



MODEL REQUIREMENTS FOR
THE MANAGEMENT OF ELECTRONIC RECORDS

MoReq SPECIFICATION



*This specification has been prepared for
the IDA Programme
of the European Commission by
Cornwell Management Consultants plc
(formerly Cornwell Affiliates plc).*



TRADUCTION FRANÇAISE

MODÈLE D'EXIGENCES POUR L'ORGANISATION DE L'ARCHIVAGE ÉLECTRONIQUE

SPECIFICATIONS MoReq

Traduit de l'anglais par Marie-Anne Chabin, archiviste-paléographe

A l'initiative d'



et grâce au soutien de



Total



RATP



Sanofi-Aventis



*Conseil général de
Seine-et-Marne*

Parker Williborg

Conseil et Expertise en Organisation et Systèmes d'Information

Parker Williborg



Commissariat à l'énergie atomique

SAINT-GOBAIN
ARCHIVES

Saint-Gobain Archives



Lobut consultant



ADBS

*Association des professionnels de
l'information et de la documentation*



*Association des Archivistes
Français (AAF)*

Note du traducteur

L'équivalent strict de l'anglais *record* n'existant pas dans la langue française, la traduction de textes traitant des *records* et du *records management* est toujours délicate. De quoi s'agit-il ?

La norme ISO 15489 définit les *records* comme les « documents créés, reçus et préservés 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 » ; tandis que la loi française du 3 janvier 1979 définit les archives comme « l'ensemble des documents quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale ou par tout service ou organisme public ou privé, dans l'exercice de leur activité. La conservation de ces documents est organisée [...] tant pour les besoins de la gestion et de la justification des droits [...] » On notera la convergence des deux définitions.

Toutefois, la pratique diffère de la théorie et le terme « archives » renvoie au quotidien à quelque chose d'ancien, les « archives courantes » étant plus communément désignées par les mots « documents » ou « dossiers ».

Peu importe, l'essentiel est que ces documents présentent une double caractéristique : a) leur contenu est « fixé » et n'est plus modifiable ; b) ils doivent être conservés pendant une certaine durée pour des raisons légales ou fonctionnelles. C'est précisément le domaine de l'archivage, dont l'importance et les enjeux ne sont plus à démontrer.

Le mot *record* est donc ici traduit tantôt par « document archivé », tantôt par « document » tout court car le sens est évident, plus rarement par « document d'archives » ou « archive ». Par opposition à *record*, le terme anglais *document* vise un document dont le contenu n'est pas fixé ou qui est une composante indissociable du *record*. *Document* a donc été traduit tantôt par « document » tantôt par « pièce ». Les concepts sont expliqués dans le glossaire et le texte de MoReq ne présente pas d'ambiguïté.

L'expression « records management », lorsqu'elle désigne cette discipline anglo-saxonne pluri-décennale et distincte des pratiques archivistiques françaises, a été conservée en anglais. Ailleurs, elle est restituée par le mot « archivage », beaucoup plus répandu et beaucoup plus large que l'anglais *archiving*. En effet, mais un *Electronic Records Management System* (ERMS) n'est pas autre chose qu'un *Système d'Archivage Electronique* (SAE) où, il est vrai, le mot archivage doit être pris dans son sens fort de maîtrise du cycle de vie (durée de conservation), distinct du stockage et distinct de la gestion électronique des documents (GED- *Document Management*) mais entretenant avec ces domaines des liens étroits.

Les projets d'archivage électronique se multiplient aujourd'hui dans les entreprises et les organismes publics ou privés. L'objectif est d'assurer la traçabilité, l'intégrité, la sécurité et la pérennité des documents de l'entreprise, de répondre aux exigences légales de conservation et de communication, de relever le défi de l'obsolescence technologique récurrente, de faciliter l'accès à l'information archivée, et de faire tout cela au meilleur coût.

Espérons que cette traduction française des spécifications MoReq permettra de conforter les cahiers des charges et contribuera à fédérer un langage commun des différents acteurs de l'archivage électronique¹.

Marie-Anne Chabin, *Archive 17*, novembre 2004

¹ MoReq ayant été diffusé initialement début 2001, certaines informations requièrent une mise à jour. Une révision de MoReq est à l'étude. Une seconde version pourrait voir le jour en 2005.



MODÈLE D'EXIGENCES POUR L'ORGANISATION DE L'ARCHIVAGE ÉLECTRONIQUE

SPECIFICATIONS MoReq

Ces spécifications sont accessibles [en anglais] sous la forme électronique à l'adresse suivante :

- <http://www.cornwell.co.uk/moreq.html>
- <http://europa.eu.int/ISPO/ida/>

et sur d'autres sites. Des traductions en plusieurs langues sont signalées et accessibles sur ces sites.

Elles sont également accessibles sous forme papier à l'Office des publications des Communautés européennes, en tant que supplément VI de l'INSAR, ISBN 92-894-1290-9

© CECA-CEE-CEEA, Bruxelles- Luxembourg, 2001

Reproduction autorisée, sauf à des fins commerciales, moyennant mention de la source.

Avis juridique : le copyright de cette publication appartient à la Communauté européenne. La Commission européenne ne garantit pas l'exactitude des informations contenues dans ce rapport, et décline toute responsabilité de l'usage qui pourrait en être fait. Ni la Communauté européenne et/ou ses institutions, ni personne agissant en son nom ne pourra être tenu responsable d'aucune perte ou dommage résultant de l'utilisation de cette publication.

Contrôle des versions

| Version | Date | Commentaire |
|---------|----------------|--|
| 5.2.1 | Mars 2001 | Première publication |
| 5.2.2 | - | Non publié |
| 5.2.3 | Septembre 2002 | Correction des URLs de téléchargement de MoReq. Correction de référence à l'Annexe 4 |
| 5.2.4 | Octobre 2002 | Mise à jour du nom de la société Cornwell. Référence aux traductions ajoutées à la page de titre. |

TABLE DES MATIERES

| | | |
|----------|--|-----------|
| 1 | Introduction..... | 1 |
| 1.1 | Historique..... | 1 |
| 1.2 | Objectif et champ d'application de ces spécifications..... | 1 |
| 1.3 | Qu'est-ce qu'un SAE ? | 2 |
| 1.4 | Quel usage pour ces spécifications? | 2 |
| 1.5 | Points forts et limites de ces spécifications..... | 3 |
| 1.6 | Utilisation de ces spécifications..... | 4 |
| 1.7 | Organisation des spécifications..... | 4 |
| 1.8 | Exigences obligatoires et souhaitables..... | 5 |
| 1.9 | Commentaires sur ces spécifications | 5 |
| 2 | Panorama des exigences d'un SAE | 6 |
| 2.1 | Terminologie fondamentale | 6 |
| 2.2 | Concepts fondamentaux..... | 8 |
| 2.3 | Modèle des relations entre entités..... | 13 |
| 3 | Plan de classement | 15 |
| 3.1 | Configuration du plan de classement..... | 15 |
| 3.2 | Séries et dossiers | 16 |
| 3.3 | Sous-dossiers..... | 17 |
| 3.4 | Maintenance du plan de classement..... | 18 |
| 4 | Contrôles et sécurité | 21 |
| 4.1 | Accès..... | 21 |
| 4.2 | Historique des événements | 23 |
| 4.3 | Sauvegarde et restauration | 26 |
| 4.4 | Traçabilité des mouvements | 27 |
| 4.5 | Authenticité..... | 28 |
| 4.6 | Indices de sécurité..... | 28 |
| 5 | Conservation et sort final | 32 |
| 5.1 | Tableaux des durées de conservation..... | 32 |
| 5.2 | Révision | 35 |
| 5.3 | Transfert, export et destruction..... | 37 |
| 6 | La capture des documents..... | 40 |
| 6.1 | La capture..... | 40 |
| 6.2 | Import par lots..... | 44 |
| 6.3 | Types de documents..... | 45 |
| 6.4 | Gestion des messages électroniques | 47 |

| | | |
|-----------|---|-----------|
| 7 | Identification | 49 |
| 8 | Recherche, repérage et restitution..... | 51 |
| 8.1 | Recherche et repérage | 51 |
| 8.2 | Restitution : affichage des documents | 55 |
| 8.3 | Restitution : impression | 55 |
| 8.4 | Restitution : autres cas | 56 |
| 9 | Fonctions d'administration..... | 57 |
| 9.1 | Administration générale..... | 57 |
| 9.2 | Reporting et statistiques..... | 58 |
| 9.3 | Modification, suppression et édition d'extrait des documents archivés | 59 |
| 10 | Autres fonctions | 63 |
| 10.1 | Gestion et archivage des documents non électroniques..... | 63 |
| 10.2 | Conservation et sort final des dossiers mixtes | 64 |
| 10.3 | GED | 65 |
| 10.4 | Workflow | 67 |
| 10.5 | Signature électronique | 70 |
| 10.6 | Chiffrement | 71 |
| 10.7 | Filigranes numériques, etc. | 72 |
| 10.8 | Interopérabilité et ouverture..... | 73 |
| 11 | Exigences non fonctionnelles..... | 74 |
| 11.1 | Facilité d'utilisation | 75 |
| 11.2 | Performance et extensibilité..... | 77 |
| 11.3 | Disponibilité du système..... | 79 |
| 11.4 | Normes techniques..... | 80 |
| 11.5 | Environnement législatif et réglementaire | 82 |
| 11.6 | Externalisation et recours à des tiers..... | 83 |
| 11.7 | Conservation à long terme et obsolescence technologique..... | 85 |
| 12 | Les métadonnées | 90 |
| 12.1 | Principes..... | 90 |
| 12.2 | Organisation de la suite de ce chapitre | 94 |
| 12.3 | Métadonnées du plan de classement | 96 |
| 12.4 | Métadonnées des séries et dossiers | 96 |
| 12.5 | Métadonnées des dossiers et sous-dossiers..... | 98 |
| 12.6 | Métadonnées des sous-dossiers..... | 99 |
| 12.7 | Métadonnées des documents..... | 100 |
| 12.8 | Métadonnées des extraits de document..... | 102 |
| 12.9 | Métadonnées concernant l'utilisateur | 103 |
| 12.10 | Métadonnées concernant les profils..... | 103 |
| 12.11 | Personnalisation des métadonnées..... | 103 |



| | | |
|----------------|--|------------|
| 13 | Modèle de référence..... | 105 |
| 13.1 | Glossaire | 105 |
| 13.2 | Modèle des relations entre entités..... | 112 |
| 13.3 | Détail du modèle des relations entre entités | 114 |
| 13.4 | Modèle de contrôle d'accès | 116 |
| ANNEXES | | 119 |

1 INTRODUCTION

1.1 Historique

Le besoin de spécifications complètes sur les exigences de l'archivage électronique à des fins de preuve a d'abord été coordonné par le DLM-Forum² en 1996, comme une des dix actions à mener à la suite de ce colloque. En conséquence le programme de la Direction générale Entreprises de la Commission européenne chargée des Echanges de données entre les administrations (IDA) a passé commande du développement de ces spécifications.

Après un appel d'offre en 1999, la rédaction de ces spécifications a commencé en 2000 et a été achevée au début de 2001. Ce travail a été mené par une petite équipe de spécialistes consultants de Cornwell Affiliates plc (aujourd'hui Cornwell Management Consultants plc), aidés et supervisés par une équipe d'experts de différents pays ; il a été validé par diverses organisations du secteur public comme du secteur privé.

L'annexe 2 donne le détail de la méthodologie suivie.

1.2 Objectif et champ d'application de ces spécifications

Ces spécifications décrivent les exigences pour l'organisation de l'archivage électronique ou « Model Requirements for the Management of Electronic Records » (MoReq). Il insiste principalement sur les exigences fonctionnelles pour l'archivage électronique à des fins de preuve à l'aide d'un système d'archivage électronique (SAE).

Les spécifications sont rédigées pour être également applicables au secteur public et aux entreprises du secteur privé qui souhaitent mettre en place un SAE, ou qui souhaitent évaluer la capacité de leur système existant au regard de l'archivage électronique.

Bien qu'il s'agisse essentiellement de spécifications fonctionnelles, il est évident que des éléments non-fonctionnels jouent un rôle central dans le succès d'un SAE, de même que pour tout système d'information. Toutefois, ces éléments non-fonctionnels varient considérablement d'un environnement à l'autre. C'est pourquoi ces éléments ne sont décrits que sommairement.

² DLM est l'acronyme de l'expression française « Données Lisibles par Machine », en anglais « Machine-readable data ». Le DLM-Forum s'appuie sur les conclusions du Conseil européen (94/C 235/03) du 17 juin 1994 relatives à une plus grande coopération dans le domaine des archives. [Aujourd'hui, DLM est généralement développé en Document Lifecycle Management – NDT]

D'autres domaines proches, comme le « document management » ou la gestion électronique de documents (GED) et la gestion électronique des archives physiques (les dossiers papier et les microfilms), sont également abordés sans toutefois être détaillés. Ainsi, les spécifications se prononcent sur les exigences de gestion des documents archivés, mais elles n'incluent pas toutes les fonctionnalités associées au suivi des adresses de localisation, au code-barre, etc. Les questions afférentes telles que la numérisation et autres moyens de créer des documents électroniques sont extérieures au champ de ces spécifications. De même, les étapes pratiques de mise en place d'un SAE ne rentrent pas dans le champ du modèle.

Ces spécifications présupposent que les utilisateurs du SAE regroupent non seulement les administrateurs et les archivistes, mais aussi les services administratifs et les opérationnels qui utilisent le SAE au quotidien en créant et recevant des documents à archiver, ou en recherchant des documents archivés.

Dans la mesure où ces spécifications comportent des exigences « modèles », elles sont nécessairement génériques et ne prennent en compte aucune plate-forme spécifique ni aucune problématique propre à un secteur d'activité. Grâce à son caractère modulaire, les communautés utilisatrices peuvent ajouter au modèle des fonctionnalités complémentaires en fonction de leurs activités particulières (voir la section 1.6 et l'Annexe 3 pour des conseils sur l'utilisation et la personnalisation de ces spécifications).

1.3 Qu'est-ce qu'un SAE ?

La maîtrise de l'archivage électronique est complexe et requiert l'implémentation correcte d'un grand nombre de fonctionnalités. Autrement dit, un système qui satisfasse à ces besoins – un SAE – requiert un outil logiciel spécifique. Cet outil peut consister en un outil unique spécialisé, un ensemble d'outils intégrés, un logiciel développé spécialement ou une combinaison de plusieurs éléments, mais dans tous les cas, il sera nécessaire de l'accompagner de procédures et de principes d'organisation. La nature d'un SAE varie d'un organisme à l'autre ou d'une entreprise à l'autre. Ces spécifications ne préjugent pas de la nature des solutions individuelles. Les utilisateurs de ce texte devront déterminer dans quelle mesure les fonctionnalités d'un SAE peuvent être implémentées afin de répondre à leurs besoins.

1.4 Quel usage pour ces spécifications?

Les spécifications MoReq sont destinées à être utilisées :

- **par les futurs utilisateurs d'un SAE** comme base de travail pour préparer un appel d'offre ;
- **par les utilisateurs d'un SAE** pour l'audit et le contrôle du système existant ;

- **par les organismes de formation** comme document de référence pour l'enseignement du records management et comme support de cours ;
- **par les institutions de l'enseignement supérieur** comme ressource pédagogique ;
- **par les fournisseurs et développeurs de systèmes d'archivage** pour aider au développement du produit en confortant les fonctionnalités exigées ;
- **pour les prestataires en archivage** pour orienter la nature des prestations ;
- **par les futurs utilisateurs d'un service d'archivage externalisé** comme une aide à la définition des prestations à fournir.

Les spécifications mettent l'accent sur l'utilisation qui peut en être faite. Elles se veulent avant tout pratiques.

1.5 Points forts et limites de ces spécifications

Les spécifications MoReq sont délibérément rédigées dans un esprit pragmatique et utilitaire. L'objectif principal est d'être un outil pratique pour aider les entreprises à répondre à leurs besoins en matière de gestion de l'archivage tant électronique que papier. Ces spécifications s'appuient à la fois sur l'archivistique traditionnelle et sur le records management mais ces disciplines ont été transposées à l'environnement électronique. Ainsi, MoReq a été élaboré en pensant aux besoins des responsables de l'archivage électronique et traditionnel.

Les exigences contenues dans ces spécifications MoReq, si elles sont implémentées, conduiront à un système en mesure de gérer les documents électroniques aux degrés de confidentialité et d'intégrité voulus, en combinant les avantages de la gestion électronique et ceux de la théorie classique de l'archivage. Cette approche pragmatique se retrouve dans la prise en compte des exigences de la GED, du workflow, des métadonnées et d'autres technologies proches.

Comme il a été expliqué plus haut, ces spécifications tentent de couvrir une large gamme de besoins – pour différents pays, dans différents domaines d'activité et avec des types de documents différents. Ce champ d'application très large est intentionnel, ce qui présente aussi des limites importantes, notamment dans le sens où ces simples spécifications ne peuvent correspondre sans aménagements à tous les besoins existants. Des pays différents ont des traditions, des manières de voir et des réglementations différentes en matière d'archivage ; il faudra sans doute en tenir compte dans l'application de ce modèle, particulièrement lors de la définition d'un nouveau système.

En outre, ce travail ne couvre pas les autres aspects pratiques de l'archivage. Ces spécifications se limitent délibérément aux fonctionnalités requises pour un logiciel d'archivage électronique. Elles évitent les considérations philosophiques sur le records management, l'archivistique théorique, les décisions et le contrôle de gestion, etc., ces sujets étant largement traités par la littérature existante dont on

trouvera une liste en Annexe 1. A titre d'exemple, les spécifications précisent à plusieurs reprises que certaines fonctions doivent être réservées à un administrateur. Ceci ne signifie pas que les administrateurs ont à prendre les décisions de fond mais simplement qu'ils doivent être les seuls utilisateurs autorisés par la direction à les exécuter au travers du SAE.

Finalement, ces spécifications sont volontairement centrées sur les utilisateurs. Elles utilisent autant que possible le vocabulaire des usagers des documents électroniques. Par exemple, le texte décrit les dossiers électroniques comme « contenant » des documents, pour une meilleure compréhension, bien que ces dossiers à proprement parler ne contiennent rien. Voir les détails au point 2.2.

1.6 Utilisation de ces spécifications

Les exigences présentées dans ces spécifications sont destinées à servir de modèle. Elles ne sont pas prescriptives pour tous les SAE possibles ; certaines exigences ne sont pas pertinentes dans certains environnements. Selon les secteurs d'activité, la taille de l'entreprise, les types d'organisation et d'autres facteurs, on ajoutera des exigences spécifiques. Ces spécifications doivent par conséquent être adaptées avant utilisation.

Ces spécifications ont été préparées pour être utilisées sous forme papier ou électronique. Elles utilisent les versions Word 97 et Word 2000 de Microsoft. L'utilisation de la forme électronique présente de nombreux avantages, voir les détails en Annexe 3.

1.7 Organisation des spécifications

Ces spécifications sont organisées en chapitres eux-mêmes divisés en sections.

Le chapitre suivant fournit un aperçu de quelques exigences clés, à commencer par la terminologie qui est centrale dans ce document.

Les chapitres 3 à 11 développent les exigences d'un SAE. Chaque chapitre présente un groupe logique d'exigences fonctionnelles. Toutefois, compte tenu du sujet traité, certains recouvrements entre les chapitres sont inévitables.

La présentation est normalisée. Les exigences sont présentées sous forme de tableau, à raison d'une exigence par ligne, selon le modèle ci-dessous :

| | |
|-------------|---------------------------|
| Réf. | Exigence |
| 13.1.1 | Le SAE doit permettre ... |
| ↑ | ↑ |
| ----- | ----- |
| NUMERO | EXIGENCE |

Chaque exigence porte un numéro et est exprimée en langage naturel.

Le chapitre 12 identifie les métadonnées nécessaires à la satisfaction de ces différentes exigences.

Le chapitre 13 comporte un modèle formel de SAE tel qu'il est compris dans ces spécifications. Ce modèle peut être utilisé pour comprendre certains aspects clés des spécifications, tels que les définitions formelles des termes utilisés (dossier, sous-dossier, niveau) et les relations existantes entre ces termes (exemple : « que peut-on stocker dans un dossier électronique ? »).

Les annexes donnent la liste des documents de référence, des indications d'ordre administratif et diverses informations.

1.8 Exigences obligatoires et souhaitables

Dans ces spécifications,

- le mot « doit » indique qu'il s'agit d'une exigence *a priori* obligatoire dans la plupart des SAE
- le mot « devrait » indique qu'il s'agit d'une exigence *a priori* souhaitable dans la plupart des SAE.

1.9 Commentaires sur ces spécifications

En cas de besoin, les commentaires et les observations sur ces spécifications peuvent être adressés à :

d1m-forum@cec.eu.int

2 PANORAMA DES EXIGENCES D'UN SAE

Ce chapitre commence par la définition de quelques mots clés (section 2.1), suivie de la présentation de quelques concepts clés (section 2.2.) et d'un diagramme des relations entre les entités qui montre le modèle de base de ces spécifications (section 2.3).

2.1 Terminologie fondamentale

Ces spécifications nécessitent de préciser le sens de certains mots. Chaque fois que possible, le sens est le sens courant ou le sens généralement admis parmi les professionnels de l'archivage. Tous les termes sont définis dans le Glossaire (section 13.1); quelques définitions fondamentales sont reprises ici pour en faciliter l'utilisation.

Les termes figurant *en italique* sont définis dans le Glossaire.

capture

Enregistrement, classement, ajout de *métadonnées* et stockage d'un *document* dans un système d'archivage.

classement

Identification et ordonnancement systématiques des activités et/ou des *documents à archiver* dans des catégories selon une organisation logique, des méthodes et des règles exposées dans un plan de classement.

Source : ISO 15489 (projet de norme internationale ; voir Annexe 1 référence [9])

document

Information enregistrée ou objet qui peut être traité comme une unité.

Source : ISO 15489 (projet de norme internationale ; voir Annexe 1 référence [9]).

NB : un *document* peut être sur papier, microfilm, support magnétique ou tout autre support électronique. Il peut comporter toute combinaison de texte, données, graphiques, son, images animées ou tout autre forme d'information. Un seul document peut être constitué d'un ou plusieurs objets de données.

NB : les simples *documents* présentent plusieurs différences importantes par rapport aux *documents d'archives (records)*. Voir *document d'archives*.

document d'archives, document archivé, archive, document

Document(s) produit(s) ou reçu(s) par une personne physique ou morale dans l'exercice de son activité et conservé(s) par cette personne physique ou morale.

Source : adapté des spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : il existe également des définitions nationales.

NB : un document d'archives peut être constitué d'une ou plusieurs pièces (par exemple un document et ses pièces jointes), et peut se présenter sous n'importe quel support et n'importe quel format. En plus du contenu initial, il devrait comporter les données de contexte et, si possible, les données de structure (c'est-à-dire les données qui décrivent les composantes du document). Une des caractéristiques fondamentales du document d'archives est qu'il ne peut pas être modifié.

document d'archives électronique

Un *document d'archives* sous forme électronique.

NB : la forme électronique peut être native, c'est-à-dire produite par une application logicielle, ou résulter d'une numérisation, c'est-à-dire du scannage de papier ou de microforme.

dossier électronique

Un ensemble logique de *documents d'archives* électroniques.

Source : spécifications fonctionnelles PRO pour le "dossier électronique" (Annexe 1 référence [2]).

NB : ce terme est souvent utilisé improprement pour désigner un *sous-dossier électronique*.

métadonnées

(dans le contexte de l'archivage) Informations structurées ou semi-structurées qui permettent la création, la gestion et l'utilisation des *documents archivés* au cours du temps, au sein du domaine d'activité qui les a créés.

Source : définition de travail du Forum « Archivage des métadonnées » (<http://www.archiefschool.nl/amf>).

NB : la distinction entre les données et les métadonnées est parfois délicate. Par exemple, il est en général admis que les données d'indexation de base d'un document archivé font partie des métadonnées du document. En revanche, l'historique des événements pour un document, ou sa durée de conservation, peuvent être considérés valablement comme des données ou des métadonnées selon le contexte. On peut définir plusieurs types de métadonnées, par exemple pour l'indexation, pour la conservation, pour la restitution, etc. Ces précisions sur l'utilisation des métadonnées dépassent le cadre des spécifications MoReq.

plan de classement

Voir classement.

Source : définition de « plan de classement » dans ISO 15489 (projet de norme internationale ; voir Annexe 1 référence [9]).

NB : un plan de classement se présente souvent comme une arborescence.

SAE

Système d'archivage électronique.

NB : un SAE présente plusieurs différences importantes par rapport à un système de GED. Voir les détails en section 10.3).

série

(dans ces spécifications seulement) Partie de l'arborescence d'un *plan de classement* partant de n'importe quel point de l'arborescence et englobant tous les dossiers inférieurs.

NB : ceci peut correspondre, dans la terminologie traditionnelle, à "chapitre", "groupe" ou "série" (ou sous-chapitre, sous-série, subdivision, etc.) à tous les niveaux du plan de classement.

sous-dossier

Subdivision d'un *dossier*, papier ou électronique.

Source : définition du mot "part" dans les spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : les subdivisions sont créées en vue de faciliter la gestion du contenu des dossiers à travers des unités de taille modeste plus aisées à manipuler. Les subdivisions sont mécaniques (c'est-à-dire basées le nombre de documents, sur des numéros ou sur un laps de temps) plutôt qu'intellectuelles.

2.2 Concepts fondamentaux

Les concepts requis pour la compréhension de ces spécifications sont :

- document d'archives et document d'archives électronique,
- dossier et sous-dossier électronique,
- plan de classement,
- série,
- SAE,
- capture des documents,
- profils utilisateurs.

Document d'archives et document d'archives électronique

Le guide du DLM Forum (Annexe 1 référence [6] section 2.4) suggère de considérer un document d'archives comme composé de :

- un contenu,
- une structure,
- un contexte,
- une présentation.

Le contenu se situe dans un ou plusieurs documents physiques ou électroniques qui portent le message de l'archive. Ces documents sont stockés de telle sorte que les futurs utilisateurs les appréhendent avec leur contexte. Ceci implique qu'une

archive contienne, outre le contenu des documents qui la composent, une information sur le contexte et la structure. La présentation dépend de la combinaison du contenu, de la structure et (dans le cas de l'électronique) du logiciel de restitution.

Dans l'environnement analogique, la grande majorité des archives sont sur papier et regroupées en dossiers, constitués physiquement d'un ou plusieurs sous-dossiers rangés dans des chemises. Des règles et des contrôles sont censés empêcher les utilisateurs de modifier les documents ou de les changer de place.

Des concepts similaires s'appliquent à l'environnement électronique. Une archive est constituée d'un ou plusieurs documents électroniques. Ces documents peuvent être des documents texte, des messages électroniques, des tableaux, des images fixes ou animées, des documents sonores ou tout autre type d'objet numérique. Les documents sont archivés quand ils sont sélectionnés, c'est-à-dire « capturés » dans le SAE. Avec la capture, les documents d'archives sont « classés », c'est-à-dire qu'ils sont reliés à la rubrique correspondante du plan de classement, ce qui permet au SAE de les gérer.

Dossier et sous-dossier électroniques

Les documents d'archives papier sont versés dans des dossiers, rangés dans des chemises. Les dossiers papiers sont ordonnés selon une structure pré-établie ou un plan de classement. Dans un SAE, les documents électroniques sont gérés comme s'ils étaient versés dans des dossiers électroniques et rangés dans des chemises électroniques. En fait, les dossiers et chemises électroniques n'ont pas besoin d'avoir une existence réelle ; ils sont virtuels, dans le sens où ils ne « contiennent » rien ; en réalité ce sont les métadonnées attachées aux documents archivés qui les constituent. Dans bien des cas, il n'est même pas besoin de distinguer dans le système électronique les dossiers et les chemises. Toutefois, ces détails sont en général transparents pour les utilisateurs du SAE ; un logiciel de SAE permet aux utilisateurs de voir et de gérer les chemises comme si elles contenaient physiquement les documents rangés logiquement dans les dossiers. C'est cette approche, centrée sur l'utilisateur, qui est retenue ici. Pour le reste, afin de faciliter la compréhension du texte, les dossiers électroniques sont décrits comme des « conteneurs » de documents. A noter cependant que si ces spécifications donnent les exigences fonctionnelles pour la gestion des dossiers électroniques, elles ne se prononcent pas sur la manière d'implémenter le concept de dossier électronique.

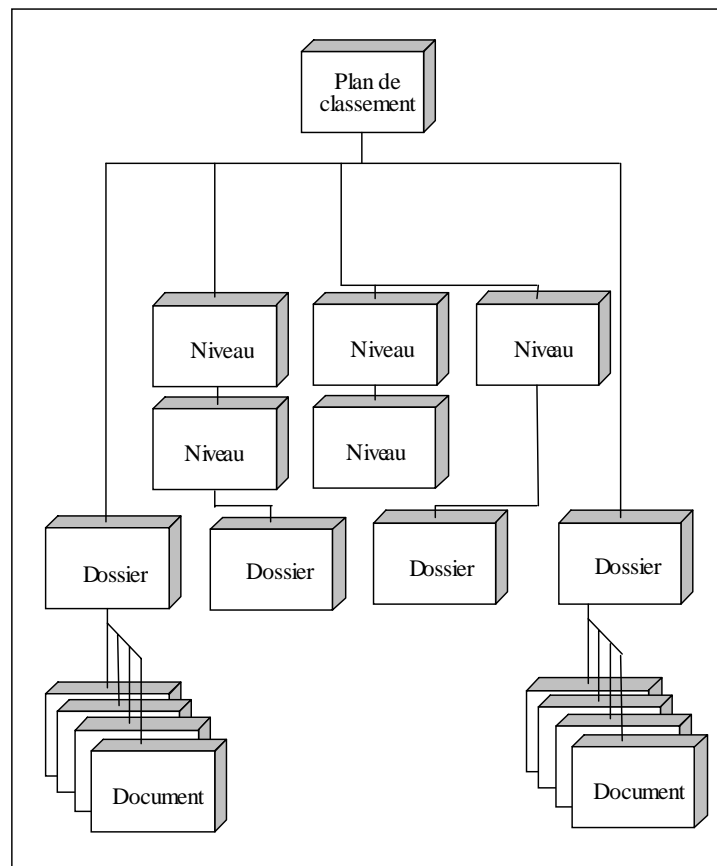
Dans certains cas, les dossiers sont divisés « mécaniquement » en sous-dossiers, selon des règles préétablies. Le terme « mécaniquement » suppose une simple adhésion à ces règles qui sont indépendantes du contenu des dossiers, mais basées sur la taille, le nombre de documents ou un laps de temps. Cette pratique, née dans l'environnement papier pour réduire le volume et le poids des dossiers, peut se poursuivre avec les dossiers électroniques, afin d'en faire des unités d'une taille plus « maniable » pour le tri, les transferts ou d'autres opérations de gestion.

Si la distinction entre les dossiers et les sous-dossiers est claire, ses conséquences le sont moins. En effet, le choix de diviser des dossiers en sous-dossiers a des conséquences variables selon les besoins. Les variations tiennent au fait que :

- certains dossiers sont clos à une date donnée, de sorte que l'unité de gestion est le dossier (même si le dossier est composé de plusieurs sous-dossiers). Par exemple, un petit dossier de marché, ou le dossier d'un projet.
- certains dossiers ont une durée de vie illimitée (ou quasiment illimitée), de sorte que l'unité de gestion est le sous-dossier. Par exemple, le dossier d'une circonscription géographique, ou un dossier traitant d'un sujet qui ne se périmé pas, comme la réglementation, ou un dossier de facturation dans lequel un nouveau sous-dossier est créé chaque année.

Plan de classement

Le records management ordonne les dossiers de manière structurée et les bonnes pratiques veulent que cette structure reflète les activités de l'entreprise ou de l'organisme. La représentation de cet agencement est dénommée « plan de classement ». Le plan de classement est en général hiérarchique, bien qu'il puisse aussi être organisé par un thésaurus sans arborescence. Les présentes spécifications ont retenu l'approche hiérarchique.



De même que les dossiers semblent exister même s'ils ne sont rien d'autre que l'agrégation de documents, de même les plus hauts niveaux du plan de classement semblent exister alors qu'ils ne sont que l'agrégation de dossiers ou de niveaux inférieurs. Comme pour les dossiers, ces spécifications établissent les exigences de hiérarchie sans préciser de quelle manière elles doivent être implémentées.

