modifier ou d'écraser les métadonnées héritées par les documents et par les agrégats.
17	Autoriser la mise à jour manuelle ou automatique de toutes les valeurs de métadonnées attribuées lors du classement ou après le reclassement d'un document ou d'un agrégat.[44]
18	Stocker les métadonnées sans limite de temps, même si le document concerné a été transféré aux archives historiques, supprimé ou détruit.[45]

L'application métier **devrait** pouvoir, seule ou en relation avec d'autres :

19	Capturer les métadonnées saisies manuellement par un utilisateur.
20	Permettre d'ajouter : • des métadonnées personnalisées pour les documents électroniques, • un jeu de métadonnées particulier pour tel ou tel type de document, • le caractère obligatoire ou non [46] des métadonnées, à préciser dans les exigences ou lors de la configuration par l'administrateur système.
21	Permettre l'ajout de métadonnées définies par les utilisateurs pour développer la description des documents et, le cas échéant, des agrégats.
22	Conserver dans les métadonnées la trace du reclassement d'un document archivé ou d'un agrégat, y compris la localisation initiale d'un agrégat.[47]

L'application métier **pourrait** :

23	Permettre à l'administrateur système de paramétrer l'outil avec des règles[48] pour l'attribution de métadonnées au moment de la capture d'un document ou, le cas échéant, d'un agrégat d'un type particulier. 23.1 Si l'application métier permet de paramétrer des règles d'affectation des métadonnées à la capture, l'élaboration et la modification de ces règles doivent être réservées à l'administrateur système.

44 Cette exigence concerne la révision de tous les plans de classement applicables dans des applications métier, et pas seulement le plan de classement pour l'archivage de cette application. Dans le cas où l'application métier n'a pas de plan de classement, la mise à jour du plan de classement de l'entreprise/organisme devra sans doute se faire manuellement.

45 Les métadonnées peuvent être stockées directement par l'application métier, dans un entrepôt d'objets numériques intégré, ou exportées vers un autre système.

46 Les degrés d'obligation devraient se conformer aux normes sur les métadonnées.

47 Voir les exigences d'historique des événements pour tout système.

48 Ces règles peuvent fournir un mécanisme de substitution pour attribuer les métadonnées lors de la production et validation du document. Cette méthode est particulièrement utile pour les systèmes gérant un nombre limité de types de documents, ou qui ne sont pas en mesure d'absorber un plan de classement pour l'archivage.

	23.2 Si l'application métier permet de paramétrer des règles d'affectation des métadonnées à la capture, elle devrait permettre, en cas de modification des règles du système, l'attribution rétrospective de métadonnées à un document ou à un agrégat.

3.1.3 Gérer les agrégats électroniques

L'application métier **pourrait**, seule ou en relation avec d'autres :

24	Permettre la production/capture et/ou la réception d'agrégats électroniques où les documents sont reliés par des métadonnées d'archivage de sorte que le processus d'archivage puisse s'appliquer à tous les documents de l'agrégat.[49] Quand l'application métier gère des agrégats, elle **doit** : 24.1 Pouvoir générer un identifiant unique pour chaque agrégat produit par le système.[50] 24.2 Pouvoir enregistrer automatiquement dans les métadonnées de l'agrégat ses date et heure de production/capture. 24.3 Permettre à l'administrateur système de paramétrer les mécanismes de nommage pour les agrégats. 24.4 Permettre à l'administrateur système ou à un utilisateur habilité de retirer des documents d'un agrégat électronique pour les affecter à un autre. 24.5 Garantir que les documents reliés à un agrégat électronique y restent bien attachés en cas de reclassement de cet agrégat et que tous les liens structurels sont maintenus. 24.6 Garantir que le détail des modifications opérées sur le contenu d'un agrégat est bien enregistré et conservé dans ses métadonnées. 24.7 Empêcher durablement la destruction ou la suppression d'agrégats, à l'exception du cas cité à la section 3.4 « Conservation et destruction selon les règles ». 24.8 Garantir que toute action de sort final appliquée à un agrégat est déclinée sur tous les documents composant cet agrégat.

3.1.4 Classement des documents archivés

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

25	Permettre de classer les documents archivés et, s'il y a lieu, les agrégats, en cohérence avec le plan de classement pour l'archivage de l'entreprise/organisme.[51]

49 La nature des agrégats dépendra du type d'application et de ses fonctionnalités.

50 L'identifiant doit être unique dans le système. Si un agrégat doit être exporté hors du système, l'identifiant devrait être unique au sein de l'entreprise/organisme, par exemple en lui ajoutant un préfixe.

51 L'intégration d'une fonctionnalité de classement des documents archivés dans l'application métier facilitera la mise en œuvre automatique du processus d'archivage.

26	Favoriser les liens et interactions entre le plan de classement pour l'archivage et les autres processus de gestion tels que la capture, l'accès, la sécurité, le sort final, la recherche, le repérage et le reporting.

3.2 Gestion et maintenance des documents archivés

A partir du moment où ils sont validés, les documents engageants doivent être gérés et conservés aussi longtemps que requis. L'archivage doit garantir aux documents engageants les caractéristiques suivantes : [52]

- **Authenticité :** on peut prouver que le document est bien ce qu'il prétend être, qu'il a bien été créé ou envoyé par la personne qui dit l'avoir créé ou envoyé et qu'il a bien été créé ou envoyé à la date indiquée.
- **Fiabilité** : on peut se fier au document pour être une représentation complète et fidèle des actions dont il atteste et s'y référer en toute confiance dans le cadre d'opérations futures.
- **Intégrité :** le document est complet, non altéré et protégé contre toute modification non autorisée. Cette caractéristique est également appelée « inviolabilité ».
- **Exploitabilité** : le document peut être localisé, repéré, préservé et interprété.

Les exigences fonctionnelles ci-dessous ne suffisent pas à garantir que tous les documents archivés dans les applications métier possèdent ces caractéristiques. Les contrôles d'accès et de sécurité traditionnels contribuent au maintien de l'authenticité, de la fiabilité, de l'intégrité et de l'exploitabilité et devraient donc être correctement activés. Toutefois, cette fonctionnalité étant en général prévue dans les applications métier (voir section 3.1), elle ne figure pas dans les exigences fonctionnelles ci-dessous.

Le niveau de rigueur des contrôles peut être défini à partir d'une évaluation des risques. Par exemple, dans un environnement à haut risque, il peut être nécessaire de prouver précisément un événement, sa date et son auteur. Ce sont les habilitations et les journaux du système qui peuvent prouver que les actions sur le système sont effectuées par des personnes habilitées. Ainsi, la sécurité, les journaux, les contrôles des accès (y compris pour la correction et la modification des données) et les outils de recherche sont des exigences courantes des systèmes pour garantir aux documents archivés les caractéristiques requises.

Ces exigences fonctionnelles visent à ce que :

- **les métadonnées d'archivage puissent être paramétrées** : l'application métier peut traiter toute une variété de métadonnées et faciliter leur gestion.
- **les documents archivés puissent être réaffectés ou reclassés et faire l'objet de copies ou d'extraits si besoin** : les documents peuvent être classés à des fins de gestion ou de recherche. Selon les circonstances, des mécanismes doivent permettre à l'application de réaffecter ou de reclasser ces documents.

Toutefois, si le logiciel métier se prête mal à l'incorporation d'un plan de classement complet, on pourra ne retenir que les séries pertinentes du plan de classement global (voir la section 2.5).

52 Conformément à la Norme ISO 15489.1 sur le Records Management, section 7.2 relative aux caractéristiques des documents engageants.

On peut avoir besoin de copier le contenu d'un document archivé pour créer un nouveau document. On peut souhaiter copier un document archivé en en enlevant ou masquant durablement une partie. C'est le cas lorsque le document n'est pas communicable dans son ensemble mais qu'une partie l'est. Si nécessaire, l'application peut gérer ces processus.

- **des rapports puissent être produits** sur les documents archivés et leur mode de gestion.
- **les documents archivés puissent être valablement gérés même s'ils ont été chiffrés ou signés électroniquement** : il est nécessaire d'apporter une vigilance particulière à la conservation des documents qui ont été chiffrés ou signés électroniquement.

  Si le chiffrement et les signatures électroniques jouent un rôle majeur pour garantir l'authenticité et l'intégrité des documents échangés, ils comportent également des risques pour l'utilisation ultérieure des documents, les clés de déchiffrement et les clés publiques des signatures électroniques pouvant expirer avant la fin de durée de conservation du document. C'est pourquoi la conservation de documents sous forme chiffrée n'est pas recommandée.

  Les processus de chiffrement et de déchiffrement peuvent être enregistrés dans les métadonnées qui attestent du succès du déchiffrement.

  En cas d'utilisation de ces mesures de sécurité pour protéger l'authenticité et l'intégrité des documents engageants, la gestion des clés doit être prise en considération.

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

27	Empêcher toute destruction ou suppression de documents électroniques archivés ou de leurs métadonnées, sauf dans les cas décrits à la section 3.4 : « Conservation et destruction selon les règles ».

3.2.1 Paramétrage des métadonnées

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

28	Pouvoir collecter toutes les métadonnées afin de créer un profil de métadonnées pour un document ou un agrégat électronique.

29	Permettre à un administrateur système, lors de la configuration du système, de définir la source de chaque métadonnée.
30	Être capable d'utiliser le contenu d'une métadonnée pour déterminer un processus fonctionnel,[53] quand la métadonnée peut être reliée à une fonction métier de l'application. 30.1 Quand l'application métier relie étroitement les métadonnées d'archivage à la fonction correspondante, les métadonnées devraient fournir des informations de description et une aide active pour exécuter cette fonction automatiquement. 30.2 Si l'application métier gère des liens entre les fonctions de mise en œuvre du sort final et d'autres mécanismes de gestion de l'archivage,[54] elle doit alerter l'administrateur en cas de révision des mécanismes de gestion des règles de conservation, et empêcher toute modification des catégories concernées jusqu'à la fin de la révision.
31	Gérer des mécanismes de validation des contenus des métadonnées tels que : • le format, • les plages de valeurs, • la validation par rapport à une liste de valeurs préétablie, et • les références à un plan de classement valide (s'il existe).
32	Pouvoir gérer durablement un profil de métadonnées, à savoir : maintenir les liens avec le document et ajouter les métadonnées de gestion de l'archivage.[55]

53 Cette fonctionnalité peut être incorporée à l'application métier ou être fournie par intégration à un système externe, tel qu'un SAE.

