Apprivoiser MoReq

Pour archiver et conserver l'information

Octobre 2007

Document élaboré à l'initiative de l'Association IALTA France

COMPOSITION DU GROUPE DE TRAVAIL

Sous l'égide de l'association IALTA, présidée par Me Thierry Piette-Coudol

Groupe de travail animé par Marie-Anne Chabin (*Archive 17*)

La rédaction de ce document a été principalement assurée par :
Jean-Yves Gresser (*GELM Entreprises - production multimédia, conseil*) ; Aline Lobut-Mader (*Lobut Consultant*) ; Elisabeth Morineau (*Desybel*) ; Éric Pichon (*Commission européenne SG*) ; Marc Rocagel (*Novarchive*) ; Gérard Weisz (*Sirius-System*).

Ont également contribué à l'élaboration de ce document :
Évelyne Alliaume (*Total*) ; Michel Atten (*France Télécom*) ; Marie-Michèle Cunin (*BNP Paribas*) ; Agnès Degoulet (*Cour des Comptes*) ; Geneviève Drouhet (*Médéric*) ; Frédérique Fleisch (*Haute Autorité de Santé*) ; Thibaut Girard (*Direction des Archives de France*) ; ; Louis-Pierre Guillaume (*Schlumberger*) ; Nathalie Le Blanc (*Safran*) ; Maud Lepeltier (*MACIF*) ; Élodie-Cécile Marrel (*Commission européenne SG*) ; Nathalie Morand-Khalifa (*France Télécom*) ; Isabelle Queroy (*Banque de France*) ; Vincent Roger (*Ministère de l'Équipement*) ; Marion Taillefer (*Secrétariat général du Gouvernement*) ; Jean-Pierre Teil (*Archives nationales*).

ABRÉVIATIONS ET SIGLES

Liste des abréviations et identification des termes soumis à définition.

GED : gestion électronique de document
ILM : information lifecycle management
KM : knowkedge management
RGAA : référentiel général d'accessibilité pour les administrations
RGI : référentiel général d'interopérabilité
RGS : référentiel général de sécurité
RM : records management
RSSI : responsable sécurité des systèmes d'information
S.A.E : système d'archivage électronique.
S.E.S. : signature électronique sécurisée
SI : système d'information

SOMMAIRE

1 Contexte et objectif de ce document

Le *Groupe de Travail MoReq* a été une structure de travail de l'association IALTA, actif entre mars 2005 et septembre 2007.
Depuis novembre 1997, IALTA est le lieu naturel de rencontre et d'échanges au plan national de ceux qui veulent assurer la sécurisation de leurs échanges électroniques par courriel ou sur la toile, ou encore en EDI (UN/EDIFACT ou XML), notamment par :

- la signature électronique, les services de certification et de confiance, l'archivage électronique et l'horodatage,
- la cryptographie, la gestion des clés privées / publiques, les certificats électroniques,
- les infrastructures de clés publiques, les infrastructures de gestion de clés, les politiques de certification, etc.

L'activité de IALTA se manifeste principalement dans les groupes de travail qu'elle crée pour étudier certains aspects ponctuels de la sécurisation des échanges électroniques. Les conclusions des groupes de travail sur l'archivage électronique, l'horodatage sécurisé et sur la gestion d'attributs sont disponibles sur le site de l'association à l'URL http://ialtafrance.org.

1.1 Origine du groupe de travail

Deux documents sont à l'origine du groupe de travail :

1. *Le Guide de l'archivage sécurisé* publié par l'association en 2000 (http://www.ialtafrance.org) ;
2. Le modèle de référence MoReq (*Model Requirements for the Management of Electronic Records*), publié par la Commission européenne en 2002, traduit en français en 2004 sous le titre *Modèle d'exigences pour l'organisation de l'archivage électronique*.

MODEL REQUIREMENTS FOR THE MANAGEMENT OF ELECTRONIC RECORDS

MoReq décrit les spécifications d'un système d'archivage électronique permettant la capture sécurisée des documents et données à valeur de preuve et de documentation pour les entreprises et les organismes publics, la gestion de leur cycle de vie avec leur destruction ou transfert à échéance, leur rattachement à un plan de classement structuré et hiérarchisé, la gestion de la confidentialité et des accès.
Une révision de MoReq (MoReq2) a été décidée lors du DLM forum de Budapest en octobre 2005. Cette nouvelle version, prévue pour 2008 inclura la notion de test à opérer sur les outils d'archivage du marché, à l'aide d'outils homologués par le DLM-Forum.