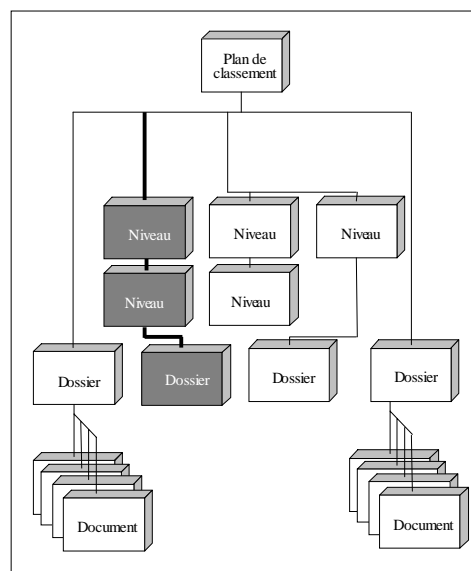
Les dossiers peuvent apparaître à n'importe quel niveau de l'arborescence, comme le montre la figure ci-dessus, adaptée de la norme ISAD(G) (Annexe 1 référence [7]).

A noter que cette figure a pour but de montrer un choix de relations possibles entre les différents niveaux. Elle ne montre pas tous les niveaux ni tous les ordonnancements possibles.

Série

Ces spécifications utilisent le mot « série » pour désigner la partie d'une arborescence qui part de n'importe quel point et englobe tous les dossiers inférieurs. Ce terme correspond à « groupe » ou « sous-groupe » ou « sous-série » dans certains textes.

Pour donner une comparaison, la série d'une arborescence correspond à la branche d'un arbre. Une série peut en inclure d'autres, elles-mêmes subdivisées en sous-séries. Les boîtes ombrées et les traits épais du schéma ci-contre sont un exemple de série.



Ces spécifications n'ont pas vocation à dire comment un plan de classement doit être élaboré ; ceci relève d'une autre discipline, voir par exemple les travaux UBC-MAS (Annexe 1 référence [8]).

Système d'archivage électronique (SAE)

Un SAE est d'abord une application pour gérer des archives électroniques, bien qu'on puisse également l'utiliser pour gérer des archives papier. Les présentes spécifications insistent délibérément sur la gestion des archives électroniques.

Un SAE est souvent étroitement articulé avec un système de gestion électronique de documents. Techniquement, un SAE gère des documents archivés, tandis qu'un système de GED gère des documents qui ne sont pas ou pas encore archivés. Toutefois, particulièrement dans le cadre du travail quotidien, il est difficile de

séparer leurs fonctionnalités. Ce point est développé dans la section 10.3 qui traite des problèmes de gestion documentaire.

La capture des documents

Les documents créés ou reçus dans l'exercice des activités sont archivés dès qu'ils sont sélectionnés, c'est-à-dire « capturés » dans le SAE. Pendant la capture, les documents sont « classés », c'est-à-dire qu'on leur affecte le code de la rubrique du plan de classement dont ils relèvent et qu'on leur assigne un identifiant unique, ce qui permet au SAE de les gérer.

Très souvent, les documents qui sont sélectionnés, ou capturés, sont archivés dans la logique d'un processus, comme cela se produit dans un workflow. Par exemple, quand une facture est émise, son archivage devrait être déclenché automatiquement. Dans d'autres cas, il peut exister une règle selon laquelle tout document relatif à un sujet donné est archivé, même s'il ne découle pas formellement d'une procédure précise. En d'autres circonstances toutefois, le processus de capture sera déclenché par un utilisateur. Le choix des documents qui doivent être capturés dans un système d'archivage devrait être basé sur une analyse de l'environnement réglementaire, des besoins des affaires, des exigences de responsabilité et du risque à ne pas archiver. Prenons l'exemple, dans une entreprise, des notes qui traitent de problèmes stratégiques : l'entreprise peut décider que seules les notes jugées significatives seront archivées (c'est-à-dire que, sauf exception, les notes courantes, concernant par exemple l'organisation des réunions, ne seront pas archivées). Ces spécifications entendent répondre à tous ces scénarios. En d'autres termes, MoReq décrit un système à usage général, et non seulement un système d'archivage pour certaines formes d'applications ou pour l'usage exclusif des archivistes ou des administrateurs de systèmes.

Profils d'utilisateurs

Ces spécifications identifient deux sortes d'utilisateurs :

« utilisateur » toute personne autorisée à accéder à l'application SAE.
Concrètement, il s'agit de toutes les personnes qui créent, reçoivent, révisent ou utilisent des documents d'archives, ainsi que celles qui administrent le SAE.

« administrateur » un utilisateur qui gère les documents archivés dans le SAE et le SAE lui-même avec ses bases de données.

En pratique, il y aura souvent plus d'une personne pour jouer ces rôles et de nombreuses entreprises ou organismes préciseront d'autres profils. Voir 13.4 pour plus d'information.

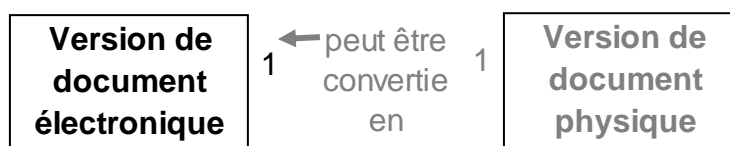
2.3 Modèle des relations entre entités

Cette section comporte un modèle des relations entre entités qui peut être utilisé pour mieux comprendre les spécifications. La section 13.3 contient une explication circonstanciée.

Il est important de noter que ce schéma ne représente pas les structures réelles d'un SAE. Il donne une vue des métadonnées associées aux documents. Un SAE utilise ces métadonnées pour gérer les documents archivés comme si la structure présentée dans le schéma existait réellement. Voir section 2.2. pour de plus amples explications sur ce point.

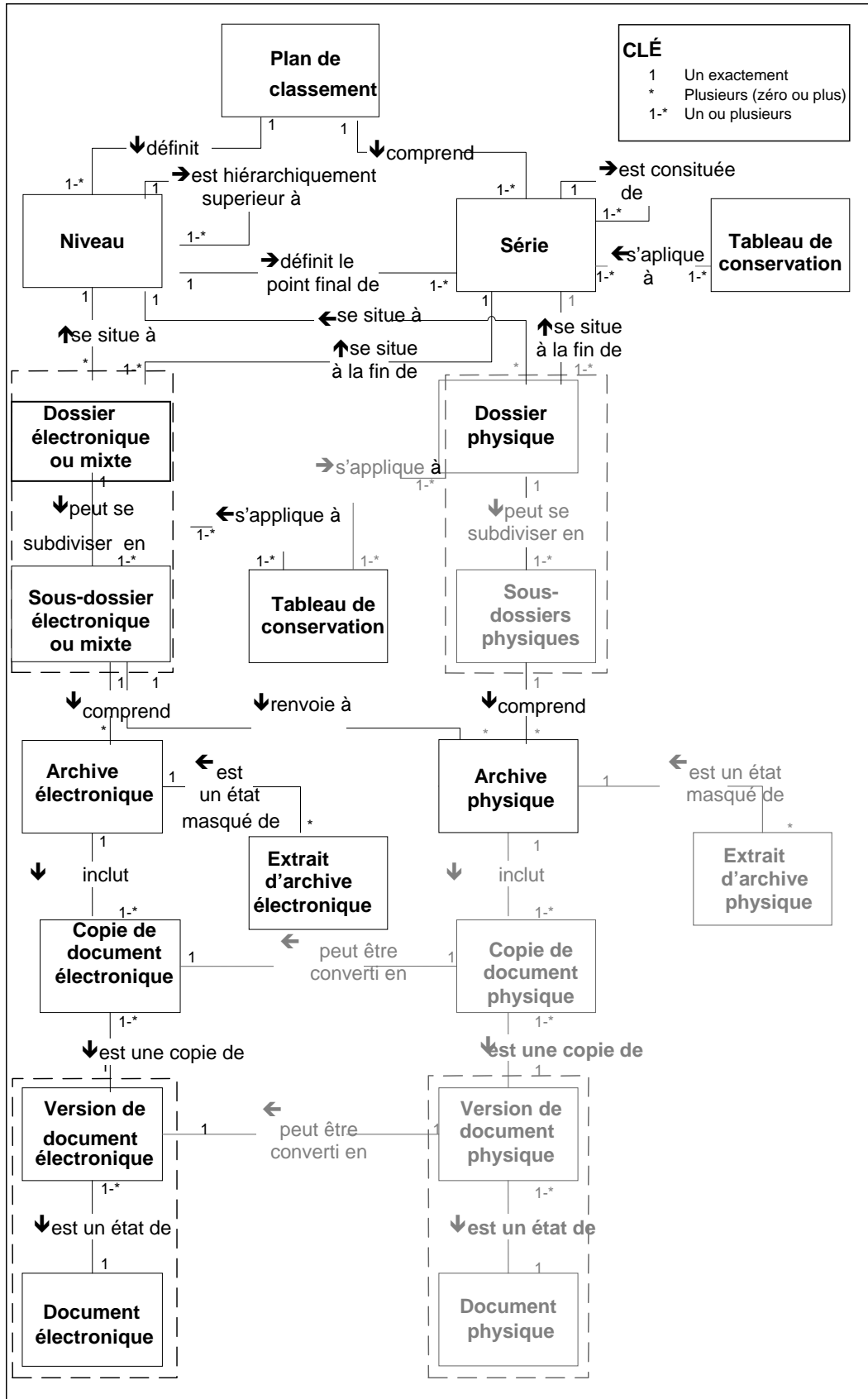
Les relations entre les dossiers, sous-dossiers, documents et autres entités sont décrites plus rigoureusement dans le schéma des relations entre entités ci-dessous. C'est une représentation formelle des structures que peut comprendre un SAE.

Dans le schéma, les entités – dossiers, documents, etc. – sont représentées par des rectangles. Les lignes qui les relient représentent les relations entre les entités. Chaque relation est décrite en toutes lettres dans une bulle au milieu de la ligne, à lire en direction de la flèche. A la fin de chaque relation, un chiffre indique le nombre d'occurrences (*stricto sensu* la cardinalité) ; les nombres sont expliqués dans la clé. Par exemple, l'extrait suivant :



signifie : « La version physique d'un document peut être convertie en document électronique » (noter la direction de la flèche).

A noter que l'entité « série » est reliée à elle-même par la relation « est constituée de ». Cette relation récursive décrit, en termes formels, la hiérarchie du classement, dans lequel une série peut comprendre une autre série. Pareillement, chaque niveau peut être supérieur hiérarchiquement à d'autres niveaux.



3 PLAN DE CLASSEMENT

Le plan de classement se situe au coeur de tout SAE, comme cela a été expliqué à la section 2.2. Il définit la façon dont les documents électroniques seront organisés en dossiers électroniques, ainsi que les relations entre les dossiers.

Ce chapitre énumère d'abord les exigences pour l'élaboration d'un plan de classement (section 3.1.). Il liste ensuite les exigences relatives aux séries et aux dossiers (section 3.2) et aux sous-dossiers (section 3.3). La dernière section (3.4) énumère les exigences liées à la maintenance du plan de classement.

3.1 Configuration du plan de classement

- | Réf. | Exigence |
|-------|--|
| 3.1.1 | Le SAE doit être compatible avec le plan de classement de l'entreprise ou de l'organisme et l'intégrer. |
| 3.1.2 | Le SAE doit pouvoir supporter un plan de classement reflétant une organisation hiérarchique des dossiers avec un minimum de trois niveaux. <i>Les trois niveaux suggérés ici sont un minimum ; certains environnements en nécessiteront davantage.</i> |
| 3.1.3 | Le SAE ne devrait pas limiter le nombre de niveaux dans la hiérarchie du plan de classement. |
| 3.1.4 | Le SAE doit permettre que les procédés de nommage soient définis au moment de la configuration. |
| 3.1.5 | Le SAE doit intégrer le plan de classement, dans sa version initiale, dès la configuration du système, afin de permettre la capture et l'import de documents électroniques. |
| 3.1.6 | Le SAE doit permettre aux administrateurs d'ajouter de nouvelles séries à n'importe quel point de l'arborescence, dès lors qu'il n'y pas de dossiers placés à cet endroit-là. <i>Noter que ceci peut se faire à tous les niveaux.</i> |
| 3.1.7 | Si le SAE doit être utilisé avec une interface graphique, il doit inclure un navigateur et la navigation dans les dossiers et le plan de classement, de même que la sélection, la recherche et l'affichage des dossiers électroniques et de leurs contenus doivent se faire à l'aide de cet outil. |
| 3.1.8 | Le SAE devrait pouvoir comporter la définition et l'utilisation simultanée de plusieurs plans de classement. <i>Ceci peut être nécessaire, par exemple, à la suite d'une fusion entre deux entreprises. Ce n'est pas nécessaire en temps normal.</i> |

Réf. Exigence

- 3.1.9 Le SAE devrait comporter un plan de classement distribué dont la maintenance puisse se faire au travers d'un réseau d'entrepôts de documents électroniques.

3.2 Séries et dossiers

Cette section énumère les exigences qui concernent les séries et les dossiers.

Réf. Exigence

- 3.2.1 Le SAE doit intégrer les métadonnées des dossiers et des séries du plan de classement ; après la capture d'un document, seuls les administrateurs doivent avoir la possibilité d'ajouter ou de modifier ces métadonnées.

Les exigences relatives aux métadonnées figurent au chapitre 12

- 3.2.2 Le SAE doit fournir au moins deux procédés de nommage pour les dossiers et les séries électroniques du plan de classement :

- un procédé d'allocation d'un code de référence structuré, numérique ou alpha-numérique (c'est-à-dire un identifiant unique au sein du plan de classement – voir chapitre 7) pour chaque dossier électronique ;
- un procédé d'allocation d'un nom de dossier en clair pour chaque dossier électronique.

Les deux identifiants doivent pouvoir être utilisés séparément ou ensemble dans la même application.

- 3.2.3 Le SAE doit permettre aux administrateurs d'ajouter (d'ouvrir) des dossiers au plus bas niveau de n'importe quelle série du plan de classement.

Noter que le plus bas niveau ne se situe pas nécessairement au même niveau pour toutes les séries.

- 3.2.4 Le SAE doit enregistrer la date d'ouverture d'une nouvelle série ou d'un nouveau dossier en tant que métadonnée du dossier.

- 3.2.5 Chaque fois qu'une nouvelle série ou un nouveau dossier est ouvert, le SAE doit automatiquement inclure dans ses métadonnées les éléments résultant de sa position dans le plan de classement (par exemple son nom et son code de classement).

Par exemple, si un dossier de correspondance présente le rattachement hiérarchique suivant :

Plan régional de développement : consultation publique : correspondance et que l'administrateur ajoute un nouveau dossier intitulé « objections formelles » au même niveau que « correspondance », ce dossier devra hériter automatiquement du préfixe « Plan régional de développement : consultation publique ».

- | Réf. | Exigence |
|-------------|--|
| 3.2.6 | Le SAE devrait comporter un procédé optionnel de nommage des séries et dossiers basé sur un vocabulaire contrôlé de termes et de relations issu d'un thésaurus conforme à ISO-2788 ou ISO 5964, avec un lien entre le thésaurus et le plan de classement. |
| 3.2.7 | Le SAE devrait comporter un procédé optionnel de nommage des séries et dossiers à partir des noms (par exemple les noms propres) et/ou des dates (par exemple les dates de naissance) utilisés comme noms de dossiers, avec une validation des noms par rapport à une liste. <i>Cette exigence s'impose plus spécialement dans un environnement transactionnel.</i> |
| 3.2.8 | Le SAE devrait permettre l'attribution de termes d'un vocabulaire contrôlé conformes à ISO 2788 ou ISO 5964 pour les métadonnées descriptives de séries ou de dossiers, en plus des autres exigences de cette section. |
| 3.2.9 | Le SAE ne doit pas imposer de limitation au nombre de séries ou dossiers à créer. |
| 3.2.10 | Le SAE doit permettre la création et la maintenance automatiques de listes ou de répertoires de dossiers. |

3.3 Sous-dossiers

Cette section concerne les exigences relatives aux sous-dossiers, qui sont plus particulièrement utilisés pour subdiviser les dossiers qui, sans cela, seraient lourds à gérer.

- | Réf. | Exigence |
|-------------|--|
| 3.3.1 | Le SAE doit permettre aux administrateurs d'ajouter (autrement dit, d'ouvrir) des sous-dossiers électroniques à tout dossier électronique non clos. |
| 3.3.2 | Le SAE doit enregistrer la date d'ouverture d'un nouveau sous-dossier parmi les métadonnées du sous-dossier. |
| 3.3.3 | Chaque fois qu'un nouveau sous-dossier est ouvert, le SAE doit automatiquement inclure dans ses métadonnées les métadonnées communes à tous les sous-dossiers (par exemple le nom et le code de classement). |

Réf. Exigence

3.3.4 Le SAE doit prendre en compte le concept d'ouverture et de clôture des sous-dossiers électroniques de la façon suivante :

- seul le sous-dossier le plus récemment créé au sein d'un dossier peut être ouvert ;
- tous les autres sous-dossiers du dossier doivent être clos (sous réserve des exceptions temporaires exposées en 3.3.6).

A noter qu'on doit pouvoir accéder aux documents de tout sous-dossier, qu'il soit ouvert ou clos..

3.3.5 Le SAE doit empêcher l'ajout par un utilisateur d'un document électronique à un sous-dossier clos (sous réserve des exceptions exposées en 3.3.6).

3.3.6 Le SAE doit permettre à un administrateur de réouvrir temporairement un sous-dossier déjà clos pour y ajouter des documents avant de clore de nouveau ce sous-dossier.

Cette facilité a pour but de permettre la correction d'une erreur de la part d'un utilisateur (clôture intempestive d'un sous-dossier).

3.4 Maintenance du plan de classement

Réf. Exigence

3.4.1 Le SAE doit permettre de déplacer un dossier électronique et ses sous-dossiers, voire une série complète, vers un autre point du plan de classement, en s'assurant que tous les documents électroniques attachés à ce ou ces dossiers et sous-dossiers y restent attachés.

Cette facilité est prévue uniquement pour des cas exceptionnels tels que des fusions ou autres réorganisations, ou encore pour corriger des erreurs d'écriture. Cette exigence doit être rapprochée des points 3.4.3, 3.4.4 et 3.4.5.

3.4.2 Le SAE doit permettre de reclasser un document électronique dans un autre dossier ou sous-dossier électronique.

Cette facilité est prévue uniquement pour des cas exceptionnels tels que la correction d'erreur d'écriture. Cette exigence doit être rapprochée des points 3.4.3, 3.4.4 et 3.4.5.

3.4.3 Le SAE doit réserver aux seuls administrateurs la possibilité de modifier les séries, dossiers, sous-dossiers et documents du plan de classement.

Réf. Exigence

3.4.4 Lors que des séries, des dossiers, des sous-dossiers ou des documents sont reclassés, le SAE doit conserver la trace de leur statut antérieur au reclassement, de sorte que l'on puisse facilement en reconstituer l'historique.

Au minimum, ces informations figureront dans l'historique des événements. Il peut être intéressant de les enregistrer également ailleurs, par exemple comme métadonnées des objets déplacés.

3.4.5 Lors que des séries, des dossiers, des sous-dossiers ou des documents sont reclassés, le SAE devrait permettre à l'administrateur de noter le motif du reclassement.

3.4.6 Le SAE doit en permanence empêcher la destruction, totale ou partielle, d'un dossier électronique, à l'exception de :

- la destruction conforme au tableau de conservation – voir chapitre 5.
- l'élimination par l'administrateur en application d'une procédure particulière – voir 9.3.

3.4.7 Le SAE doit permettre à l'administrateur de clore un dossier électronique à l'aide une procédure spécifique ; cette fonction est réservée à l'administrateur.

3.4.8 Le SAE devrait être capable de clore automatiquement un sous-dossier électronique dès que certains critères, prédéfinis lors de la configuration, sont remplis, à savoir, au minimum :

- les sous-dossiers délimités par une date de fin d'année, par exemple la fin de l'année civile, la fin d'une année budgétaire ou la fin d'un cycle annuel ;
- un laps de temps après un événement particulier, par exemple, après l'ajout de la dernière pièce de ce sous-dossier ;
- le nombre de documents électroniques contenus dans un sous-dossier.

D'autres critères peuvent être intéressants dans certaines circonstances, par exemple quand la taille des sous-dossiers dépasse les capacités de stockage d'un disque amovible.

3.4.9 Le SAE doit enregistrer la date de clôture d'un sous-dossier comme métadonnée du sous-dossier.

3.4.10 Le SAE ne doit pas permettre qu'un sous-dossier temporairement ré-ouvert (voir 3.3.6) reste ouvert après que l'administrateur a fermé sa session de travail.

3.4.11 Le SAE devrait permettre aux utilisateurs de créer des références croisées entre les dossiers (mention « voir aussi » ou création de liens).

Réf. Exigence

3.4.12 Le SAE doit maintenir en permanence l'intégrité interne (intégrité relationnelle ou autre), en dépit :

- des opérations de maintenance ;
- des manipulations des utilisateurs ;
- de la défaillance des composantes du système.

En d'autres termes, il doit être rigoureusement impossible que le geste d'un utilisateur ou une panne logicielle puisse provoquer une rupture de continuité au sein du SAE ou de ses bases de données.

3.4.13 Le SAE devrait offrir la possibilité de créer plusieurs entrées pour un même document électronique lié à plusieurs dossiers, sans pour autant dupliquer physiquement le document.

En d'autres termes, il devrait utiliser des pointeurs lors de la capture de plusieurs documents comportant la même pièce.

3.4.14 Le SAE devrait offrir des outils de reporting pour fournir à l'administrateur des états statistiques sur l'évolution du plan de classement : nombre de dossiers électroniques, de sous-dossiers ou de documents créés, clos ou détruits pendant une période donnée, etc..

4 CONTRÔLES ET SÉCURITÉ

Ce chapitre regroupe les exigences relatives aux différents contrôles liés à la sécurité des documents archivés.

Les administrations et les entreprises doivent être en mesure de contrôler qui a accès aux archives et dans quelles circonstances, car elles peuvent contenir des données personnelles, commerciales ou sensibles. Des restrictions d'accès peuvent également être apportées aux utilisateurs extérieurs. Par exemple, la législation sur l'information de certains pays permet aux usagers de demander à voir des documents publics. Ces contrôles sont abordés à la section 4.1.

Tout accès aux archives et toute opération qui les met en cause ou qui touche aux documents et données associés doit être tracé dans un historique des événements afin de garantir la traçabilité et aider à la récupération des données. Ces exigences sont abordées à la section 4.2.

La sécurité des documents archivés inclut également leur protection contre une faille du système par le biais de sauvegardes et la possibilité de restaurer les données à partir de ces sauvegardes. Ces exigences sont abordées à la section 4.3.

Pour différentes raisons, il arrive que des documents archivés soient déplacés d'un système à l'autre et d'un endroit à l'autre. Les exigences de ces transferts sont abordées à la section 4.4.

Les exigences relatives à l'authenticité des documents sont abordées à la section 4.5.

Enfin, la question des documents confidentiels (comme on en trouve dans certains ministères ou chez leurs partenaires) est abordée dans la section 4.6.

4.1 Accès

D'une façon générale, les entreprises et les administrations doivent contrôler l'accès à leurs archives. Elles doivent notamment restreindre ou ouvrir l'accès à certains documents ou dossiers pour les utilisateurs ou groupes d'utilisateurs. En cas d'enjeu national de sécurité, elles peuvent aussi prendre en considération les niveaux d'habilitation des utilisateurs.

L'attribution de ces droits d'accès doit être réservée à certains profils. Dans le tableau 13.4, c'est le profil de l'administrateur. Toutefois, l'administrateur ne fait que gérer dans le système les droits définis par la direction. Ces décisions sont notamment basées sur la législation et la réglementation : lois sur l'information, lois sur la sécurité des données, lois sur les archives patrimoniales et réglementation industrielle ; ces points sont évoqués à la section 11.5.

Réf. Exigence

- 4.1.1 Le SAE doit permettre à l'administrateur de réserver l'accès aux documents archivés, aux dossiers et aux métadonnées à des utilisateurs ou à des groupes d'utilisateurs identifiés.
- 4.1.2 Le SAE doit permettre à l'administrateur de paramétrer les profils d'utilisateurs selon les fonctions, les types de métadonnées, les documents et les dossiers auxquels l'utilisateur a accès. Ce paramétrage devra :
- interdire l'accès au SAE sans procédé d'authentification du profil utilisateur ;
 - restreindre l'accès à des dossiers ou documents précis ;
 - restreindre l'accès à des séries précises du plan de classement ;
 - restreindre l'accès au niveau d'habilitation de l'utilisateur ;
 - restreindre l'accès à des fonctions particulières (par exemple lecture, mise à jour et/ou destruction de métadonnées précises) ;
 - refuser l'accès après une certaine date ;
 - affilier l'utilisateur à un ou plusieurs groupes.
- Un exemple de procédé d'authentification est le mot de passe.*
- 4.1.3 Le SAE doit être en mesure de fournir les mêmes fonctions de contrôle pour les profils et pour les utilisateurs.
- Cette fonction permet aux administrateurs de gérer et de maintenir une série limitée de profils d'accès plutôt qu'un très grand nombre d'utilisateurs individuels. Les profils sont par exemple : gestionnaire, responsable des réclamations, analyste financier, administrateur de base de données.*
- 4.1.4 Le SAE doit être en mesure de constituer des groupes avec les utilisateurs qui travaillent sur les mêmes dossiers.
- Les groupes peuvent être par exemple : ressources humaines, équipe de vente.*
- 4.1.5 Le SAE doit permettre à un utilisateur d'être membre de plusieurs groupes.
- 4.1.6 Seul l'administrateur du SAE doit avoir la possibilité de créer des profils d'utilisateurs et d'affilier les utilisateurs à des groupes.
- Voir aussi section 13.4.*
- 4.1.7 Le SAE devrait permettre à un utilisateur de déclarer quels autres utilisateurs ou groupes peuvent avoir accès aux documents dont il est responsable. Ce rôle devrait être attribué à l'utilisateur par l'administrateur en vertu des principes d'organisation définis.
- 4.1.8 Seuls les administrateurs du SAE doivent avoir la possibilité de changer les paramètres de sécurité pour les groupes et les utilisateurs (droits d'accès, niveau de sécurité, privilèges, attribution de mots de passe et gestion).

Réf. Exigence

4.1.9 Si un utilisateur recherche ou veut accéder à un document archivé, un sous-dossier ou un dossier pour lequel il n'a pas de droits d'accès, le SAE doit donner une des réponses suivantes (à choisir lors de la configuration) :

- afficher le titre et les métadonnées ;
- signaler l'existence du dossier ou du document (c'est-à-dire afficher son identifiant) sans donner son titre ou d'autres métadonnées ;
- ne délivrer aucune information sur le document, même son existence.

Ces options sont présentées par ordre d'importance en termes de sécurité. A noter que la troisième option (c'est-à-dire la plus stricte) implique que le SAE ne fasse pas figurer de tels documents dans les résultats de recherche ; ce niveau de sécurité s'applique normalement aux documents relevant de la sécurité nationale.

4.1.10 Si un utilisateur effectue une recherche en texte intégral, le SAE ne doit en aucun cas faire figurer dans les résultats des documents auxquels l'utilisateur n'a pas accès.

A noter que ce point peut paraître contradictoire avec la première option du paragraphe 4.1.9 si elle est retenue, mais ceci est délibéré car, en l'absence de cette contrainte, les utilisateurs pourraient utiliser la fonction de recherche textuelle pour consulter des documents auxquels ils n'ont pas accès. En conséquence, cette exigence doit passer avant l'exigence 4.1.9.

4.1.11 Si le SAE permet à des utilisateurs d'accéder de manière indue à des dossiers, des sous-dossiers ou des documents archivés, ces accès devront être historisés.

On pourra limiter l'application de cette fonction à des catégories sécurisées définies par l'administrateur (comme défini au point 4.6).

4.1.12 Si le SAE conserve un répertoire des dossiers (voir 3.2.10), il doit permettre de limiter l'accès des utilisateurs à certaines parties du répertoire précisées lors de la configuration.

4.2 Historique des événements

Un historique des événements consiste en l'enregistrement systématique des opérations qui touchent le SAE. Cela comprend les opérations faites par les utilisateurs ou les administrateurs et les opérations initiées automatiquement par le SAE en fonction des paramètres du système. Voir la définition du glossaire à la section 13.1. Les données d'historique peuvent être considérées comme des métadonnées (dans la mesure où il s'agit d'informations descriptives de l'histoire des documents), bien que ceci ne soit pas essentiel.

Le SAE doit être capable de gérer et de contrôler les documents électroniques en respectant les normes visant à la satisfaction des exigences légales de traçabilité et de sécurité, et doivent être en mesure de démontrer leur conformité à ces

exigences. L'historique est un facteur clé dans la satisfaction de ces exigences car il procure un enregistrement complet de toutes les opérations sur chaque document.

L'historique peut produire un volume de données important si toutes les opérations sont contrôlées. C'est pourquoi, dans certaines implémentations, la direction peut décider que certaines opérations n'ont pas besoin d'être contrôlées ; par ailleurs, l'historique en ligne est en général périodiquement transféré hors-ligne, et peut être détruit quand les documents correspondants sont eux-mêmes détruits. C'est une question de politique managériale ou d'exigences légales ou réglementaires ; MoReq intègre donc les exigences permettant ces actions mais ne se prononce pas sur leur degré d'utilisation.

Réf. Exigence

4.2.1 Le SAE doit contenir un historique des événements inaltérable capable de capturer et de stocker automatiquement toute information sur :

- toute opération effectuée sur un document ou un dossier électronique ou sur le plan de classement ;
- l'utilisateur qui prend l'initiative et/ou exécute cette opération ;
- la date et l'heure de l'opération.

Le terme « inaltérable » signifie que les données de l'historique ne peuvent être modifiées en aucune façon ni détruites par qui que ce soit : l'historique peut toutefois être réorganisé et recopié sur un support amovible pour des raisons logicielles par exemple, dès lors que son contenu reste inchangé.

4.2.2 Une fois la fonctionnalité d'historique activée, le SAE doit tracer tous les événements sans intervention manuelle, et stocker dans l'historique toute l'information correspondante.

4.2.3 Le SAE doit maintenir l'historique aussi longtemps que nécessaire, c'est-à-dire au minimum pendant toute la vie des documents et dossiers électroniques correspondants.

4.2.4 Le SAE doit fournir un historique de tous les changements concernant :

- les groupes de dossiers électroniques,
- les dossiers électroniques individuellement,
- les sous-dossiers électroniques,
- les documents électroniques,
- les pièces électroniques,
- les métadonnées de chacune des entités ci-dessus.

4.2.5 Le SAE doit fournir un historique de tous les changements de paramètres administratifs.

Par exemple, si l'administrateur change les droits d'accès d'un utilisateur.

Réf. Exigence

4.2.6 Le SAE doit être en mesure de capturer et stocker dans l'historique les informations relatives aux opérations suivantes :

- la date et l'heure de la capture de tous les documents électroniques ;
- le reclassement d'un document électronique dans un autre sous-dossier (voir 3.4.2) ;
- le reclassement d'un dossier électronique à l'intérieur du plan de classement (voir 3.4.1) ;
- toute modification de la durée de conservation d'un dossier électronique ;
- toute modification des métadonnées d'une série, d'un dossier ou d'un document électronique ;
- la date et l'heure de la création, de la correction et de la destruction des métadonnées ;
- les modifications de droits d'accès touchant un dossier électronique, un document électronique, ou un utilisateur ;
- les opérations d'export ou de transfert d'un dossier électronique ;
- la date et l'heure des restitutions (voir le Glossaire section 13.1) ;
- les opérations d'élimination / destruction de dossier ou document électronique.

4.2.7 Le SAE devrait permettre à l'administrateur de configurer l'historique des événements et de choisir quelles informations seront enregistrées automatiquement ; le SAE doit garantir que ce choix et tous les changements qui y seraient apportés seront stockés dans l'historique.

4.2.8 Le SAE doit garantir que les données de l'historique sont accessibles en cas de contrôle ou d'audit, de sorte qu'un événement particulier et toutes les données afférentes soient identifiés et accessibles, et que ce contrôle puisse être effectué par une personne extérieure autorisée, peu ou pas familière du système.

4.2.9 Le SAE doit être capable d'exporter l'historique des événements concernant tels documents, dossiers ou groupes de dossiers particuliers (sans modifier l'historique global du SAE).

Cette fonctionnalité peut être utilisée par des auditeurs externes qui souhaiteraient examiner ou analyser le fonctionnement du système.

4.2.10 Le SAE doit être capable de tracer et de conserver les tentatives de violation du système (c'est-à-dire les tentatives d'accès à des documents, sous-dossiers ou dossiers non autorisés), et (en cas de réussite) de tracer les violations des procédés de contrôle d'accès.

Voir en 4.1.9. les cas de tentative de violation du système.

Réf. Exigence

- 4.2.11 Il est indispensable que le SAE puisse fournir des rapports sur les opérations effectuées sur les séries, dossiers et documents :
- par document, dossier ou série,
 - par utilisateur,
 - dans l'ordre chronologique.
- 4.2.12 Le SAE devrait pouvoir fournir des rapports d'opérations sur les dossiers et documents par station de travail et par adresse réseau (si cela est pertinent).

4.3 Sauvegarde et restauration

La conduite des affaires et la réglementation requièrent l'une et l'autre que le SAE soit doté d'un dispositif complet de sauvegarde régulière des documents et des métadonnées, afin de restituer rapidement des documents perdus par suite de défaillance du système, d'accident, de violation de la sécurité, etc.