54 Ces mécanismes d'archivage peuvent être incorporés à l'application métier ou fournis par intégration à des logiciels spécialisés ou à d'autres applications, telles qu'un système d'archivage électronique.

55 Il arrive que l'application métier gère les profils de métadonnées de manière autonome, que les documents numériques soient conservés dans l'application en question ou dans un système externe. Mais quand une application métier ne peut pas gérer seule et durablement un profil de métadonnées alors qu'elle stocke les documents archivés, elle doit pouvoir :

- exporter le profil de métadonnées vers un système externe (par exemple un SAE) capable de gérer correctement le profil en le reliant aux documents numériques conservés dans l'application d'origine. Dans ce cas, l'application externe doit impérativement permettre d'importer les métadonnées à partir de l'application d'origine. L'application cible doit pouvoir gérer le profil de métadonnées conformément aux exigences d'un bon archivage énoncées dans ces spécifications ; ou
- permettre une interface avec un système externe (par exemple un SAE) qui gère le profil de métadonnées maintenu dans l'application d'origine. Ce système doit pourvoir prendre le relais de la gestion du profil de métadonnées, conformément aux exigences d'un bon archivage énoncées dans ces spécifications.

Si l'application métier n'est pas en mesure de gérer seule et durablement un profil de métadonnées comme le veut l'exigence 32 alors que les documents électroniques sont

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

33	Pouvoir gérer un profil de métadonnées comme une entité unique.
34	Ne pas poser de limite au nombre de métadonnées accepté par document archivé dans l'application ou par composant de document.[56]
35	Permettre de préciser quelles métadonnées doivent être saisies et gérées manuellement, à l'aide d'exigences particulières ou via le paramétrage.
36	Gérer plusieurs formats ou combinaisons de formats pour les métadonnées, notamment : • alphabétique, • alphanumérique, • numérique, • date/heure, • et logique (i.e. Oui/Non ou Vrai/Faux).
37	Permettre de renseigner les métadonnées à partir de tables de correspondance ou en appelant le système d'exploitation ou la plateforme d'application ou d'autres systèmes, selon les besoins.

L'application métier **pourrait** :

38	Permettre la validation de métadonnées en faisant appel à une autre application.

3.2.2 Réaffectation, reclassement, duplication et extraction des documents archivés

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

39	Permettre de déplacer les documents électroniques archivés dans l'application en fournissant des mécanismes de réaffectation ou de reclassement des documents (y compris, lorsqu'elle gère la notion d'agrégat, la réaffectation d'un document à un autre agrégat).
40	Gérer les mécanismes de duplication des documents électroniques.[57] 40.1 Si l'application métier peut copier le contenu d'un document archivé électroniquement et créer un nouveau document indépendant, elle doit garantir que l'original demeure intact et intègre. 40.2 Si l'application métier permet de dupliquer les documents électroniques, elle pourrait fournir un moyen de contrôler la copie ou s'interfacer avec un système externe capable de le faire. 40.3 L'application métier peut faciliter la traçabilité des copies d'un document électronique donné, en enregistrant les accès à ces copies dans le journal des événements.[58]

stockés à l'extérieur du système, elle doit pouvoir exporter métadonnées et documents vers un entrepôt d'objets numériques centralisé, tel un SAE, qui poursuivra sa gestion.

56 Cette exigence est sans objet si le système a été spécialement conçu pour répondre aux besoins de l'entreprise/organisme, y compris les exigences relatives aux métadonnées.

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

41	Autoriser la création d'un extrait d'un document électronique, dans lequel l'information sensible est retirée ou masquée à la vue, sans que le document originel soit altéré. 41.1 Si l'application métier permet l'extraction, elle doit mentionner la création de l'extrait dans les métadonnées du document originel, y compris la date, l'heure, l'auteur de l'extrait et le motif de sa création.[59] 41.2 Si l'application métier permet l'extraction, elle doit pouvoir recopier les métadonnées du document originel dans celles de l'extrait – en permettant de les modifier si nécessaire.[60] 41.3 Si le système métier permet l'extraction, il pourrait créer un lien hypertexte entre l'extrait et le document dont il est issu. Ce lien devrait préserver la relation entre l'extrait et sa source sans remettre en cause les contrôles d'accès et de sécurité applicables à l'original.
42	Fournir des solutions pour supprimer l'information sensible des documents archivés via la production d'extraits pour tous les formats gérés par le système, y compris audio et vidéo.

3.2.3 Reporting sur les documents engageants archivés

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

43	Pouvoir faire un rapport sur les actions menées sur les documents ou sur les agrégats électroniques par l'application elle-même ou par un mécanisme d'archivage électronique intégré ou interfacé pendant une période donnée.

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

44	Pouvoir produire un rapport décrivant le déroulement et les résultats d'une migration afin de s'assurer de l'intégrité des documents migrés.[61]

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

45	Pouvoir produire des statistiques sur les documents ou les agrégats électroniques capturés et conservés par l'application, comme le nombre et la localisation des documents par type et version de logiciels.

57 Les copies peuvent être réalisées dans l'application métier ou en dehors. Quand elles sont créées hors de l'application, leur existence peut être mentionnée dans le profil de métadonnées de l'original.

58 Le journal des événements peut mentionner les copies créées en dehors ou au sein de l'application métier.

59 C'est l'analyse du besoin métier qui dira si l'extrait doit lui-même être archivé ou non (voir section 2.1).

60 Un extrait peut par exemple avoir un niveau de sécurité différent de celui de l'original.

61 Le processus de migration pouvant être assez rare, le rapport peut nécessiter une intervention manuelle.

3.2.4 Processus de sécurité en ligne

On entend par processus de sécurité en ligne à la fois le chiffrement et les signatures électroniques. La majeure partie de ces exigences est liée aux systèmes métier nécessitant un processus de sécurité en ligne.

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

46	Enregistrer automatiquement les métadonnées relatives à la sécurité en ligne par exemple dans l'historique des événements.
47	Gérer l'horodatage pour tous les documents engageants nécessitant une sécurité en ligne.

Chiffrement

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

48	Gérer le chiffrement des documents engageants archivés électroniquement. Dans le cas où l'application métier gère le chiffrement des documents électroniques, elle **doit**, seule ou en relation avec d'autres systèmes : 48.1 Gérer la capture de métadonnées des documents archivés ou reçus sous forme chiffrée conformément aux normes du domaine, notamment pour : • le numéro de série ou l'identifiant unique du certificat numérique, • le type d'algorithme et le niveau de chiffrement, et • l'horodatage relatif aux processus de chiffrement et de déchiffrement.[62] 48.2 Garantir que seuls les utilisateurs détenteurs de la clé de chiffrement peuvent accéder au document chiffré, en plus des autres contrôles d'accès. 48.3 Lorsque l'application métier gère la capture, l'identification et/ou la transmission de documents électroniques chiffrés et de leurs métadonnées, elle doit permettre la mise en œuvre d'un plan de gestion de clés.[63] 48.4 Lorsque l'application métier gère la capture, l'identification et/ou la transmission de documents électroniques chiffrés et de leurs métadonnées, elle doit être capable de conserver les clés de chiffrement pendant la durée de conservation du ou des documents correspondants. 48.5 Lorsque l'application métier gère la capture, l'identification et/ou la transmission de documents électroniques chiffrés et de leurs métadonnées, elle doit prévoir un stockage séparé et sécurisé des documents chiffrés et de leurs clés de déchiffrement. Lorsque l'application métier gère le chiffrement des documents électroniques, elle **devrait**, seule ou en relation avec d'autres systèmes : 48.6 Pouvoir stocker les documents électroniques chiffrés sous une forme déchiffrée. 48.7 Permettre le déchiffrement d'un document au moment de sa capture ou de son identification, sauf si le chiffrement est exigé pour maintenir la sécurité du document durant sa présence dans l'application.[64]

62 Dans le cas d'une intégration à un système externe.

63 Soit en intégrant le plan de gestion de clés dans l'application, soit en intégrant le système à un système externe ou à un logiciel spécialisé capable d'assurer un plan de gestion de clés.

64 Certaines applications peuvent avoir des exigences légitimes de capture et de stockage de documents numériques chiffrés à des fins de preuve ou de sécurité. Si l'application fournit des contrôles d'accès et de sécurité adaptés, il devrait être possible d'y stocker à la fois les documents numériques déchiffrés, les documents chiffrés et les clés de déchiffrement, voir l'exigence 48.6.

Signatures électroniques

Ces exigences ne s'appliquent que si le système envoie ou reçoit des documents signés. Elles ne s'appliquent pas si la signature électronique est utilisée uniquement pour sécuriser la transmission. Ce document ne couvre pas les exigences spécifiques aux systèmes de gestion des signatures électroniques.

L'application métier **devrait** :

49	Lorsqu'elle stocke les certificats numériques des documents chiffrés ou signés électroniquement, avertir l'administrateur système de l'expiration prochaine des certificats.

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

50	Pouvoir garantir que tout document électronique produit ou reçu par l'application et qui utilise la technologie de signature électronique peut être capturé ou identifié par l'application avec ses métadonnées d'authentification.[65] Lorsque l'application métier utilise la signature électronique, elle doit, seule ou en relation avec d'autres systèmes : 50.1 Gérer les métadonnées des documents validés, reçus ou capturés avec une signature électronique, conformément aux normes de référence sur les métadonnées. Au minimum, les métadonnées doivent noter le fait qu'une signature numérique a été authentifiée. 50.2 Pouvoir vérifier la validité de la signature électronique au moment de la capture du document. 50.3 Pouvoir stocker avec le document électronique : • la signature numérique correspondante, • le certificat numérique authentifiant la signature, • toute autre mention de conformité, de sorte qu'ils soient gérés avec le document mais sans remettre en cause l'intégrité de la clé privée. 50.4 Permettre à l'administrateur système de paramétrer quelles métadonnées d'authentification seront systématiquement stockées avec le document électronique. Par exemple: • ne conserver que les éléments d'authentification réussie ; • conserver les métadonnées relatives au processus d'authentification ; et • conserver toutes les métadonnées d'authentification, y compris les signatures.

65 Cette exigence vise prioritairement les systèmes qui envoient et reçoivent régulièrement des documents numériques utilisant la technologie de signature électronique.