Autre référence susceptible d'apporter des éclairages : la méthode australienne de mise en œuvre d'un projet de « records management » dite méthode DIRKS.

Pour mettre en pratique MoReq dans un contexte professionnel et en conformité avec les règles juridiques, il manquait cependant un guide pratique pour la mise en œuvre d'un système d'archivage adapté à l'environnement français. C'est pourquoi le présent document a vocation à décliner les éléments de modalités pratiques, à destination des chefs de projet d'archivage électronique des organisations françaises, quels que soient leur activité et leur statut :

- Définir le périmètre de la problématique de l'archivage électronique intégrant les contraintes réglementaires et culturelles des organisations françaises ;
- Identifier et proposer les modalités pratiques permettant à toute entreprise, publique ou privée, de mettre en place leur propre organisation électronique en vue d'intégrer et de pérenniser des documents et données dans un système d'archivage électronique.

1.2 La traduction française de MoReq

MoReq a été diffusé en anglais par la Commission européenne en mars 2002. La traduction de MoReq dans les différentes langues européennes n'a pas été programmée par la Commission, l'initiative étant laissée à chaque pays membre.
En 2003, les institutions françaises n'ayant annoncé aucun projet de traduction en langue française et n'ayant pas communiqué officiellement sur ce modèle européen, Marie-Anne Chabin a décidé de réaliser cette traduction qu'elle estimait particulièrement intéressante pour les acteurs de l'archivage en France. Les travaux de traduction ont été supportés par le cabinet d'expertise *Archive 17* que préside Marie-Anne Chabin, avec l'aide d'une dizaine de parrains rapidement convaincus de l'apport de ce texte européen à la communauté francophone.
Voir :

http://ec.europa.eu/transparency/archival_policy/moreq
http//www.archive17.fr/MoReq_en_francais.pdf

Les parrains de la traduction sont les entreprises, collectivités et associations suivantes :

- Total
- la RATP
- Sanofi-Aventis
- Conseil général de Seine-et-Marne
- Parker Williborg
- Commissariat à l'Energie Atomique
- Saint-Gobain Archives
- Lobut Consultants
- ADBS (association des professionnels de l'information et de la documentation)
- Association des archivistes français (AAF).

Comme l'indique la « Note du traducteur » en tête de la version française, Marie-Anne Chabin a pris le parti de traduire « records management » par le terme français « archivage », sauf lorsqu'il s'agissait de la discipline en tant que telle. En effet, il est facile d'observer que lorsqu'une entreprise française se dote d'une politique d'archivage, on y trouve ce qu'on trouverait dans la « records management policy » d'une entreprise anglo-saxonne.
Pareillement, lorsque dans cette même entreprise française, les décideurs, les techniciens ou les utilisateurs parlent de documents, de données ou d'informations *à archiver* ou de documents, de données et d'informations *archivées*, ils parlent exactement de ce que leurs homologues de l'entreprise anglo-saxonne appellent « records ».

Le contexte de la traduction, initiative privée, influe sans doute sur le fait que MoReq apparaît aujourd'hui en France comme un document destiné aux entreprises, de même que le « records management » est souvent perçu comme quelque chose qui concerne peu la sphère publique. Ceci est toutefois sans fondement. Les questions de sélection, de description, de stockage et d'accès sont globalement les mêmes dans le secteur privé et dans le secteur public, même si les contenus et les enjeux diffèrent. Du reste, dans les pays anglo-saxons, le « records management » est perçu comme une démarche du secteur public beaucoup plus que comme une pratique des entreprises privées.

Les spécifications MoReq et le présent document s'adressent autant au secteur public qu'au secteur privé, les deux partageant le souci d'organiser et de gérer l'information dans le temps.

1.3 La composition du groupe de travail

Après quelques réunions d'échanges assez ouverts, le groupe de travail de l'association Ialta France s'est restreint à un noyau dur de contributeurs, représentatifs des acteurs du records management/archivage, à savoir :

- les archivistes et documentalistes du secteur public
- les archivistes et documentalistes du secteur privé
- la Commission européenne
- les juristes
- les responsables de projets informatiques et de systèmes d'information
- les consultants en « records management », archivage et documentation
- les consultants en archivage et conservation électronique sécurisée
- les prestataires en gestion externalisée de documents.

1.4 Présentation du document

Après l'exposé de la problématique, la méthode proposée pour la mise en œuvre d'un projet d'archivage et de conservation avec MoReq s'articule autour de trois axes :

1. la politique d'archivage et ses aspects méthodologiques : périmètre documentaire, contraintes réglementaires, plan de classement, durées de conservation, métadonnées ; la méthode est illustrée par quelques exemples de plan de classement et de métadonnées ;
2. la sécurité et les aspects techniques de la conservation : capture, destruction, stockage, pérennisation, restitution ;
3. le projet d'archivage : son périmètre, son déroulement, les risques, les coûts et les bénéfices.