Des sauvegardes et restaurations automatiques et régulières peuvent être fournies par le SAE ou intégrées dans les fonctionnalités d'un système de gestion électronique de documents (GED) ou effectuées par un système de gestion de bases de données relié au SAE.

En pratique, les fonctions de sauvegarde et de restauration peuvent être partagées entre les administrateurs du SAE et les responsables des technologies de l'information.

Réf. Exigence

- 4.3.1 Le SAE doit fournir des procédures de sauvegarde et de restauration automatiques pour la sauvegarde régulière de la totalité ou d'une sélection des séries, dossiers, documents et métadonnées conservés dans le SAE, avec leurs règles de gestion.
- 4.3.2 Le SAE doit permettre à l'administrateur de programmer des sauvegardes :
- en fonction de la fréquence voulue ;
 - selon un choix de séries, dossiers ou documents à sauvegarder ;
 - selon les supports de stockage, le système ou la localisation des fichiers sauvegardés (par ex. : stockage hors ligne, système distinct, site distant).
- 4.3.3 Seul l'administrateur du SAE doit avoir la possibilité de restaurer les sauvegardes. L'intégrité des données doit être maintenue après la restauration.
- 4.3.4 Seul l'administrateur doit pouvoir relancer le SAE à partir d'une sauvegarde, en préservant l'intégrité des données.

Réf. Exigence

4.3.5 Le cas échéant, le SAE devrait pouvoir notifier aux utilisateurs qui se reconnectent au système, que leurs mises à jour ont pu être incomplètement restaurées.

4.3.6 Le SAE doit permettre aux utilisateurs de signaler quels documents ils considèrent comme des archives vitales.

Les archives vitales sont les documents qui sont absolument nécessaires à la poursuite des activités d'une entreprise, que ce soit en termes de capacité à réagir à une situation d'urgence ou de catastrophe ou pour la protection de ses intérêts financiers et légaux. L'identification et la préservation de ces documents revêtent donc une très grande importance dans toute entreprise.

4.3.7 Le SAE devrait permettre de distinguer les opérations de restauration des archives vitales et celles des autres documents.

4.4 Traçabilité des mouvements

Au cours de leur vie, les dossiers et leurs métadonnées peuvent être transférés sur un autre support ou dans un autre lieu, si leur actualité décroît et/ou que leur utilisation change. Ce transfert peut se faire localement : *near-line* (par ex. sur un support amovible dans un dispositif automatisé, tel qu'un CD-R dans un juke-box), hors-ligne (par ex. dans une zone de stockage locale ou distante), ou dans un autre centre d'archivage (par ex. les Archives nationales). La traçabilité de ces changements de localisation doit être assurée à la fois pour faciliter l'accès et pour satisfaire aux obligations réglementaires.

Réf. Exigence

4.4.1 Le SAE doit fournir un dispositif de contrôle pour assurer la traçabilité de la localisation et des mouvements des dossiers, tant électroniques que papier.

4.4.2 Cette fonction doit enregistrer toute information relative aux mouvements, à savoir :

- identifiant unique du dossier ou des documents ;
- localisation courante ainsi que l'indication des localisations précédentes (en principe définies par les utilisateurs) ;
- date d'envoi ou de changement de localisation ;
- date de réception (pour les transferts) ;
- utilisateur responsable du mouvement (le cas échéant).

Réf. Exigence

- 4.4.3 Le SAE doit préserver l'accès au contenu des documents électroniques, y compris la possibilité de les restituer, en respectant leur structure et leur présentation, et ce sur le long terme et au travers de plusieurs générations logicielles.

Ceci peut se faire, mais ce n'est pas une obligation, via l'utilisation d'un viewer multi-formats. Pour plus de détails sur la restitution sur le long terme, voir section 11.7.

4.5 Authenticité

La politique de l'entreprise et les règles de conservation des archives définiront quels documents doivent être capturés et à quel moment. Il est capital qu'après la capture, aucune composante du document, ni sa structure ni les métadonnées nécessaires pour établir son authenticité, ne soient altérées. Les documents doivent être conservés dans une forme non-modifiable et protégés contre des changements intentionnels ou accidentels de leur contenu, de leur contexte, de leur structure ou de leur apparence et ce toute leur vie afin de maintenir leur authenticité.

Réf. Exigence

- 4.5.1 Le SAE doit restreindre l'accès aux fonctions du système en fonction des profils utilisateurs et des contrôles administratifs.

Ceci est nécessaire pour préserver l'authenticité des archives électroniques.

- 4.5.2 Quand cela est possible et opportun, le SAE devrait fournir une alerte sur les tentatives de capture d'un document incomplet ou dont l'état compromettrait l'authenticité dans le futur.

Par exemple, un bon de commande sans signature électronique valide, ou une facture de fournisseur non identifié.

- 4.5.3 Quand cela est possible et opportun, le SAE devrait fournir une alerte sur les tentatives de capture d'un document dont il serait impossible de vérifier ultérieurement l'authenticité.

- 4.5.4 Le SAE doit prévenir tout changement, par les utilisateurs ou les administrateurs, du contenu d'un document électronique archivé (sauf quand ces changements sont inhérents à l'activité de l'entreprise ou à un processus documentaire, comme cela est exposé ailleurs dans ces spécifications).

4.6 Indices de sécurité

La section 4.1 décrit les exigences relatives au contrôle d'accès des utilisateurs et des groupes d'utilisateurs. Dans certains cas, notamment quand la sécurité nationale est en cause, il est nécessaire de limiter l'accès à l'aide d'indices de sécurité et de niveaux d'habilitations. Ces habilitations priment sur tout droit

d'accès reposant sur les critères définis à la section 4.1. Les exigences de cette section ne s'appliquent que lorsque ce besoin existe.

Il s'agit d'attribuer un ou plusieurs « indices de sécurité » aux séries, dossiers et documents. Le terme « indice de sécurité » est utilisé ici pour désigner « une ou plusieurs données associées à un document pour préciser les règles et conditions d'accès ».

Les utilisateurs se voient alors attribuer un ou plusieurs niveaux d'habilitations qui empêchent l'accès aux séries/dossiers/documents dotés d'indices plus élevés.

Les indices de sécurité peuvent être divisés en catégories qui sont soit de nature hiérarchique, soit organisées en fonction d'autres critères spécifiques à une entreprise ou à un domaine d'activité. MoReq développe seulement les exigences pour les catégories hiérarchiques.

Réf. Exigence

4.6.1 Le SAE doit permettre d'affecter des indices de sécurité aux documents archivés.

4.6.2 Le SAE doit permettre un des choix suivants au moment de la configuration :

- indices de sécurité affectés aux séries, dossiers et sous-dossiers ;
- séries, dossiers et sous-dossiers électroniques sans indice de sécurité.

Ceci est souhaitable dans la mesure où certaines entreprises préfèrent affecter aux dossiers électroniques des indices de sécurité qui imitent les procédures papier, tandis que d'autres préfèrent protéger seulement les documents fondamentaux.

4.6.3 Le sous-système de sécurité du SAE devrait pouvoir être compatible avec les outils de sécurité générale de l'entreprise.

4.6.4 Le SAE doit permettre, mais non imposer, la subdivision des indices de sécurité en une ou plusieurs catégories.

Par exemple, les indices de sécurité peuvent être composés de trois catégories, comme dans l'exemple fictif suivant :

Réf. Exigence

| <i>Catégorie</i> | <i>Valeurs possibles</i> |
|----------------------|---|
| <i>Niveau</i> | <i>Ultra secret Secret Confidentiel Réservé Non classifié</i> |
| <i>Avertissement</i> | <i>Accès réservé à l'OTAN Accès réservé à l'UEO</i> |
| <i>Descripteur</i> | <i>Commercial Personnel Direction Audit et contrôle</i> |

Dans cet exemple fictif, la catégorie « niveau » est hiérarchique (voir 4.6.4) tandis que les autres ne le sont pas. Les exigences des catégories hiérarchiques sont communes, voir ci-dessous. Toutefois, elles peuvent être complexes ; à l'exception de l'exigence 4.6.4, elles ne sont pas détaillées ici.

- 4.6.5 Le SAE devrait permettre des implémentations spécifiques de règles de sécurité complexes ou uniques.

Une série d'interfaces applicatives peut répondre à ce besoin. Cela est nécessaire si l'on veut gérer des documents se référant à des conventions de marquage non prises en compte ici comme celle de l'IDO (International Defence Organisation) ou à des restrictions d'accès aux données médicales

- 4.6.6 Pour une catégorie au moins, le SAE doit supporter une hiérarchie d'au moins cinq valeurs, depuis l'accès sans restriction jusqu'au plus haut degré de sécurité.

La catégorie « niveau » du point 4.6.4 en est un exemple.

- 4.6.7 Le SAE doit permettre d'attribuer des niveaux d'habilitation aux utilisateurs, correspondant aux catégories.

A la suite de l'exemple en 4.6.4, les utilisateurs se verront affecter un des niveaux d'habilitation suivants :

*Ultra secret
Secret
Confidentiel
Réservé
Non classifié*

Réf. Exigence

4.6.8 Le SAE doit refuser aux utilisateurs l'accès aux documents électroniques (et aux séries et dossiers correspondants selon le choix fait au le point 4.6.2) qui ont un indice de sécurité plus élevé que leur niveau d'habilitation.

A noter que le bon niveau d'habilitation n'est pas une condition suffisante. L'accès aux documents électroniques peut être également réservé à des utilisateurs, des profils ou des groupes identifiés, selon les critères décrits à la section 4.1.

4.6.9 Le SAE doit permettre l'affectation automatique, par défaut, de la valeur la plus basse de chaque catégorie à une série, un dossier ou un document électronique qui n'aurait pas reçu d'autre indice de sécurité.

Par exemple, à la suite de l'exemple 4.6.4, la valeur par défaut serait « non classifié ».

4.6.10 Le SAE devrait pouvoir interdire qu'un dossier électronique reçoive un indice de sécurité inférieur à ceux des documents qui le composent (selon le choix fait au le point 4.6.2).

4.6.11 L'administrateur devrait pouvoir attribuer l'indice de sécurité le plus élevé à tout document, série ou dossier par le biais d'une requête simple.

Dans certains cas, ceci sera un critère important de maniabilité.

4.6.12 Le SAE devrait comporter un programme de révision des indices de sécurité.

5 CONSERVATION ET SORT FINAL

L'utilisation de tableaux de conservation pour piloter la sortie des documents à archiver des systèmes opérationnels est un des aspects fondamentaux du records management. Les tableaux de conservation définissent la période pendant laquelle les documents sont gardés dans le SAE et leur sort final à l'issue de cette période. Les exigences sur ce thème sont abordées au point 5.1.

Les opérations à mener à l'échéance indiquée par le tableau de conservation sont décrites à la suite. Les exigences relatives au processus de vérification sont indiquées au point 5.2, et les exigences concernant les transferts, les exports et la destruction sont énoncées au point 5.3.

Terminologie

Les documents archivés sont constitués tantôt en dossiers, tantôt en sous-dossiers (voir section 2.2 « Dossiers et sous-dossiers électroniques »). Ceci est valable pour toutes les étapes des processus de ce chapitre. Toutefois, pour simplifier, le mot « dossier » est utilisé dans les deux cas.

5.1 Tableaux des durées de conservation

| Réf. | Exigence |
|-------|--|
| 5.1.1 | Le SAE doit permettre d'élaborer des tableaux des durées de conservation, d'automatiser les opérations de reporting et de planifier la destruction, et offrir des moyens d'export des documents et de leurs métadonnées. |
| 5.1.2 | Le SAE doit permettre de réserver à l'administrateur l'élaboration et la modification des tableaux de conservation. |
| 5.1.3 | Le SAE doit permettre à l'administrateur d'élaborer de conserver dans le système une collection validée de tableaux de conservation adaptés. |
| 5.1.4 | Le SAE doit être en mesure de relier n'importe quel document, dossier ou série du plan de classement à un tableau de conservation. |

La durée de conservation peut être choisie parmi les tableaux de référence ou saisie manuellement à création du dossier.

- Réf. Exigence**
- 5.1.5 Le SAE devrait pouvoir relier un dossier ou une série du plan de classement à plusieurs durées de conservation.
- Exemples :*
- *un dossier peut relever d'un tableau de référence pour l'activité dont il procède, et d'un second tableau, spécifique, en raison du contenu lié à ce dossier ;*
 - *une série peut relever d'un délai de conservation légal tandis qu'un segment de cette série relèvera en outre d'une durée de conservation différente en application des règles de conservation des archives médicales.*
- 5.1.6 Tout document archivé dans un dossier ou une série doit, par défaut, relever du tableau de conservation associé à ce dossier ou à cette série.
- 5.1.7 Chaque tableau de conservation doit indiquer le sort final (exigence 5.1.10), la durée de conservation (5.1.10), le motif et sa justification.
- 5.1.8 Pour chaque dossier, le SAE doit :
- assurer un suivi automatique des durées de conservation attribuées à un dossier ou à la série dont il dépend ;
 - appliquer le sort final dès l'échéance de la durée de conservation.
- 5.1.9 Si un dossier ou une série est relié à plusieurs tableaux de conservation, le SAE doit assurer le suivi automatique de toutes les durées prescrites dans les tableaux, et appliquer le sort final à échéance des différentes dates.
- 5.1.10 Le SAE doit permettre, pour chaque tableau de conservation, au minimum les choix suivants :
- la conservation à titre définitif ;
 - le renvoi à une date ultérieure de révision, comme indiqué au point 5.1.11 ;
 - la destruction à une date ultérieure, comme indiqué au point 5.1.11 ;
 - le transfert à une date ultérieure, comme indiqué au point 5.1.11 ;

Réf. Exigence

5.1.11 Chaque tableau de conservation doit permettre que les durées de conservation (voir 5.1.10) soit définies en fonction d'une date ultérieure, elle-même définie de la façon suivante :

- écoulement d'un certain laps de temps à partir de l'ouverture du dossier ;
- écoulement d'un certain laps de temps à partir de la clôture du dossier ;
- écoulement d'un certain laps de temps à partir de l'ajout au dossier du document le plus récent ;
- écoulement d'un certain laps de temps depuis la consultation du dossier ;
- écoulement d'un certain laps de temps après un événement particulier (l'événement est précisé dans le tableau et sa notification au SAE sera effectuée par l'administrateur plutôt qu'automatisée) (par exemple, « ... après la signature du contrat ») ;
- mention « illimité » pour indiquer une conservation à long terme.

Ces cas de figure sont généralement pris en compte ; toutefois, il est possible que certains types de documents requièrent d'autres exigences.

5.1.12 Le SAE doit supporter des durées de conservation d'un an à plus d'un siècle selon les exigences du point 5.1.11.

Ces durées minimum et maximum, qui sont arbitraires, visent à éviter toute limitation. Bien qu'il soit improbable qu'un SAE vive plus d'un siècle, ce type d'exigence permet d'envisager l'export des documents vers d'autres systèmes sans avoir besoin de réviser les tableaux de conservation.

5.1.13 Le SAE doit enregistrer et signaler automatiquement à l'administrateur toutes les opérations de sort final.

5.1.14 Le SAE doit permettre d'associer un dossier à une durée de conservation qui primera sur la durée de conservation attribuée à la série dont ce dossier fait partie.

5.1.15 Le SAE doit permettre à l'administrateur de corriger la durée de conservation attribuée à un dossier à tout moment de son cycle de vie.

5.1.16 Le SAE doit permettre à l'administrateur de rattacher un dossier à un autre tableau à tout moment de son cycle de vie.

5.1.17 Le SAE devrait permettre de définir diverses règles en vue de constituer un système d'alerte pour certains dossiers ou séries avant la mise en œuvre du dispositif de sort final. Par exemple :

- révision d'un dossier et de son contenu par un gestionnaire identifié ou par l'administrateur ;
- signalement à l'administrateur des dossiers portant tel indice de sécurité.

Réf. Exigence

- 5.1.18 Quand l'administrateur déplace des dossiers ou des documents entre les séries du plan de classement, le SAE devrait permettre, comme option, que la durée de conservation initiale de ces documents soit remplacée par la durée de conservation de la nouvelle série.

5.2 Révision

La révision est le processus de contrôle des dossiers qui ont atteint la date ou l'événement mentionné dans le tableau de conservation, afin de décider s'ils seront conservés, transférés vers un autre système, ou détruits. La révision peut prendre en compte les métadonnées, les contenus ou les deux. Dans certaines situations, le sort final prescrit par les tableaux de conservation est appliqué sans révision.

Le sort final de certains documents archivés relève de la législation et de la réglementation. La révision doit en tenir compte et, le cas échéant, se faire sous l'autorité de l'administration des Archives. Le développement de ces questions dépasse le cadre des présentes spécifications.

Réf. Exigence

- 5.2.1 Le SAE devrait pouvoir notifier régulièrement à l'administrateur les durées de conservation qui prennent effet à un moment donné, et fournir des statistiques sur les volumes et les types de documents concernés.
- 5.2.2 L'administrateur devrait pouvoir déterminer la fréquence de ces statistiques, le type de données à y faire figurer et le signalement des anomalies telles que des éliminations en retard.
- 5.2.3 Le SAE doit comporter un processus de révision qui dresse la liste des dossiers électroniques à réviser, avec leurs métadonnées, la durée de conservation et son motif, de façon qu'on puisse parcourir et examiner efficacement les contenus et/ou les métadonnées des dossiers.

Concrètement, ceci implique des fonctionnalités de navigation souples entre les dossiers et les documents et entre les métadonnées.

- 5.2.4 Le SAE devrait alerter l'administrateur quand un dossier électronique à détruire fait l'objet d'un lien avec un autre dossier ; et devrait différer la destruction pour permettre une des opérations suivantes :
- confirmation de la destruction par l'administrateur ou annulation ;
 - émission d'un rapport détaillé sur les dossiers ou documents concernés, avec toutes leurs références et liens.

Réf. Exigence

- 5.2.5 Le SAE doit permettre que, lors de la révision, on puisse effectuer pour chaque dossier, au moins l'une des opérations suivantes :
- cocher les dossiers à détruire ;
 - cocher les dossiers à transférer (voir 5.3.7) ;
 - modifier la durée de conservation (ou attribuer une durée différente) renvoyant à une révision ultérieure dont la date sera déterminée selon le point 5.1.11.
- 5.2.6 Le SAE doit permettre, lors de la révision, de saisir des commentaires parmi les métadonnées du dossier, afin de tracer le motif des décisions prises.
- 5.2.7 Le SAE doit signaler à l'administrateur les dossiers à éliminer avant la mise en œuvre des opérations de destruction, et, après validation par l'administrateur, déclencher le processus de destruction mentionné au point 5.1.10.
- 5.2.8 Le SAE doit comporter des outils de reporting et d'analyse pour la gestion des tableaux de conservation par l'administrateur, y compris la possibilité de :
- lister tous les tableaux de conservation ;
 - lister tous les dossiers électroniques visés par une durée de conservation donnée ;
 - lister les tableaux de conservation relatifs à tous les dossiers en dessous d'un niveau donné de l'arborescence du plan de classement ;
 - identifier, comparer et réviser les tableaux de conservation (et leur contenu) par rapport au plan de classement ;
 - identifier les contradictions formelles entre les tableaux de conservation par rapport au plan de classement.
- 5.2.9 Le SAE doit conserver dans l'historique des événements toutes les décisions prises à l'occasion des révisions.
- 5.2.10 Le SAE devrait comporter ou fournir la possibilité d'une interface avec un système de workflow pour gérer le calendrier des opérations de révision, d'export ou de transfert, en traçant :
- l'état d'avancement de la révision (en attente ou en cours, nom du responsable et date) ;
 - les documents en attente d'élimination après la révision ;
 - l'avancement du processus de transfert.
- 5.2.11 Le SAE devrait pouvoir générer des statistiques sur l'activité de révision au cours d'une période donnée et produire les tableaux et les graphiques correspondants.

5.3 Transfert, export et destruction

Les entreprises ou organismes peuvent avoir besoin de déplacer les documents archivés de leur SAE vers d'autres lieux ou d'autres systèmes. Cette opération est appelée « transfert ». A noter que ce terme est utilisé même lorsqu'il ne s'agit que de l'envoi de copies. Les motifs d'un transfert comprennent :

- la conservation définitive des documents pour des raisons légales, administratives ou de recherche ;
- le recours à des prestataires externes pour la conservation à moyen et long terme.

Cette opération consiste souvent à transférer les documents archivés vers un environnement d'archivage différent. Parfois, les documents seront détruits dans le SAE après le transfert ; d'autres fois, ils y seront conservés.

Dans d'autres cas, les documents archivés devront être exportés, c'est-à-dire déplacés ailleurs sous forme de copie tout en restant dans le système. Dans d'autres cas encore, il sera nécessaire de détruire les documents.

En tout état de cause, il est indispensable de contrôler l'exécution du transfert, de l'export ou de la destruction. Dans tous les cas, les métadonnées et les historiques des événements doivent être pris en compte en même temps que les documents auxquels ils se rapportent.

A noter que dans ce contexte, « destruction » est différent de « suppression ». La suppression des documents archivés est traitée à la section 9.3.

Réf. Exigence

- 5.3.1 Le SAE doit fournir un processus rigoureux de transfert des documents vers un autre système ou un tiers.
- 5.3.2 Pour tout transfert d'une série, d'un dossier ou d'un sous-dossier du SAE, le transfert doit inclure :
- (pour les séries) tous les dossiers de la série ;
 - (pour les dossiers) tous les sous-dossiers qui en découlent hiérarchiquement ;
 - tous les documents de tous ces dossiers et sous-dossiers ;
 - toutes les métadonnées associées à ces dossiers, documents et sous-dossiers.

Réf. Exigence

- 5.3.3 Le SAE doit pouvoir transférer ou exporter un dossier ou une série en une séquence d'opérations, de telle sorte que :
- le contenu et la structure de ses documents électroniques ne soient pas altérés ;
 - toutes les composantes d'un document électronique (quand le document possède plusieurs composantes) soient exportées comme une unité solidaire, par exemple un message électronique avec ses pièces attachées ;
 - tous les liens entre le document et ses métadonnées soient préservés ;
 - tous les liens entre documents, sous-dossiers et dossiers soient préservés.
- 5.3.4 Lors d'un transfert ou d'un export de documents archivés, le SAE doit pouvoir inclure une copie de l'historique relatif aux documents, sous-dossiers et dossiers transférés.
- 5.3.5 Le SAE devrait fournir un outil de conversion pour la restitution des documents à transférer ou à exporter dans un ou des format(s) validé(s).
Par exemple, un format PDF (portable document format) ou équivalent, et un format XML (extensible mark-up language).
- 5.3.6 Le SAE doit produire un rapport détaillé de toutes les anomalies de transfert, d'export ou de destruction. Le rapport doit identifier tous les documents à transférer qui ont généré des erreurs de traitement, et tous les dossiers ou documents dont le transfert, l'export ou la destruction a échoué.
- 5.3.7 Le SAE doit conserver tous les dossiers électroniques transférés au minimum jusqu'à la confirmation du succès de l'opération.
Il s'agit là d'une mesure de sauvegarde, pour s'assurer que les documents ne sont pas détruits avant l'annonce de la réussite du transfert par le destinataire.
- 5.3.8 Le SAE devrait pouvoir exporter une série entière du plan de classement en une seule séquence d'opération garantissant que :
- la localisation respective de chaque dossier dans le plan de classement est maintenue, de sorte que la structure des dossiers puisse être reconstruite ;
 - toutes les métadonnées, depuis le sommet du plan de classement, sont prises en compte et exportées avec la série.
- 5.3.9 En cas de transfert, export ou suppression de dossiers mixtes, le SAE devrait demander à l'administrateur de confirmer que la partie papier correspondante a bien été transférée, exportée ou détruite avant le transfert, l'export ou la destruction de la partie électronique.
- 5.3.10 Le SAE devrait fournir la possibilité d'ajouter aux dossiers sélectionnés pour le transfert des métadonnées définies par l'utilisateur et nécessaires à la gestion des archives.

Réf. Exigence

5.3.11 Le SAE devrait fournir la possibilité de trier les dossiers électroniques sélectionnés pour le transfert en fonction de métadonnées choisies par les utilisateurs.

5.3.12 Le SAE devrait fournir la possibilité de créer des formulaires personnalisés pour décrire les dossiers électroniques à exporter ou à transférer.

5.3.13 Le SAE devrait permettre la destruction intégrale de séries et de dossiers individuels conservés sur des supports réinscriptibles, par un effacement complet et irréversible, de sorte qu'aucun système de restauration de données ne puisse les récupérer.

Dans certains cas, ceci peut nécessiter plusieurs réécritures des données selon des normes particulières.

Lorsqu'un certificat de destruction est requis, il peut être nécessaire de prendre en considération l'existence de copies de sauvegarde. Cette question dépasse le cadre de ces spécifications.

5.3.14 Si les documents sont stockés sur des supports non-réinscriptibles, le SAE doit pouvoir empêcher d'y accéder afin qu'ils ne puissent être restaurés via l'utilisation normale du système ou par des fonctionnalités courantes du système d'exploitation.

Ceci suppose normalement la destruction des données d'index (sur support réinscriptible) qui comportent les localisations des données sur support non réinscriptible.

Lorsqu'un certificat de destruction est requis, il peut être nécessaire de prendre en considération l'existence de copies de sauvegarde. Cette question dépasse le cadre de ces spécifications.

5.3.15 Le SAE doit donner la possibilité de conserver les métadonnées des dossiers et documents détruits ou transférés.

Dans certains cas, il est souhaitable de conserver des informations précises sur les documents détruits. Il peut s'agir aussi d'une simple identification des documents détruits ou transférés ; ce point est détaillé en 5.3.16.

5.3.16 Le SAE doit permettre à l'administrateur de définir un sous-ensemble de métadonnées à conserver pour tous les dossiers détruits, transférés ou déplacés hors-ligne.

Ceci est souhaitable pour qu'on puisse toujours savoir quels documents ont été détenus et les dates de leur destruction ou de leur sort final, sans nécessairement être tenu de conserver le détail des métadonnées des dossiers.

5.3.17 Le SAE doit permettre de transférer ou exporter les documents plusieurs fois.

6 LA CAPTURE DES DOCUMENTS

Terminologie

Le terme « capture » est utilisé pour désigner l'ensemble des opérations d'enregistrement d'un document, de rattachement de ce document à un niveau du plan de classement, d'ajout de métadonnées complémentaires et de stockage dans le SAE.

Dans le contexte d'un SAE, l'enregistrement et les autres opérations peuvent être séparées ou regroupées.

Des définitions de ces termes figurent dans le Glossaire en 13.1.

Généralités

Ce chapitre expose les exigences relatives aux modalités d'entrée des documents dans un SAE. La première section (6.1) concerne l'opération de capture standard. La section suivante (6.2) concerne l'importation par lots de documents d'autres systèmes. La section (6.3) aborde quelques types de documents particuliers et, en raison de l'accroissement de la messagerie électronique, une section particulière(6.4) est consacrée aux e-mails.

6.1 La capture

Cette section présente les exigences pour le processus de capture.

Les documents électroniques créés ou reçus dans l'exercice des activités sont produits aussi bien en interne qu'à l'extérieur. Les documents électroniques peuvent être de formats variés, produits par des auteurs différents et peuvent être reçus comme de simples pièces ou sous forme de dossiers. Ils peuvent arriver via divers canaux de communication, c'est-à-dire le réseau local (LAN), un réseau étendu, la messagerie, le fax, le courrier postal (avec scan), à des fréquences et avec des volumes variables. La capture des documents requiert un système souple doté de contrôles pertinents de sorte que les diverses exigences soient respectées.

Réf. Exigence

- 6.1.1 Le processus de capture du SAE doit posséder les fonctionnalités suivantes :
- enregistrer et gérer tous types de documents quelles que soient la méthode d'encodage ou les caractéristiques techniques en général ;
 - s'assurer que les documents archivés sont reliés au plan de classement et rattachés à un ou plusieurs dossiers ;
 - prendre en compte l'application qui a produit le document ;
 - contrôler et valider la saisie des métadonnées dans le SAE.

Réf. Exigence

- 6.1.2 Le SAE doit être capable d'intégrer dans son environnement électronique :
- le contenu du document électronique archivé, y compris une description de sa forme et de sa présentation, mais aussi de sa structure et de son organisation, garantes de son intégrité archivistique (par exemple, tous les éléments d'un message électronique avec ses pièces jointes, ou d'une page web avec ses liens) ;
 - des informations sur le document électronique en question, par exemple le nom du fichier ;
 - la date de création et autres métadonnées sur les composantes du document ;
 - des informations sur le contexte de production, de création et de validation, par exemple la procédure à l'origine du document, la provenance, l'auteur (les auteurs) ;
 - des informations sur l'application qui a produit le document, y compris sa version.

Les informations sur la présentation sont parfois implicites dans l'extension du nom de fichier, par exemple « .doc » ou « .pdf ». Ceci peut suffire dans de nombreux cas mais peut se révéler insuffisant en cas de conservation à long terme, ou si des précisions du type « espace couleur » sont nécessaires.

- 6.1.3 Le SAE doit permettre la capture de toutes les métadonnées définies lors de la configuration des systèmes, et veiller à ce qu'elles ne soient jamais dissociées du document électronique qu'elles complètent.

- 6.1.4 Le SAE doit garantir que le contenu des métadonnées sélectionnées pour un document électronique ne peut être modifié que par les utilisateurs autorisés ou les administrateurs.

- 6.1.5 Le SAE devrait comporter la possibilité d'affecter le même document électronique à plusieurs dossiers, à partir d'un seul fichier physique, sans dupliquer le document électronique.

Par exemple, une facture peut être classée dans un dossier « fournisseur » par un utilisateur et dans un dossier « produit » par un autre utilisateur. Autre exemple, on peut vouloir classer un document qui traite de deux sujets dans deux dossiers distincts.

Ceci se fait normalement par l'utilisation de pointeurs.

Réf. Exigence

- 6.1.6 Le SAE doit comporter une fonction d'assistance à l'enregistrement des documents électroniques, par l'extraction automatique des métadonnées, pour au minimum les types de documents suivants :
- les documents bureautiques (courriers en traitement de texte normalisés par exemple) ;
 - les messages électroniques sans pièces jointes, entrant ou sortant ;
 - les messages électroniques avec pièces jointes, entrant ou sortant ;
 - les fax, entrant ou sortant.
- 6.1.7 Le SAE doit conserver la date et l'heure de l'enregistrement comme des métadonnées.
- Si la date et l'heure font partie de l'identifiant unique, dès lors qu'on peut les en extraire facilement, il n'est pas nécessaire de les conserver séparément.*
- L'exactitude de l'heure dépend de l'application.*
- 6.1.8 Le SAE doit garantir que tout document enregistré a une fiche d'enregistrement comportant les métadonnées définies lors de la configuration.
- Certaines métadonnées peuvent préexister ou peuvent être extraites automatiquement du document. Le SAE doit réclamer la saisie des métadonnées manquantes.*
- 6.1.9 Le SAE doit permettre la saisie d'autres métadonnées descriptives ou autres :
- lors de l'enregistrement ;
- et/ou :
- à une étape ultérieure du traitement.
- 6.1.10 Lorsqu'un document possède plusieurs versions, le SAE doit permettre aux utilisateurs de choisir au moins une des actions suivantes :
- archiver toutes les versions du document comme une seule entité ;
 - archiver une seule version du document ;
 - archiver chaque version séparément.

Réf. Exigence

- 6.1.11 Le SAE devrait fournir un module d'aide au classement des documents dans les dossiers électroniques grâce à quelques unes ou à la totalité des actions suivantes :
- afficher seulement la partie du plan de classement accessible à l'utilisateur ou à son profil ;
 - conserver la liste des dossiers les plus récemment utilisés par chaque utilisateur ou profil ;
 - proposer les dossiers les plus récemment utilisés par cet utilisateur ;
 - proposer des dossiers comportant des documents liés ;
 - proposer des dossiers repérés à partir des métadonnées du document, par exemple, les mots importants du titre ;
 - proposer des dossiers repérés à partir du contenu du document.
- 6.1.12 Le SAE devrait permettre à un utilisateur de transmettre les documents électroniques à archiver à un autre utilisateur pour compléter le processus de capture.
- 6.1.13 Pour les documents électroniques composites, le SAE doit :
- traiter le document comme une entité unique indivisible, en préservant la relation entre les composantes ;
 - préserver l'intégrité archivistique du document ;
 - comporter des fonctions de recherche, d'affichage et de gestion globale du document archivé ;
 - appliquer le sort final à toutes les composantes du document électronique comme à une entité unique (c'est-à-dire en une seule opération).

Exemples de documents composites : les pages web comportant des graphiques.

Réf. Exigence

6.1.14 Le SAE doit fournir un module d'assistance à l'enregistrement des documents électroniques par l'extraction automatique d'un maximum de métadonnées, pour le plus grand nombre de documents possibles.