	50.5 Pouvoir prouver l'intégrité sans faille d'un document signé électroniquement, même si des modifications (autorisées) ont été apportées aux métadonnées du document.[66] Lorsque l'application métier gère les signatures électroniques, elle **devrait**, seule ou en relation avec d'autres systèmes : 50.6 Pouvoir intégrer ou s'interfacer avec les technologies de signature électronique de telle sorte que les métadonnées d'authentification puissent être capturées automatiquement. Lorsque l'application métier gère les signatures électroniques, elle **pourrait**, seule ou en relation avec d'autres systèmes : 50.7 Pouvoir appliquer une signature électronique à : • un document électronique engageant, ou • un agrégat électronique, pendant un processus de transfert ou d'export de façon à faciliter son authentification de l'extérieur.[67]

Authentification

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

51	Gérer l'authentification au travers d'une interface avec des technologies de sécurité basées sur les infrastructures à clés publiques (ICP, PKI). Lorsque l'application métier gère l'authentification avec des technologies basées sur les ICP, elle doit : 51.1 Pouvoir stocker les métadonnées relatives au processus d'authentification, notamment : • le numéro de série ou l'identifiant unique du certificat numérique, • l'autorité d'enregistrement et l'autorité de certification concernées, • la date et l'heure de l'authentification. 51.2 Lorsque l'application métier gère les signatures électroniques, elle doit permettre de stocker les métadonnées d'authentification : • avec le document électronique concerné, ou • séparément mais en étroite relation avec le document électronique.
52	Fournir une architecture souple pour s'adapter aux nouvelles technologies de sécurité en ligne au fur et à mesure de leur parution.

66 Il est possible de modifier les métadonnées mais pas le contenu des documents archivés.

67 Cette exigence ne concerne que les systèmes dotés d'une fonction de signature électronique intégrée pour la production et la transmission de documents signés électroniquement dans le cadre quotidien des affaires.

3.3 Import, export et interopérabilité

La possibilité d'exporter ou d'importer des documents archivés dans une application et l'interopérabilité entre les systèmes sont des fonctionnalités fréquemment exigées. On peut avoir besoin d'exporter les documents archivés vers un autre système, tel un SAE, ou vers un(e) autre entreprise/organisme dans le cas d'une fusion ou d'une réorganisation administrative (secteur public).

Il est fréquent de devoir conserver les documents archivés plus longtemps que la durée de vie du logiciel lui-même, et il faut alors pouvoir exporter les documents au moment du remplacement du système. On peut aussi avoir besoin d'importer des documents archivés dans un autre système, notamment dans des environnements collaboratifs. On devrait également prendre en compte le transfert des documents archivés vers une institution archivistique ou un système de stockage secondaire.

L'utilisation de formats ouverts et de standards industriels augmentera le niveau d'interopérabilité en cas d'import ou d'export, et réduira tant les difficultés que les coûts induits par ces processus.

Bien que ces questions se manifestent avec plus d'acuité en fin de vie du système, il est important d'en tenir compte au stade de la conception.

On pourra se reporter, parmi d'autres ressources, aux *Spécifications du standard d'échange pour l'archivage du Centre européen de normalisation*, et au *Standard d'export des archives numériques* de l'*Australasian Digital Recordkeeping Initiative.*[68].

3.3.1 Import

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

53	Pouvoir importer tout historique associé à des documents électroniques voire à des agrégats, capturés et conservés par l'application, en garantissant l'intégrité de l'information importée.

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

68 Disponible à: http: //www.adri.gov.au/content.asp?cID=3.

54	Pouvoir effectuer un import de masse de documents électroniques engageants depuis leur système de production,[69] en capturant : • les documents électroniques dans leur format de production/validation, en conservant leur contenu et leur structure ; • les documents électroniques et leurs métadonnées, afin de conserver leurs relations et établir une correspondance entre les métadonnées et la structure cible ; • la structure du système dont dépendent les documents et leurs métadonnées ou les agrégats, en conservant toutes leurs relations. 54.1 Lorsque le système métier gère l'import en masse de documents électroniques, il doit permettre l'utilisation de mécanismes facilitant le processus d'import, notamment : • des imports de fichiers batch ; • des règles modifiables pour personnaliser l'identification automatique des documents ; • des processus de validation de l'intégrité des données ; et • la saisie de files d'attente, y compris des files d'attente par type de document.
55	Pouvoir effectuer un import indirect de documents électroniques sans métadonnées, ou avec des métadonnées dans un format non-standard, et établir une correspondance dans la structure cible.

3.3.2 Export

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

56	Pouvoir exporter les documents électroniques engageants ou les agrégats, avec leurs métadonnées, vers : • un autre système de l'entreprise/organisme, • un système dans une autre entreprise, • une institution archivistique ou un organisme de conservation sur le long terme des documents électroniques sélectionnés comme archives historiques.
57	S'assurer que tout export comporte : • tous les documents électroniques ou tous les agrégats, • toutes les métadonnées des documents et agrégats exportés, et • tous les historiques des données des documents exportés.

[69] Il peut s'agir de documents exportés depuis un logiciel de gestion documentaire ou un logiciel d'archivage électronique.

58	Pouvoir exporter en une seule fois tous les documents électroniques et, s'il y a lieu, les agrégats, de manière à ce que : • le contenu et la structure des documents et des agrégats ne soient pas altérés ; • les liens entre les documents exportés et leurs métadonnées soient préservés ; • les liens entre tous les composants d'un même document électronique, et les liens entre les documents électroniques exportés ou entre les agrégats soient préservés, afin qu'on puisse rétablir la structure de l'information ans le système cible.
59	Pouvoir exporter tous les types de documents qu'elle peut capturer, indépendamment du format et de l'application de production.
60	Permettre d'exporter les mêmes objets plus d'une fois.[70]

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

61	Garantir que tout export est tracé dans les métadonnées du document concerné.

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

62	Pouvoir exporter des documents électroniques convertis en formats ouverts intégralement décrits.

3.4 Conservation et destruction selon les règles

Les exigences fonctionnelles de cette section visent à garantir :

- **la conformité aux référentiels de conservation.** Un des processus de l'archivage consiste à définir la durée de conservation des documents engageants (à archiver) pour répondre aux obligations légales, aux besoins des métiers et aux attentes de la communauté. Un référentiel de conservation définit les durées de conservation des différentes catégories de documents engageants à archiver. Ces durées, explicitées dans le référentiel, devraient être validées au plus haut niveau, en accord avec les exigences réglementaires. Les exigences fonctionnelles qui suivent supposent l'existence d'un référentiel de conservation pour l'ensemble des documents engageants de l'application métier.
- **que le sort final est effectivement appliqué.** Des dispositions doivent être prises afin de faciliter la conservation et la destruction des documents soit dans l'application, soit par l'intégration à un logiciel extérieur.

  Tout garder pendant toute la durée de vie du système peut s'avérer coûteux et nuire au bon fonctionnement de l'application. Dans certaines circonstances cependant, une analyse des coûts et des risques peut mettre en évidence l'intérêt de conserver les documents dans l'application jusqu'à son expiration.

70 Même si on décide de supprimer l'information du système après l'export, le but de cette exigence est de s'assurer que le système ne limite pas de lui-même le processus d'export.

Mais cela ne fait que repousser les décisions relatives au sort final des documents jusqu'à la mise hors service de l'application.[71]

- **que les actions de sort final puissent être révisées.** Avant d'exécuter un sort final, les utilisateurs doivent pouvoir reconsidérer l'action préconisée et être en mesure de la modifier ou d'en choisir une autre.
- **que les documents sont détruits selon les règles.** Il devrait être impossible de détruire des documents archivés en dehors des règles du référentiel de conservation validé, et sans l'obtention préalable du visa des personnes habilitées.
- **que les métadonnées des documents détruits soient conservées.** L'action de destruction doit être tracée, soit par des métadonnées dans l'application métier, soit via l'intégration à un autre système.
- **qu'un rapport puisse être établi** sur les actions de destruction.

A noter que certaines exigences relatives au sort final renvoient à la notion d'agrégat. Ces exigences étant conditionnées à l'utilisation d'agrégats, elles se trouvent à la section 3.1.3.

3.4.1 Conformité avec les référentiels de conservation applicables

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

63	Faciliter le contrôle des actions de sort final des documents dûment validées.
64	Permettre la définition de règles de conservation[72] applicables aux documents archivés et à leurs métadonnées, ou aux agrégats, à l'aide d'une fonctionnalité de l'application métier[73], ou par un mécanisme externe, automatique[74] ou manuel[75] (voir l'exigence 77).

71 Le Queensland State Archives, *Public Records Brief: Decommissioning business Systems*, disponible à l'adresse http://www.archives.qld.gov.au/publications/PublicRecordsBriefs/DecommissioningbusinessSystems.pdf, présente les points à examiner lors de la mise hors service du système, dans certains contextes réglementaires.

72 Une application métier doit proposer au moins une règle de conservation pour chaque catégorie de documents engageants qu'elle gère. Ces règles de conservation doivent être établies de façon à être facilement associées et appliquées aux bons documents.

73 Certaines applications métier pourront sans doute fournir des fonctionnalités intégrées permettant la définition de règles de conservation et leur application aux documents engageants créés ou reçus par l'application.

74 Un tel mécanisme peut comprendre une application métier externe dotée de fonctionnalités d'archivage, tel un SAE ou une autre application logicielle spécialement conçue pour aider à la mise en œuvre du sort final. Ce mécanisme externe sera alors intégré ou interfacé avec l'application métier.

75 Une application métier ne disposant pas de fonctionnalité de gestion automatique du sort final peut cependant satisfaire à cette exigence en fournissant un mécanisme manuel de définition des règles de conservation. Il faudra alors associer manuellement les règles de conservation du référentiel de conservation aux documents électroniques engageants créés ou reçus par l'application.

65	Assurer que la définition de chaque règle de conservation comprend : • un événement déclencheur pour initialiser la conservation ; • une durée de conservation, établissant la période durant laquelle le document doit être conservé ; et • une action de sort final, fixant le sort du document.
66	Faciliter la définition et l'application du processus de sort final, soit : • révision, • export, • transfert[76], et • destruction.
67	Donner de la souplesse dans la définition des règles de conservation pour permettre à l'administrateur l'application métier de définir d'autres durées de conservation ou actions de sort final.[77]
68	Permettre d'avoir un identifiant unique pour chaque règle de conservation, et, le cas échéant, permettre que cette règle soit associée au référentiel de conservation correspondant.
69	Permettre des durées de conservation allant de un jour à une durée illimitée.
70	Réserver à l'administrateur système ou aux utilisateurs habilités la possibilité de créer, de corriger et de supprimer les règles et les référentiels de conservation.
71	Conserver l'historique de toutes les modifications apportées aux règles de conservation (date et motif de la modification, etc.).
72	Garantir que les modifications apportées à une règle de conservation s'appliquent immédiatement à tous les documents relevant de cette règle (avec leurs métadonnées) et aux agrégats correspondants.