Le présent document se présente essentiellement sous forme de tableaux en deux colonnes :

1. Questions ou thèmes à aborder,
2. Réponse(s), avis du groupe de travail.

Chaque ensemble question/réponse porte une référence qui permet de gérer les renvois d'un chapitre à l'autre.

Les chapitres sont éventuellement complétés par des références « pour en savoir plus » et une table de concordance des sujets abordés avec le texte de MoReq.

Le document ne comporte pas de glossaire spécifique mais il est accompagné d'un document annexe qui regroupe les définitions préexistantes d'une soixantaine de notions utilisées dans le monde de la documentation, du droit ou des technologies informatiques et toutes liées à l'archivage.

1.5 A qui s'adresse ce document ?

Les utilisateurs, auxquels ce document est destiné, sont avant tout les professionnels de la gestion de l'information et de l'archivage:

responsables d'archivage en entreprise
archivistes et documentalistes
« records managers »
qualiticiens
chefs de projet informatique
juristes
…

Sont également pris en compte les différents niveaux d'utilisateurs et plus particulièrement les utilisateurs dits « finaux », ou les personnes qui les encadrent.

En bref : l'objectif de ce document, fondé sur la mise en commun d'expériences multiples, est de fournir à tout responsable d'un projet d'archivage électronique, quel que soit son profil (informaticien, archiviste, responsable métier, juriste…) un guide pratique des questions à poser et des actions à mener pour mettre en place un système cohérent, fiable et assimilable par l'ensemble des acteurs concernés, à l'appui d'une politique d'archivage de l'entreprise.

1.6 Résumé du document : enjeux et livrables

	Chapitre/ Section	Enjeux	Livrables
2	**Politique d'archivage**	Maîtrise des risques de toute nature et des coûts. L'archivage est une politique d'entreprise. Tous sont concernés.	Un document d'entreprise où objectifs et rôles sont clairement exposés
2.1	Contexte et environnement réglementaire de l'archivage	Clarté des motivations et des objectifs. Capacité à répondre aux évolutions de toute nature.	Référentiel(s) interne(s) et/ou externe(s), gardé(s) à jour.
2.2	L'archivage et les autres aspects de la gestion de l'information	Cohérence horizontale et verticale des processus. Responsabilisation des créateurs et des gestionnaires des systèmes d'information.	Actualisation des processus et de la définition du système d'information (SI) de l'entreprise.
2.3	Recensement de l'information à archiver/conserver	Minimiser les risques. Optimiser les ressources.	Inventaire qualifié.
2.4	Organiser et structurer les documents à archiver	Disposer de fondations solides pour construire le SAE, faciliter son utilisation et le faire évoluer.	Le plan de classement
2.5	Les durées de conservation	Paramètre essentiel.	Élément déterminant de l'inventaire.
2.6	Les métadonnées	Disposer des données adaptées à la bonne gestion (la traçabilité) des archives.	Définitions. Modalités de création et de mise à jour.
3	**Sécurisation de l'archivage**	Qualité du SAE et des procédures associées. Situer la sécurité (du SI, de certaines procédures) dans la durée. Cohérence des différents plans sécurité (entreprise, SI…).	Mise en cohérence du (ou des) plan(s) existants. Définition de l'organisation. Spécifications fonctionnelles.
3.1	Sécurité ou sécurisation ?	Clarté des motivations et répartition des rôles.	Analyse de risques. Définition des rôles.
3.2	Les notions et exigences liées à la sécurisation des documents	Appréciation correcte des risques juridiques et techniques.	Contributions : - au plan du cahier des

3.3	Processus de capture et de destruction	Adaptation des solutions aux risques.	charges du SAE, - à la mise à jour des procédures et référentiels internes.
3.4	Notions liées à la conservation et à la restitution des documents électroniques		
3.5	Technologies et moyens techniques	Adéquation des solutions techniques aux risques.	Contribution au cahier des charges du SAE (spécifications techniques).
4	**Le projet d'archivage électronique**	Bon déroulement du projet en termes techniques, financiers et humains. Conformité du SAE aux attentes en termes techniques, financiers et humains.	
4.1	Le contexte et les acteurs	Clarté des engagements et des responsabilités.	Document de mission.
4.2	Le déroulement du projet	Clarté et tenue des objectifs du projet.	Plan détaillé. Définition du tableau de bord et des conditions de sa production.
4.3	Clés du succès et risques du projet	Au départ : clarté (voir 4.1) En cours de projet : suivre les évolutions du contexte, rendre compte de la progression, pouvoir procéder aux recadrages ou aux corrections nécessaires à moindre coût. En fin de projet : pouvoir apprécier l'adéquation du résultat aux objectifs. Après mise en place et rodage du SAE : pouvoir apprécier les résultats par rapport aux attentes de toute nature. Ensuite : disposer d'un pilotage efficace.	Tableau(x) de bord. Rapport, audits, enquêtes.
4.4	Les contraintes		
4.5	Les coûts		
4.6	Les bénéfices		