La motivation de cette exigence est de réduire le nombre de données saisies par les utilisateurs et d'accroître ainsi l'exactitude des métadonnées. Les métadonnées concernées et les types de documents pour lesquels cela est possible dépendent de l'environnement. Par exemple, pour un service qui produit des documents textes non structurés ou semi-structurés, il serait raisonnable d'inclure :

- *les courriers en traitement de texte, les notes et autres documents utilisant des modèles, validés par l'entreprise ou l'organisme et permettant une identification automatique des métadonnées ;*
- *les messages électroniques avec ou sans pièces jointes, entrant et sortant ;*
- *les fax sortant.*

6.1.15 Le SAE doit émettre une alerte si un utilisateur tente d'enregistrer un document déjà enregistré dans le même dossier.

6.2 Import par lots

Les documents peuvent être archivés par lots de plusieurs façons. Par exemple, en provenance d'un autre SAE, tel qu'un dossier électronique constitué d'un ensemble de documents de même type (par ex. : les factures journalières) ou un transfert massif d'un système de GED. Le SAE doit pouvoir les accepter et gérer le processus de capture.

Réf. Exigence

6.2.1 Le SAE doit offrir la possibilité de capturer les documents transactionnels produits par d'autres systèmes. Ceci impose de :

- accepter les imports de fichiers séquentiels prédéfinis ;
- fournir des règles pour personnaliser l'enregistrement automatique des documents ;
- conserver la validation de l'intégrité des données.

6.2.2 Le SAE doit fournir la possibilité de gérer des files d'attente.

6.2.3 Le SAE devrait pouvoir créer plusieurs files d'attentes pour les différents types de documents.

Par exemple, dans des environnements différents, on peut avoir des files d'attentes pour les messages électroniques, le courrier scanné, les documents d'un service, d'un groupe ou d'une personne, les transactions issues d'applications, ou les documents issus d'un système de gestion.

6.3 Types de documents

Généralités

Les entreprises et organismes ont besoin d'archiver des types de documents très variés, de formats et de structures différentes. Les exigences techniques de capture de ces documents varient en fonction de leur complexité. Dans certains cas, il est impossible d'identifier *a priori* tous les types de documents, particulièrement ceux qui proviennent de l'extérieur.

Documents « auto-modifiés »

Il est quelquefois nécessaire de capturer des documents qui semblent être, ou qui sont, « auto-modifiés ». Ceci peut engendrer des exigences complexes qui ne sont étudiées ici que sommairement.

Certains documents semblent se modifier tous seuls, comme si leur contenu changeait sans intervention d'un utilisateur. Il est courant, par exemple, que des documents de traitement de texte ou de tableur contiennent un champ ou un code qui affiche automatiquement la date du jour. La restitution (voir Glossaire section 13.1) du document varie selon la date de la consultation. Dans des cas extrêmes, le champ ou le code peuvent varier au point de changer notablement l'apparence du document (par exemple un code qui affiche le chemin d'accès complet des documents : parfois, les modifications du chemin d'accès, dues à un nom très long dans une hiérarchie importante, peuvent provoquer des changements importants dans la pagination). Toutefois, le document n'a pas réellement changé ; seule sa présentation est modifiée, et cela dépend du logiciel de visualisation. Les documents d'apparence « auto-modifiée » ne remettent pas en cause l'exigence de fixation du contenu mais ils peuvent donner l'impression de le faire et il vaut donc mieux les éviter.

D'autres fois, les documents peuvent contenir un code qui modifie réellement le document, ainsi un tableau modifié par une macro sophistiquée (via un logiciel de visualisation) et sauvegardé automatiquement. Dans ce cas, il y a un risque que le document se modifie pendant le processus de capture, selon le degré de précision du processus ou les contrôles du SAE. Il est clair que c'est inacceptable.

Dans la plupart des cas, les documents « auto-modifiés » de ce type devraient être évités, stockés dans un format qui neutralise le code gênant, ou encore consultés uniquement via un logiciel qui ne déclenche pas de modification. Si le code en question constitue un élément important du document, une réponse appropriée sera donnée au cas par cas.

Pour les documents imprimables, les formats qui neutralisent les codes « auto-modifiés » sont notamment les formats propriétaires PDF de Adobe, et ENVOY de Tumbleweed. Dans ce cas, il est important de s'assurer que la conversion au format désiré ne s'accompagne pas d'une modification automatique et non souhaitée des

documents ; par exemple, pour une lettre à la date « auto-modifiée », la conversion devrait prendre en compte la date visible sur la lettre.

Lorsque l'archivage de documents « auto-modifiés », réellement ou en apparence, est inévitable, ces caractéristiques devraient être mentionnées et conservées comme métadonnées du document.

Réf. Exigence

6.3.1 Le SAE doit pouvoir capturer et archiver des documents électroniques de formats et de structures très variés.

La liste de ces formats et structures devrait être précisée avant l'utilisation de ces spécifications par un système.

6.3.2 Le SAE doit pouvoir capturer les documents bureautiques les plus courants, qu'il s'agisse de documents simples ou complexes. Les types de formats gérés comprennent obligatoirement :

- documents simples : fax, documents bureautiques, présentations, texte, image, messages électroniques (voir section 6.4), voix ;
- documents composites : message électronique avec pièces jointes, éditique, pages web, graphiques.

La liste des types de documents que doit accepter le SAE varie d'une entreprise à l'autre.

6.3.3 La liste des formats gérés (6.3.2) sera complétée au fur et à mesure de l'apparition de nouveaux formats.

6.3.4 Le SAE devrait pouvoir capturer les types de documents suivants :

- agendas électroniques ;
- données provenant d'autres applications informatiques, par ex. Comptabilité, Paie, DAO ;
- documents papiers numérisés ;
- dossiers vocaux ;
- vidéo-clips ;
- cartes et schémas numériques ;
- données structurées (par ex. EDI) ;
- bases de données ;
- documents multimédias.

La liste des types de documents que devrait accepter le SAE varie d'une entreprise à l'autre.

6.3.5 Le SAE ne doit imposer aucune limite quant au nombre de documents capturés et archivés dans un dossier, ni quant au nombre de documents stockés dans le SAE.

Réf. Exigence

6.3.6 Le SAE devrait permettre la capture d'un document composite de deux façons :

- soit comme un document unique ;
- soit comme une suite organique de documents simples, chacun constituant un élément du document composite.

6.4 Gestion des messages électroniques

La messagerie électronique est utilisée à la fois pour envoyer de simples messages et des documents (pièces jointes), en interne et à l'extérieur. Les caractéristiques d'un message électronique rendent sa traçabilité et son enregistrement difficiles. Les entreprises et les organismes doivent pouvoir renforcer les contrôles de gestion pour :

- capturer la totalité des messages entrant ou sortant avec leurs pièces jointes ;

et/ou :

- fournir aux utilisateurs la possibilité de capturer une sélection de messages et pièces jointes.

Cette dernière option exige des utilisateurs une évaluation de la pertinence et de l'importance de chaque message et du risque à ne pas les archiver.

Réf. Exigence

6.4.1 Le SAE doit permettre le choix entre un des modes opératoires suivants au moment de la configuration :

- le SAE permet aux utilisateurs de capturer les messages électroniques (après sélection) ;

ou

- le SAE comporte un procédé automatique de capture de tous les messages entrant et sortant.

Réf. Exigence

- 6.4.2 Le SAE devrait permettre aux utilisateurs individuels de procéder à la capture des messages entrant à partir de leur système de messagerie. L'utilisateur devrait pouvoir capturer chaque message de la boîte de réception, au sein du système de messagerie, comme suit :
- voir chaque message avec signalement de pièces jointes (le cas échéant) ;
 - voir les contenus des pièces jointes à l'aide d'un visualiseur multi-formats ;
 - enregistrer le message et ses pièces jointes comme un nouveau document dans le SAE ;
 - relier le message et ses pièces jointes à un document déjà archivé dans le SAE.
- 6.4.3 Le SAE devrait garantir la capture de l'adresse électronique sous une forme compréhensible par l'homme, associant un nom au message original ; par exemple « Jean Durand » plutôt « jdd97@xyz.int ».

7 IDENTIFICATION

Les différentes entités d'un SAE (séries, dossiers, sous-dossiers, documents) exigent des identifiants. Ces identifiants doivent être uniques pour chaque occurrence de chaque entité ; l'unicité doit s'étendre ou bien à tout le SAE, ou bien à un niveau hiérarchique. Dans la mesure où les exigences d'identification sont communes aux séries, dossiers, sous-dossiers et documents, elles sont regroupées ici.

Réf. Exigence

7.1.1 A chaque occurrence nouvelle d'une des entités suivantes, le SAE doit lui attribuer un identifiant unique (comme décrit ci-dessous) :

- série,
- dossier,
- sous-dossier,
- document,
- extrait de document.

7.1.2 Tous les identifiants uniques dans le SAE doivent être :

- unique pour tout le SAE,

ou :

- unique pour la partie de l'arborescence définie à partir du niveau supérieur à celui où se trouve l'entité en cause.

A titre d'exemple de la seconde option, le libellé

Contrats : nom de la société : correspondance

est unique, mais son segment final peut figurer dans d'autres libellés, par exemple :

Plan de développement régional : consultation publique : correspondance

7.1.3 Le SAE doit pouvoir stocker les identifiants uniques comme des métadonnées des entités correspondantes.

7.1.4 Le SAE devrait permettre de préciser le format de l'identifiant unique au moment de la configuration.

L'identifiant peut être numérique ou alphanumérique, ou peut inclure la concaténation des identifiants des sous-dossiers et dossiers électroniques supérieurs au document dans le plan de classement.

Réf. Exigence

7.1.5 Le SAE doit :

- générer l'identifiant unique automatiquement et empêcher l'utilisateur de saisir l'identifiant unique manuellement, et par conséquent de le modifier (par exemple un nombre séquentiel) ;

ou :

- permettre aux utilisateurs de saisir l'identifiant unique mais en validant son unicité avant acceptation (par exemple, un numéro de compte).

Une alternative est de générer l'identifiant unique automatiquement, en le masquant à l'utilisateur et en lui permettant de saisir une chaîne de caractères non unique (par ex. un nom) comme identifiant. L'utilisateur utiliserait cette chaîne comme identifiant mais le SAE le considérerait comme une métadonnée définie par l'utilisateur.

7.1.6 Lors de la création d'une nouvelle série ou d'un nouveau dossier électronique dans le plan de classement avec une identification à structure numérique basée sur une séquence de nombres, le SAE devrait générer automatiquement le numéro immédiatement disponible au sein du plan de classement.

Par exemple, si une série du plan de classement contient déjà les dossiers :

900 - 23 - 01 Fabrication : commandes : validation des bons de commandes

900 - 23 - 02 Fabrication : commandes : facturation

900 - 23 - 03 Fabrication : commandes : traitement des notes de crédit

Alors, si l'administrateur ajoute un nouveau dossier à la série, le SAE devrait automatiquement lui attribuer l'identifiant 900 - 23 - 04.

Pareillement, si l'administrateur ajoute une nouvelle série à la série « Fabrication », le SAE devrait automatiquement lui attribuer l'identifiant 900 - 24.

7.1.7 Quand un SAE génère automatiquement des identifiants uniques, il devrait permettre à l'administrateur de préciser au moment de la configuration les nombres initiaux (0, 00, 100, etc.) et les modes d'incrémementation (1, 10, etc.).

8 RECHERCHE, REPÉRAGE ET RESTITUTION

La possibilité pour l'utilisateur de retrouver les dossiers et les documents fait partie intégrante d'un SAE, y compris la recherche des documents en l'absence d'indications précises et leur restitution. La restitution consiste à produire une représentation à l'écran (affichage) ou imprimée ; il peut aussi s'agir de produire du son ou de la vidéo (voir le Glossaire section 13.1).

L'accès aux dossiers et aux documents, puis leur visualisation exigent toute une série de fonctions de recherche, localisation et restitution afin de répondre aux besoins des différents types d'utilisateurs. Bien qu'on puisse considérer qu'il ne s'agit pas là d'une fonction classique du records management, les fonctionnalités requises sont décrites ici en partant du principe qu'un SAE sans possibilités de recherche est d'un intérêt limité.

Ce chapitre énumère les exigences pour la recherche et la localisation à la section 8.1. Les exigences liées à la restitution sont divisées en trois sections : exigences pour l'affichage (section 8.2), impression (section 8.3) et restitution des documents archivés non imprimables (section 8.4).

Sécurité

Toutes les caractéristiques et les fonctionnalités de ce chapitre sont concernées par les contrôles d'accès décrits plus haut, y compris les contrôles de sécurité. En d'autres termes, le SAE ne doit jamais fournir une information à un utilisateur non autorisé à la recevoir. Pour éviter la complexité, ce point est énoncé ici et n'est pas répété pour chaque exigence.

8.1 Recherche et repérage

La recherche est le processus d'identification des documents et dossiers au travers de paramètres prédéfinis afin de vérifier l'existence des documents, des dossiers et/ou de leurs métadonnées, de les localiser, d'y accéder et de les consulter.

Les outils de recherche et de navigation du SAE pour localiser métadonnées, documents, sous-dossiers et dossiers exigent un ensemble de techniques de recherche pour les utilisateurs expérimentés et une aide pour les utilisateurs occasionnels moins familiers de l'informatique.

Réf. Exigence

- 8.1.1 Le SAE doit fournir un ensemble souple de fonctions visant les métadonnées à chaque niveau d'agrégation de documents (dossier, série) ainsi que les contenus au travers des paramètres définis par les utilisateurs, afin de localiser, retrouver et consulter les documents et/ou les métadonnées, individuellement ou en groupe.

Réf. Exigence

8.1.2 Les moyens de recherche du SAE devraient être intégrés et se présenter de la même façon à l'utilisateur à tous les niveaux du plan de classement.

Autrement dit, l'interface, ses caractéristiques et ses options devraient être les mêmes pour l'utilisateur, qu'il recherche une série, un dossier ou un document.

8.1.3 Concernant les dossiers, le SAE devrait offrir les mêmes fonctionnalités de recherche pour les dossiers électroniques, mixtes (voir 10.1) et papier.

8.1.4 Le SAE doit permettre la recherche de toute métadonnée de document, de sous-dossier ou de dossier.

8.1.5 Le SAE doit permettre la recherche textuelle dans les contenus des documents.

8.1.6 Le SAE doit permettre à l'utilisateur de créer une requête simple en combinant les métadonnées et/ou le contenu des documents.

8.1.7 Le SAE doit permettre à l'administrateur de configurer et de modifier les champs de recherche, notamment :

- de définir n'importe quelle métadonnée de document, sous-dossier ou dossier, voire le contenu global du document comme champ d'interrogation ;
- de changer la configuration des champs d'interrogation.

8.1.8 Le SAE doit fournir des outils de recherche incluant les techniques suivantes :

- recherche en texte intégral combinant les métadonnées des documents et des dossiers avec les contenus ;
- les recherches booléennes de métadonnées.

8.1.9 Le SAE devrait intégrer de façon cohérente la recherche en texte intégral et sur les métadonnées.

8.1.10 Le SAE devrait permettre la recherche des concepts à travers un thésaurus intégré tel qu'un index en ligne.

Ceci permettrait la recherche de documents à l'aide d'un terme générique, spécifique ou associé du contenu ou des métadonnées. Par exemple, une recherche « service ophtalmologique » pourrait donner « services de santé », « soins oculaires » ou « ophtalmologie ».

8.1.11 Le SAE doit permettre la recherche approximative de métadonnées à l'aide d'abréviations et de troncatures.

*Par exemple, la recherche "proj" donnera « projet » ou le nom « PROJA » ; les lettres « C*n » retrouveront « Commission ».*

8.1.12 Le SAE devrait permettre la recherche de proximité qui peut exiger la présence d'un mot à une certaine distance d'un autre dans le document recherché pour valider la réponse.

Réf. Exigence

8.1.13 En cas d'utilisation d'interface graphique, le SAE doit fournir un navigateur qui offre des techniques de navigation graphique ou autre tant au niveau de la série que du dossier.

Ceci sera utilisé avec les techniques de recherche décrites ci-dessus pour présenter un premier niveau de métadonnées pour un groupe de documents ou de dossiers répondant aux critères de recherche indiqués.

8.1.14 Le SAE doit permettre la recherche au sein d'un dossier électronique (à n'importe quel niveau du plan de classement) et dans la masse des dossiers.

8.1.15 Le SAE doit être capable de rechercher et de retrouver un dossier ou un sous-dossier complet, avec son contenu et ses métadonnées contextuelles, et de restituer toutes les données de ce dossier, et elles seules, comme un ensemble discret, résultat d'une seule requête.

Ceci est nécessaire, par exemple, quant un utilisateur souhaite imprimer la totalité d'un dossier pour l'emporter en réunion, ou simplement comme document de travail papier.

8.1.16 Le SAE doit pouvoir rechercher, retrouver et restituer un dossier électronique au travers de tous types de nommage implémentés, notamment :

- nom de fichier ;
- identifiant de fichier (code de classement).

8.1.17 Le SAE doit afficher à l'écran le nombre total des réponses à la requête d'un utilisateur et permettre à l'utilisateur soit d'afficher la liste des résultats, soit de préciser ses critères de recherche et de lancer une autre requête.

8.1.18 Le SAE doit permettre de sélectionner les documents, dossiers, etc. dans la liste des résultats puis de les ouvrir (avec contrôle d'accès) par un simple clic.

8.1.19 Le SAE devrait permettre de rechercher les métadonnées de n'importe quel objet (document, sous-dossier, dossier ou série) à l'aide des techniques présentées dans ce chapitre, que l'objet soit électronique ou non, et qu'il soit stocké en ligne, near-line ou hors ligne.

8.1.20 Le SAE devrait permettre aux utilisateurs de sauvegarder leurs requêtes et de les réutiliser.

8.1.21 Le SAE devrait permettre aux utilisateurs d'affiner leurs recherches.

Un utilisateur devrait par exemple pouvoir partir des résultats d'une recherche pour lancer une nouvelle recherche sur cette base.

8.1.22 Le SAE devrait permettre d'utiliser dans les requêtes des expressions telles que « la semaine dernière », « ce mois-ci », etc.

Ceci est en contradiction avec la recommandation d'indiquer le temps avec des dates extrêmes ou des nombres de jours.

Réf. Exigence

8.1.23 Le SAE doit permettre aux utilisateurs de retrouver les dossiers et les documents directement par l'identifiant unique.

Si l'identifiant unique n'est pas accessible à l'utilisateur (voir note en 7.1.5), ceci est sans objet.

8.1.24 Le SAE devrait comporter plusieurs formats d'affichage des résultats paramétrables par les utilisateurs ou les administrateurs, avec des fonctions du type :

- sélection de l'ordre de présentation des résultats ;
- indication du nombre de réponses affichées sur chaque page d'écran ;
- fixation d'un nombre maximum de réponses pour une recherche ;
- sauvegarde des résultats ;
- choix des métadonnées à afficher dans la liste des résultats.

8.1.25 Le SAE devrait proposer un classement pertinent des résultats de recherche.

8.1.26 Le SAE devrait pouvoir relier un « extrait » de document électronique (voir section 9.3) au document d'origine, de sorte que le repérage de l'un permette d'accéder à l'autre, tout en gérant séparément leurs métadonnées respectives ainsi que les contrôles d'accès.

8.1.27 En consultant ou étudiant un document ou une agrégation de documents (dossier, série), à la suite d'une requête ou non, un utilisateur devrait pouvoir utiliser les fonctions du SAE pour trouver facilement des informations sur le niveau de documents immédiatement supérieur, sans avoir à quitter ou fermer le document.

Par exemple, en lisant un document, on devrait pouvoir savoir de quel sous-dossier ou dossier il relève ; en regardant les métadonnées d'un dossier, on devrait pouvoir trouver des informations sur la série où il est classé.

8.1.28 Aucune fonction de recherche et de repérage du SAE ne doit révéler à un utilisateur quelque information que ce soit (métadonnée ou contenu) que les contrôles d'accès et de sécurité (sections 4.1 et 4.6) sont censés lui cacher.

8.1.29 Le SAE devrait inclure la possibilité de gérer les restrictions d'accès aux documents visés par la propriété intellectuelle, et de produire les données correspondantes.

Ce court énoncé comprend un vaste ensemble de fonctionnalités qui dépassent le cadre de ces spécifications. L'exigence peut être satisfaite en créant la possibilité d'un lien vers une autre application.

8.2 Restitution : affichage des documents

Un SAE peut contenir des documents de différents formats et structures. L'utilisateur a besoin de disposer d'un visualiseur générique qui permette l'affichage, la restitution et l'impression de divers formats.

Réf. Exigence

- 8.2.1 Le SAE doit restituer les documents qui forment le résultat d'une recherche.
Si le SAE stocke les documents dans un format propriétaire, on peut accepter d'effectuer la restitution en utilisant une application extérieure au SAE.
- 8.2.2 Le SAE devrait restituer les documents qui forment le résultat d'une recherche sans chargement du logiciel associé.
Une solution courante est d'intégrer au SAE un progiciel de visualisation. Cela est souvent souhaitable pour accélérer la vitesse de restitution.
- 8.2.3 Le SAE devrait pouvoir restituer tous les types de documents électroniques définis par l'entreprise d'une façon qui respecte le contenu informatif des documents (caractéristiques de présentation et de mise en page du progiciel d'origine, etc.), et qui restitue ensemble toutes les composantes du document électronique.
L'entreprise doit définir les progiciels et formats dont elle a besoin.

8.3 Restitution : impression

Cette section concerne les documents imprimables, et l'information de contrôle dans le SAE.

Le SAE doit fournir des facilités d'impression pour permettre aux utilisateurs d'obtenir des copies imprimées des documents et de leurs métadonnées ou d'autres informations. Dans tous les cas, « impression » doit s'entendre à un niveau applicatif, avec tous les contrôles et caractéristiques d'usage (tels que rapports multi-pages, en-têtes, utilisation d'une imprimante correctement configurée). L'envoi brut d'une image d'écran à une imprimante n'est en général pas suffisant pour répondre à cette exigence.

Réf. Exigence

- 8.3.1 Le SAE doit fournir à l'utilisateur diverses facilités d'impression des documents et de leurs métadonnées, y compris la possibilité d'imprimer un ou des documents dont les métadonnées seront définies par l'utilisateur.
- 8.3.2 Le SAE doit permettre d'imprimer les métadonnées d'un dossier.
- 8.3.3 Le SAE doit permettre d'imprimer tous les documents d'un dossier, dans un ordre défini par l'utilisateur, en une seule opération.

Réf. Exigence

- 8.3.4 Le SAE doit permettre à l'utilisateur d'imprimer le sommaire de sa sélection de documents (le contenu d'un dossier par exemple), consistant en une liste de métadonnées définie par lui (intitulé, auteur, date de création, etc.) pour chaque document.
- 8.3.5 Le SAE devrait permettre à l'administrateur de préciser que toutes les impressions ou documents sont dotés de métadonnées spécifiques, par exemple : intitulé, numéro d'enregistrement, date, indice de sécurité.
- 8.3.6 Le SAE doit permettre à l'utilisateur d'imprimer la liste des réponses à sa recherche.
- 8.3.7 Le SAE doit permettre à l'administrateur d'imprimer une partie ou la totalité des paramètres de gestion.
- 8.3.8 Le SAE doit permettre à l'administrateur d'imprimer les tableaux de conservation.
- 8.3.9 Le SAE doit permettre à l'administrateur d'imprimer le thésaurus.
- 8.3.10 Le SAE doit permettre à l'administrateur d'imprimer le plan de classement.
- 8.3.11 Le SAE doit permettre à l'administrateur d'imprimer le répertoire des fichiers (si besoin ; voir 3.2.10).
- 8.3.12 Le SAE doit permettre à l'administrateur d'imprimer l'historique des événements (voir 4.2).
- 8.3.13 Le SAE doit pouvoir imprimer tous les types de documents électroniques définis par l'entreprise. L'impression doit :
- respecter la mise en page du progiciel d'origine ;
 - inclure toutes les composantes (imprimables) du document électronique.
- L'entreprise doit définir les progiciels et formats dont elle a besoin.*

8.4 Restitution : autres cas

Cette section ne concerne que les documents non imprimables.

Réf. Exigence

- 8.4.1 Le SAE doit comporter des fonctions d'exportation vers les supports appropriés des documents non imprimables.
- Par exemple : le son, la vidéo, des sites web, etc.*

9 FONCTIONS D'ADMINISTRATION

Les évolutions organisationnelles sont normales et doivent être prises en compte dans les fonctions de maintenance du système. Un SAE doit aussi procurer à l'administrateur les moyens de gérer des événements tels que le changement du nombre d'utilisateurs, l'accroissement de la demande en capacité de stockage, la restauration en cas de défaillance du système et la surveillance des erreurs système.

Certaines de ces fonctions peuvent être fournies par un système de GED ou de gestion de bases de données associé.

Les exigences de ce chapitre concernent d'abord l'administration générale (section 9.1), puis le système de reporting (section 9.2) et la rédaction des documents (section 9.3).

9.1 Administration générale

Cette section concerne les exigences de gestion des paramètres du système, la sauvegarde et la restauration, l'administration du système et des utilisateurs.

Réf. Exigence

9.1.1 Le SAE doit permettre aux administrateurs, de manière fiable et sans effort particulier, de retrouver, d'afficher et de reconfigurer les paramètres du système et les choix faits au moment de la configuration – par exemple les éléments à indexer – et de redéfinir les profils d'utilisateurs.

9.1.2 Le SAE doit comporter une fonction de sauvegarde, et les moyens de reconstituer les données à l'aide des restaurations et de l'historique des événements, tout en maintenant l'intégrité du système.

Autrement dit, le SAE doit permettre de revenir à un état antérieur de la base (documents et métadonnées), grâce à la combinaison des restaurations et des historiques.

9.1.3 Le SAE doit comporter des fonctions de restauration et de récupération des données en cas de défaillance du système ou d'erreur de mise à jour, et doit notifier les résultats aux administrateurs.

Autrement dit, le SAE doit permettre aux administrateurs d'annuler une série de transactions jusqu'à un état de la base dont l'intégrité est garantie. Ceci est uniquement nécessaire en cas d'erreur.

9.1.4 Le SAE doit surveiller l'espace de stockage disponible et alerter les administrateurs quand l'espace disponible atteint un seuil critique ou que la situation exige une intervention.

Réf. Exigence

9.1.5 Le SAE devrait surveiller les taux d'erreur sur les supports de stockage, et signaler à l'administrateur tout support ou dispositif pour lequel le taux d'erreur est supérieur à ce qui a été défini lors de la configuration.

Ceci s'applique en particulier aux supports optiques.

9.1.6 Le SAE doit permettre aux administrateurs d'apporter des « modifications globales » au plan de classement, tout en garantissant une gestion permanente, correcte et complète, de toutes les métadonnées et des historiques, afin de gérer les changements organisationnels suivants :

- unité organisationnelle scindée en deux ;
- deux unités organisationnelles regroupées en une seule ;
- réorganisation ou nouvelle dénomination d'une unité ;
- scission de l'entreprise ou de l'organisme en deux structures.

Dans ce genre de situation, les dossiers clos doivent rester clos et conserver leur identification par rapport au plan de classement antérieur ; les dossiers ouverts doivent :

- ou bien, être fermés et conserver leur référencement dans le plan de classement antérieur, assortie d'une concordance avec le nouveau dossier ;
- ou bien, être référencés selon le nouveau plan de classement, mais en conservant toutes les références antérieures.

Les changements organisationnels décrits ci-dessus peuvent entraîner des modifications dans les plans de classements des unités concernées et chez les utilisateurs.

L'expression « modification globale » implique que toutes les séries, dossiers et documents concernés peuvent être traités avec un minimum d'opérations plutôt que de devoir procéder individuellement.

9.1.7 Le SAE doit pouvoir gérer les mouvements d'utilisateurs entre les unités organisationnelles.

9.1.8 Le SAE doit permettre la définition de profils d'utilisateurs, plusieurs utilisateurs pouvant être affectés à chaque profil.

Voir aussi 4.1.3.

9.2 Reporting et statistiques

Cette section ne donne qu'un aperçu de la question ; il n'est pas pertinent de reproduire ici les exigences d'un sous-système complet de reporting. Dans toute implémentation, l'importance et la complexité des rapports dépendront de la taille, de la complexité et de l'importance des modifications apportées au plan de classement, du volume et de la nature des documents et des utilisateurs.

Réf. Exigence

- 9.2.1 Le SAE doit fournir à l'administrateur des outils de reporting souples. Ils viseront au minimum :
- le nombre de dossiers, sous-dossiers et documents ;
 - les statistiques de consultation pour les dossiers, sous-dossiers et documents ;
 - un rapport d'activité par utilisateur.
- 9.2.2 Le SAE doit permettre aux administrateurs de faire des requêtes et de produire des états statistiques à partir de l'historique des événements. Ces états viseront au minimum :
- les séries,
 - les dossiers,
 - les sous-dossiers,
 - les documents,
 - les utilisateurs,
 - les durées.
- 9.2.3 Le SAE devrait permettre aux administrateurs de faire des requêtes et de produire des états statistiques à partir de l'historique des événements pour :
- les indices de sécurité,
 - les profils utilisateurs,
 - diverses métadonnées.
- 9.2.4 Le SAE doit pouvoir produire la liste des dossiers et sous-dossiers, structurée selon le plan de classement, pour une partie ou la totalité du plan de classement.
- 9.2.5 Le SAE devrait comporter des fonctions de tri et de sélection des données statistiques.
- 9.2.6 Le SAE devrait comporter des fonctions de compilation et de résumé des données statistiques.
- 9.2.7 Le SAE devrait permettre aux administrateurs de disposer de rapports statistiques à dates régulières ou à la demande.
- 9.2.8 Le SAE devrait permettre aux administrateurs de restreindre les droits d'accès aux statistiques.

9.3 Modification, suppression et édition d'extrait des documents archivés

Le fait que les documents archivés ne doivent pas être modifiés est un principe de base. Normalement, les dossiers et les documents ne peuvent donc pas être supprimés (sauf à la fin de leur cycle de vie dans le SAE). Toutefois, il peut y avoir

des exceptions, par exemple, par suite d'une erreur d'utilisateur. C'est l'objet de cette section.

Les administrateurs peuvent avoir besoin de « supprimer » des documents pour corriger les erreurs d'utilisateurs (documents attribués au mauvais dossier, etc.) ou en application de la législation sur la protection des données. L'action de suppression peut signifier deux choses :

- la destruction (voir 5.3.13 et 5.3.15) ;
- la conservation définitive, avec ajout d'une métadonnée spécifiant que le document est considéré comme soustrait au contrôle du records management.

Cette possibilité de suppression doit être étroitement contrôlée afin de protéger l'intégrité générale des archives. Les données relatives aux suppressions devront notamment être stockées dans l'historique des événements, et une trace du document supprimé doit rester dans le dossier.

Par ailleurs, les administrateurs ont parfois besoin de publier, ou de rendre accessibles, des documents comportant des informations encore sensibles, à cause de la protection des données, de considérations liées à la sécurité, du risque commercial, etc. Les administrateurs doivent donc pouvoir retirer l'information sensible sans altérer le document en cause. Ce procédé est appelé ici « édition d'extrait » ; le SAE conserve à la fois le document original et la copie éditée, dénommée « extrait ». A noter que le besoin de créer des extraits varie d'un pays à l'autre selon les traditions.

A noter que la suppression et la modification sont également traitées au chapitre 5.

Réf. Exigence

- 9.3.1 Le SAE doit interdire, par défaut ou via une fonction optionnelle, qu'un document, une fois archivé, puisse être supprimé ou déplacé par un administrateur ou un utilisateur. Ceci signifie que l'administrateur ne peut considérer qu'un document est « supprimé » (voir 9.3.7) ou « reclassé » (voir 3.4.1) s'il n'a pas été noté comme tel ; et dans le cas d'un reclassement, une copie ou un pointeur est placé à la nouvelle adresse.

Cette exigence ne concerne pas le transfert ou la destruction des documents en application du tableau de conservation, comme exposé en section 5.3.

- 9.3.2 Le SAE devrait permettre, lors de la configuration, une option alternative au point 9.3.1, assimilant la « suppression » d'un document à sa destruction.

- 9.3.3 L'administrateur doit pouvoir modifier l'indice de sécurité de tout document.

Cette fonction vise à réduire le niveau de protection des documents dont le caractère sensible décroît avec le temps.

Réf. Exigence

9.3.4 L'administrateur doit pouvoir modifier l'indice de sécurité de tous les documents d'un dossier ou d'une série en une seule opération ; le SAE doit générer une alerte si des documents voient baisser leur indice de sécurité et attendre confirmation avant d'achever l'opération.

Cette fonction vise à réduire le niveau de protection des documents dont le caractère sensible décroît avec le temps.

9.3.5 En lien avec les exigences 12.4.10 et 4.6.2, l'administrateur doit pouvoir modifier l'indice de sécurité des dossiers.