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

73	Pouvoir importer[78] et exporter[79] un ensemble de règles de conservation dans un format normalisé[80].

76 Le transfert correspond à un export suivi d'une destruction après vérification du succès de l'export.

77 Par exemple : « Destruction après remplacement » ou « Destruction interdite ».

78 C'est-à-dire importer un ensemble de règles de conservation dans l'application métier ou dans le mécanisme externe de gestion du sort final, afin que l'administrateur système n'ait pas à configurer manuellement les règles de conservation.

79 Il s'agit de la possibilité d'exporter un ensemble de règles de conservation à partir de l'application métier ou d'un mécanisme externe de gestion du sort final, afin qu'elles puissent être transférées vers un autre système, comme un SAE.

80 Un ensemble structuré de règles de conservation émanant d'une autorité archivistique peut s'appeler référentiel de conservation ou calendrier de conservation/destruction.

74	Pouvoir gérer une cardinalité « n-1 » lorsque plusieurs règles de conservation visent un seul et même document engageant ou un seul et même agrégat. 74.1 Si l'application métier ne peut pas gérer la relation « n-1 » pour les règles de conservation, elle doit au minimum permettre une relation « 1-1 » pour associer une règle de conservation à un document ou à un agrégat électronique ; elle doit alors permettre à l'administrateur ou à un utilisateur habilité de déterminer manuellement la bonne règle de conservation en fonction de la durée de conservation la plus longue.[81]

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

75	Faciliter la définition de règles de conservation à partir de plusieurs référentiels de conservation.[82]
76	Permettre la fusion de plusieurs référentiels de conservation lors d'un processus d'import.

3.4.2 Application du sort final

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

77	Permettre d'appliquer systématiquement les règles de conservation aux documents et aux agrégats archivés électroniquement (avec leurs métadonnées). L'application métier peut appliquer les règles de conservation et les processus liés au sort final à l'aide de : • l'ajout d'une fonctionnalité de gestion du sort final dans l'application métier;[83] • l'intégration à l'application métier d'une solution externe disposant de la fonctionnalité de gestion du sort final;[84] • une vérification manuelle des règles et de leur application par l'administrateur métier ou un utilisateur habilité,[85] ou • toute combinaison des précédents.[86] 77.1 Quand l'application métier permet de prédéfinir des règles et qu'une nouvelle règle de conservation est paramétrée, elle doit permettre la mise à jour manuelle des métadonnées de sort final ou leur héritage rétrospectif.

81 Reporter manuellement les règles de conservation peut s'avérer chronophage les règles associées aux documents numériques archivés dans l'application sont très nombreuses.

82 Pour aider les entreprises/organismes utilisant simultanément plusieurs référentiels de conservation.

83 Le niveau de complexité de cette fonctionnalité au sein de l'application métier dépendra de la nature et de la complexité de l'application elle-même.

84 Il peut s'agir de logiciels spécialisés dans la gestion du sort final ou de l'intégration à une application externe dotée des fonctionnalités d'archivage tel un SAE. Deux possibilités : ou bien les documents archivés sont exportés vers une application externe qui les capture et effectue les contrôles de sort final appropriés ; ou bien l'application externe s'interface avec l'application métier de sorte que les contrôles de gestion du sort final soient effectués sur les documents à l'intérieur de l'application métier.

85 Quand une application métier ne peut pas gérer les processus automatisés de sort final, il

78	Permettre d'appliquer les règles de conservation à tous les documents archivés (avec leurs métadonnées) et aux agrégats capturés par le système.
79	Enregistrer toutes les actions de sort final dans les métadonnées.
80	Tracer automatiquement le déclenchement et le déroulement des durées de conservation afin de définir les dates de sort final des documents engageants (avec leurs métadonnées) et des agrégats.
81	Permettre à un administrateur système ou à un utilisateur habilité d'appliquer à un document électronique, à un moment donné, une règle de conservation différente.
82	Réserver à un administrateur système ou à un utilisateur habilité la possibilité d'appliquer ou de modifier une règle de conservation.
83	Gérer un processus de sort final consistant à : • identifier les documents (avec leurs métadonnées) et les agrégats dont la durée de conservation est échue ; • alerter l'administrateur système ou un utilisateur habilité ; • réviser[87] la règle de conservation si nécessaire ; • effectuer les actions de sort final appropriées, après confirmation par un administrateur système ou un utilisateur habilité ; ce qui peut être fait automatiquement ou manuellement selon le mécanisme utilisé par l'application métier (voir l'exigence 77).
84	Réserver à un administrateur système ou à un utilisateur habilité le droit de lancer le processus de sort final.
85	Gérer une liste d'événements déclencheurs sur la base des métadonnées actives.[88] Par exemple: • date de validation du document archivé, • dernière date de consultation, • date d'ouverture ou de clôture d'un agrégat de documents, • date de la dernière révision du document ou de l'agrégat.
86	Permettre l'utilisation d'événements déclencheurs externes à partir d'un fait donné saisi manuellement dans l'application par un utilisateur ou capturé automatiquement via une application extérieure intégrée au mécanisme de sort final.
87	Garantir que la durée de conservation est calculée en temps réel et non définie artificiellement à l'avance.

peut être nécessaire de relier manuellement les documents archivés et contrôlés par le système aux règles de conservation et d'effectuer manuellement les actions de sort final sur les documents ou les agrégats électroniques.

86 Les applications automatisées de gestion du sort final peuvent se révéler insuffisantes dans certains cas, obligeant alors à effectuer manuellement certaines actions (cas d'actions de sort final non normalisées).

87 Une règle de conservation modifiée doit être prise en compte immédiatement dans le processus de sort final.

88 Les métadonnées peuvent être soit générées directement par une fonctionnalité de l'application métier, soit fournies par un ou plusieurs mécanismes d'archivage intégrés à l'application (un SAE par exemple).

88	Permettre le gel du sort final d'un document engageant (avec ses métadonnées) voire d'un agrégat, afin d'empêcher toute action de destruction pendant la période de gel.[89]
89	Empêcher la suppression ou la destruction de tout document visé par un gel.[90]
90	Réserver à un administrateur système ou à un utilisateur habilité la possibilité de lever un gel.
91	Être capable d'identifier toute contradiction entre plusieurs actions de sort final et, le cas échéant : • appliquer automatiquement la bonne règle en fonction de la préséance définie par l'entreprise/organisme;[91] ou • alerter l'administrateur système ou un utilisateur habilité en demandant une action corrective.

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

92	Être capable de définir le sort d'un document dès sa validation[92] en affectant automatiquement une règle de conservation à un document nouvellement produit ou reçu (avec ses métadonnées) ou à un agrégat, sur la base de critères prédéfinis.[93]
93	Être capable de notifier régulièrement à l'administrateur système toutes les actions de sort final à effectuer au cours d'une période donnée.

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

89 Un gel de destruction peut, par exemple, être appliqué à des documents visés par une procédure en cours liée à la législation sur la liberté d'information ou à une procédure de communication préalable. Pour satisfaire à cette exigence, le système n'a pas besoin de disposer d'une fonctionnalité spécialisée de gel ; il suffit que l'application métier permette à l'administrateur système ou à un utilisateur autorisé d'identifier manuellement les documents numériques concernés et de déclencher les contrôles nécessaires pour empêcher leur destruction jusqu'à la fin du gel.

90 Dans d'autres circonstances, la suppression ou la destruction peuvent être prises en charge par un administrateur système ou un utilisateur habilité. Voir l'exigence 86.

91 C'est en principe la durée la plus longue qui s'applique.

92 Il s'agit de la durée de conservation d'un document engageant au moment où il est validé.

93 Ces critères peuvent être mis en œuvre à l'aide de métadonnées héritées d'entités plus élevées dans le plan de classement, s'il cela est prévu (voir l'exigence 23), ou bien établies au travers de règles système prédéfinies, conçues pour attribuer les métadonnées de sort final (voir les exigences 25 et 26).

94	Pouvoir valider automatiquement le sort final d'un document (avec ses métadonnées) ou d'un agrégat, sur la base de son contenu, de métadonnées particulières ou d'une combinaison des deux.[94] 94.1 Quand le sort final est automatique, l'application métier doit demander automatiquement à un administrateur ou à un utilisateur habilité une confirmation avant de mettre en œuvre l'action de destruction.
95	Faciliter le processus de sort final à l'aide d'un workflow interfacé avec le système.

3.4.3 Révision

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

96	Fournir un moyen de vérifier le contenu d'un document électronique ou d'un agrégat arrivé à échéance avant d'appliquer l'action de sort final.
97	Rendre accessible, lors de la révision d'un document archivé électroniquement (ou d'un agrégat), l'ensemble de son contenu, même s'il est soumis à des restrictions d'accès.
98	Permettre à l'administrateur système d'affecter aux documents (ou aux agrégats) un nouveau sort final qui : • prolonge la conservation, avant une nouvelle révision ; • implique un export, un transfert, un traitement de pérennisation (une migration par exemple) ou une destruction immédiat(e) ; • prolonge la conservation, avant un futur export, un transfert, un traitement de pérennisation (migration) ou une destruction.

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

99	Permettre l'accès, par recherche ou par navigation, à tous les détails de la règle de conservation associée à un document électronique (ou à un agrégat) en cours de révision.
100	Enregistrer automatiquement la date de la dernière révision dans les métadonnées actives et permettre l'ajout du motif de la décision de révision dans les métadonnées descriptives.

3.4.4 Destruction

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

94 Il devrait être possible de prédéfinir des règles dans le système pour attribuer automatiquement les règles de conservation, sur la base des caractéristiques des documents engageants produits ou reçus par l'application métier. Une application toute simple n'aura que peu de types de documents, faciles à identifier et à regrouper selon leurs caractéristiques, permettant ainsi l'attribution automatique dès la capture de la bonne règle de conservation et de destruction.