9.3.6 Le SAE doit enregistrer le détail de toute modification d'indice de sécurité dans les métadonnées du document, du sous-dossier ou du dossier concerné.

9.3.7 L'administrateur doit être autorisé à supprimer des séries, dossiers, sous-dossiers et documents (en fonction de l'option choisie en 9.3.1). Toutefois, pour toute suppression de ce type, le SAE doit :

- enregistrer le détail de la suppression dans l'historique des événements ;
- émettre un rapport exceptionnel pour l'administrateur ;
- supprimer complètement le contenu d'un dossier ou d'un sous-dossier supprimé ;
- s'assurer qu'aucune suppression n'a pour conséquence de modifier un autre document (par exemple, si une pièce appartient à deux dossiers– voir 6.1.5 – dont l'un seulement doit être supprimé) ;
- signaler à l'administrateur tout lien entre un dossier ou un sous-dossier à supprimer et un autre dossier ou document ; demander confirmation avant l'achever l'opération ;
- maintenir en permanence l'intégrité des métadonnées (particulièrement au regard des exigences 12.4.20 et 12.7.24).

Cette fonctionnalité ne vise que des cas exceptionnels.

9.3.8 L'administrateur doit pouvoir modifier les métadonnées définies par les utilisateurs. Ces modifications doivent être tracées dans l'historique des événements.

Cette fonctionnalité vise à permettre aux administrateurs de corriger les erreurs de saisies des utilisateurs et à gérer les accès.

9.3.9 Le SAE doit permettre à l'administrateur de faire une copie d'un document, dans un but d'édition d'extrait.

Cette copie est dénommée ici « extrait » du document.

Réf. Exigence

9.3.10 Le SAE devrait comporter une fonctionnalité pour retirer ou masquer l'information sensible dans un extrait, permettant au minimum :

- le retrait d'une ou plusieurs pages d'un document ;
- l'ajout de rectangles opaques pour masquer les noms ou mots sensibles ;
- toute fonction correspondante pour les formats vidéo et audio, le cas échéant.

Si le SAE ne fournit pas directement ces fonctionnalités, il doit permettre de le faire faire par un autre logiciel.

Il est essentiel que, en cas d'utilisation de ces fonctions d'édition d'extrait, aucune des informations retirées ou masquées ne puisse être vue dans l'extrait, sur l'écran ou le papier, ou lors de l'audition, y compris en recourant à des fonctions du type rotation, zoom ou autre manipulation.

9.3.11 Quand un extrait est créé, le SAE doit enregistrer sa création parmi les métadonnées, au minimum la date, l'heure, le motif de l'extrait et l'auteur.

9.3.12 Le SAE devrait inviter l'auteur d'un extrait à l'attribuer à un dossier.

9.3.13 Le SAE devrait conserver un double renvoi (voir 11.1.18) entre l'extrait et le dossier ou sous-dossier du document d'origine, même si ce sous-dossier est clos.

9.3.14 Le SAE doit conserver dans l'historique des événements toute modification effectuée en réponse aux exigences de cette section.

10 AUTRES FONCTIONS

Ce chapitre traite des exigences relatives aux fonctions connexes de l'archivage électronique et du records management. Elles concernent la gestion des archives physiques via le SAE, la gestion électronique de documents (GED), le workflow, la signature électronique et d'autres processus d'authentification.

A noter que ces spécifications n'abordent pas le problème de la conservation physique des archives qui peut exister ou non, selon l'environnement législatif et réglementaire en cause ; s'il existe, il faut prendre des mesures pour préserver l'intégrité et l'exploitabilité des documents électroniques et physiques comme un tout. Ces questions devraient être traitées par des directives organisationnelles spécifiques.

Dans tous les cas, le niveau de ces exigences est assez élevé mais, dans la mesure où elles ne constituent pas des fonctions essentielles de l'archivage, elles ne sont pas détaillées ici.

Les différentes sections de ce chapitre énumèrent les exigences relatives à :

- la gestion et l'archivage des documents non électroniques (section 10.1) ;
- la conservation et le sort final des dossiers mixtes (section 10.2) ;
- la GED (section 10.3) ;
- le workflow (section 10.4) ;
- les signatures électroniques (section 10.5) ;
- le chiffrement (section 10.6) ;
- les filigranes électroniques, etc. (section 10.7) ;
- l'interopérabilité et l'ouverture (section 10.8).

10.1 Gestion et archivage des documents non électroniques

Le centre d'archivage d'une entreprise ou d'un organisme peut stocker également des documents papier ou sur d'autres supports tels que des vidéos, des cassettes audio, appelés « dossiers physiques ». Le SAE doit pouvoir enregistrer les dossiers physiques dans le même plan de classement que les documents électroniques, et permettre la gestion des dossiers mixtes (physiques et électroniques).

Réf. Exigence

- 10.1.1 Le SAE doit être en mesure d'intégrer les sous-dossiers et les dossiers physiques dans le plan de classement ; il doit signaler la présence de documents physiques dans ces dossiers et les gérer de la même façon que les documents électroniques.
- 10.1.2 Le SAE doit intégrer dans le plan de classement les dossiers qui mêlent, de façon organique, des documents électroniques et des documents physiques, et doit pouvoir gérer les deux types de documents de manière unifiée.
Ces dossiers sont appelés ici « dossiers mixtes ». En réalité, les dossiers mixtes consistent en un dossier électronique et un dossier physique.
- 10.1.3 Le SAE doit permettre d'attribuer à un dossier physique associé à un dossier électronique dans un dossier mixte le même nom de dossier et le même identifiant numérique, en précisant qu'il s'agit d'un dossier mixte.
- 10.1.4 Le SAE doit permettre de définir des métadonnées distinctes pour les dossiers physiques et les dossiers électroniques ; les métadonnées du dossier physique doivent inclure l'indication de localisation du dossier physique (voir 12.5.7).
- 10.1.5 Le SAE devrait gérer la traçabilité des dossiers physiques au travers d'un module de contrôle des entrées, sorties et communications qui donne en permanence la localisation du dossier.
- 10.1.6 Le SAE doit garantir que le repérage d'un dossier mixte signale conjointement les métadonnées des documents électroniques et celles des documents papier associés.
- 10.1.7 Quand les dossiers possèdent un indice de sécurité (voir 4.6), le SAE devrait garantir que la partie physique d'un dossier mixte a reçu le même indice de sécurité que la partie électronique du même dossier.
- 10.1.8 Le SAE doit inclure un module de contrôle de l'accès aux dossiers physiques, basé notamment sur les indices de sécurité, comparable à ce qui a été défini pour les dossiers électroniques (voir chapitre 4).
- 10.1.9 Le SAE devrait permettre l'impression et la reconnaissance de codes barre, ou comporter un autre système pour automatiser la traçabilité des mouvements physiques des dossiers.

10.2 Conservation et sort final des dossiers mixtes**Réf. Exigence**

- 10.2.1 Le SAE doit pouvoir gérer l'attribution de durées de conservation à tous les dossiers physiques relevant du plan de classement. Les durées doivent être cohérentes avec les durées de conservation des dossiers électroniques ; le système doit signaler à l'administrateur les durées échues, mais en tenant compte des processus différents de destruction ou d'archivage historique des documents papier et des documents électroniques.

Réf. Exigence

- 10.2.2 Le SAE doit permettre d'attribuer les mêmes durées au dossier physique et au dossier électronique qui constituent un dossier mixte.
- 10.2.3 Le SAE doit pouvoir appliquer toute décision de révision sur la partie électronique d'un dossier mixte à la partie physique correspondante.
- 10.2.4 Le SAE doit avertir l'administrateur de l'existence et de la localisation de tout dossier physique associé à un dossier électronique mixte exporté ou transféré.
- 10.2.5 Le SAE doit pouvoir enregistrer dans l'historique des événements tous les changements intervenus sur les métadonnées de dossiers ou documents physiques ou mixtes.
- 10.2.6 Le SAE devrait permettre l'application d'une décision de révision portant sur un groupe de dossiers à tout dossier physique compris dans ce groupe, en indiquant à l'administrateur les actions à effectuer sur les dossiers physiques.
- 10.2.7 Le SAE devrait pouvoir exporter et transférer les métadonnées des dossiers et documents physiques.
- 10.2.8 Le SAE devrait offrir des possibilités de contrôle des mouvements des dossiers physiques gérés dans le système, et en particulier permettre d'enregistrer le nom de l'utilisateur ou le lieu pour lequel un dossier a été sorti et afficher cette information si le dossier physique est demandé par un autre utilisateur.
- 10.2.9 Le SAE devrait pouvoir faciliter la communication des dossiers physiques gérés dans le système, en permettant à un utilisateur de saisir une demande de dossier physique ou une date de réservation, le gestionnaire du dossier ou l'administrateur étant automatiquement informé de l'opération, en fonction de la configuration du système.

Tenir compte des critères de sécurité définis section 4.6.

Tenir compte des critères de sécurité définis section 4.6.

10.3 GED

Les systèmes de gestion électronique de documents – GED – sont largement utilisés pour la gestion et le contrôle des documents électroniques. De nombreuses fonctionnalités de GED se chevauchent avec les systèmes d'archivage. Un système de GED, typiquement, inclut l'indexation des documents, la gestion du stockage, le contrôle des versions, l'intégration des applications bureautiques et des outils de recherche pour accéder aux documents. Certains systèmes d'archivage électronique fournissent des fonctions de GED complètes, d'autres une partie seulement. Inversement, certains systèmes de GED ont incorporé des fonctions caractéristiques du records management et de l'archivage.

Pour clarifier les choses, le tableau ci-dessous met en évidence les différences essentielles entre les deux systèmes :

| Un système de GED... | Un SAE... |
|---|---|
| <ul style="list-style-type: none"> • permet la modification des documents et la production de plusieurs versions ; | <ul style="list-style-type: none"> • interdit la modification des documents ; |
| <ul style="list-style-type: none"> • peut permettre la destruction des documents par leurs auteurs ; | <ul style="list-style-type: none"> • interdit la destruction de documents en dehors d'un contrôle strict ; |
| <ul style="list-style-type: none"> • peut comporter la gestion de durées de conservation ; | <ul style="list-style-type: none"> • comprend obligatoirement un contrôle rigoureux des durées de conservation ; |
| <ul style="list-style-type: none"> • peut comprendre une structure organisée de stockage, sous le contrôle des utilisateurs ; | <ul style="list-style-type: none"> • comprend obligatoirement une structure rigoureuse de classement (le plan de classement), gérée et contrôlée par l'administrateur ; |
| <ul style="list-style-type: none"> • est <i>a priori</i> dédié à la gestion quotidienne des documents pour la conduite des affaires. | <ul style="list-style-type: none"> • peut faciliter les tâches quotidiennes mais est aussi destiné à la constitution d'un fonds sécurisé des documents probants de l'entreprise. |

La suite de cette section expose les exigences clés pour la fourniture d'une solution intégrée de GED et d'archivage électronique. Ces exigences ne s'appliquent que lorsque les fonctionnalités de GED font partie de la solution.

Réf. Exigence

10.3.1 Lorsqu'une GED fait partie du SAE ou y est étroitement associée, le système de GED doit pouvoir capturer automatiquement les documents électroniques produits dans l'exercice des activités et les transmettre au SAE pour enregistrement.

10.3.2 Le SAE doté de fonctionnalités de GED doit pouvoir :

- capturer un document électronique en une seule opération ;
- enregistrer un document électronique et compléter le processus de capture ultérieurement.

10.3.3 Les utilisateurs devraient pouvoir archiver un document depuis la GED ou une application intégrée à la GED.

Cette exigence est particulièrement importante pour les services administratifs. Dans bien des cas, elle peut être considérée comme obligatoire.

10.3.4 L'utilisateur de la GED, ou de l'application intégrée à la GED, doit pouvoir communiquer facilement avec le SAE, afin d'enregistrer et d'archiver les documents à partir de la GED.

Réf. Exigence

10.3.5 Le SAE doté de fonctionnalités de GED doit pouvoir capturer les métadonnées directement à partir des applications de production, et permettre à l'utilisateur d'ajouter des métadonnées supplémentaires.

Par exemple, l'heure de création et le nom de l'auteur, ainsi que les métadonnées repérables à partir des champs structurés du document, le cas échéant, comme la date ou l'objet.

10.3.6 Le SAE doit être capable d'ajouter des interfaces avec de nouvelles applications de GED au fur et à mesure de leur installation.

10.3.7 Le SAE doté de fonctionnalités de GED devrait pouvoir gérer des documents électroniques non encore enregistrés et archivés, avec le même plan de classement et les mêmes mécanismes de contrôle d'accès que les documents archivés.

10.3.8 Lorsqu'une GED fait partie du SAE ou y est étroitement associée, un module de maintenance du plan de classement devrait y être intégrée.

10.3.9 Le SAE doté de fonctionnalités de GED devrait pouvoir gérer les différentes versions d'un document électronique comme des entités distinctes mais reliées entre elles et conserver ce lien.

10.3.10 Le système de GED devrait pouvoir restreindre l'accès des utilisateurs :

- à la dernière version d'un document ;
- à toutes ou une partie des versions d'un document ;
- aux versions qui ont été capturées ou enregistrées et archivées ;

le choix étant opéré au moment de la configuration.

10.3.11 Le SAE doté de fonctionnalités de GED devrait pouvoir s'interfacer avec d'autres logiciels, notamment des systèmes de traitement et de numérisation, ou des systèmes de workflow, tout en gardant le contrôle des documents électroniques archivés.

10.3.12 Le SAE doit être capable de copier le contenu d'un document archivé pour créer un nouveau document électronique distinct, tout en garantissant la conservation du document original.

Par exemple, un utilisateur peut recopier un document pour l'envoyer à un destinataire non utilisateur du SAE. Cette copie peut être déclarée comme nouveau document du SAE ou non, selon le contexte.

10.4 Workflow

La Workflow Management Coalition (WfMC) – une association internationale pour le développement des normes de workflow et la compatibilité des différents systèmes de workflow – définit le workflow comme « l'automatisation de tout ou d'une partie d'un processus de travail, au cours duquel les documents,

l'information ou les tâches sont transmises d'un participant à l'autre, pour action, en application des procédures préétablies ». Dans cette définition, un « participant » peut être un utilisateur ou un groupe (c'est-à-dire une équipe), ou encore une application informatique.

Les exigences qui suivent ne s'appliquent que lorsque le SAE inclut un workflow. Elles couvrent les fonctions de base ainsi que des fonctionnalités plus élaborées de workflow qui peuvent être fournies par l'intégration d'une solution de workflow au SAE.

La technologie de workflow fait passer les objets électroniques entre les participants grâce à un programme de contrôle automatique. Dans le contexte d'un SAE, le workflow est utilisé pour faire circuler les documents archivés entre les utilisateurs et les services. Il sert normalement à :

- la gestion des processus ou des tâches essentielles telles que l'enregistrement et les procédures d'élimination des dossiers ou documents ;
- la vérification et l'approbation des documents avant leur enregistrement ;
- l'acheminement contrôlé des documents ou dossiers d'un utilisateur à l'autre pour des actions de vérification du document, approbation de nouvelle version, etc. ;
- la notification aux utilisateurs de mise à disposition des documents ;
- la diffusion des documents ;
- la mise en ligne des archives sur le web.

Les possibilités d'un système de workflow varient du simple routage (vérification et approbation des documents avant enregistrement) jusqu'au traitement d'un grand nombre d'opérations, avec traitement des exceptions, états statistiques sur le système et l'activité de chacun.

Réf. Exigence

- 10.4.1 La fonction workflow du SAE doit mettre en œuvre une circulation par étape, chaque étape consistant (par exemple) dans le mouvement d'un document ou d'un dossier d'un participant vers un autre pour une action précise.
- 10.4.2 Le SAE ne devrait pas limiter en principe le nombre des étapes de chaque workflow.
- 10.4.3 La fonction workflow du SAE doit permettre d'alerter un utilisateur participant qu'un dossier ou document lui a été adressé sur son poste de travail en vue d'une action spécifique.

Réf. Exigence

- 10.4.4 La fonction workflow du SAE doit permettre à un utilisateur de signaler des documents à l'attention d'autres utilisateurs à l'aide de la messagerie électronique.
Ceci implique l'intégration d'un système de messagerie existant plutôt que le recours à un système indépendant ou propriétaire.
- 10.4.5 La fonction workflow du SAE doit permettre à l'administrateur de définir et de gérer des workflows pré-programmés.
- 10.4.6 La fonction workflow du SAE doit empêcher la modification des workflows pré-programmés par d'autres que l'administrateur ou des utilisateurs dûment autorisés par lui.
- 10.4.7 L'administrateur devrait pouvoir autoriser certaines personnes à ré-attribuer des tâches ou des actions à un autre utilisateur ou groupe.
Un utilisateur peut souhaiter envoyer un dossier ou un document à un autre en raison du contenu du document ou parce que l'utilisateur en titre est absent.
- 10.4.8 La fonction workflow du SAE doit enregistrer dans l'historique des événements toutes les modifications apportées aux workflows pré-programmés.
- 10.4.9 La fonction workflow du SAE doit tracer l'avancement d'un document ou d'un dossier dans le workflow afin que les utilisateurs puissent connaître son statut dans le processus en cours.
- 10.4.10 Le SAE ne devrait pas limiter en principe le nombre des workflows dans le système.
- 10.4.11 La fonction workflow du SAE devrait gérer les dossiers et documents sous forme de listes que l'administrateur puisse consulter et contrôler.
- 10.4.12 La fonction workflow du SAE devrait permettre aux participants de voir la liste des documents qui leur ont été adressés et d'y sélectionner les documents à traiter.
- 10.4.13 La fonction workflow d'un SAE devrait permettre de conditionner le workflow aux instructions d'un utilisateur ou aux données du système.
Il s'agit des flux qui acheminent les documents ou les dossiers à l'un des participants sur la base d'une décision de l'un d'eux. Par exemple, un flux peut acheminer un document soit à un contrôleur financier soit à un service de consolidation des achats, selon les instructions du chef des ventes ; ou encore, le flux peut dépendre de la valeur de l'achat, calculée par le système.
- 10.4.14 La fonction workflow du SAE devrait fournir une possibilité de rappel ou de retour des documents et dossiers.
- 10.4.15 La fonction workflow du SAE devrait permettre aux utilisateurs d'interrompre (de suspendre) temporairement un flux pour se consacrer à une autre tâche.

Réf. Exigence

- 10.4.16 La fonction workflow du SAE doit accepter comme « participants » aussi bien des individus que des groupes.
- 10.4.17 Lorsque le participant est un groupe, la fonction workflow du SAE devrait permettre de faire tourner les documents entre les membres du groupe, ou de tenir compte de l'achèvement des tâches courantes par tel ou tel afin d'équilibrer la charge de travail des membres de l'équipe.
- 10.4.18 La fonction workflow du SAE devrait permettre de prioriser les tâches en attente.
- 10.4.19 La fonction workflow du SAE devrait permettre de gérer des « rendez-vous ».
Ceci exige de suspendre le workflow en attendant l'arrivée d'un document électronique requis ; à son arrivée, le processus reprend automatiquement.
- 10.4.20 La fonction workflow du SAE devrait pouvoir associer une date limite à chaque étape individuelle ou à chaque processus, et signaler les tâches pour lesquelles l'échéance est dépassée.
- 10.4.21 La fonction workflow du SAE devrait permettre qu'un workflow soit déclenché automatiquement par la réception d'un document électronique.
- 10.4.22 La fonction workflow du SAE doit fournir des fonctions complètes de reporting afin de gérer les volumes en cause, la performance et les exceptions.

10.5 Signature électronique

La signature électronique (parfois appelée signature numérique) est une séquence de caractères qui, en liaison avec des algorithmes sophistiqués et sécurisés et des clés (un long train de bits analogue à un mot de passe), peut être utilisée pour attester de l'intégrité d'un document, ou pour authentifier l'identité de son expéditeur. Un des algorithmes de signature électronique les plus largement reconnus est MD5.

L'adoption très large, par les entreprises et les organismes, de la messagerie électronique et du web a accru le nombre de documents échangés en interne et plus encore en externe, dans des environnements qui ne sont pas toujours contrôlés. L'utilisation de la signature électronique pour authentifier et assurer l'intégrité est en passe d'être généralisée.

Les exigences ci-après ne s'appliquent que lorsqu'il y a besoin de gérer des documents signés électroniquement. A ce jour, la signature électronique utilise des technologies émergentes sujettes au changement et à l'incertitude. Les utilisateurs de ces spécifications devront valider ces exigences et leurs implications pour la conservation à long terme auprès des experts du domaine.

- | Réf. | Exigence |
|-------------|--|
| 10.5.1 | Le SAE doit pouvoir conserver les informations concernant les signatures électroniques, le chiffrement et les agences de vérification. |
| 10.5.2 | Le SAE devrait avoir une structure permettant d'introduire facilement différentes technologies de signature électronique. <i>Ce point doit être souligné étant donné les changements en cours dans ce domaine.</i> |
| 10.5.3 | Le SAE devrait pouvoir vérifier la validité d'une signature électronique. |
| 10.5.4 | Le SAE doit pouvoir conserver comme métadonnées les éléments descriptifs du processus de vérification d'une signature électronique, notamment : <ul style="list-style-type: none">• le fait que la validité de la signature a été vérifiée ;• l'autorité de certification qui a validé la signature ;• la date et l'heure de la vérification. |
| 10.5.5 | Le SAE devrait être capable de vérifier la validité d'une signature électronique au moment de la capture du document. |
| 10.5.6 | Le SAE devrait inclure la possibilité de préserver l'intégrité des documents signés électroniquement (et de prouver qu'elle a été préservée), même si un administrateur a modifié certaines métadonnées du document (à l'exception du contenu) après la signature. <i>La manière de procéder sur ce point n'est pas prédéterminée.</i> |
| 10.5.7 | Le SAE devrait pouvoir stocker avec un document électronique : <ul style="list-style-type: none">• la (les) signature(s) électronique(s) associée(s) à ce document ;• le(s) certificat(s) électronique(s) attestant cette signature ;• tout contresign appposé par une autorité de certification de façon à ce qu'il puisse être retrouvé en même temps que le document et sans préjudice pour l'intégrité de la clé privée. |

10.6 Chiffrement

Le chiffrement est un processus qui consiste en une transformation complexe d'un objet électronique de telle sorte qu'aucune application ne puisse le rendre lisible ou intelligible sans application du processus inverse de déchiffrement. Ce processus sert à sécuriser les objets électroniques, par une transformation qui exige l'utilisation de codes électroniques sécurisés.

Les exigences ci-après ne s'appliquent que lorsqu'il y a besoin de gérer des documents chiffrés.

Réf. Exigence

- 10.6.1 Lors de l'expédition ou de la réception d'un document électronique chiffré par une application interfacée avec le SAE, le SAE doit pouvoir en restreindre l'accès aux seuls utilisateurs identifiés comme détenteurs de la clé de déchiffrement correspondante, en sus des autres contrôles d'accès attribués à ce document.
- 10.6.2 Lors de la transmission d'un document électronique chiffré par une application interfacée avec le SAE, le SAE devrait pouvoir conserver comme métadonnées de ce document :
- le fait même d'une transmission chiffrée ;
 - le type d'algorithme ;
 - le niveau de chiffrement.
- 10.6.3 Le SAE devrait pouvoir assurer la capture de documents chiffrés directement à partir d'une application qui possède une fonction de chiffrement, et d'en restreindre l'accès aux utilisateurs identifiés comme détenteurs de la clé de déchiffrement correspondante.
- 10.6.4 Le SAE devrait permettre de supprimer le chiffrement lors de l'import ou de la capture du document.
- Cette fonction peut être souhaitable dans les grands centres d'archives qui ont une exigence d'accès sur le long terme (dans la mesure où le chiffrement est susceptible de réduire la possibilité de lire le document sur le long terme). Dans ce cas, on s'appuiera sur l'historique des événements ou d'autres annotations pour prouver l'existence du chiffrement puis du déchiffrement. Dans d'autres cas, les contraintes réglementaires peuvent s'opposer à cette fonction.*
- Voir les détails sur les transferts et les imports en 5.3.*
- 10.6.5 Le SAE devrait avoir une structure permettant d'introduire facilement différentes technologies de chiffrement.

10.7 Filigranes numériques, etc.

Les filigranes numériques servent à marquer une image électronique d'une information de provenance ou de propriété. Ils superposent à l'image bitmap un motif complexe, visible ou non, qui ne peut être supprimé que par le biais d'un algorithme et d'une clé sécurisée. Des technologies analogues peuvent être utilisées pour la numérisation des sons et des images animées. Les filigranes servent notamment à protéger la propriété intellectuelle.

Les exigences de cette section ne s'appliquent que lorsqu'il y a besoin de gérer des documents comportant un filigrane électronique ou la marque d'une technologie similaire.

Réf. Exigence

- 10.7.1 Le SAE doit pouvoir stocker des documents comportant un filigrane numérique ainsi que les informations sur ce filigrane.
- 10.7.2 Le SAE devrait permettre de retrouver l'information figurant dans les filigranes numériques.
- 10.7.3 Le SAE devrait avoir une structure permettant d'introduire facilement différentes technologies de tatouage.

10.8 Interopérabilité et ouverture

Les exigences ci-après concernent plus particulièrement les environnements qui nécessitent la communication entre plusieurs SAE, par exemple dans les grands groupes ou l'administration gouvernementale.

Réf. Exigence

- 10.8.1 Le SAE devrait pouvoir interopérer avec d'autres systèmes d'archivage électroniques.
- 10.8.2 Le SAE devrait pouvoir mettre à jour d'autres systèmes d'entreprise.
- 10.8.3 Le SAE devrait pouvoir interopérer avec d'autres applications.
La nature de l'interopérabilité devra être précisée pour chaque application.
- 10.8.4 Le SAE devrait pouvoir traiter en temps réel les transactions générées par des systèmes applicatifs externes.

11 EXIGENCES NON FONCTIONNELLES

Le succès d'un système ne repose pas que sur ses fonctionnalités. En effet, un certain nombre d'exigences non fonctionnelles y contribue. Bien que les exigences non fonctionnelles soient souvent difficiles à définir et à mesurer objectivement, il vaut toutefois la peine de les identifier afin de pouvoir les prendre en considération, au moins à un niveau général. Du reste, elles sont souvent communes à plusieurs types de systèmes informatiques.

En outre, les utilisateurs de ces spécifications devront articuler leurs besoins avec les normes techniques et organisationnelles en vigueur et les services d'assistance du fournisseur du SAE, notamment la documentation, la formation et le conseil.

Les entreprises devront ajouter leurs propres exigences dans ces domaines, en fonction de leur taille et de leur organisation, des caractéristiques physiques et de l'environnement technique en place. Cette section tente d'énumérer les points à examiner par les utilisateurs pour compléter les exigences génériques exposées dans les chapitres précédents.

Certains exemples d'exigences utilisent des crochets pour indiquer que l'utilisateur des spécifications doit entrer une valeur ou une information spécifique. Par exemple,

<xx minutes/heures>

signifie que l'utilisateur des spécifications devrait saisir une durée, sans doute en minutes et en heures, pour compléter cette exigence. De même,

<4 secondes>

signifie que l'utilisateur des spécifications devrait préciser un intervalle de temps ; les 4 secondes sont proposées à titre d'exemple.

Les sections de ce chapitre étudient les domaines suivants :

- facilité d'utilisation (section 11.1) ;
- performance et évolutivité (section 11.2) ;
- disponibilité du système (section 11.3) ;
- normes techniques (section 11.4) ;
- environnement législatif et réglementaire (section 11.5) ;
- externalisation et recours à des tiers (section 11.6) ;
- conservation à long terme et obsolescence technologique (section 11.7).

11.1 Facilité d'utilisation

La facilité d'utilisation est particulièrement importante. La mise en œuvre d'un SAE que les utilisateurs jugeraient difficile à manipuler risquerait d'échouer.

Les utilisateurs de ces spécifications doivent tenir compte de la facilité d'utilisation dans la définition d'un SAE : quel niveau de facilité requis et comment le définir. Cela dépendra des types d'utilisateurs ciblés et de l'importance de la formation. Des exemples sont donnés ci-dessous.

Réf. Type d'exigence

- 11.1.1 Le SAE doit comporter une aide en ligne à tous les niveaux.
- 11.1.2 L'aide en ligne du SAE devrait être contextuelle.
- 11.1.3 Tous les messages d'erreur émis par le SAE doivent être explicites, de sorte que, le cas échéant, les utilisateurs puissent apporter la correction voulue.
Dans l'idéal, chaque message d'erreur sera accompagné d'un texte explicatif avec la liste des actions propres à résoudre la difficulté.
- 11.1.4 Le SAE doit utiliser un seul jeu de règles pour l'interface utilisateur, ou un nombre limité de jeux. Les règles doivent être cohérentes avec le système d'exploitation du SAE.
Les règles devraient être cohérentes avec les principales applications existantes.
- 11.1.5 Le SAE doit pouvoir afficher plusieurs documents en même temps (sauf exigence contraire suite au point 11.1.4).
- 11.1.6 Lorsque le SAE utilise des fenêtres, elles devraient pouvoir être configurées par l'utilisateur (sauf exigence contraire suite au point 11.1.4).
- 11.1.7 L'interface utilisateur du SAE doit satisfaire aux besoins particuliers des utilisateurs, c'est-à-dire être compatible avec des logiciels spécialisés qui utilisent des interfaces spécifiques.
Les guides suivants, utiles dans ce contexte, sont indiqués dans l'Annexe 7 chapitre 3 :
- *SPRITE-S² initiative ACCENT – Guide pour l'acquisition des TIC ;*
 - *W3C Guide d'accès au contenu Web ;*
 - *Microsoft : Guide officiel pour des développeurs et des concepteurs d'interface utilisateur.*
- 11.1.8 Le SAE doit fournir des fonctions faciles et intuitives pour l'utilisateur final et l'administrateur (telles que peut les définir un panel représentatif d'utilisateurs).
- 11.1.9 Lorsque que le SAE utilise des fenêtres, il doit permettre aux utilisateurs de les déplacer, de les re-dimensionner, de modifier leur apparence, et de sauvegarder ces modifications dans le profil utilisateur.

Réf. Type d'exigence

- 11.1.10 Le SAE devrait permettre aux utilisateurs de choisir des alertes sonores (son et volume), et de sauvegarder ces modifications dans le profil utilisateur.
- 11.1.11 Le SAE doit permettre la saisie de valeurs par défaut selon les besoins. Ces valeurs par défaut seraient notamment :
- valeurs définies par l'utilisateur ;
 - valeurs identiques à l'enregistrement précédent ;
 - valeurs empruntées au contexte : date, référence du dossier, identifiant de l'utilisateur, etc. ;
- selon le cas.
- 11.1.12 Les opérations les plus courantes du SAE doivent être conçues de telle sorte qu'elles puissent être exécutées à l'aide d'un petit nombre de gestes (clics de souris par exemple).
- 11.1.13 Le SAE devrait être étroitement intégré au système de messagerie de l'entreprise pour permettre aux utilisateurs d'envoyer des dossiers et des documents électroniquement sans quitter le SAE.
- 11.1.14 Dans le cas où le point 11.1.13 est acquis, le SAE devrait, lors de l'envoi d'un dossier ou d'un document à un autre utilisateur du SAE, envoyer des pointeurs vers les documents plutôt que des copies.
- Il peut y avoir des exceptions, par exemple pour un utilisateur éloigné qui n'a pas accès à la base centrale.*
- 11.1.15 Lorsque le SAE utilise une interface graphique, il doit permettre aux utilisateurs de la personnaliser. Les modifications concernent notamment, mais non exclusivement :
- le contenu des menus,
 - la mise en page des écrans,
 - l'utilisation des touches de fonction,
 - les couleurs, polices et taille des caractères,
 - les alertes sonores.
- 11.1.16 Le SAE devrait comporter des fonctions programmables par l'utilisateur.
- Par exemple, des macros créées par l'utilisateur ; mais attention aux documents auto-modifiés (voir la section 6.3).*
- 11.1.17 Lorsque les utilisateurs doivent saisir des métadonnées pour des documents numérisés, le SAE devrait permettre le recours à la reconnaissance optique de caractères pour capturer les métadonnées à partir de certaines zones de l'image.

Réf. Type d'exigence

- 11.1.18 Le SAE devrait permettre aux utilisateurs de créer des liens croisés entre les documents, au sein d'un même dossier et entre dossiers différents, afin de faciliter la navigation entre les documents.
- 11.1.19 Le SAE devrait comporter une aide sur l'utilisation du plan de classement.

11.2 Performance et extensibilité

Les utilisateurs de ces spécifications devraient évaluer dans quelle mesure le SAE fournit des temps de réponse rapides (en ligne par rapport aux attentes des utilisateurs) et peut répondre aux différentes tailles de populations d'utilisateurs qu'il est censé desservir. Certaines remarques et exemples figurent ci-dessous

Les temps de réponse pour les utilisateurs dépendront de facteurs extérieurs au SAE, par exemple :

- bande passante du réseau ;
- utilisation du réseau ;
- configuration et utilisation des ressources des différents serveurs.

Ces spécifications ne peuvent pas traiter des facteurs externes mais simplement rappeler qu'ils ne peuvent être ignorés. Normalement, des tests grandeur nature sont nécessaires pour avoir une vision fiable de la performance.

En conséquence, les exigences ci-dessous devraient être interprétées avec une définition-type des temps de réponse. Cette définition-type peut varier d'un environnement à l'autre, selon le type d'infrastructure. Par exemple, si le SAE est défini pour une infrastructure existante, il peut être opportun de définir les temps de réponse comme le laps de temps entre la réception d'une requête par le serveur et l'envoi de la réponse. Inversement, si les spécifications concernent un système clé en main incluant serveurs et réseau, il peut être opportun de définir les temps de réponse comme le laps de temps entre la saisie de la requête et l'affichage de la réponse sur le poste de travail.

Les utilisateurs de ces spécifications pourront aussi se reporter utilement à la directive européenne 90/270/CEE sur les équipements comportant des écrans de visualisation qui traite des performances logicielles.

Réf. Type d'exigence

- 11.2.1 Le SAE doit fournir des temps de réponse appropriés pour toutes les fonctions courantes exécutées dans des conditions normales, par exemple :
- 75% de la population prévue pour le système connectée et active ;
 - 100% du volume de documents prévus gérés par le système ;
 - des utilisateurs effectuant différents types de transaction à des débits variés ;
- avec une performance d'au moins dix transactions simultanées.
- 11.2.2 Le SAE doit pouvoir exécuter une simple recherche dans les <3 secondes> et une recherche complexe (combinant quatre termes) dans les <10 secondes>, quelle que soit la capacité de stockage ou le nombre des dossiers et documents.
- Dans ce contexte, l'exécution d'une recherche s'entend comme la fourniture d'une liste de résultats. Elle n'inclut pas l'accès aux documents eux-mêmes.*
- 11.2.3 Le SAE doit pouvoir retrouver et afficher dans les <4 secondes> la première page d'un document qui a été consulté au cours des <xx> mois précédents, quelle que soit la capacité de stockage ou le nombre des dossiers et documents.
- Cette exigence vise à permettre une recherche rapide des documents les plus utilisés, étant entendu que la fréquence d'utilisation est en général liée à une utilisation récente. L'entreprise ou l'organisme précisera les délais à partir desquels on estime que la fréquence de consultation des documents décroît.*
- 11.2.4 Le SAE doit pouvoir retrouver et afficher dans les <20 secondes> la première page d'un document qui n'a pas été consulté au cours des <xx> mois précédents, quelle que soit la capacité de stockage ou le nombre des dossiers et documents.
- Cette exigence concerne les cas d'utilisation d'une forme de stockage hiérarchique, où les documents plus rarement consultés sont stockés sur des supports de performance moindre que les documents plus vivants. L'entreprise ou l'organisme précisera les délais à partir desquels on estime que la fréquence de consultation des documents décroît.*
- 11.2.5 Le SAE doit permettre une implémentation unique du système avec une capacité de stockage électronique d'au moins <xx gigaoctets/téraoctets> ou <xx milliers/millions> de documents, desservant au moins <xx centaines/milliers> d'utilisateurs simultanés.
- Les fourchettes de documents et d'utilisateurs sont à préciser par l'entreprise ou l'organisme.*
- 11.2.6 Il doit être possible d'étendre le SAE, d'une manière contrôlée, jusqu'à au moins <xx centaines/milliers> d'utilisateurs, sans rupture de continuité du service.

Réf. Type d'exigence

11.2.7 Le SAE doit permettre ce qui précède, avec un programme de maintenance pour :

- les données sur les utilisateurs et les groupes ;
- les profils d'accès ;
- les plans de classement ;
- les bases de données ;
- les tableaux de conservation ;

en vue de changements organisationnels, sans imposer un surcroît d'administration du système (voir aussi chapitre 9).

Dans les cas où les exigences de performance sont strictes, il peut être nécessaire de quantifier les niveaux de changement.

11.2.8 Le SAE doit être extensible et ne doit comporter aucune caractéristique qui interdirait son usage dans de petites ou grandes entreprises, avec des entités de tailles différentes et en nombre variable.

11.3 Disponibilité du système

Dans de nombreux cas, l'utilisation conjointe d'un SAE et d'une GED modifiera l'utilisation du système d'information. Un des changements majeurs est l'accroissement radical de la dépendance des utilisateurs envers le réseau informatique, dans la mesure où, si le SAE / la GED ne fonctionne pas, ils peuvent être dans l'incapacité de continuer leur travail. Par conséquent, les utilisateurs de ces spécifications à la recherche d'un système devraient s'efforcer d'identifier les exigences de disponibilité et les spécifier dans le cahier des charges. Des exemples sont donnés ci-dessous.

Réf. Type d'exigence

11.3.1 Le SAE doit être accessible aux utilisateurs :

- de <xx :00> à <xx :00> ;
- <toutes les semaines/xxx jours par an>.

Réf. Type d'exigence

11.3.2 Les temps d'arrêt planifiés du SAE ne doivent pas excéder <xx> heures par <trimestre glissant>.

La définition des pannes peut dépendre de l'infrastructure et de l'architecture. Par exemple, dans certains environnements, une défaillance causée par un serveur sera considérée comme une défaillance du SAE ; dans d'autres cas, la défaillance de l'ordinateur central sera analysée différemment et ne sera pas imputable au SAE. Il convient de s'accorder sur une définition ; comme base de travail, on peut proposer : « Le SAE est dit en panne lorsque des utilisateurs sont dans l'incapacité d'exécuter les fonctions courantes du SAE si cette panne est imputable à une composante du SAE autre que le poste de travail.

11.3.3 Les temps d'arrêt non planifiés du SAE ne doivent pas excéder <xx heures/minutes> par <trimestre glissant>.

11.3.4 Le nombre d'incidents liés à des arrêts non planifiés du SAE ne doit pas excéder <xx> par <trimestre glissant>.

11.3.5 En cas de défaillance logicielle ou matérielle, il doit être possible de restaurer un état précédent du SAE (ne pas remonter au-delà de la sauvegarde de la veille) dans les <xx> heures suivant la restauration du matériel.

11.4 Normes techniques

Le SAE devrait être conforme aux normes de droit et de fait du domaine. Lorsque c'est possible, il est souhaitable que le SAE utilise des spécifications et des formats ouverts plutôt que propriétaires.

Les utilisateurs de ces spécifications devront préciser les exigences pour les normes concernant :

- l'environnement matériel (plates-formes, postes de travail, etc.) ;
- l'environnement du système d'exploitation (Microsoft Windows – NT4, 98, 2000 – MacOS, Unix) ;
- les normes industrielles pour les interfaces utilisateur (Microsoft Windows, Macintosh, X-Windows, navigateur intranet) ;
- les bases de données relationnelles (ODBC, OLE DB ; les solutions possibles : Oracle, Sybase) ;
- les protocoles réseau et le système d'exploitation (TCP/IP, Ethernet, Novell, Microsoft Windows NT) ;
- les différents formats d'encodage (ASCII, Unicode ISO 10646, ISO 8859, Adobe PDF ou autres spécifications propriétaires équivalentes) ;

- les normes d'échange (XML, HTML, SGML) ;
- l'interface de programmation et les kits de développement (COM, DCOM, CORBA).

Lors de l'utilisation de ces spécifications pour un cahier des charges, il sera nécessaire de préciser l'environnement technique, notamment toutes les interfaces du SAE (système patrimonial, système administratif) ainsi que les prévisions d'évolution.

En outre, les utilisateurs de ces spécifications évalueront leurs exigences à la lumière de leur contexte particulier, dans les domaines suivants :

Réf. Type d'exigence

- 11.4.1 Si le SAE est doté d'un thésaurus monolingue, il devra être conforme à la norme ISO 2788 – Principes directeurs pour l'établissement et le développement de thésaurus monolingues.
- 11.4.2 Si le SAE est doté d'un thésaurus multilingue, il devra être conforme à la norme ISO 5964 – Principes directeurs pour l'établissement et le développement de thésaurus multilingues.
- 11.4.3 Si le SAE comprend la numérisation de documents papier, il convient de respecter les normes suivantes :
- les interfaces de numérisation TWAIN et/ou Isis ;
 - le format image TIFF v6 Groupe IV avec compression des images noir et blanc ;
 - JPEG, PNG, GIF ou tout autre format paramétrable par l'utilisateur supportant les couleurs ou les niveaux de gris.
- Le non respect de ces normes devrait être justifié.*
- 11.4.4 Le SAE doit permettre le stockage de documents dont les formats de fichiers et d'encodage sont soit normalisés, soit complètement documentés.
- 11.4.5 Le SAE devrait respecter les normes d'échange pour la recherche et le repérage de l'information, notamment ISO 23950 – Repérage de l'information – définition et protocole.
- Cette norme est également connue sous le nom de ANSI Z39.50.*
- 11.4.6 Si le SAE utilise une base de données relationnelle, il doit respecter la norme SQL, ISO/IEC 9075 – Technologies de l'information – Langages de base de données – SQL.
- 11.4.7 Le SAE devrait stocker toutes les dates dans un format conforme à ISO 8601 – Éléments de données et formats d'échange – Échange d'information – Représentation de la date et de l'heure.
- 11.4.8 Le SAE devrait stocker tous les noms de pays dans un format conforme à ISO 3166 – Codes pour la représentation des noms de pays.

Réf. Type d'exigence

- 11.4.9 Le SAE devrait comporter tous les noms de langue dans un format conforme à ISO 639 – Codes pour la représentation des noms de langue.
- 11.4.10 Si le SAE doit gérer des documents en plusieurs langues ou utilisant des caractères non latins, il doit pouvoir d'utiliser l'encodage d'ISO 8859-1.
- 11.4.11 Si le SAE doit gérer des documents en plusieurs langues ou utilisant des caractères non latins, il devrait pouvoir d'utiliser l'encodage ISO 10646 (Unicode).

11.5 Environnement législatif et réglementaire

Le SAE doit se conformer à l'environnement législatif et réglementaire qui varie forcément d'un pays à l'autre et selon les domaines d'activité.

A noter que ces spécifications ne traitent pas des besoins de conservation des archives physiques. Ce besoin peut exister ou non, selon l'environnement législatif et réglementaire ; lorsqu'il existe, on doit veiller à préserver l'intégrité et l'exploitabilité des documents électroniques et physiques comme un tout. Ces problèmes devront être traités par des directives organisationnelles *ad hoc*.

Les exigences ci-après nécessiteront une adaptation locale.

Réf. Type d'exigence

- 11.5.1 Le SAE doit respecter les normes applicables pour le passage à l'an 2000 et doit traiter toutes les dates correctement.
- Certains SAE doivent gérer des périodes de plus d'un siècle. Un système correct peut devoir traiter des dates de différents siècles. On trouvera en Annexe 6 un exemple de fiche détaillant ce point.*
- 11.5.2 Le SAE doit respecter les normes nationales concernant la traçabilité légale et la force probante des documents électroniques.
- 11.5.3 Le SAE doit se conformer à la législation nationale sur l'archivage et le records management.
- 11.5.4 Le SAE ne doit comporter aucun élément qui soit incompatible avec la protection des données ou toute autre législation.
- 11.5.5 Le SAE doit se conformer <aux exigences réglementaires européennes, nationales ou locales du domaine, ou au code des bonnes pratiques pour les secteurs de l'industrie, des affaires et de l'administration>.
- Cette exigence peut être personnalisée pour des environnements spécifiques.*

11.6 Externalisation et recours à des tiers

De nombreuses entreprises utilisent des prestataires pour stocker et gérer les documents qui ne sont plus actifs (ou qui sont très peu consultés) mais qui doivent être conservés pendant un certain délai pour des raisons légales ou industrielles, ou qui sont destinés à une conservation à long terme.

On constate également un accroissement du recours à des fournisseurs de services applicatifs (ASP) pour gérer les documents vivants aussi bien que les archives. Les entreprises envoient au prestataire leurs documents – factures, correspondance clients, demandes de prêt hypothécaire, etc. – pour indexation et stockage. Les documents sont alors consultables par les collaborateurs de l'entreprise via Internet ou un réseau étendu.

La gestion et l'archivage des documents électroniques par un tiers exigent que le contrat avec le prestataire de service énonce clairement les procédures et les contrôles pour le respect des exigences réglementaires, adopte les bonnes pratiques pour la recevabilité légale des documents électroniques, et réponde aux besoins du client en termes d'accès et de disponibilité.

Le contrat doit comporter des clauses afin que :

- la qualité de la gestion chez le prestataire de service soit d'un niveau au moins égal à celle du client pour sa gestion interne ;
- le client puisse récupérer les documents auprès du prestataire à n'importe quel moment et être en mesure de poursuivre la gestion des documents conformément à ses règles et aux exigences légales de traçabilité.

Cette sous-section s'appuie largement sur le code PD 0008 (voir Annexe 1 référence [5]), section 4.14 « Sous-traitance »

Réf. Exigence

11.6.1 Il convient d'établir un contrat avec le prestataire de service détaillant l'ensemble des prestations.

11.6.2 Les procédures de transfert des documents du client vers le prestataire et du prestataire vers le client doivent être décrites en détail.

Il peut s'agir de liens de communication entre les sites avec transfert automatique des dossiers et des documents quotidiennement ou régulièrement. Le client doit être assuré que le lien entre les deux sites est sécurisé, qu'il existe une procédure de vérification des documents reçus ainsi que des états statistiques.

11.6.3 Le prestataire de service doit pouvoir fournir au client une copie de l'historique traçant tous les mouvements et le stockage des dossiers/documents.

Réf. Exigence

- 11.6.4 Le prestataire de service doit prouver qu'il a pris toutes les mesures pour que les dossiers/documents et leurs métadonnées puissent être renvoyés facilement sur le SAE du client sans perte de structure ou de contenu. Le prestataire de service doit également donner au client la possibilité de transférer des dossiers et des documents individuellement.
- 11.6.5 Le prestataire de service doit être en mesure de fournir au client un accès immédiat aux documents. Il doit lui fournir soit une image du document archivé, soit le document original selon les conditions de délai et de prix fixées.
- 11.6.6 Le prestataire devrait pouvoir permettre au client d'effectuer des requêtes, de visualiser et d'imprimer les documents ou dossiers depuis ses bureaux.
Ceci peut se faire, par exemple, via une connexion réseau.
- 11.6.7 Le prestataire de service devrait fournir au client la possibilité de demander en ligne le téléchargement ou la transmission de documents ou de dossiers entre le SAE du client et les outils de stockage du prestataire.
- 11.6.8 Le client devrait pouvoir demander des comptes sur les documents détenus par le prestataire et sur l'application des durées de conservation, etc. Ceci devrait se faire en ligne, depuis les bureaux du client.
- 11.6.9 Les prestations énoncées en 11.6.6, 11.6.7 et 11.6.8 devraient :
- avoir des délais et temps de réponse contractualisés ;
 - être effectuées dans un environnement sécurisé.
- 11.6.10 Le client devrait vérifier que les locaux du prestataire sont corrects et obéissent aux critères de sécurité correspondant à ses besoins.
- 11.6.11 Le client devrait vérifier que les procédures proposées et la gestion du stockage ne présentent pas plus de risque pour les documents que ses propres procédures.
Le prestataire de services devra prouver que tous les documents du client sont sauvegardés et que, en cas de perte, ils peuvent être récupérés dans les délais contractualisés.
- 11.6.12 Lorsque les documents sont particulièrement sensibles, le client devrait vérifier que le prestataire garantit la fiabilité de son personnel.
La signature, par tous les employés du prestataire, d'un engagement de confidentialité au moment de leur recrutement est un plus.
- 11.6.13 Tout envoi de documents entre le client et le prestataire devrait être accompagné d'un bordereau comportant l'intitulé et le nombre des documents et dossiers envoyés.
- 11.6.14 Les tiers prestataires de transport devraient répondre aux exigences de qualité et de fiabilité du client et pouvoir en apporter la preuve.

11.7 Conservation à long terme et obsolescence technologique

Cette section concerne la conservation à long terme. L'expression « long terme » n'est pas définie précisément mais signifie ici globalement « pour une période de plus de 10 ans ». Dans tous les cas, les durées de conservation devraient être fixées d'après la législation et le besoin des affaires. Il s'agira parfois de plusieurs décennies ; dans certains centres d'archives, cela peut aller jusqu'à plusieurs siècles. Dans les deux cas, la durée est trop longue pour que les méthodes pratiquées pour les périodes plus courtes puissent convenir.

Les archives électroniques à long terme sont confrontées à trois types de risques :

- dégradation des supports ;
- obsolescence du matériel ;
- obsolescence des formats.

Ces risques sont analysés ci-dessous. L'analyse est suivie d'exigences spécifiques.

Toutefois, le lecteur doit noter que ces spécifications ne fournissent pas d'exigences détaillées sur tous les aspects de cette question, chaque entreprise ou organisme devant développer et mettre en œuvre sa propre stratégie de conservation à long terme de ses archives électroniques, comme c'est le cas généralement pour les archives papier.

Dans l'analyse qui suit, la conservation des documents d'archives implique la conservation des métadonnées et de l'historique des événements qui les accompagnent.

Dégradation des supports

Le risque de dégradation des supports tient au fait que tous les supports de stockage numérique ont une durée de vie limitée. La durabilité varie d'un support à l'autre et en fonction des conditions de stockage (température, hygrométrie et variations). Quand un support atteint ou dépasse sa durée de vie théorique, la probabilité d'erreur de lecture (défiance des bits) augmente radicalement. La plupart des matériels de stockage ont un module de correction d'erreur intégré ; cela peut régler un certain nombre d'erreurs de lecture avec des résultats satisfaisants. Mais au bout du compte, les erreurs de lecture sont si nombreuses que le module de correction automatique ne suffit plus ; à ce stade, les documents sont irrémédiablement corrompus. De nombreux facteurs interviennent mais cela peut conduire à des documents isolés ou des disques ou bandes entières, etc. totalement illisibles.

Les précautions suivantes peuvent éviter des pertes d'information dues à la dégradation des supports :

- s'assurer que tous les supports sont stockés, utilisés et manipulés dans des conditions satisfaisantes. En règle générale, plus l'environnement est propre,

frais, sec et stable, plus la durabilité est grande. Toutefois, pour des types particuliers de supports, il convient de suivre les spécifications du constructeur (la fraîcheur de l'air ne doit pas excéder telle température, le support doit, ou ne doit pas, être nettoyé régulièrement, etc.) ;

- remplacer régulièrement les supports (en recopiant l'information sur de nouveaux supports) avant l'échéance théorique ;
- conserver plusieurs copies de chaque document, et tenir à jour un tableau comparatif de ces copies ; à partir de là, remplacer toute copie de document et toute partie de support qui présente une erreur irrécupérable. Cette méthode est particulièrement utilisée dans les centres d'archives spécialisés dans le long terme ; cela exige des systèmes automatisés et des outils de recherche dont la description dépasse le cadre de ces spécifications.

Obsolescence du matériel

Les périphériques de stockage – lecteurs de bandes et de disques – ont une durée de vie limitée sur le marché. Au-delà, ils exigent forcément plus de maintenance, alors même que la maintenance et la réparation deviennent plus coûteuses ; au bout du compte, ils deviennent pratiquement irréparables. Dans certains cas, des conventions peuvent être établies avec d'autres utilisateurs d'équipements similaires et compatibles ; mais cela ne peut durer indéfiniment. Il arrive un moment où les données stockées sur des dispositifs obsolètes, sans recopie sur d'autres supports, risquent d'être définitivement perdues si le dispositif tombe en panne.

Le même phénomène se produit avec les ordinateurs qui gèrent les applications et le stockage.

Il est évident que la stratégie pour éviter ces risques est de surveiller l'état du matériel et de migrer les données vers de nouveaux supports avant qu'il ne soit trop tard. Dans tous les cas, les supports et le matériel devraient être choisis en fonction leur durabilité ; autrement dit, la popularité et la position de « leader du marché » peuvent être préférables à des produits nouveaux ou de pointe.

Obsolescence des formats

L'obsolescence des formats constitue la principale difficulté pour toute période supérieure à quelques décennies.

Le problème tient au fait que la plupart des composants logiciels intervenant dans la chaîne de traitement entre le support et la restitution des données sont en constante évolution. Ces composants sont :

- les normes d'encodage ;
- les formats de fichiers ;
- les applicatifs ;

- les bases de données et autres logiciels utilitaires ;
- les systèmes d'exploitation.

Ils évoluent très rapidement et les différents composants évoluent de différentes façons, à différents rythmes. Certaines évolutions restent compatibles avec les formats antérieurs et d'autres non, et ceci est particulièrement vrai pour les périodes supérieures à quelques décennies. Il n'est pas possible d'éviter les évolutions en « gelant » la configuration à cause du besoin de migration vers les systèmes en cours (voir ci-dessus) ; les nouveaux matériels requièrent souvent de nouveaux pilotes logiciels, qui requièrent à leur tour un nouveau système d'exploitation et ainsi de suite.

Les techniques suivantes sont généralement reconnues :

- migration (conversion des données à de nouveaux formats accessibles par les matériels et logiciels courants) ;
- émulation (transfert des données vers un nouveau matériel avec ajout d'un composant logiciel qui émule l'ancien matériel, permettant ainsi l'exécution de l'ancienne application) ;
- conservation technologique (maintenance permanente du matériel original ; impraticable sur le long terme) ;
- groupage des données et du logiciel (approche théorique qui n'est pas encore mûre à ce jour ; voir BS 7978, Annexe 7 partie 1).

Bien que la recherche actuelle s'efforce de minimiser les risques, il n'y a à ce jour aucune méthode simple et générique qui garantisse un accès à long terme aux archives électroniques. La migration et/ou l'émulation sont considérées comme les solutions les plus sûres ; en pratique, les deux exigent de prendre en compte la préservation de métadonnées – voir ci-dessous.

Toutefois, les migrations à grande échelle sont rarement exemptes de problèmes ; il peut s'agir de la perte de données et, parfois, de la perte d'une fonctionnalité, d'un élément ou d'une autre caractéristique.

De même, l'émulation à grande échelle, sur le long terme n'est pas bien maîtrisée. Elle présente aussi des risques de pertes de fonctionnalités ou autres caractéristiques.

Les difficultés se corsent dans la perspective de migrations et émulations répétées. Personne ne peut prévoir la nature des migrations ou des émulations qui seront nécessaires ; et personne ne peut prévoir les conséquences de migrations répétées ou de plusieurs « couches » d'émulation.

La meilleure stratégie est de ne stocker les données que dans des formats largement acceptés, stables, ouverts (c'est-à-dire des formats complètement décrits dans des spécifications publiées) et dotés d'une longue durée de vie. Comme pour le matériel, ceci plaide pour des formats « leaders du marché » plutôt

qu'expérimentaux ou de pointe ; les formats propriétaires devraient être évités lorsque leurs spécifications ne sont pas publiées. Cela suppose en outre certaines compétences dans l'entreprise ou l'organisme pour le choix des formats.

Ces remarques visent tout particulièrement le multimédia, en raison de la volatilité du marché et des formats propriétaires dans ce domaine.

Ce problème requiert une réponse propre à chaque entreprise ou organisme et, au niveau général de ces spécifications, une argumentation plus détaillée ne serait guère utile. Toutefois, il est opportun de souligner que toute démarche suppose des dépenses – en matériel, logiciel, préparation et conversion des données et gestion – et personne ne garantira l'accès sans mettre en œuvre une stratégie de conservation à long terme avant l'apparition des difficultés. Autrement dit, la conservation à long terme exige des dépenses préventives qui peuvent être importantes ; le principe est le même que pour les archives papier, mais la dépense peut être plus importante. Quand la conservation à long terme est exigée, il est donc essentiel que la direction générale s'implique dans l'effort et la dépense engagés pour la préservation de l'accès aux données. Des informations complémentaires figurent dans l'Annexe 7 partie 4.

Conservation des métadonnées

En cas de stockage à long terme, il est indispensable que les métadonnées de conservation soient stockées avec les documents. Ces métadonnées fournissent les informations présentées dans le cadre de ces spécifications : informations sur l'environnement technique, sur le logiciel qui a créé le document et sur le logiciel indispensable à sa restitution – ainsi que toutes leurs composantes. Quand la durée de conservation est illimitée, le nombre des métadonnées peut être assez important. Plusieurs projets de recherche en Europe, en Amérique du Nord et en Australie développent à ce jour des listes de métadonnées : les résultats sont accessibles via Internet. La complexité de la conservation des métadonnées a conduit au développement du modèle de référence OAIS (voir Annexe 7 partie 4) qui peut être utilisé pour structurer les métadonnées dans une optique de conservation.

Exigences particulières

Les exigences ci-dessous représentent les exigences techniques minimales pour un stockage à long terme. Toutefois, comme indiqué ci-dessus, l'implication de la direction générale est tout aussi important.

| Réf. | Exigence |
|-------------|-----------------|
|-------------|-----------------|

- | | |
|--------|---|
| 11.7.1 | Les supports de stockage du SAE doivent être utilisés et stockés dans des environnements compatibles avec la durée de vie souhaitée ou prévue, inférieure ou égale à celle qui est annoncée par les fabricants de supports. |
|--------|---|

Dans certains cas, on peut citer la norme BS 4783 (voir Annexe 7 partie 1).

Réf. Exigence

- 11.7.2 Le SAE devrait permettre d'automatiser la comparaison périodique des copies réalisées et le remplacement de toute copie fautive, afin de prévenir la dégradation des supports.
- 11.7.3 Le SAE doit permettre une conversion en masse des documents (avec leurs métadonnées et l'historique des événements) vers d'autres supports et/ou systèmes, en accord avec les normes relatives au format en usage.
- 11.7.4 Le fournisseur du SAE doit posséder un programme de mise à jour de la technologie de base du SAE, et pouvoir prouver qu'il permet la continuité de l'accès à l'information existante, sans modification des contenus.
- 11.7.5 Le SAE devrait utiliser uniquement des produits largement acceptés dont les spécifications d'encodage, de stockage et de structure de bases de données sont ouvertes et publiées.
- 11.7.6 Si le SAE utilise des formats d'encodage et de stockage ou des structures de bases de données propriétaires, ils doivent être pleinement documentés et la documentation accessible à l'administrateur.
- Nota bene : le fait que le fournisseur conserve une copie de la documentation ne suffit pas ; compte tenu des durées en cause, la pérennité du fournisseur est incertaine. C'est pourquoi, il est souhaitable qu'une copie de cette documentation soit gardée dans l'entreprise utilisatrice ou chez un tiers.*
- 11.7.7 Le SAE devrait être capable de gérer toute une série de métadonnées de conservation pour les documents et leurs composantes.

Voir le point 12.7.13.

12 LES MÉTADONNÉES

Dans le contexte de ces spécifications, les métadonnées incluent les données d'indexation ainsi que d'autres données telles que les droits d'accès. Une définition formelle est donnée dans le Glossaire, section 13.1.

Ce chapitre suit un plan différent des chapitres précédents, voir section 12.2.

12.1 Principes

Il est impossible de définir toutes les exigences relatives aux métadonnées pour toutes les mises en œuvre possibles de SAE. Des entreprises et des applications de types différents ont des besoins particuliers et des traditions très variées. Par exemple, certaines entreprises auront besoin d'une indexation centrée sur les intitulés de comptes et les dates des transactions, tandis que pour d'autres le besoin se limitera à un numéro d'ordre ; certaines auront besoin de dossiers par exercice financier, d'autres non ; certaines auront besoin de contrôler l'accès pour des raisons de sécurité, d'autres de gérer la propriété intellectuelle, etc.

C'est pourquoi ce chapitre des spécifications MoReq suggère un minimum d'exigences d'ordre générique, mais qui demandent à être personnalisées. Il s'agit notamment de listes de métadonnées spécifiques que le SAE doit être capable de capturer et de traiter.

Pratiquement, tout SAE est susceptible d'être configuré avec suffisamment de champs pour gérer les métadonnées ci-dessous ; toutefois, cet élément seul ne suffit pas. Il est important que :

- le SAE utilise les métadonnées qui permettent le bon fonctionnement des fonctionnalités définies dans le reste de ces spécifications (voir 12.1.2) ;
- le SAE comporte des fonctions pour la validation, l'héritage et les valeurs par défaut lors de la capture des métadonnées.

Réf. Exigence

12.1.1 L'application SAE ne doit en aucune façon limiter le nombre de métadonnées autorisées pour chaque article (dossier, sous-dossier, document).

Cette notion de limite peut varier selon l'application. Par exemple, les entreprises de petite taille, avec un plan de classement modeste, n'ont pas besoin d'autant de métadonnées que les grandes entreprises dotées d'un plan de classement complexe.

Réf. Exigence

12.1.2 Lorsque le contenu d'une métadonnée peut être relié à une fonctionnalité du SAE, le SAE doit utiliser le contenu de cette métadonnée pour définir la fonctionnalité.

Par exemple, si le SAE stocke les indices de sécurité des documents ainsi que les habilitations des utilisateurs, il doit utiliser ces dernières pour déterminer si un utilisateur peut ou non accéder à tel document. Si le SAE se contente de stocker ces informations d'habilitation et de sécurité uniquement dans des champs texte non contrôlés lors de l'accès, l'exigence n'est pas satisfaite.

A noter qu'il s'agit d'une exigence d'ordre général applicable à de nombreuses métadonnées ; il n'est pas prévu ici de recenser tous les cas de figure.

12.1.3 Le SAE doit permettre de définir différents jeux de métadonnées pour différents types de documents électroniques au moment de la configuration.

Par exemple, les documents numérisés requièrent des métadonnées relatives à la numérisation et à l'indexation ; les factures requièrent des métadonnées sous forme de nombres, le courrier des champs de métadonnées multi-valeurs, etc.

12.1.4 Le SAE doit permettre à l'administrateur, lors de la configuration, de préciser pour chaque métadonnée si elle est obligatoire ou facultative et si elle est interrogeable.

12.1.5 Le SAE doit accepter au moins les formats de métadonnées suivants :

- alphabétique,
- alphanumérique,
- numérique,
- date,
- logique (OUI/NON, VRAIX/FAUX, etc.).

12.1.6 Le SAE devrait accepter des formats de métadonnées définis par l'administrateur sur la base d'une combinaison des formats du point 12.1.5.

Par exemple, une application peut avoir un identifiant du type nnnnn/aa-n.

12.1.7 Le SAE doit accepter tous les formats de date définis dans ISO 8601.

12.1.8 Lors de la configuration, le SAE doit permettre de préciser la source des données pour chaque métadonnée.

Les sources possibles sont décrites aux points 12.1.9, 12.1.10, 12.1.11 et 12.1.12.

Réf. Exigence

12.1.9 Le SAE doit comporter la possibilité d'extraire automatiquement des métadonnées des documents au moment de leur capture.

Il y a des applications où cette fonction n'est pas obligatoire mais elle l'est ici parce qu'elle est particulièrement importante dans de nombreux cas. Par exemple : extraction automatique des dates, des titres, des noms des destinataires, identifiants à partir de documents issus de traitement de texte ou de documents structurés tels que des factures.

12.1.10 Le SAE doit permettre à l'administrateur de préciser les métadonnées qui doivent être saisies au clavier et celles qui sont choisies dans un menu déroulant.

12.1.11 Le SAE devrait permettre que certaines métadonnées soient produites automatiquement à partir du niveau immédiatement supérieur du plan de classement.

Par exemple, pour un sous-dossier, la valeur de certaines métadonnées doit être héritée du dossier mère ; et pour un document, la valeur de certaines métadonnées peut être héritée du sous-dossier où il est classé.

12.1.12 Le SAE devrait permettre que certaines métadonnées soient obtenues à partir de tables de conversion ou en interrogeant d'autres applications.

Par exemple, le SAE pourrait fournir les noms et les codes postaux à une application d'adressage qui en retour fournit un nom de rue comme métadonnée.

12.1.13 Le SAE doit gérer la validation des métadonnées lorsqu'elles sont saisies par les utilisateurs, ou quand elles sont importées. La validation doit utiliser au minimum les éléments suivants :

- format des contenus ;
- ensemble de valeurs ;
- validation par rapport à une liste de valeurs gérée par l'administrateur ;
- validité de la référence au plan de classement.

Exemple de validation de format : tous les contenus sont numériques ou sous forme de date (en cohérence avec le point 12.1.5.).

Exemple de validation par rapport à un ensemble de valeurs : les contenus sont compris entre le 1^{er} janvier 1999 et le 31 décembre 2001.

Exemple de validation par rapport à une liste de valeurs : vérification que le nom exporté figure sur une liste.

Réf. Exigence

12.1.14 Le SAE devrait permettre la validation de métadonnées utilisant des algorithmes de calcul.

Par exemple, des dossiers peuvent être identifiés par des numéros de cartes de crédit à 16 chiffres, dont le dernier chiffre est calculé à partir des 15 premiers par un algorithme (mod 10).

Une interface de programmation, permettant aux entreprises d'introduire l'algorithme de leur choix, devrait normalement convenir.