101	Garantir que la destruction se traduit bien par un effacement ou une inaccessibilité complète de tous les documents électroniques (avec tous leurs composants) sans aucune restauration possible par des outils du système d'exploitation ou des techniques de récupération de données.[95]
102	Demander confirmation de la destruction à un administrateur de l'application métier ou à un utilisateur habilité dans le cadre du processus de destruction.
103	Empêcher la destruction de documents électroniques engageants (ou d'agrégats) jusqu'à réception de cette confirmation et permettre d'annuler le processus si elle n'est pas donnée.
104	Faire la distinction entre une fonction de suppression ponctuelle et la fonction de destruction dans le processus d'application du sort final, afin qu'elles puissent être attribuées séparément aux utilisateurs.
105	Empêcher l'utilisation de la fonction de suppression dans le processus de sort final : la destruction effective des documents électroniques archivés ne peut être effectuée qu'en lien avec une règle de conservation associée au document.

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

106	Pouvoir garantir que, lorsque la destruction d'un document électronique engageant est validée, toutes les copies de ce document sont également détruites. 106.1 Quand l'application métier prend en charge la destruction des autres copies, elle devrait permettre à l'administrateur système, si besoin est, de désactiver la fonctionnalité présentée dans l'exigence 105.[96]

3.4.5 Métadonnées de sort final

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

107	Permettre l'ajout progressif de métadonnées aux documents et aux agrégats, pour faciliter l'application du sort final, conformément aux normes sur les métadonnées.
108	Créer un lien actif entre les métadonnées de sort final et la fonctionnalité correspondante, afin de pouvoir déclencher automatiquement le processus.[97]

95 Bien que la gestion des sauvegardes pour la continuité ou la reprise d'activité après sinistre soit hors du champ de ce document, la bonne pratique voudrait que l'on s'assure que les sauvegardes ne sont pas conservées plus longtemps que ne l'exige le besoin de continuité d'activité.

96 Par exemple, si un référentiel de conservation ne mentionne pas toutes les copies ou si un(e) entreprise/organisme a des raisons de conserver une copie particulière.

97 Cette fonctionnalité peut être une fonctionnalité propre à l'application métier ou fournie par un mécanisme externe intégré au système, comme un SAE.

109	Pouvoir détecter tout changement dans les métadonnées qui affectent la durée de conservation d'un document électronique engageant et calculer sur cette base une nouvelle date d'application du sort final.[98]
110	Pouvoir réserver la modification des métadonnées relatives à la durée de conservation d'un document archivé à un administrateur système ou à un utilisateur habilité.
111	Pouvoir conserver les métadonnées des documents et des agrégats qui ont été transférés ou détruits.
112	Pouvoir enregistrer la date et le détail de toutes les actions de sort final dans les métadonnées du document ou de l'agrégat.

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

113	Autoriser les utilisateurs à ajouter les métadonnées nécessaires à la gestion archivistique des documents électroniques sélectionnés pour le transfert aux archives historiques.
114	Pouvoir conserver un historique des règles de conservation appliquées à un document particulier dans ses métadonnées.
115	Autoriser un administrateur système à définir un jeu de métadonnées[99] à conserver pour les documents et les agrégats de documents électroniques transférés, détruits ou déplacés hors ligne.

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

116	Exporter les métadonnées, comme indiqué dans les normes sur les métadonnées.
117	Comporter des champs en texte libre pour les notes des utilisateurs.[100]
118	Permettre l'ajout de métadonnées de gestion des règles de conservation et des référentiels de conservation, notamment : • une date de révision programmée ; • la date et les détails de la révision ; et • la date et les détails en cas de remplacement.
119	Permettre à un administrateur système de conserver à titre d'archives historiques[101] les métadonnées des documents et agrégats de documents électroniques transférés ou détruits.

3.4.6 Reporting de sort final

L'application métier **doit**, seule ou en relation avec d'autres systèmes :

120	Pouvoir produire des états de toutes les actions de sort final effectuées par l'application, y compris celles effectuées par des mécanismes externes intégrés ou interfacés avec l'application.

98 Quand ceci ne peut être fait de façon automatique par l'application métier, en interne ou grâce à des mécanismes externes, le système doit au moins permettre de le faire manuellement.

99 Idéalement les métadonnées obligatoires indiquées par les normes sur les métadonnées.

100 Par exemple, pour lier une décision de sort final à une exigence réglementaire.

101 C'est-à-dire une copie gérée hors du contrôle de l'application métier.

121	Pouvoir produire des listes de : • toutes les règles de conservation en vigueur dans l'application, • tous les documents (avec leurs métadonnées) et tous les agrégats associés à une règle de conservation donnée, • tous les documents visés par une action particulière de sort final pour une période donnée, • tous les documents arrivés à échéance pour une période donnée (avec des données quantitatives sur les volumes et les types de documents), et • tous les documents dont l'échéance de conservation est dépassée depuis une date donnée (avec des données quantitatives sur les volumes et les types de documents).
122	Pouvoir produire un état détaillé des anomalies d'export des documents électroniques, identifiant ceux qui ont généré des erreurs ou dont l'export a échoué.
123	Pouvoir produire un rapport détaillé du processus de destruction, donnant le détail de tous les documents électroniques qui ont été effectivement détruits ainsi que des documents électroniques dont la destruction n'est pas effective.[102]

L'application métier **devrait**, seule ou en relation avec d'autres systèmes :

124	Pouvoir éditer la liste de tous les documents visés par un gel de destruction.[103]

L'application métier **pourrait**, seule ou en relation avec d'autres systèmes :

125	Pouvoir signaler les décisions de révision au cours d'une période donnée.

102 Les conditions de réussite de la destruction des documents électroniques sont exposées dans l'exigence 101. On considère que la destruction d'un document électronique a échoué si le document peut être restauré, partiellement ou totalement, après l'application du processus de destruction.

103 Un gel de destruction concernera par exemple les documents numériques visés par une procédure en cours liée à la législation sur la liberté d'information ou par une procédure de communication préalable.

4 ANNEXES

A Glossaire

Terme	*Définition*
Accès / Access	Droit, modalités et moyens de recherche, d'exploitation ou de repérage de l'information. Source: ISO 15489, Part 3, Clause 3.1.
Action / Transaction	La plus petite unité de l'activité métier. L'exploitation d'un document archivé est elle-même une action. Troisième niveau du plan de classement métier. Voir aussi **Activité, Plan de classement métier et Mission.** Source : adapté de AS 4390, Part 1, Clause 4.27; AS ISO 15489, Part 2, Clause 4.2.2.2.
Administrateur d'application métier / Business system administrator	Rôle qui correspond à la personne responsable de l'administration d'une application métier : configuration, contrôle, gestion et utilisation. On peut avoir plusieurs niveaux de responsabilité et tout un panel d'habilitations pour organiser l'administration du système et les processus d'archivage.
Agrégat / Aggregation	Tout regroupement organique d'entités documentaires élémentaires (document, objet numérique), par exemple un dossier numérique, une série. Voir aussi **Dossier** et **Catégorie de documents.**
Application du sort final / Disposition action	Destination d'un document archivé, notée dans le référentiel de conservation avec la durée minimale de conservation et l'événement déclencheur du calcul du sort final. Voir aussi **Événement déclencheur du sort final** et **Durée de conservation.**
Application métier / Business system	Dans le cadre de ce document : système automatisé qui crée ou gère les données d'un(e) entreprise/organisme. Ceci comprend les applications dont le rôle premier est de faciliter les transactions entre une unité organisationnelle et ses clients – par exemple, commerce électronique, gestion de la relation client, bases de données spécifiques ou personnalisées, systèmes relatifs aux finances ou aux ressources humaines. Une application métier contient normalement des données dynamiques sujettes à des mises à jour constantes (pertinentes), modifiables (manipulables), et ce sont des données vivantes (actives). A l'inverse, les données des systèmes d'archivage électronique n'évoluent pas au rythme de l'activité métier (elles sont figées), ne peuvent pas être altérées (elles sont inviolables) et peuvent être inactives (non utilisées). Voir aussi **Système d'archivage électronique (SAE).**
Authentification / Authentication	Processus qui permet de tester une affirmation, afin de déterminer le niveau de confiance qu'on peut lui accorder. Source : Australian Government Information Management Office, *The Australian Government e-Authentication Framework.*
Autorité de certification / Certification authority	Organisme qui produit, signe et délivre des certificats de clé publique reliant les signataires à leur clé publique. Source : Australian Government Information Management Office, *The Australian Government e-Authentication Framework.*

Terme	***Définition***
Base de données relationnelles / Relational database	Collection de données élémentaires organisée en une série de tables formalisées où l'on peut accéder aux données et les assembler de toutes les façons possibles sans avoir à modifier les tables de la base. Voir aussi **Donnée**, **Base de données**, **Champ** et **Table.**
Base de données / Database	Collection organisée de données. Les bases de données sont souvent structurées et indexées pour améliorer l'accès des utilisateurs et la recherche d'informations. Elles peuvent exister dans un format physique ou numérique. Voir aussi **Donnée, données, Champ**,**Table** et **Base de données relationnelle.**
Capture / Capture	Processus consistant à faire passer un document ou un objet numérique dans un système d'archivage, à lui attribuer des métadonnées pour le décrire et le contextualiser, permettant ainsi de le gérer dans le temps. Pour certaines activités métier, cette fonctionnalité peut être native dans l'application métier, de sorte que la capture des documents à archiver et leurs métadonnées est concomitante à la validation des documents. Voir aussi **Enregistrement.** Source : National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004. Adapté de AS 4390, Part 1, Clause 4.7
Catégorie de conservation / Disposition class	Description des caractéristiques d'un groupe de documents traçant des activités similaires et auquel on peut appliquer le même sort final. La description comprend l'énoncé de la mission et de l'activité, un descriptif du document et le sort final. Composant du référentiel de conservation intégré à l'application métier sous la forme d'une série de règles applicables à toutes les entités archivées et comprenant : l'événement déclencheur du sort final, la durée de conservation et l'action de sort final.
Catégorie de document / Record category	Subdivision du plan de classement pour l'archivage qui peut elle-même être subdivisée en une ou plusieurs catégories sur un ou plusieurs niveaux. Une catégorie de document est constituée par des métadonnées qui peuvent être héritées d'un « parent » (catégorie de documents) et transmises aux « enfants » (répertoire ou agrégat de documents numériques). La somme des catégories, tous niveaux confondus, constitue le plan de classement pour l'archivage. Voir aussi **Plan de classement pour l'archivage**. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.
Certificat numérique / Digital certificate	Document électronique signé par une autorité de certification identifiant un propriétaire de clé et l'entité qu'il représente, associant ce propriétaire à une paire de clés en spécifiant laquelle est la clé publique, et devant contenir toute autre information exigée par le profil du certificat. Source : National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Champ / Field	Lot d'une ou plusieurs données représentant une catégorie d'information au sein d'une base de données. Voir aussi **Donnée, Base de données** et **Table.**

Terme	***Définition***
Chiffrement / Encryption	Processus de conversion des données dans un code sécurisé à l'aide d'un algorithme de chiffrement, pour la transmission dans un réseau public. La clé mathématique de l'algorithme de chiffrement est encodée et transmise avec les données fournissant ainsi les moyens de déchiffrement à l'arrivée et de restauration des données originales. Source : National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004. Adapté de The Australian Government Information Management Office, *Trusting the Interne:A Small business Guide to E-security,* 2002, p. 43.
Classement / Classification	1. Identification systématique et organisation des activités métier et/ou des documents en catégories selon des conventions logiques, des méthodes et des règles articulées dans un plan de classement. 2. Le classement inclut des conventions de nommage des documents et des fichiers, les habilitations des utilisateurs et les restrictions d'accès. Voir aussi **Plan de classement pour l'archivage.** Source : adapté de ISO 15489, Part 1, Clause 3.5; AS 4390, Part 1, Clause 4.8.
Classer / File (verb)	Action de localiser les documents selon un plan de contrôle.
Clé cryptographique / Cryptographic key	Données utilisées pour le chiffrement ou le déchiffrement de messages électroniques. Elle consiste en une séquence de symboles qui contrôle les opérations de transformation cryptographique, comme le chiffrement. Voir aussi **Chiffrement** et **Infrastructure à clé publique (ICP, PKI)**. Source : National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Composant / Component	Les composants sont les parties constitutives d'un document numérique (ex : les composants multimédias d'une page web). Il est nécessaire de capturer les métadonnées des composants si on veut gérer le document dans le temps, par exemple pour une migration. A ne pas confondre avec le concept de composant logiciel ou de composant système. Voir aussi **Objet numérique, Donnée et Document engageant électronique.** Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.
Contrôle / Control	Gestion physique et/ou intellectuelle des documents s'appuyant sur une description grâce aux informations concernant leur état physique et logique, leur contenu, leur provenance et leurs relations. Les systèmes et procédure de contrôle sont notamment l'enregistrement, le classement, l'indexation et la traçabilité. Voir aussi **Classement** et **Enregistrement.**
Contrôle d'accès / Access controls	Ensemble de mécanismes non hiérarchiques applicables aux documents électroniques pour empêcher l'accès à des utilisateurs non habilités. Il peut inclure la définition de groupes utilisateurs et de listes nominatives d'utilisateurs. Voir aussi **Contrôles de sécurité**, **Règles d'accès, Groupes d'utilisateurs**. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document,*

Terme	***Définition***
	2002, p. 28.
Contrôle d'accès / System access control	Tout mécanisme utilisé pour empêcher l'accès l'application métier par des utilisateurs non habilités, pouvant inclure des profils utilisateurs, ou des identifiants utilisateur et des mots de passe. Voir aussi **Contrôle d'accès** et **Contrôle de sécurité.**
Contrôle de sécurité / Security controls	Niveau de protection pouvant être attribué aux utilisateurs, aux documents numériques et aux entités du plan d'archivage pour restreindre les accès. Il peut inclure un niveau hiérarchique de sécurité parallèlement à un qualificatif non hiérarchique. Voir aussi **Contrôle d'accès et Descripteur.**
Conversion de fichier / Rendition	Instance d'un document numérique rendu disponible dans un autre format ou sur un autre support par un processus entièrement contrôlé par l'application métier et sans perte de contenu. Un fichier converti devrait présenter les mêmes métadonnées et être géré en étroite relation avec le document natif. Le besoin de conversion est lié à la conservation, à l'accès ou à la consultation. Voir aussi **Conversion.**
Conversion / Conversion	Processus de changement de support ou de format appliqué aux documents. La conversion implique un changement de format du document mais garantit que celui-ci conserve à l'identique l'information primaire (le contenu). Voir aussi **Migration** et **Conversion de fichier**. Source : adapté de ISO 15489, Part 1, Clause 3.7 et Part 2, Clause 4.3.9.2
Descripteur / Descriptor	Dans ce document, qualificatif non hiérarchisé (par exemple « personnel ») attribué à un niveau de sécurité dans le but de limiter l'accès à certains documents. Informatif ou consultatif, il ne peut véritablement contrôler les accès. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, pp. 27–8.
Destruction / Destruction	1. Processus d'élimination ou de suppression des documents sans aucune possibilité de restauration. 2. Dans ce document, la destruction renvoie au processus d'élimination où les documents numériques, les entités du plan de classement et leurs métadonnées sont retirées, effacées ou oblitérées selon les règles du référentiel de conservation. Voir aussi **Suppression.** Source : adapté de la norme ISO 15489, Part 1, Clause 3.8.
DIRKS / DIRKS	Acronyme pour « Designing and implementing recordkeeping systems » ; méthodologie de gestion des documents engageants et de l'information métier préconisée par la norme internationale sur le Records management (ISO 15489, Part 1, Section 8.4) et développée en 2001 dans une publication des Archives nationales d'Australie : *DIRKS: A Strategic Approach to Managing Business Information.*
Document composite / Compound record	Un document engageant (à archiver) composé de plusieurs objets numériques élémentaires (ex : des pages web avec des graphiques et des feuilles de style embarquées).

Terme	***Définition***
Document électronique engageant / Electronic record	Document engageant sur support électronique, produit, transmis, conservé et/ou consulté via des outils électroniques.
Document engageant / Record (noun)	Toute information, sous tout format, produite, reçue ou conservé à titre de preuve et d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité. Voir aussi **Document électronique engageant.** Source : ISO 15489, Part 1, Clause 3.15.
Donnée / Data element	Unité logique identifiable constituant le plus petit composant organisationnel d'une base de données. Il s'agit d'une combinaison de caractères ou d'octets correspondant à un élément d'information indépendant. Une donnée se combine avec d'autres données ou des objets numériques pour former un document électronique. Voir aussi **Données, Composant, Base de données**, **Document engageant électronique**, **Champ** et **Table.**
Données / Data	Faits ou idées énoncés d'une manière formalisée et adaptée à leur transmission, leur interprétation ou leur traitement manuel ou automatique. Source : Conseil International des Archives, *Dictionnaire de terminologie archivistique*, KG Saur, Munich, 1988, p. 48.
Dossier / File (noun)	Unité organisée de documents accumulés pendant leur utilisation courante et conservés ensemble parce qu'ils traitent du même sujet, de la même activité ou action. *Note des traducteurs : en anglais le mot « file » désigne également un fichier informatique (groupe d'informations doté d'un nom, stocké sur un ordinateur et traité comme une entité basique).* Source : adapté de J -Ellis (ed.), *Keeping Archives*, 2nd edition, Australian Society of Archivists and Thorpe, Melbourne 1993, p. 470.
Durée de conservation / Retention period	Période de temps, après l'événement déclencheur, pendant laquelle un document engageant doit être conservé et accessible. A l'expiration de cette durée, on peut appliquer le sort final. Voir aussi **Application du sort final et Événement déclencheur du sort final.**
Événement déclencheur du sort final / Disposition trigger	Evénement à partir duquel on peut calculer la date du sort final. Ce peut être la date d'achèvement d'une action ou la date de survenance d'un fait. Voir aussi **Durée de conservation**.
Export / Export	Processus de sort final consistant à transférer des copies de documents numériques (ou de groupes de documents) avec leurs métadonnées, d'un système vers un autre, en interne ou à l'extérieur. Avec l'export, les documents ne sont pas supprimés dans le système d'origine. Voir aussi **Transfert.** Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 3.

Terme	***Définition***
Extrait / Extract	Copie d'un document électronique engageant dont on a retiré ou masqué durablement certains éléments. On réalise un extrait quand le document n'est pas communicable dans son ensemble mais qu'une partie l'est. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document,* 2002, p. 3.
Fixité / Fixity	État ou qualité de ce qui est figé.
Format natif / Native format	Format dans lequel un document engageant est produit ou dans lequel l'application source le conserve. Voir aussi **Conversion**. Source : adapté de NSW Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B: Specifications*, 2001, p. 13.
Format / Format	Forme physique (papier, microfilm) ou format de fichier informatique dans laquelle (lequel) un document est conservé. Voir aussi **Format natif.** Source : adapté de Department of Defense (US), *Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD*, 2002, p. 14.
Gestion de l'archivage (archivage) / Records management	Champ de la gestion responsable du contrôle efficace et systématique de la production et capture, réception, conservation, utilisation et destruction des documents engageants, y compris les processus de capture et de maintenance de la preuve et de la description des activités et des actions nécessitant d'être tracées. Source : ISO 15489, Part 1, Clause 3.16.
Groupe d'utilisateurs / User access group	Liste nominative de personnes (utilisateurs connus du système métier) qui fonde un groupe stable et identifié. L'accès à certains documents ou à certaines entités du plan de classement peut être restreint aux membres de certains groupes. Voir aussi **Contrôle d'accès**. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 28.
Hériter / Inherit	Recevoir une métadonnée d'une entité de niveau supérieur. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document,* 2002, p. 4.
Historique des événements / Audit trail	Données qui permettent la reconstitution d'une action passée, ou la conservation des caractéristiques des modifications (date, heure, opérateur), de sorte qu'une séquence d'événements puisse être remise dans le bon ordre chronologique. Ce peut être une base de données ou une ou plusieurs listes de données d'activité. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.
Identification / Identification	Action d'attribuer à un document ou un dossier engageant un identifiant unique qui constitue une trace formelle de ce qui est validé et capturé. L'identification implique une brève description du contexte et des liens entre les documents.
Importer / Import	Recevoir dans un système des documents numériques archivés avec leurs métadonnées, en provenance d'un autre système, interne ou extérieur.