12.1.15 Le SAE doit, le cas échéant, permettre la validation de métadonnées en interrogeant d'autres applications (par exemple, pour un système nominatif, vérifier si un numéro personnel a été attribué, ou pour une base de données de codes postaux).

12.1.16 Lorsque la valeur des métadonnées est saisie manuellement, le SAE doit permettre l'itération de valeurs par défaut définies par l'utilisateur.

La valeur est réitérée dans le champ de la métadonnée pour toutes les entrées jusqu'à ce qu'elle soit modifiée par un utilisateur. Une fois modifiée, c'est cette nouvelle valeur qui est réitérée.

12.1.17 Le SAE devrait présenter une configuration telle que toutes les métadonnées soient interrogeables lors d'une recherche non structurée (recherche en texte intégral).

12.1.18 Lorsque qu'une métadonnée est stockée dans un format date, le SAE devrait permettre de rechercher la valeur de la date.

Par exemple, le SAE devrait permettre les recherches sur une série de dates. Il ne suffit pas que la date soit stockée dans un champ texte.

12.1.19 Lorsque qu'une métadonnée est stockée dans un format numérique, le SAE devrait permettre de rechercher la valeur du nombre.

12.1.20 Le SAE doit restreindre la possibilité de modifier les valeurs des métadonnées comme précisé dans la matrice au point 13.4.

12.1.21 Le SAE doit permettre à l'administrateur de reconfigurer les jeux de métadonnées et doit enregistrer ces modifications dans l'historique des événements.

Par exemple, il peut être nécessaire d'ajouter un nouvel élément tel que « identifiant du département » à certains types de documents à la suite d'une réorganisation.

12.1.22 Le SAE devrait pouvoir recevoir des métadonnées provenant :

- du logiciel applicatif qui a créé le document ou du système d'exploitation ou du réseau ;
- des utilisateurs au moment de la capture ou de l'enregistrement manuel ;
- de règles prédéfinies lors de la configuration pour la production de métadonnées par le SAE au moment de l'archivage.

Réf. Exigence

- 12.1.23 Le SAE doit pouvoir empêcher toute modification des métadonnées générées directement par d'autres logiciels applicatifs, le système d'exploitation ou le SAE, par exemple, les données de messagerie électronique.
- 12.1.24 Le SAE doit empêcher la modification du contenu des champs de métadonnées définis lors de la configuration.

12.2 Organisation de la suite de ce chapitre

Le reste de ce chapitre énumère les métadonnées fonctionnelles pour chacun des différents niveaux de classement :

- plan de classement ;
- dossier ;
- sous-dossier ;
- document.

La présentation des listes d'exigences relatives aux métadonnées est différente des autres chapitres. Il s'agit toujours de tableaux mais avec de nouvelles colonnes dont l'intitulé est indiqué ci-dessous.

Réf.

Numéro d'ordre de l'exigence

Métadonnées

La capacité du SAE à intégrer toutes les métadonnées est présentée comme une seule exigence.

Les exigences commencent toutes par "le SAE doit" ou "le SAE devrait". Comme dans l'ensemble de ces spécifications, le mot « doit » introduit une obligation et le mot « devrait » une option.

Pour simplifier la lecture, les listes ne reprennent pas les valeurs héritées des niveaux supérieurs de la hiérarchie. Ainsi, les sous-dossiers héritent naturellement des métadonnées telles que le nom, l'identifiant, etc. du dossier mère ; mais ceci n'apparaît pas.

Occurrences

Pour chaque métadonnée, l'exigence inclut le nombre d'occurrences que doit accepter le SAE (les cardinalités en langage technique). Le nombre d'occurrences est présenté comme suit :

- 1 indique que la métadonnée doit apparaître une seule fois pour l'objet qu'elle décrit (dossier, sous-dossier ou document).

Exemple : il ne doit y avoir qu'un et un seul *identifiant unique* par document électronique dans le SAE.

- 1-n indique que la métadonnée doit figurer au moins une fois pour chaque objet décrit mais peut apparaître davantage.

Exemple : chaque utilisateur doit avoir au moins un profil, mais peut en avoir plusieurs.

- 0-1 indique que la métadonnée peut ne pas exister mais si elle existe, elle n'apparaît qu'une fois. A noter que cette catégorie comprend des métadonnées qui seront nécessaires à un certain moment du cycle de vie des dossiers, sous-dossiers et documents, et des métadonnées qui ne seront peut-être jamais requises.

Exemple : la *date de clôture d'un dossier électronique* sera absente tant que le dossier n'est pas clos mais doit apparaître dès la clôture du dossier.

Exemple : on peut attribuer ou non un indice de sécurité à un document électronique pour le protéger ; mais si on protège le document, un seul indice doit être attribué.

- 0-n indique que la métadonnée peut ne pas exister, ou apparaître une ou plusieurs fois pour chaque objet.

Exemple : un *commentaire de révision* d'un dossier électronique peut ne pas exister ou se répéter plus d'une fois, selon l'histoire de ce dossier et de sa révision.

Exigence

Enfin, chaque métadonnée est mise en relation avec l'exigence qui la fait naître. Ainsi, cette section peut servir à comprendre une exigence qui nécessite une métadonnée, de sorte que la métadonnée soit à son tour mieux comprise.

Parfois, plusieurs exigences requièrent la même métadonnée ; dans ce cas, elles ne sont pas toutes énumérées. Il est donc important de noter que cette section ne peut pas aider à déterminer toutes les exigences relatives à telle métadonnée.

A noter une exception : les exigences correspondantes ne sont pas indiquées pour les métadonnées définies par les utilisateurs.

Dans la version électronique de ces spécifications, la référence de l'exigence est un hyperlien vers celle-ci.

La mention « S O » signifie « sans objet ».

12.3 Métadonnées du plan de classement

Le SAE devrait comporter les métadonnées suivantes pour tout plan de classement :

| Réf. | Métadonnée | Occurrence | Exigence |
|--------|--|------------|----------|
| 12.3.1 | Nom <i>Il peut s'agit du nom de l'unité organisationnelle (département, service, etc.) responsable du plan de classement.</i> | 0-1 | 3.2.8 |
| 12.3.2 | Identifiant. | 0-1 | 3.2.8 |
| 12.3.3 | Description. | 0-1 | 3.2.8 |
| 12.3.4 | Métadonnées définies par les utilisateurs. | 0-n | S O |

Note bene : au minimum, une des trois métadonnées 12.3.1, 12.3.2 ou 12.3.3 est obligatoire..

12.4 Métadonnées des séries et dossiers

Le SAE doit comporter les métadonnées suivantes pour toute série et tout dossier :

| Réf. | Métadonnée | Occurrence | Exigence |
|--------|---|------------|----------------|
| 12.4.1 | Identifiant. | 1 | 3.2.2 7.1.1 |
| 12.4.2 | Nom. | 1 | 3.2.2 7.1.1 |
| 12.4.3 | Mots-clés descriptifs. | 0-n | 3.2.8 |
| 12.4.4 | Description. | 0-1 | 3.2.2 |
| 12.4.5 | Date d'ouverture. | 1 | 3.2.4 |
| 12.4.6 | Date de clôture. | 1 | 3.3.4 |
| 12.4.7 | Personne ou service responsable de la maintenance. | 1 | 4.1.1 4.1.7 |
| 12.4.8 | Droit d'accès des groupes d'utilisateurs. <i>Information sur les groupes d'utilisateurs qui peuvent consulter ou non les dossiers ou la série, et types d'accès autorisés.</i> | 0-n | 4.1.1 4.1.7 |
| 12.4.9 | Droit d'accès des utilisateurs. <i>Information sur les utilisateurs qui peuvent consulter ou non les dossiers ou la série, et types d'accès autorisés.</i> | 0-n | 4.1.1 4.1.7 |

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|----------------|
| 12.4.10 | Indice de sécurité. | 0-1 | 4.6.2 |
| 12.4.11 | Si la métadonnée 12.4.10 existe, historique des indices de sécurité, c'est-à-dire pour chaque indice : <ul style="list-style-type: none"> • indice, • date de modification, • motif de la modification, • utilisateur responsable de la modification. | 0-n | 9.3.6 |
| 12.4.12 | Critère(s) de clôture des sous-dossiers. | 1-n | 3.4.8 |
| 12.4.13 | Si le SAE est utilisé pour la gestion des dossiers papier, signalement du dossier papier (ou indication de l'existence d'un dossier mixte). <i>Sans objet pour les séries</i> | 0-1 | 10.1.1 |
| 12.4.14 | Métadonnées définies par les utilisateurs. | 0-n | S O |
| 12.4.15 | Date de suppression. | 0-1 | 9.3.7 |
| 12.4.16 | Auteur de la suppression. | 0-1 | 9.3.7 |
| 12.4.17 | Durée de conservation. | 0-n | 5.1.4 5.1.5 |
| 12.4.18 | Historique des reclassements. | 0-n | 3.4.4 9.1.6 |
| 12.4.19 | Motif de reclassement. | 0-n | 3.4.5 |

Le SAE devrait comporter les métadonnées suivantes pour toute série et tout dossier :

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|----------|
| 12.4.20 | Mention des dossiers liés. <i>Sans objet pour les séries.</i> | 0-n | 3.4.11 |
| 12.4.21 | Autres informations concernant l'accès. <i>Par exemple, impact de la convention des Droits de l'Homme ou des règles de propriété intellectuelle sur la communication des dossiers.</i> | 0-n | 8.1.29 |
| 12.4.22 | Mot-clé (nom). | 0-n | 3.2.6 |
| 12.4.23 | Autre nom. | 0-1 | 3.2.7 |
| 12.4.24 | Descripteurs. | 0-n | 3.2.8 |

12.5 Métadonnées des dossiers et sous-dossiers

Certaines métadonnées peuvent être rattachées valablement soit à des dossiers soit à des sous-dossiers. Cela dépend des différentes façons de constituer des sous-dossiers (voir section 2.2 « Dossiers et sous-dossiers électroniques »).

Les utilisateurs de ces spécifications doivent donc ajuster le niveau de ces métadonnées à leurs besoins. Par exemple, les décisions de la direction concernant la classification (sécurité), le sort final et la révision peuvent être appliquées au niveau du dossier ou du sous-dossier. Dans certains SAE, ce peut être au niveau du dossier ; dans d'autres, au niveau du sous-dossier ; dans d'autres encore, cela dépend de la nature du dossier.

Le SAE doit comporter les métadonnées suivantes pour tout dossier et sous-dossier :

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|--------------------------------------|
| 12.5.1 | Durée de conservation (ou, si l'exigence 5.1.5 n'est pas remplie, date ou événement déclencheur de la révision et prescriptions de sort final). | 1-n | 5.1.4 5.1.5 10.2.1 |
| 12.5.2 | Date d'ouverture. | 1 | 3.3.2 |
| 12.5.3 | Date de clôture. | 0-1 | 3.4.9 |
| 12.5.4 | Lorsque le transfert à une autre institution est prévu (les Archives nationales par exemple), identifiant de l'institution. | 0-n | 5.3.1 5.3.17 |
| 12.5.5 | Statut du transfert. | 0-n | 5.3.7 |
| 12.5.6 | Mention de dossier physique ou mixte. | 1 | 10.1.1 10.1.2 10.1.3 10.2.4 |
| 12.5.7 | Adresse physique (pour les dossiers physiques). | 1 | 4.4.2 10.1.4 |
| 12.5.8 | Mention d'entrée/sortie (pour les dossiers physiques). | 1 | 4.4.2 10.1.5 10.2.8 |
| 12.5.9 | Date de sortie (pour les dossiers physiques). | 1 | 4.4.2 10.2.8 |
| 12.5.10 | Destinataire du dossier (pour les dossiers physiques). | 1 | 4.4.2 10.2.8 |
| 12.5.11 | Date de communication (pour les dossiers physiques). | 1-n | 10.2.9 |
| 12.5.12 | Destinataire de la communication (pour les dossiers physiques). | 1-n | 10.2.9 |

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|-----------------|
| 12.5.13 | Message de communication (pour les dossiers physiques). | 1-n | 10.2.9 |
| 12.5.14 | Statut de destruction. | 1 | 5.1.4 5.3.17 |
| 12.5.15 | Date et auteur de la destruction. | 0-1 | 9.3.7 |
| 12.5.16 | Commentaire de révision. | 0-n | 5.2.6 |
| 12.5.17 | Date de destruction. | 0-1 | 5.3.15 |
| 12.5.18 | Métadonnées définies par les utilisateurs. | 0-n | S O |

Le SAE devrait comporter les métadonnées suivantes pour tout dossier et sous-dossier :

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|--|------------|----------|
| 12.5.19 | Si la métadonnée 12.4.10 existe, date de révision de l'indice de sécurité. | 0-1 | 4.6.12 |
| 12.5.20 | Code-barre et/ou données de localisation (pour les dossiers physiques). | 0-1 | 10.1.9 |
| 12.5.21 | Suppression logique ou déplacement du dossier. | 0-1 | 9.3.1 |
| 12.5.22 | Statut (transfert, déplacement ou suppression) d'un dossier hybride. | 0-n | 5.3.9 |

12.6 Métadonnées des sous-dossiers

Le SAE doit comporter les métadonnées suivantes pour tout sous-dossier :

| Réf. | Métadonnée | Occurrence | Exigence |
|--------|---|------------|----------------------------|
| 12.6.1 | Identifiant. | 1 | 3.3.1 7.1.1 |
| 12.6.2 | Indicateur de sous-dossier physique ou mixte. | 0-1 | 10.1.1 10.1.2 10.1.3 |
| 12.6.3 | Métadonnées définies par les utilisateurs. | 0-n | S O |

12.7 Métadonnées des documents

Le SAE doit comporter les métadonnées suivantes pour tout document :

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|--------------------------|
| 12.7.1 | Identifiant. | 1 | 7.1.1 |
| 12.7.2 | Objet. | 1 | 6.1.2 10.3.5 |
| 12.7.3 | Auteur. <i>Ce peut être un individu ou une personne morale. A capturer automatiquement si possible.</i> | 1 | 6.1.2 6.4.3 10.3.5 |
| 12.7.4 | Personne ou service responsable de la maintenance du document dans le SAE. | 0-1 | 4.1.7 |
| 12.7.5 | Date (et heure le cas échéant) de la constitution du document. <i>Par exemple :</i> <ul style="list-style-type: none"> • <i>si le document est une lettre, la date en tête de la lettre ;</i> • <i>si le document est un enregistrement sonore ou audiovisuel, heures de début et de fin.</i> <i>A capturer automatiquement si possible.</i> | 1 | 6.1.2 10.3.5 |
| 12.7.6 | Destinataire(s). <i>Individu(s) et/ou personne(s) morale(s) à qui l'information du document est destinée. A capturer automatiquement si possible.</i> | 1-n | 6.1.2 6.4.3 |
| 12.7.7 | Type de document. <i>Par exemple lettre, facture, mémoire, etc. A capturer automatiquement si possible.</i> | 1 | 6.1.2 10.3.5 |
| 12.7.8 | Date et heure d'enregistrement. <i>A capturer automatiquement..</i> | 1 | 6.1.7 |
| 12.7.9 | Droits d'accès des groupes. <i>Mention des groupes qui ont accès au document, et types d'accès autorisés.</i> | 0-n | 4.1.1 |
| 12.7.10 | Droits d'accès des utilisateurs. <i>Mention des utilisateurs qui ont accès au document, et types d'accès autorisés.</i> | 0-n | 4.1.1 |

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|--------------------------------------|
| 12.7.11 | Indice de sécurité. <i>A capturer automatiquement si possible, à partir du document lui-même.</i> | 0-1 | 4.6.1 |
| 12.7.12 | Historique de l'indice de sécurité, c'est-à-dire, pour chaque classification antérieure : <ul style="list-style-type: none"> • indice ; • date de modification ; • motif de modification ; • utilisateur responsable de la modification. | 0-n | 9.3.6 |
| 12.7.13 | Métadonnées de conservation (si le SAE est supposé conserver le document plus longtemps que la durée de vie prévue des applications sources). Il s'agit notamment, mais non uniquement, de : <ul style="list-style-type: none"> • noms de fichiers, • matériel qui a produit le document, • système d'exploitation qui a produit le document, • logiciel ou application qui a produit le document (nom et version), • formats de fichier, • résolution, • version et paramètres de l'algorithme de compression, • schéma d'encodage, • information sur la restitution. <i>Les valeurs peuvent être multiples en cas de documents composites.</i> | 1-n | 6.1.2 8.2 8.3 8.4 11.7.7 |
| 12.7.14 | Mention d'archives vitales. | 1 | 4.3.6 |
| 12.7.15 | Identifiant(s) d'extrait(s). | 0-n | 8.1.26 |
| 12.7.16 | Durée de conservation. | 0-n | 5.1.4 5.1.5 |
| 12.7.17 | Etat du transfert. | 0-n | 5.3.17 |
| 12.7.18 | Métadonnées définies par les utilisateurs. | 0-n | S O |

Le SAE devrait comporter les métadonnées suivantes pour tout document électronique :

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|------------------|
| 12.7.19 | Date de révision de l'indice de sécurité. | 0-1 | 4.6.12 |
| 12.7.20 | Signature(s) électronique(s), certificat(s), contreseing(s). | 0-n | 10.5.7 |
| 12.7.21 | Authentification de la signature électronique, c'est-à-dire autorité de certification, date et heure. | 0-n | 10.5.1 10.5.4 |
| 12.7.22 | Date d'envoi. <i>A capturer automatiquement si possible.</i> | 1 | 6.1.2 |
| 12.7.23 | Date de réception. <i>A capturer automatiquement si possible.</i> | 1 | 6.1.2 |
| 12.7.24 | Mention des documents liés. | 0-n | 11.1.18 |
| 12.7.25 | Restrictions dues à la propriété intellectuelle. <i>Par exemple, contraintes d'exploitation de l'information et droits de copyright.</i> | 0-n | 8.1.29 |
| 12.7.26 | Version du document. | 0-n | 6.1.10 |
| 12.7.27 | Langue. | 0-n | 11.4.11 |
| 12.7.28 | Mention de cryptage. | 0-1 | 10.6.2 |
| 12.7.29 | Mention de filigrane électronique. | 0-1 | 10.7.1 |

12.8 Métadonnées des extraits de document

Le SAE doit comporter les métadonnées suivantes pour tout extrait de document :

| Réf. | Métadonnée | Occurrence | Exigence |
|--------|---|------------|-----------------|
| 12.8.1 | Identifiant. | 1 | 7.1.1 9.3.11 |
| 12.8.2 | Identifiant du document original. | 1 | 8.1.26 |
| 12.8.3 | Date de création de l'extrait. | 1 | 9.3.11 |
| 12.8.4 | Identifiant de l'utilisateur auteur de l'extrait. | 1 | 9.3.11 |
| 12.8.5 | Motif de création. | 0-1 | 9.3.11 |
| 12.8.6 | Métadonnées définies par l'utilisateur. | 0-n | S O |

12.9 Métadonnées concernant l'utilisateur

Le SAE doit comporter les métadonnées suivantes pour tout utilisateur :

| Réf. | Métadonnée | Occurrence | Exigence |
|--------|---|------------|----------|
| 12.9.1 | Identifiant de l'utilisateur. | 1 | 4.1.1 |
| 12.9.2 | Profil de l'utilisateur. | 1-n | 4.1.3 |
| 12.9.3 | Rattachement à des groupes. | 0-n | 4.1.5 |
| 12.9.4 | Droits d'accès de l'utilisateur. | 0-n | 4.1.1 |
| 12.9.5 | Date d'expiration des droits d'accès. | 1 | 4.1.2 |
| 12.9.6 | Niveau d'habilitation (le cas échéant). | 1 | 4.6.7 |
| 12.9.7 | Date d'expiration de l'habilitation. | 1 | 4.6.12 |
| 12.9.8 | Métadonnées définies par l'utilisateur. | 0-n | S O |

12.10 Métadonnées concernant les profils

Le SAE doit comporter les métadonnées suivantes pour tout profil :

| Réf. | Métadonnée | Occurrence | Exigence |
|---------|---|------------|----------|
| 12.10.1 | Nom du profil. | 1 | 4.1.3 |
| 12.10.2 | Participation à des groupes. | 0-n | 4.1.3 |
| 12.10.3 | Droits d'accès du profil. | 0-n | 4.1.1 |
| 12.10.4 | Date d'expiration des droits d'accès. | 1 | 4.1.2 |
| 12.10.5 | Niveau d'habilitation (le cas échéant). | 1 | 4.1.3 |
| 12.10.6 | Date d'expiration de l'habilitation. | 1 | 4.6.12 |
| 12.10.7 | Métadonnées définies par l'utilisateur. | 0-n | S O |

12.11 Personnalisation des métadonnées

Les utilisateurs de ces spécifications devraient analyser les exigences de leurs applications en termes de métadonnées et ajuster ce chapitre en conséquence.

Une fois identifiées les métadonnées nécessaires, ils devraient identifier les attributs de chaque élément :

- format (voir 12.1.5) et longueur du champ ;

- statut de la métadonnée (obligatoire ou optionnelle) ;
- sources des données (voir 12.1.9, 12.1.10, 12.1.11 et 12.1.12) ;
- type de validation (voir 12.1.13, 12.1.14 et 12.1.15) ;
- règles d'héritage (voir 12.1.11) ;
- règles pour les valeurs par défaut (par exemple, une date déclarative peut remplacer la date courante en cas de saisie manuelle d'un type de document).

Ces éléments doivent être définis pour pouvoir détailler davantage les exigences.

A noter que les règles de validation, capture automatique, héritage et valeurs par défaut sont particulièrement importantes pour une exploitation fluide et un taux d'erreur minimal, lorsque le système est utilisé au quotidien dans les services (par opposition à un centre d'archives spécifique).

13 MODÈLE DE RÉFÉRENCE

13.1 Glossaire

Ce glossaire définit les principaux termes utilisés dans les spécifications MoReq (dans les exigences aussi bien que dans le modèle).

Quelques définitions importantes sont tirées ou adaptées des glossaires des publications citées en référence dans l'Annexe 1 ; les sources sont indiquées après chaque définition.

Les mots définis dans le glossaire figurent *en italique*.

administrateur

Personne responsable au quotidien de l'application de la politique d'archivage et de records management au sein de l'entreprise.

NB : il s'agit d'une simplification. Dans les grandes entreprises notamment, les tâches dévolues ici à l'administrateur peuvent être réparties entre plusieurs personnes nommées : records manager, gestionnaire des documents, documentaliste, archiviste, etc.

authenticité

(dans le contexte du records management uniquement) Qualité de ce qui est original.

Source : adapté et résumé de la définition d'"authenticité archivistique" dans le glossaire UBC-MAS (Annexe 1 référence [8]).

NB : pour un document archivé, cette qualité implique le document soit ce qu'il prétend être ; elle ne vise pas la fiabilité du contenu du document en tant que tel.

NB : l'authenticité du document archivé tient à son mode de production, sa forme, son mode de transmission, son mode de conservation. Pour plus de détails, voir le glossaire UBC-MAS (référence ci-dessus).

capture

Enregistrement, classement, ajout de métadonnées et stockage d'un *document* dans un système d'archivage.

classement

Identification et ordonnancement systématiques des activités et/ou des *documents* dans des catégories selon l'organisation logique, les méthodes et les règles exposées dans le *plan de classement*.

Source : ISO 15489 (projet de norme internationale ; voir Annexe 1 référence [9]).

clôture

Processus consistant à modifier les attributs d'un *sous-dossier* électronique de sorte qu'il ne soit plus en mesure d'accepter de nouveaux documents.

clos

Qualificatif d'un *sous-dossier* électronique qui, après clôture, n'est plus en mesure d'accepter de nouveaux documents.

configuration

Etape de la vie d'un *SAE* correspondant à son installation et à la définition de ses paramètres.

destruction

Processus irréversible d'élimination ou de suppression de *documents*.

Source : ISO 15489 (projet de norme internationale ; voir Annexe 1 référence [9]).

document

Information enregistrée ou objet qui peut être traité comme une unité.

Source : ISO 15489 projet de norme internationale ; voir Annexe 1 référence [9]).

NB : un *document* peut être sur papier, microfilm, support magnétique ou tout autre support électronique. Il peut comporter toute combinaison de texte, données, graphiques, son, images animées ou tout autre forme d'information. Un seul document peut être constitué d'un ou plusieurs objets de données.

NB : les simples *documents* présentent plusieurs différences importantes par rapport aux *documents d'archives (records)*. Voir *document d'archives*.

document d'archives, document archivé, archive, document

Document(s) produit(s) ou reçu(s) par une personne physique ou morale dans l'exercice de son activité et conservé(s) par elle.

Source : adapté des spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : il existe également des définitions nationales.

NB : un document d'archives peut être constitué d'une ou plusieurs pièces (par exemple un document et ses pièces jointes), et peut se présenter sous n'importe quel support et n'importe quel format. En plus du contenu initial, il devrait comporter les données de contexte et, si possible, les données de structure (c'est-à-dire les données qui décrivent les composantes du document). Une des caractéristiques fondamentales du document d'archives est qu'il ne peut pas être modifié.

document d'archives électronique

Un *document d'archives* sous forme *électronique*.

NB : la forme électronique peut être native, c'est-à-dire produite par une application logicielle, ou résulter d'une numérisation, c'est-à-dire du scan de papier ou de microfilm.

document électronique

Document qui se présente dans une forme électronique.

NB : l'utilisation de l'expression « document électronique » ne se limite pas aux documents texte issus du traitement de texte. Elle vise aussi les messages électroniques, tableaux, graphiques et images, documents HTML/XML et multimédia, ainsi que les documents composites et d'autres types de documents administratifs.

dossier

(1) Utilisé isolément, ce mot renvoie à la fois aux dossiers électroniques et aux dossiers papier.

(2) Avec un qualificatif, c'est-à-dire dossier électronique ou dossier papier, voir la définition correspondante.

dossier électronique

Un ensemble cohérent de *documents d'archives électroniques*.

Source : spécifications fonctionnelles PRO pour le « dossier électronique » (Annexe 1 référence [2]).

NB : ce terme est souvent utilisé improprement pour désigner un *sous-dossier électronique*.

dossier mixte

Ensemble cohérent de *documents d'archives électroniques* et papier stockés en partie dans le SAE sous forme d'un *dossier électronique* et en partie hors du SAE sous forme d'un *dossier papier*.

Source : définition de « dossier mixte » dans les spécifications fonctionnelles PRO (Annexe 1 référence [2]).

dossier papier

Moyen pour maintenir ensemble des *documents physiques*.

Source : spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : les types de dossiers papier sont notamment les enveloppes, les boîtes d'archives et les classeurs.

édition

Processus qui consiste à cacher certaines données sensibles d'un *document*.

NB : cela peut consister à recouvrir les noms avec des rectangles opaques, etc. (équivalent électronique du fait de rayer les documents papier à l'encre) ou à retirer certaines pages.

NB : le document électronique original n'est en aucun cas altéré. L'édition se pratique sur une copie du document ; cette copie est appelée *extrait*.

électronique

Dans ces spécifications, le mot « électronique » est utilisé dans le même sens que « numérique ».

NB : les enregistrements analogiques, bien qu'ils puissent être considérés comme électroniques, ne sont pas dans le cadre de ces spécifications parce qu'ils ne peuvent être stockés dans un système informatique dans être numérisés. Il s'ensuit que, dans la présente terminologie, les documents analogiques ne peuvent être archivés que comme documents physiques.

enregistrement

Action d'attribuer à un *document archivé* un identifiant unique dans le système.

Source : ISO 15489 (projet de norme internationale ; voir Annexe 1 référence [9]).

NB : l'enregistrement implique généralement de consigner dans un « registre » les métadonnées importantes, c'est-à-dire « toutes les données nécessaires à l'identification des personnes et des actions en cause ainsi que le contexte documentaire des documents » (glossaire UBC-MAS, Annexe 1 référence [8]).

export

Processus consistant à copier l'intégralité de *dossiers électroniques* dans un autre système.

NB : les dossiers restent dans le SAE après l'export, à la différence du transfert.

extrait

(d'un *document d'archives*) Copie d'un *document* sur laquelle des données ont été retirées ou masquées mais sans ajout et sans altération du sens.

Source : définition d'« instance » dans les spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : les modifications tiennent généralement aux restrictions de communication de l'information. Par exemple, un document peut n'être accessible qu'après que les données nominatives ont été masquées ou retirées ; dans ce cas, un *extrait* du document est créé où les noms sont illisibles. Ce processus est parfois appelé « édition ».

GED

Gestion électronique de *documents*.

NB : les fonctionnalités d'une GED ne sont pas incluses dans ces spécifications. Toutefois, la GED est souvent étroitement liée à un SAE. Voir section 10.3 pour plus de détails.

indice de sécurité

Un ou plusieurs termes associés à un *document* pour régler son accès.

NB : les indices de sécurité sont souvent définis au niveau général de l'entreprise ou au plan national. Les indices de sécurité utilisés dans la plupart des administrations gouvernementales européennes sont : « Secret Défense », « Secret », « Confidentiel », « Accès réservé », « Non classifié ». Ils sont parfois complétés par d'autres termes tels que « Réservé à l'Union européenne occidentale » ou « Personnel ».

habilitation

Voir niveau d'habilitation.

historique des événements

Informations sur les opérations ou autres événements qui concernent ou modifient les entités gérées (c'est-à-dire des *métadonnées*), suffisamment détaillées pour permettre une reconstitution des opérations passées.

NB : un historique des événements consiste en une ou plusieurs listes, ou en une base de données consultable sous forme de liste. Les listes peuvent être générées par un système informatique (pour les opérations électroniques) ou manuellement (pour les opérations manuelles); ce sont les premières qui sont plus spécialement visées ici.

métadonnées

(dans le contexte du records management et de l'archivage) Informations structurées ou semi-structurées qui permettent la création, la gestion et l'utilisation des *documents* au cours du temps et au sein du domaine d'activité qui les a créés.

Source : définition de travail du Forum « Archivage des métadonnées » (<http://www.archiefschool.nl/amf>).

NB : la distinction entre les données et les métadonnées est parfois délicate. Par exemple, il est en général admis que les données d'indexation de base d'un document archivé font partie des métadonnées du document. En revanche, l'historique des événements d'un document, ou sa durée de conservation, peuvent être considérés valablement comme des données ou des métadonnées selon le contexte. On peut définir plusieurs types de métadonnées, par exemple pour l'indexation, pour la conservation, pour la restitution, etc. Ces détails sur l'utilisation des métadonnées dépassent le cadre des spécifications MoReq.

niveau habilitation

Un ou plusieurs termes associés à un utilisateur pour définir les indices de sécurité auxquels un utilisateur a le droit d'accéder.

numérique

Voir *électronique*.

ouverture

Processus consistant à créer un nouveau *sous-dossier* électronique.

ouvert

Qualificatif d'un *sous-dossier* électronique qui n'est pas encore clos et qui est donc susceptible de recevoir de nouveaux documents.

PDF

Portable Document Format.

NB : ce format est la propriété de la société Adobe, mais il est largement utilisé. Sa présence dans le glossaire n'implique pas un cautionnement.

plan de classement

Voir classement

Source : définition de « système de classement » dans ISO 15489 (projet de norme internationale, voir Annexe 1 référence [9]).

NB : un plan de classement se présente souvent comme une arborescence.

profil

Groupe d'autorisations fonctionnelles allouées à un ensemble d'*utilisateurs* prédéfini.

Source : spécifications fonctionnelles PRO (Annexe 1 référence [2]).

répertoire

Liste des intitulés des dossiers à tous les niveaux du plan de classement.

restitution

Représentation tangible d'un document électronique dont peut disposer un utilisateur.

NB : il peut s'agir d'un affichage à l'écran, d'une impression ou d'une représentation audiovisuelle ou multimédia.

NB : la nature exacte de la restitution peut être affectée par l'environnement matériel et logiciel. Par exemple, plusieurs restitutions d'un même document peuvent varier au niveau des polices de caractères, fins de ligne et pagination, résolution, profondeur, espace couleur, etc. Généralement, ces différences sont acceptables. Mais parfois, leurs conséquences éventuelles méritent d'être prises en considération ; ces questions dépassent le cadre des présentes spécifications.

SAE

Système d'archivage électronique.

NB : un SAE présente plusieurs différences importantes avec un système de GED. Voir les détails en section 10.3).

série

(dans ces spécifications seulement) Partie de l'arborescence d'un *plan de classement* partant de n'importe quel point de l'arborescence et englobant tous les dossiers des niveaux inférieurs.

NB : ceci peut correspondre, dans la terminologie traditionnelle, à "chapitre", "groupe" ou "série" (ou sous-chapitre, sous-série, subdivision, etc.) à tous les niveaux du plan de classement.

sous-dossier

Subdivision d'un *dossier*, papier ou électronique.

Source : définition du mot « partie » dans les spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : les subdivisions sont créées en vue de faciliter la gestion du contenu des dossiers à travers des unités de taille modeste plus aisées à manipuler. Les subdivisions sont mécaniques (c'est-à-dire basées le nombre de documents, sur des numéros ou sur un laps de temps) plutôt qu'intellectuelles.