Terme	***Définition***
Instance / Instance	Occurrence d'un document numérique dans un format donné ou à un moment donné. Par exemple, un document dans son format natif est une instance tandis que le fichier converti en est une autre. Les instances peuvent être le produit des processus de migration ou de conversion.
Intégration / Integration	Relation étroite créée entre l'application métier et une autre application ou un autre mécanisme. L'intégration exige le partage des données entre les systèmes, une apparence commune et le sentiment qu'il ne s'agit que d'un seul et même système. Source : adapté de NSW Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B: Specifications*, 2001, p. 13.
Interface / Interface	Mécanisme qui permet d'échanger des données entre applications. Source : adapté de NSW Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B: Specifications*, 2001, p. 13.
Messages électroniques / Electronic messages	Tout système de communication utilisant l'électronique dans la conduite des activités, en interne, entre les entreprises/organismes ou avec le reste du monde. Les exemples les plus connus sont le courriel, la messagerie instantanée et les SMS (service de messagerie courte). Source : National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004.
Métadonnées / Metadata	Informations structurées qui décrivent et/ou permettent de retrouver, gérer, contrôler, interpréter ou conserver d'autres informations dans le temps. Source : adapté de A Cunningham, 'Six degrees of separation: Australian metadata initiatives and their relationships with international standards', *Archival Science*, vol. 1, no. 3, 2001, p. 274.
Métadonnées d'archivage / Record metadata	Métadonnées qui identifient, authentifient et contextualisent les documents engageants (à archiver) ainsi que les personnes, processus et systèmes de création, gestion, conservation et utilisation afférents, et les règles associées. Voir aussi **Métadonnées.** Source: ISO 23081, Part 1, Clause 4.
Migration / Migration	Action de transférer des documents archivés d'un système vers un autre, tout en préservant leur authenticité, leur intégrité, leur fiabilité et leur exploitabilité. La migration renvoie à des tâches précises visant à assurer le transfert périodique de données numériques d'un matériel ou logiciel informatique vers un autre, ou d'une génération technologique vers une autre. Voir aussi **Conversion**. Source : adapté de ISO 15489, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.
Mission / Function	1. Premier niveau d'un plan de classement métier. Les missions sont les principales responsabilités de l'entreprise/organisme pour atteindre ses objectifs. Source : adapté de AS 4390, Part 4, Clause 7.2. 2. Unité la plus grande de l'activité métier dans un(e) entreprise/organisme ou un État.

Terme	***Définition***
Niveau de sécurité / Security category	Désignation hiérarchisée (« très secret », « protégé », etc.) attribuée à un utilisateur, à un rôle utilisateur, à un document numérique ou autre entité du plan d'archivage pour indiquer le niveau d'accès autorisé. Le niveau de sécurité reflète le niveau de protection qui doit être appliqué pendant l'utilisation, le stockage, la transmission, le transfert et la conservation du document. Voir aussi **Contrôle de sécurité.** Source : adapté de Cornwell Management Consultants (for the European Commission Interchange of Documentation between Administrations Programme), *Model Requirements for the Management of Electronic Records* (MoReq Specification), 2001, p. 107.
Objet numérique / Digital object	Objet pouvant être représenté par un ordinateur tel un type de fichier généré par un système particulier ou un logiciel (par exemple, un document en traitement de texte, un tableau, une image). Un document numérique peut comprendre un ou plusieurs objets numériques. Voir aussi **Composant** et **Document engageant électronique.**
Outil de classement / Records classification tool	Dispositif ou méthode d'aide au classement, au nommage, à l'accès, au contrôle et au repérage des documents engageants, comprenant un plan de classement pour l'archivage, un thésaurus, un plan d'indexation ou un vocabulaire contrôlé.
Plan de classement pour l'archivage / Records classification scheme	Outil de classement hiérarchique qui, intégré à une application métier, peut faciliter la capture, le nommage, le repérage, la conservation et la destruction des documents. Un plan de classement pour l'archivage découle du plan de classement métier de l'entreprise/organisme.
Profil utilisateur / User profile	Résumé de tous les attributs d'un utilisateur d'une application métier, soit toutes les données connues du système : nom d'utilisateur, identifiant et mot de passe, droits de sécurité et d'accès et droits d'accès fonctionnels. Voir aussi **Contrôle d'accès.**
Référentiel de conservation / Disposition authority	Outil méthodologique qui décrit les différentes séries de documents et définit pour chacune la durée de conservation et le sort final associé. Voir aussi **Application du sort final, Catégorie de conservation** et **Durée de conservation.**
Règles système / System rules	Politiques internes au logiciel qui peuvent être établies et/ou configurées par un administrateur pour gouverner les fonctionnalités d'un système donné et déterminer la nature des processus opérationnels qui s'y rapportent.
Répertoire / Folder	Regroupement de documents formalisé dans une application métier auquel on assigne une catégorie documentaire du plan de classement pour l'archivage. Un répertoire est constitué par des métadonnées qui peuvent être héritées d'un « parent » (catégorie de documents) et transmises aux « enfants » (documents). Voir aussi **Répertoire numérique.** Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 3.

Terme	***Définition***
Répertoire numérique / Digital folder	Ensemble de documents numériques reliés logiquement, maintenus en relation étroite dans l'application métier et gérés comme un objet unique. Type d'agrégat de documents numériques. Peut également être dénommé « contenant ». Voir aussi **Agrégat** et **Dossier.**
Rôle utilisateur / User role	Compilation ou liste normalisée de permissions fonctionnelles de l'application métier pouvant être accordées à un groupe déterminé d'utilisateurs. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 6.
SAE / ERMS	Voir **Système d'archivage électronique.**
Signature électronique / Digital signature	Mécanisme de sécurité inclus dans un document numérique rendant possible l'identification du producteur de l'objet numérique et pouvant aussi être utilisé pour détecter et tracer tout changement subi par lui. Source: National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records, exposure draft,* 2004. Adapté de *The Australian Government Information Management Office, Trusting the Internet: A Small business Guide to E-security,* 2002, p. 43.
Sort final / Disposition	Destinations possibles des documents lors de la mise en œuvre des décisions de conservation, destruction ou transfert des documents archivés, selon les règles énoncées dans le référentiel de conservation ou dans d'autres outils. Source : ISO 15489, Part 1, Clause 3.9
Suppression / Deletion	Processus qui retire, efface ou oblitère des informations archivées sur un support, en dehors du processus de destruction. La suppression, au sein des systèmes électroniques, correspond au retrait du pointeur (l'information de localisation) qui permet au système de localiser une donnée particulière sur le support. Voir aussi **Destruction** et **Sort final.**
Système d'archivage électronique (SAE) / Electronic records management system (ERMS)	Système automatisé de gestion pour la production, l'utilisation, la maintenance et le sort final des documents produits et validés sous forme numérique et constituant une trace probante des activités. Ces systèmes conservent l'information contextuelle (métadonnées) et les liens entre les documents archivés afin de consolider leur valeur probante. L'objectif premier d'un système d'archivage électronique est la capture et la gestion des documents électroniques engageants. Voir aussi **Système de gestion documentaire et d'archivage électroniques**. Source : National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft,* 2004.
Système de classification pour la sécurité / Security classification system	Série de procédures pour l'identification et la protection de l'information officielle dont la divulgation pourrait avoir des conséquences néfastes. Le système de classification pour la sécurité est mis en œuvre par des marqueurs qui montrent la valeur de l'information et indiquent le niveau minimum de protection à appliquer. Voir aussi **Classement et Niveau de sécurité**. Source : adapté de Attorney-General's Department, *Commonwealth Protective Security Manual*, 2000.

Terme	***Définition***
Système de gestion des documents et d'archivage électronique / Electronic document and records management system (EDRMS)	Système d'archivage électronique possédant des fonctionnalités de gestion documentaire. *NdT : l'acronyme anglais est EDRMS.*
Systèmes de messagerie électronique / Electronic messaging systems	Applications utilisées par les entreprises/organismes ou les individus pour envoyer, recevoir, stocker et retrouver des messages électroniques. Ces systèmes ne possèdent généralement pas de fonctionnalités d'archivage. Source : National Archives of Australia, *Digital Recordkeeping : Guidelines for Creating, Managing and Preserving Digital Records, exposure draft,* 2004.
Table / Table	Ensemble de champs d'une base de données relationnelle, comprenant chacun une série de valeurs. Une base de données peut être faite d'une ou plusieurs tables. Voir aussi **Donnée, Base de données** et **Champ**
Traçabilité / Tracking	Production, capture et conservation de l'information relative aux mouvements et à l'utilisation des documents archivés. Source : ISO 15489, Part 1, Clause 3.19.
Trace probante / Evidence	Preuve d'une action.
Transfert / Transfer	Processus de sort final consistant en un export effectif de documents électroniques (avec leurs métadonnées) ou d'agrégats électroniques, suivi de leur destruction dans l'application d'origine. Les transferts peuvent s'effectuer d'un(e) entreprise/organisme vers une autre avec un changement de responsabilité, d'un(e) entreprise/organisme vers un service d'archives historiques, d'un(e) entreprise/organisme vers un tiers archiveur, d'une administration vers le secteur privé ou d'une administration à une autre. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3:Reference Document,* 2002, p. 6.
Type de document / Record type	Dénomination d'un objet engageant qui possède certaines exigences de production, de métadonnées et de gestion. Les types de documents sont en principe normalisés ; des types de documents spécifiques sont des variantes de la norme qui permettent à un(e) entreprise/organisme de faire face aux exigences réglementaires (données personnelles ou concordance de données) pour certains groupes de documents. Source : adapté de The National Archives (UK), *Requirements for Electronic Records Management Systems, 3 : Reference Document*, 2002, p. 5.

B Intégration des exigences d'archivage dans le cycle de vie des applications

Le développement des applications métier passe en général par une série de phases, depuis la planification et la production d'un dossier de projet jusqu'à la mise en œuvre et la maintenance et évaluation du système en passant par le développement des spécifications conceptuelles et des exigences fonctionnelles. Si l'archivage doit être intégré dans la conception des applications métier, il est essentiel que la problématique d'archivage soit prise en compte à toutes les phases de développement des applications. De toutes les phases du cycle de vie d'une application, la planification est la plus importante car c'est à ce moment là que les exigences fondamentales de l'archivage sont identifiées et actées, ainsi que les ressources correspondantes.

Si on attend les dernières phases de développement des applications pour y inclure les besoins d'archivage, ce sera particulièrement difficile. En effet, la démarche sera perçue comme un ajout exigeant de nouvelles ressources plutôt que comme un composant essentiel du système dont les ressources sont déjà identifiées et dont les objectifs de conception et de mise en œuvre sont déjà intégrés au projet.

Ci-après, un panorama des différentes phases de développement du cycle de vie des applications avec les exigences d'archivage associées.[104]

1 Initialisation du projet

La phase d'initialisation du développement de l'application démarre avec la décision de la direction générale de renforcer les processus métier à l'aide des technologies de l'information. Les objectifs de la phase d'initialisation consistent :

- identifier et valider le choix d'améliorer les résultats de l'entreprise/organisme ou de réduire un dysfonctionnement dans la conduite des activités ;
- identifier les principaux pré-requis et les contraintes afférentes aux solutions ; et
- recommander l'étude de concepts et de méthodes alternatives pour répondre au besoin.

Le projet peut résulter d'un processus d'amélioration des activités, de changements dans les missions ou d'avancées technologiques; il peut aussi être provoqué par des facteurs extérieurs tels que la législation ou une politique, l'instauration d'une nouvelle stratégie de gouvernance ou une opportunité offerte par un acteur externe (par exemple, des entreprises de développement et d'assistance). Le « sponsor » du projet traduit ce besoin dans le contexte de l'entreprise/organisme pour initier le cycle de vie du projet/de l'application. Pendant cette phase, on nomme un responsable ou chef de projet qui prépare une expression des besoins ou des propositions d'orientation. Les questions liées à la sécurité et à l'archivage (saura-t-on maintenir l'authenticité des documents engageants dans le temps ? quelles règles de conservation des documents ? quelle articulation des documents papier et des documents électroniques ? comment organiser les destructions nécessaires ? etc.) et la responsabilité de ces questions sont identifiées à un niveau général (c'est-à-dire

---

104 La description des différentes phases du cycle de vie des systèmes est inspirée de *Department of Justice Systems Development Life Cycle Guidance Document,* Information Resources Management, US Department of Justice, Washington, DC, 2003.

comme des questions à prendre en compte dès le début du projet). C'est pourquoi, le responsable ou chef de projet s'entoure logiquement de tous ceux qui pourront ou devront contribuer à l'effort de développement (c'est-à-dire, tous ceux qui devront intervenir dans la résolution de la problématique d'archivage et dans son intégration à l'application).

2 Planification

Au cours de cette phase, on procède à une analyse plus poussée des besoins (nouvelle application ou modification du système existant ?), afin de procurer une « vision » un peu documentée du futur fonctionnement concret des choses une fois que la solution choisie aura été mise en œuvre. Pour s'assurer que les phases ultérieures du cycle de vie de l'application pourront être menées à bien, à temps et dans le cadre du budget alloué, on définit les ressources, les activités, le calendrier d'exécution, les outils et les revues du projet. Les autres exigences d'ordre général, comme les exigences de sécurité (c'est-à-dire certification et accréditation en matière de sécurité) et d'archivage sont définies ensuite sur la base d'une évaluation des risques.

3 Analyse des exigences

Les exigences fonctionnelles de l'utilisateur sont décrites dans un cahier des charges et se déclinent en termes de données, performance, sécurité et facilité de maintenance du système. Elles sont suffisamment détaillées pour permettre la conception. Toutes les exigences doivent pouvoir être mesurées et testées, et êtres reliées aux besoins et perspectives métier identifiés durant la phase d'initialisation. La documentation relative aux exigences des utilisateurs, rassemblée durant la phase de planification, sert de base à une analyse plus précise des besoins et à une description plus poussée des exigences. Durant cette phase d'analyse, le système est précisé en termes d'entrées et sorties de données, de processus et d'interfaces. Il s'agit là d'une définition fonctionnelle (c'est-à-dire que le système est décrit en termes de fonctionnalités et non en termes de programmes informatiques, de fichiers ou de flux de données). Durant cette phase, l'accent est mis sur les fonctionnalités à mettre en œuvre plutôt que sur la manière de les mettre en œuvre.

4 Conception

Cette phase concerne la conception des caractéristiques physiques de l'application. L'environnement opérationnel, avec ses sous-systèmes, entrées et sorties de données, est défini ; les processus sont reliés aux ressources. L'utilisateur passe en revue et documente les actions qui requièrent son intervention ou son approbation. Les caractéristiques physiques de l'application sont précisées dans un schéma détaillé. Les sous-systèmes identifiés au cours de la conception permettre de créer l'architecture du système. Chaque sous-système est subdivisé en une ou plusieurs unités ou modules qui donnent lieu à des spécifications détaillées.

L'étape de conception doit rendre compte des exigences fonctionnelles pour l'archivage et autre (la gestion, les procédures, la technique, etc.) résultant de la phase d'analyse. De même que les exigences de sécurité, les spécifications conceptuelles en matière d'archivage doivent être étroitement liées aux spécifications conceptuelles en matière d'architecture physique et logique (architecture des données, modèles de données, etc.).

5 Mise en œuvre

L'objectif de cette phase est de faire du système issu de la phase de conception un système d'information actif capable de répondre aux exigences. La phase de développement va permettre la construction de l'application, ainsi que des tests techniques et fonctionnels afin de vérifier que le système satisfait aux exigences fonctionnelles. Avant d'installer et de mettre l'application en production, il est important d'effectuer une démarche de certification qualité et d'accréditation. Cette phase donne lieu à plusieurs types de tests. Tout d'abord, l'équipe développement s'assure que les programmes s'intègrent bien dans les sous-systèmes et qu'eux-mêmes s'intègrent dans l'application. C'est à ce moment là que la capacité de l'application à capturer et conserver les documents archivés (en accord avec les exigences fonctionnelles) est testée. Ensuite, on s'assure que l'application répond bien à toutes les exigences techniques, y compris de performance. Le processus de test et d'évaluation inclut bien sûr les tests sur les fonctionnalités archivistiques. Des tests spécifiques d'intégrité des données (du point de vue de la sécurité et de l'archivage) valideront la capacité du système à respecter les exigences d'authenticité, de fiabilité, de complétude, etc. Pour finir, les utilisateurs participent à un dernier test afin de confirmer que l'application répond à leurs exigences, y compris pour la recherche et l'accès aux documents. Une fois le système accepté, il est mis en production, après notification aux utilisateurs de la mise en œuvre, réalisation des formations prévues, reprise des données et recette du système.

6 Maintenance

Pendant cette phase, on contrôle la performance du système au regard des besoins des utilisateurs et on effectue les modifications qui s'imposent. Le système opérationnel fait l'objet d'une évaluation périodique, au travers de revues de processus, afin d'essayer de le rendre plus efficace et plus économique. Ces opérations se poursuivent tant que l'on peut trouver des réponses adaptées à l'amélioration des besoins. Du point de vue de l'archivage, cela signifie que les changements dans les exigences d'archivage (du fait de nouvelles lois, d'une modification des exigences métier, d'une révision des processus métier, etc.) doivent être pris en compte dans le pilotage et exécutés pendant cette phase. L'assistance aux utilisateurs est une préoccupation permanente. Les nouveaux utilisateurs doivent être formés. Le point fort de cette phase est de s'assurer que les besoins des utilisateurs sont satisfaits et que l'application fonctionne comme prévu dans l'environnement opérationnel. Lorsque des modifications ou des changements sont absolument nécessaires, il convient de faire une nouvelle planification. Les actions liées à la suppression du système garantissent que la désactivation du système s'opère correctement, en préservant les informations vitales sur le système, de façon que tout ou partie des données (y compris les données sur les documents archivés) puissent être réactivées ultérieurement en cas de besoin. On prêtera plus spécialement attention à ce que les documents archivés dans l'application soient correctement conservés (migration des documents majeurs vers d'autres systèmes, y compris les systèmes d'archivage externes), en cohérence avec la réglementation et les politiques d'archivage, en vue d'un possible accès ultérieur.

7 Revue du projet et évaluation

La revue du projet et l'évaluation du système interviennent de deux façons. Tout d'abord, du point du vue de l'application métier elle-même. Des revues de processus sont effectuées à toutes les phases du cycle de vie de l'application pour vérifier que toutes les actions entreprises ont atteint leur but et rempli leurs objectifs de

performance. Ces revues de processus doivent être organisées au moyen de modèles de mesure de performance et de méthodes d'évaluation. Si l'on veut mesurer la capacité de l'application à produire, capturer et gérer des documents engageants, il faut absolument développer et utiliser des outils de mesure de la performance d'archivage et des méthodes de conduite d'évaluation des fonctionnalités d'archivage. Dans la mesure du possible, ces outils et méthodes seront intégrés aux mesures de la performance et aux méthodes d'évaluation utilisés pour les revues de processus réalisées à chaque phase du développement de l'application.

Le second point de vue est celui de la méthode utilisée pour développer les systèmes. La méthodologie de développement est-elle efficace, économique, complète, etc. ? L'évaluation de la méthodologie peut intervenir à la fin du projet de cette application, ou faire partie d'une évaluation plus large du développement et du management du système d'information. Là aussi, la problématique d'archivage, incluant notamment la mesure de la performance, doit être développée et intégrée dans les outils et techniques d'évaluation générale de développement du système d'information.

C Lectures complémentaires

Cornwell Management Consultants (Programme de la Commission européenne relatif aux échanges de documentation entre administrations Programme de la Commission européenne relatif aux échanges de documentation entre administrations), *Modèle d'exigence pour l'organisation de l'archivage électronique*, mars 2001. http: www.cornwell.co.uk/edrm/moreq.asp

Indiana University,: *Electronic Records Project,* http: //www.libraries.iub.edu/index.php?pageId=3313.

Conseil international des Archives, *Authenticité des archives électroniques*, études 13-1, novembre 2002 et 13-2, janvier 2004.

International Standards Organization, ISO 15489 –1 : 2001, Information et Documentation – Records Management – Partie 1: Généralités.

International Standards Organization, ISO 23081 – 1: 2006*,* Information et Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles.

International Standards Organization, ISO TR 15489 - 2: 2001 Information et Documentation – Records Management – Part 2: Guidelines.

International Standards Organization, ISO TR 26122: 2008 Information et Documentation – Work Process Analysis for Records.

International Standards Organization, ISO/TS 23081 – 2: 2007, Information et Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues.

University of Pittsburgh, *Functional Requirements for Evidence in Recordkeeping: The Pittsburgh Project*, 1996, http: //www.archimuse.com/papers/nhprc/BACartic.html.