SQL

Langage de recherche structuré (Structured Query Language).

Note : il s'agit une norme pour les bases de données relationnelles qui sont fréquemment utilisées pour stocker les métadonnées d'un SAE. Cette norme correspond à ISO 9075 (voir Annexe 7).

tableau des durées de conservation

Règles associées aux *séries* ou aux *dossiers* afin de déterminer pendant combien de temps un producteur aurait intérêt à conserver ses *documents d'archives*, et le devenir de ces documents à l'issue de ce laps de temps.

Source : adapté de la définition de « tableau d'élimination » des spécifications fonctionnelles PRO (Annexe 1 référence [2]).

transfert

Processus consistant à faire passer un lot de *dossiers électroniques* vers un autre système.

Source : adapté des spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : les dossiers sont souvent transférés par groupes au sein d'une série du plan de classement quand il s'agit d'un versement à un centre d'archives historiques pour conservation définitive.

NB : voir aussi *export*.

utilisateur

Toute personne utilisatrice du *SAE*.

NB : il s'agit (entre autres) : des administrateurs, du personnel de bureau, du public et de personnes extérieures tels que des auditeurs.

version

(pour un *document*) Etat d'un *document* à une certaine étape de son développement.

Source : spécifications fonctionnelles PRO (Annexe 1 référence [2]).

NB : une version est généralement une des étapes du document, ou le document final. Dans certains cas toutefois, le document final existe en plusieurs versions, par exemple les manuels techniques. A noter que les documents archivés ne peuvent avoir plus d'une version ; voir aussi *extrait*.

13.2 Modèle des relations entre entités

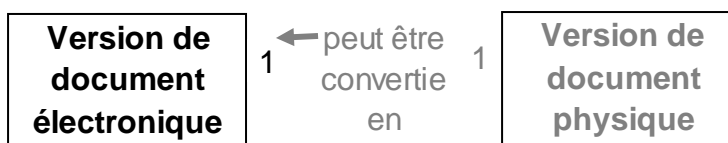
Cette section reprend la section 2.3, pour faciliter la consultation.

Cette section comporte un modèle des relations entre entités qui peut être utilisé pour mieux comprendre les spécifications. La section 13.3 contient une explication plus complète.

Il est important de noter que ce schéma ne représente pas les structures réelles d'un SAE. Il donne une vue des métadonnées associées aux documents archivés. Un SAE utilise ces métadonnées pour générer un fonctionnement comparable à la structure du schéma. Voir section 2.2. pour de plus amples explications sur ce point.

Les relations entre les dossiers, sous-dossiers, documents et autres entités sont décrites plus rigoureusement dans le schéma des relations entre entités ci-après. C'est une représentation formelle des structures d'un SAE.

Dans le schéma, les entités – dossiers, documents, etc. – sont représentées par des rectangles. Les lignes qui les relient représentent les relations entre les entités. Chaque relation est décrite en toutes lettres dans une bulle au milieu de la ligne, à lire en direction de la flèche. A la fin de chaque relation, un nombre indique le nombre d'occurrences (très exactement la cardinalité) ; les nombres sont expliqués dans la clé. Ainsi, par exemple, l'extrait suivant :



signifie : « La version physique d'un document peut être convertie en document électronique » (noter la direction de la flèche).

A noter que l'entité « série » est reliée à elle-même par la relation « est constituée de ». Cette relation récursive décrit, en termes formels, la hiérarchie du classement, dans lequel une série peut comprendre d'autres séries. Pareillement, chaque niveau peut englober d'autres niveaux.

13.3 Détail du modèle des relations entre entités

Le schéma des relations entre entités de la section 13.2 présente un contexte qui dépasse celui des documents électroniques. Par souci de clarté, il donne plus de détails sur les relations entre les documents papier et les documents électroniques que les autres chapitres de ces spécifications.

Les spécifications n'insistent pas sur la gestion des archives physiques ; elles se limitent à traiter la continuité de la gestion papier et électronique dans le SAE. C'est pourquoi, la plupart des entités papier et leurs relations figurent en gris plutôt qu'en noir, utilisé pour leurs équivalents électroniques.

A noter que le schéma est un modèle simplifié ; il ne vise pas à représenter tous les cas de figure possibles. Il ne met en évidence que les relations les plus significatives. Ainsi, les utilisateurs, les profils, etc. n'apparaissent pas.

La suite de la présentation décrit les entités du schéma et leurs inter-relations.

Plan de classement

Pour pouvoir appliquer les principes du records management, une entreprise ou un organisme doit avoir au moins un plan de classement. Celui-ci décrit la structure de classement (généralement hiérarchique, avec des numéros, des noms, des descriptions) pour un secteur donné de l'entreprise ou de l'organisme.

Niveau

Le plan de classement se présente généralement sous la forme d'une hiérarchie ou d'une arborescence. La hiérarchie comprend un certain nombre de niveaux, correspondant aux « sommets » des séries, groupes, sous-séries, etc. utilisés pour décrire les plans de classement dans les systèmes physiques. Chaque niveau peut être prolongé par des ramifications.

Série

Le plan de classement peut être considéré comme l'organisation hiérarchique d'un certain nombre de séries, comme les branches d'un même arbre. Chaque série est reliée à un niveau de l'arborescence, peut s'étendre sur plusieurs niveaux, et peut contenir d'autres séries. Plusieurs séries peuvent démarrer au même niveau mais chaque série ne commence qu'en un seul niveau.

Dossier

Les dossiers apparaissent après les séries, à n'importe quel niveau de l'arborescence, de même que les feuilles se trouvent au bout de toutes les branches. Un dossier est électronique, physique ou mixte. Un dossier physique est le

conteneur traditionnel pour stocker des documents physiques (papier, bande audio, etc.) plutôt qu'électronique.

Sous-dossier

Les dossiers peuvent être divisés en sous-dossiers, suivant certaines règles. En pratique, certains dossiers n'ont pas de subdivisions. Cela dépend de la taille et du nombre des documents archivés, ou bien des actes ou des périodes en cause. L'origine des sous-dossiers est liée aux dossiers papier, afin de les ramener à une taille et un poids raisonnables. Cette pratique se poursuit, le cas échéant, avec les dossiers électroniques, afin de limiter leur volume pour la révision, le transfert, etc.

En réalité, les termes dossier et sous-dossier sont parfois utilisés improprement ou l'un pour l'autre. Par exemple, un utilisateur demandera « un dossier » plutôt qu'un « sous-dossier » (terme plus exact). C'est particulièrement le cas quand le dossier papier ne comporte qu'un seul sous-dossier : bien que le dossier soit de fait constitué d'un sous-dossier, il n'est jamais référencé comme tel (en général, l'appellation apparaît avec le second sous-dossier). *Stricto sensu*, les utilisateurs finaux manipulent des sous-dossiers, mais on dit dossiers pour simplifier. Un pointillé apparaît sur le schéma autour des dossiers et sous-dossiers électroniques (et autour des entités physiques correspondantes). Ceci traduit le fait que l'utilisation de l'expression « sous-dossier électronique » au lieu de « dossier électronique » peut conduire à un malentendu.

Tableau de conservation

Deux rectangles figurent les tableaux de conservation, pour des facilités de mise en page du schéma, mais les deux rectangles ne représentent qu'une seule entité.

Un tableau de conservation précise les règles de conservation et d'élimination des archives. Le SAE peut comporter plusieurs tableaux et chaque série, dossier ou sous-dossier relève d'un tableau au moins.

Document d'archives

Les documents archivés, entité la plus importante, se situent au cœur du système. En tant que traces des activités de l'entreprise ou de l'organisme, ils justifient l'infrastructure globale de records management.

Chaque archive peut comporter un ou plusieurs documents et un même document peut appartenir à plusieurs archives. Les archives sont organisées en dossiers avec plusieurs documents par dossier.

Extrait

Il est parfois nécessaire de produire une copie toilettée (censurée) d'un document, par exemple pour en retirer des mentions sensibles comme les noms de personnes. Dans la mesure où les documents archivés ne peuvent eux-mêmes être modifiés, on

convient d'en produire un extrait. Ce processus consiste à faire une copie du document (sans toucher à l'original) et à toiler la copie.

Document et version de document

Les documents peuvent exister sous une forme électronique ou physique.

Les documents physiques peuvent être sur papier, bande magnétique, film ou un autre support. Par commodité, on les désigne dans ces spécifications par l'expression générique « documents papier ». Les documents électroniques sont l'équivalent numérique des documents papier. Il s'agit le plus souvent de documents issus d'un traitement de texte ou de messages électroniques et ils peuvent être composés de plusieurs fichiers électroniques : par exemple, un rapport texte intégrant des tableaux ou une page intranet incluant des graphiques. Ils peuvent aussi prendre la forme de fichiers images issus de la scannérisation de documents papier.

Il peut exister plusieurs versions des documents. Comme pour le dossier et le sous-dossier, la distinction est parfois malaisée dans la mesure où les documents à version unique ne portent généralement pas de numéro de version. Un pointillé entoure le document électronique et la version de document électronique. Ceci traduit le fait que l'expression « version de document électronique » pour « document électronique » n'apporte rien. C'est pourquoi, l'expression « document électronique » désigne ici le plus souvent une version de document électronique.

Un document physique peut être converti en un document électronique par scannérisation ou autre moyen de numérisation. Plusieurs documents physiques peuvent aussi être convertis en un seul fichier électronique, par exemple une lettre et le rapport qu'elle accompagne. Inversement, un document physique peut être converti en plusieurs fichiers électroniques, par exemple une facture pourrait être convertie en document électronique pour un dossier « fournisseur » et pour un dossier « produit ».

13.4 Modèle de contrôle d'accès

Cette section présente un modèle simple des profils d'utilisateurs. Pour être générique, la matrice se limite à deux profils d'utilisateurs. Les profils – utilisateur et administrateur – sont définis en termes d'accès aux fonctionnalités du SAE.

Le profil d'administrateur est ici simplifié. Dans les grandes entreprises notamment, les tâches dévolues dans ces spécifications aux administrateurs peuvent être réparties entre plusieurs profils qui sont l'administrateur, le records manager, le gestionnaire de documents, le documentaliste, l'archiviste et l'administrateur des données ou le chef de projet informatique, etc.

A noter que le profil de l'administrateur se résume souvent à la mise en œuvre, du point de vue du système, des décisions prises par la direction et basées sur la législation et la réglementation, telles que lois sur l'information, sur la sécurité des

données, sur les archives, la réglementation industrielle et les différents codes de lois (voir section 11.5). Cette matrice ne veut pas signifier que les administrateurs doivent prendre des décisions de fond, bien que cela puisse se produire dans certains cas.

Plus généralement, les utilisateurs accèdent aux fonctionnalités dont a besoin un employé ou un chercheur qui utilise les documents. Ce sont : ajout d'un document, recherche et repérage d'un document archivé ; c'est le contenu des documents qui les intéresse. Les administrateurs prennent en charge la gestion proprement dite de l'archivage ; ils sont davantage concernés par les documents en tant qu'entités archivistiques que par leur contenu. Ils gèrent aussi les aspects matériel, logiciel et stockage du SAE, s'assurant des sauvegardes et de la performance du SAE.

Dans le tableau qui suit :

- OUI signifie que le SAE doit permettre cette combinaison de profils et de fonctions ;
- NON signifie que le SAE doit interdire cette combinaison de profils et de fonctions ;
- OPTIONNEL signifie que le SAE peut permettre ou interdire cette combinaison de profils et de fonctions, selon les procédures décidées par l'entreprise ou l'organisme.

A noter que cette matrice est divisée en rubriques qui regroupent, par commodité, les fonctions normalement associées aux dossiers et aux documents, au records management et à l'administration.

Cette matrice doit être considérée comme un point de départ, la base formelle de l'attribution des droits. Les utilisateurs de ces spécifications devront prendre en compte les exigences supplémentaires liées à leur environnement spécifique. Par exemple, on peut avoir un profil de « responsable des révisions » qui soit distinct du profil d'administrateur ; dans ce cas, il faudra préciser les droits d'accès de ce profil.

Matrice d'accès

| Fonction | Profil d'utilisateur | |
|--|----------------------|------------------|
| | Utilisateur | Administrateur |
| Créer de nouveaux dossiers | OPTIONNEL | OUI |
| Mettre à jour les plans de classement | NON | OUI |
| Supprimer des dossiers | NON | OUI |
| Capturer les documents | OUI | OUI |
| Rechercher et lire les documents | OUI ³ | OUI ² |
| Modifier le contenu des documents | NON | NON ⁴ |
| Modifier les métadonnées des documents | NON | OUI |
| Supprimer des documents | NON | OUI |
| Appliquer les tableaux de conservation et pratiquer des éliminations. | NON | OUI |
| Exporter et importer des dossiers et des documents | NON | OUI |
| Consulter les historiques des événements | OPTIONNEL | OUI |
| Modifier les historiques des événements | NON | NON |
| Transférer les historiques des événements sur un support de stockage hors ligne | NON | OUI |
| Réaliser toutes les opérations concernant les utilisateurs et leurs droits d'accès | NON | OUI |
| Maintenir la base de données et le stockage | NON | OUI |
| Mettre à jour d'autres paramètres du système | NON | OUI |
| Définir et consulter d'autres rapports du système | NON | OUI |

³ Sujet à droits d'accès pour les documents individuels.

⁴ Sauf pour l'édition – voir section 9.3.



ANNEXES

Annexe 1 - Publications de référence

Ces spécifications ont été préparées en se référant aux publications et modèles de référence suivants :

| Réf. | Nom et propriétaire de la Source | URL ou détail de la publication |
|------|--|---|
| [1] | Dublin Core Metadata Element Set (Métadonnées du Dublin Core), Version 1.1 : description de référence | http://purl.oclc.org/dc/documents/rec-dces-19990702.htm ou http://mirrored.ukoln.ac.uk/dc/ |
| [2] | Functional Requirements for Electronic Records Management Systems (Exigences fonctionnelles pour l'archivage électronique), GB Public Record Office | http://www.pro.gov.uk/recordsmanagement/eros/invest/default.htm |
| [3] | Functional Requirements for Evidence in Record Keeping (Exigences fonctionnelles relatives à la preuve dans la conservation d'archives), US University of Pittsburgh | http://www.lis.pitt.edu/~nhprc/ |
| [4] | Guide for Managing Electronic Records from an Archival Perspective (Guide pour une gestion archivistique des documents électroniques), Comité des archives électroniques, Conseil international des Archives, Etude CIA n° 8 | http://data1.archives.ca/ica/ceer/guide_0.html |
| [5] | Code of Practice for legal admissibility and evidential weight of information stored electronically (Recueil d'instructions pour la recevabilité légale et la force probante de l'information stockée électroniquement), British Standards Institution | Publié par l'organisme de normalisation britannique (www.bsi-global.com) sous le nom BSI DISC PD 0008 |
| [6] | Guidelines on best practices for using electronic information (Guide des bonnes pratiques pour l'utilisation de l'information électronique), DLM Forum | http://europa.eu.int/ISPO/dlm/document/guidelines.html |
| [7] | ISAD(G) : General International Standard Archival Description (Norme internationale de description archivistique), seconde édition, Comité de normalisation de la description, Conseil international des Archives | http://www.ica.org/cgi-bin/ica.pl?04_e |
| [8] | The Preservation of the Integrity of Electronic Records (UBC-MAS Project)(University of British Columbia) | http://www.slais.ubc.ca/users/duranti/ |
| [9] | Records Management, ISO 15489 (International Organization for Standardization) | Publication prévue par l'ISO ; la norme était à l'état de projet DIS au moment de la rédaction de MoReq. |
| [10] | Records/Document/Information Management : Integrated Document Management System for the Government of Canada - Request for Proposal - Requirements (RDIM) (National Archives of Canada) | Publié initialement en 1996 sous le nom http://www.archives.ca/06/4rdims.pdf ; éventuellement indisponible aujourd'hui, voir aussi http://www.rdims.gc.ca/ |

| Réf. | Nom et propriétaire de la Source | URL ou détail de la publication |
|-------------|--|---|
| [11] | Standard 5015.2 « Design Criteria Standard For Electronic Records Management Software Applications » (« Conception des logiciels d'archivage électronique », Département de la Défense des Etats-Unis. | http://jrtc.fhu.disa.mil/recmgt/ |

Annexe 2 - Développement de ces spécifications

Les spécifications MoReq ont été développées pour le compte de la Commission européenne par Cornwell, une société de conseil située au Royaume-Uni. L'équipe projet comportait des consultants spécialisés qui ont rédigé les spécifications, et un groupe d'experts en records management / archivage de différents pays ; voir la liste détaillée des auteurs et contributeurs à l'Annexe 4, 1ère partie.

Une réunion de lancement s'est tenue à Londres avec l'ensemble de l'équipe. Lors de cette rencontre, des protocoles de travail ont été arrêtés et quelques références clés identifiées. Cela a été la seule réunion plénière de l'équipe, le projet ayant été par la suite animé uniquement via la messagerie électronique.

L'étape suivante a consisté à effectuer des recherches, à repérer et à obtenir des copies des textes de référence. Ces documents ont été étudiés par les consultants : la liste des textes de référence utilisés figure à l'Annexe 1.

L'étape suivante a été d'analyser le contenu et la structure des textes de référence retenus. Une étude comparative a permis d'élaborer un projet de structure à partir des index de ces textes.

Les consultants ont alors commencé à rédiger un premier jet des spécifications. Ils ont passé en revue les textes de référence, ligne par ligne dans la majorité des cas, vérifiant que chaque exigence – implicite ou explicite – était intégrée à MoReq. Au cours de cette période d'élaboration, la structure du document a lentement évolué, au fur et à mesure où s'opéraient des regroupements logiques d'exigences, jusqu'à la fin du projet.

Cette première version a alors fait l'objet d'une relecture, première d'une longue série, selon un processus itératif traditionnel de relecture et révision. Il y a eu plusieurs types de relecture :

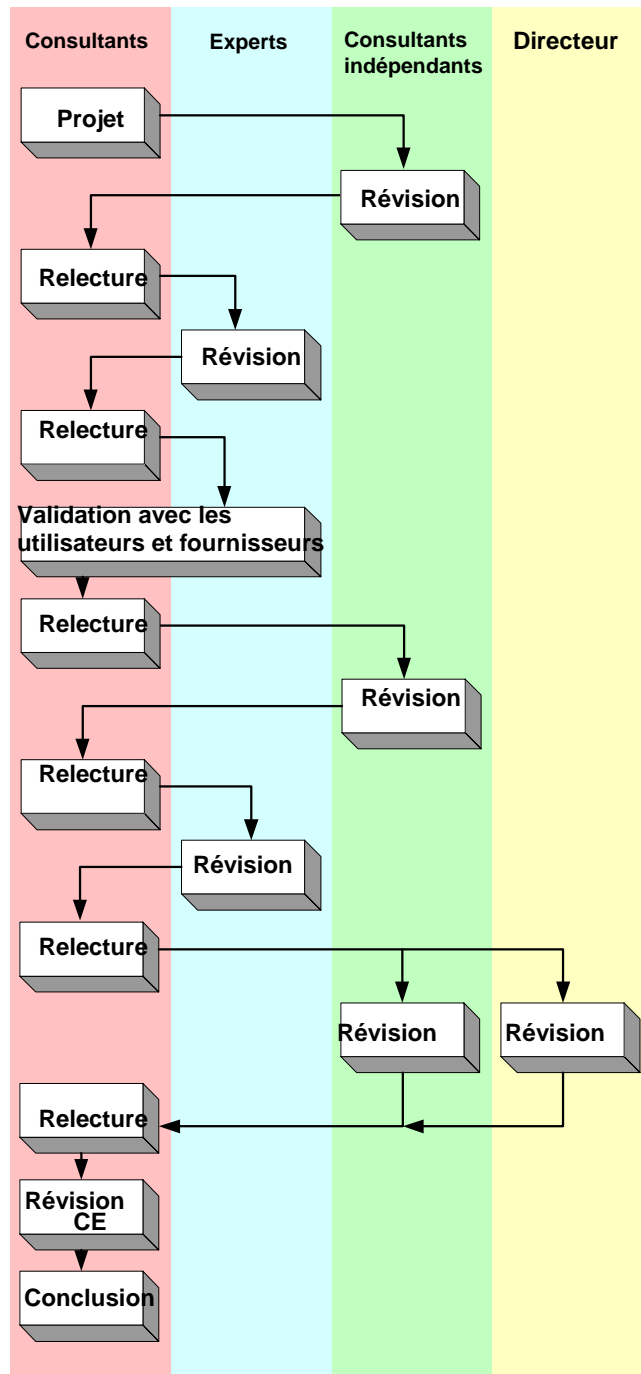
- relecture croisée des travaux de chaque consultant ;
- relectures par un expert en records management semi-indépendant qui n'était pas impliqué dans l'élaboration du texte ni dans les discussions. Il a été spécialement chargé d'homogénéiser les premières versions avec les publications de référence ;
- relectures par un groupe d'experts internationaux ;
- relectures par le chef de projet de la Commission européenne ;
- contrôle d'assurance qualité par le directeur de projet de Cornwell.

Pendant ce processus itératif les consultants et les experts ont échangé des idées et des commentaires divers.

Les spécifications étant en voie d'achèvement, le processus formel de validation a été lancé. Un questionnaire a été élaboré et envoyé, avec le projet des spécifications à un certain nombre de fournisseurs de solutions de records management et de directeurs de

projet qui ont aimablement accepté de participer (voir Annexe 4, 2e partie). Ils ont relu le produit en vérifiant sa cohérence avec les produits existants et son exploitabilité dans le contexte de leur organisation.

Le processus est décrit sous forme de diagramme dans le schéma ci-dessous.



Annexe 3 - Utilisation des spécifications sous forme électronique

Ces spécifications ont été préparées pour être utilisées sous forme électronique, avec le format Microsoft® Word 97

Le principal avantage de l'utilisation de MoReq sous forme électronique est que les spécifications peuvent être facilement personnalisées.

Tous les renvois sont des hyperliens qui peuvent être utilisés pour la navigation à l'aide d'un simple clic. Par exemple, dans la phrase « voir le Glossaire, section 13.1 » le numéro de la section et son nom sont liés.

Les exigences sont présentées sous forme de tableaux, à raison d'une exigence par ligne, comme ci-dessous.

| Ref. | Exigence | |
|--------|-------------------------|--|
| 13.1.1 | Le SAE doit fournir ... | |



Le tableau se compose de trois colonnes :

- **numéro** : numéro de référence pour l'exigence. Il est généré automatiquement par Word, puisque les numéros utilisent un style de titre. Le résultat est que si des chapitres, sections ou exigences sont ajoutées ou supprimées, la numérotation s'ajuste automatiquement.
- **exigence** : libellé de l'exigence. Il utilise toujours le verbe « doit » (pour signifier une obligation) ou le verbe « devrait » (pour indiquer un souhait) ;
- **colonne vierge** : elle peut être utilisée pour des annotations si ces spécifications servent à proposer ou ajouter des pondérations ou toute autre information. Elle peut être élargie ou rétrécie, voire supprimée. Le style de Word utilisé est « Mand/Des ».

En cas de suppression d'un chapitre, d'une section ou d'une exigence, Word remplacera tout double renvoi (le cas échéant) par un message d'erreur. On pourra les identifier en recherchant le mot « error » dans le texte. Ceci est tout spécialement utile pour le chapitre 12 (Métadonnées) qui comporte de nombreux renvois.

Le quadrillage du tableau n'est pas apparent. On peut le faire apparaître à l'aide de la commande « quadrillage ».

Le chapitre 12 utilise une variante du tableau présenté ci-dessus, avec une colonne supplémentaire qui renvoie aux détails des exigences. Ces doubles renvois sont des hyperliens vers ces exigences.

Annexe 4 - Remerciements

1 Equipe projet

Ces spécifications ont été rédigées par :

- Marc Fresko
- Martin Waldron

avec une relecture et des contributions des experts suivants :

- Francisco Barbedo, Archives d'Etat de Porto (Portugal)
- Keith Batchelor, consultant indépendant (Royaume-Uni)
- Nils Brübach, Ecole d'archivistique de Marburg (Allemagne)
- Miguel Camacho, SADIEL S.A. (Espagne)
- Luciana Duranti, Ecole de Bibliothéconomie et des Sciences de l'Information, Université de Colombie Britannique (Canada)
- Mariella Guercio, Université d'Urbino, Institut d'Archivistique et de Bibliothéconomie (Italie)
- Peter Horsman, Institut néerlandais d'enseignement et de recherche archivistiques (Pays-Bas)
- Jean-Pierre Teil, Archives nationales (France)

Le directeur du projet a été Keith Cornwell, administrateur délégué de Cornwell, et le chef de projet pour la Commission européenne Paul E. Murphy, Programme IDA, DG Entreprises.

Nous remercions pour leur assistance Sue Wallis, Jane Burnand et Neil Grosse de Cornwell.

2 Organismes ayant participé à la validation

L'équipe projet est reconnaissante aux entreprises et institutions ci-dessous qui ont aimablement participé à la relecture et à la validation.

| Entreprise/organisme | Type | Pays |
|-----------------------------|----------------------------|-------------|
| Pfizer | Laboratoire pharmaceutique | Royaume-Uni |
| DERA | Agence pour la Défense | Royaume-Uni |
| HM Treasury | Administration centrale | Royaume-Uni |
| Tower Software | Fournisseur de GED | Royaume-Uni |
| Technostock | Société de conseil | Espagne |
| Ministère de la Justice | Administration centrale | Italie |

3 Marques

Toutes les marques mentionnées dans ces spécifications sont connues. Les produits propriétaires ne sont cités qu'à titre d'exemple ; leur présence ne vaut en aucun cas caution. De même, l'absence d'autres produits ne sous-entend aucune critique à leur égard.

Annexe 5 - Correspondance avec les autres modèles

1 Correspondance avec le modèle de métadonnées du Dublin Core

Les métadonnées présentées au chapitre 12 peuvent être comparées aux métadonnées du Dublin Core (voir Annexe 1 réf. [1]). Le tableau ci-dessous donne un exemple de correspondance.

| Nom des métadonnées du Dublin Core | MoReq | |
|------------------------------------|--|--|
| | N° d'exigence | Intitulé |
| Titre | 12.7.1 | Identifiant |
| Créateur | 12.7.3 | Auteur |
| Objet | 12.4.2 12.4.3 12.4.22 12.7.2 | Nom Mots-clés descriptif Mot-clé (nom) Objet |
| Description | 12.4.4 | Description |
| Editeur | - | néant |
| Contributeur | - | néant |
| Date | 12.7.5 12.7.8 12.7.22 12.7.23 | Date/heure Date/heure d'enregistrement Date d'envoi Date de réception |
| Type | 12.7.7 | Type de document |
| Format | 12.7.13 | Métadonnées de conservation |
| Identifiant | 12.7.1 | Identifiant unique |
| Source | 12.8.2 | Identifiant du document original (pour les extraits) |
| Langue | - | néant |
| Liens | 12.7.24 | Documents liés |
| Couverture | - | néant |
| Droits | 12.7.25 | Restrictions à la propriété intellectuelle |

2 Correspondance avec le modèle de métadonnées de Pittsburgh

Les métadonnées présentées au chapitre 12 peuvent être comparées aux métadonnées du modèle de Pittsburgh (voir Annexe 1 réf. [9]). Le tableau ci-dessous donne un exemple de correspondance, pour information. Toutefois, la correspondance n'est pas faite terme à terme en raison des différences dans les paradigmes et de la différence d'approche entre MoReq et les travaux de Pittsburgh. C'est pourquoi, certaines correspondances sont sujettes à caution.

| Modèle de description de Pittsburgh | MoReq | |
|-------------------------------------|---|--|
| | Exigence n° | Description |
| Gestion | | |
| Enregistrement | 12.7.1 12.7.8 | Identifiant Date/heure |
| Identifiant du document | 12.7.1 | Identifiant |
| Données de recherche et repérage | 12.4.2 12.4.3 12.4.22 12.7.2 | Nom Mots-clés descriptif Mot-clé Objet |
| Termes et conditions | | |
| Statut des droits | 12.4.8 12.4.9 12.4.10 12.7.9 12.7.10 12.7.11 | Droits d'accès des groupes Droits d'accès des utilisateurs Indice de sécurité Droits d'accès des groupes Droits d'accès des utilisateurs Indice de sécurité |
| Accès | 12.7.25 12.4.21 | Restrictions à la propriété intellectuelle- Autres informations sur l'accès |
| Utilisation | - | néant |
| Conservation | 12.4.17 12.5.1 | Tableau des durées de conservation |

| Modèle de description de Pittsburgh | MoReq | |
|--|--|--|
| | Exigence n° | Description |
| Structure | | |
| Identification du fichier | - | néant |
| Encodage du fichier | 12.7.20 12.7.21 12.7.28 12.7.29 | Signature électronique (etc.) Authentification de la signature électronique Cryptage Filigrane. |
| Restitution du fichier | 12.7.13 | Métadonnées de conservation |
| Restitution du document | 12.7.13 | Métadonnées de conservation |
| Structure du contenu | - | néant |
| Source | 12.7.27 | Langue |

Annexe 6 - Traitement des dates

Le SAE est censé traiter toutes les dates correctement, quels que soient le millénaire, le siècle ou les types de présentation des dates – voir 11.5.1. Cette annexe présente un état des exigences pour le traitement de l'année 2000, lequel pourra être adapté, le cas échéant, à d'autres types de dates. Cette question est particulièrement pertinente pour les systèmes d'archivage électronique qui peuvent gérer, parmi les métadonnées, des dates de plusieurs siècles, passés ou futurs.

Le texte qui suit extrait de BSI DISC PD2000 -1 :1998 - Définition des exigences de conformité à l'an 2000 (voir Annexe 7 section 2) [reproduction autorisée].

La conformité à l'an 2000 signifiera qu'aucune date, avant, pendant ou après l'an 2000 n'affecte la performance ni les fonctionnalités du système.

Notamment :

- Règle 1** Aucune valeur de date courante ne causera d'interruption des opérations.
- Règle 2** Les processus de datation doivent être homogènes pour toutes les dates, avant, pendant ou après l'an 2000.
- Règle 3** Dans toutes les interfaces et au niveau du stockage, l'expression des siècles doit être explicite ou définie par des algorithmes clairs ou des règles d'inférence.
- Règle 4** L'année 2000 doit être reconnue comme une année bissextile.

Annexe 7 – Normes et autres références

Cette annexe énumère les normes et les autres textes de références cités dans MoReq.

1 Normes

BS 4783

Recommandations relatives au stockage, au transport et à l'entretien des bandes magnétiques utilisées pour le traitement des données et la mémorisation de l'information (plusieurs parties)

BS 7978

Ensemble de recommandations pour la pérennisation des documents électroniques et des objets associés

ISO 639

Codes pour la représentation des noms de langue

ISO 3166

Codes pour la représentation des noms de pays

ISO 8601

Éléments de données et formats d'échange – Échange d'information – Représentation de la date et de l'heure

ISO 8859

Technologies de l'information – codage des caractères sur un octet

ISO 9075

Technologies de l'information – Langages de base de données – SQL

ISO 10646

Technologies de l'information – Jeu universel de caractères codes sur plusieurs octets

ISO 23950

Information et documentation – Recherche d'information – Définition du service de l'application et spécification du protocole

2 Autres références

90/270/CEE

Directive européenne sur les écrans de visualisation

BSI DISC PD 0008

Recueil d'instructions pour la recevabilité légale et la force probante de l'information stockée électroniquement

BSI DISC PD2000-1 :1998

Définition des exigences en matière de conformité en vue de l'an 2000

<http://www.bsi.global.com>)

3 Accès

Initiative SPRITE-S2

Projet ACCENT – Guide pour l'acquisition des TIC

(<http://www.statskontoret.se/accenteng.htm>)

Guide d'accès au contenu du Web du W3C

(<http://www.w3.org/TR/WAI-WEBCONTENT>)

Guide officiel Microsoft pour les développeurs et les concepteurs d'interfaces utilisateur

Chapitre 15, considérations particulières, accès

(<http://msdn.microsoft.com/library/books/winguide/ch15c.htm>)

4 Conservation à long terme

Projet InterPARES (<http://www.interpares.org>)

Projet Préservation de l'Accès à l'Information Numérique (PADI, Preserving Access to Digital Information)

Bibliothèque nationale d'Australie (<http://www.nla.gov.au/padi/>)

Public Record Office du Royaume-Uni

Guide pour la gestion, le tri et la conservation des documents d'archives électroniques, voir particulièrement le chapitre 5 du volume 2

(<http://www.pro.gov.uk/recordsmanagement/eros/guidelines/default.htm>)

Modèle de référence pour un Système d'archivage ouvert (OAIS)

projet de norme ISO (disponible à l'époque de la rédaction de MoReq sur <http://www.ccsds.org/documents/pdf/CCSDS-650.0-R-1.pdf>) [norme ISO 14721 :2003]