2 Politique d'archivage

La mise en œuvre d'un système d'archivage ne se résume pas à un projet technique. Il s'agit aussi d'une question d'organisation au niveau global de l'institution ou de l'entreprise. Si le mot français « archivage » est souvent employé par ceux qui l'utilisent dans une acception purement technique ou logistique, l'expression « records management » induit un préalable d'identification et d'organisation des données archivées.

En effet, avant de répondre à la question du « Comment ? » gérer les documents archivés, il importe de poser la question du « Quoi ? » et du « Pourquoi ? » : quels documents faut-il archiver et pour quels motifs ? Le système d'archivage que décrit MoReq constitue la réponse à un besoin : celui de préserver dans le temps des données et des documents parce que l'institution ou l'entreprise a ou aura (sûrement ou simplement peut-être) besoin de ces données et de ces documents demain ou après-demain. Disposer dans le futur de ces informations est l'objectif ; le système d'archivage est le moyen de l'atteindre.

Par ailleurs, dès que le volume de données dépasse un certain seuil, il est inévitable d'établir une structuration logique, intellectuelle des documents à gérer : c'est le rôle du plan de classement.

Enfin la maintenance du système suppose que les données et documents préalablement archivés mais qui sont périmés sortent du système, ce qui exige une gestion rigoureuses des durées de conservation.

C'est cet aspect d'organisation qui fait l'objet de ce premier chapitre. L'archivage requiert une politique, c'est-à-dire des principes directeurs validés par la direction générale et applicable à toute l'entité juridique concernée. A l'époque de l'information numérique, de même que toute institution et toute entreprise doit se doter d'une politique de sécurité informatique, d'une politique de gestion des risques ou d'une charte d'utilisation de la messagerie électronique, elle doit se doter d'une politique d'archivage ou d'une charte d'archivage, les deux expressions étant aujourd'hui employées en France pour désigner ce document de référence au plus haut niveau.

2.1 Contexte et environnement réglementaire de l'archivage

2.1.1	L'archivage au sens de MoReq	Le groupe de travail MoReq traite ici d'archivage au sens du « records management » : le document *Model requirements for the management of electronic records* a été traduit en français sous le titre *Modèle d'exigences pour l'organisation de l'archivage électronique,* voir l'avant-propos du traducteur.
2.1.2	**Archivage et conservation**	Les deux termes « archivage » et « conservation » sont souvent employés conjointement sans être toujours définis l'un par rapport à l'autre. Globalement, deux problèmes sont en cause : 1. sélectionner ce qu'il faut conserver, 2. assurer l'accès dans le temps. On peut dire que la conservation est l'obligation légale ou la nécessité qui s'impose aux entreprises ; l'archivage est le moyen, le processus qui permet de garantir la conservation. Dans ce sens, l'archivage possède une dimension de "records management".

2.1.3	**Définition** du « records management »	Le records management est une fonction d'organisation, de gestion et de conservation de l'ensemble des documents/objets d'information produits ou reçus par une personne ou un organisme dans l'exercice de ses activités, ou de ses obligations légales. *voir le document rédigé par le groupe de travail AAF-ADBS sur le records management et intitulé « Comprendre et pratiquer le records management : analyse de la norme ISO 15489 au regard des pratiques archivistiques françaises » : http ://www.adbs.fr/site/publications/rm/evalnorme_iso15489.pdf* *voir aussi la définition de la CSTIC (*Commission spécialisée de terminologie et de néologie de l'informatique et des composants électroniques) : www.ensmp.net/cstic
2.1.4	Archivage/Records management **papier ou électronique** ?	Le champ d'application de l'archivage (et/ou du records management) est indépendant du support des documents et des données. Les principes énoncés pour l'archivage électronique sont également valables pour l'archivage sur support papier, et bien sûr pour l'archivage mixte (papier et électronique) ; si le support papier est encore aujourd'hui largement utilisé, le support électronique est appelé à devenir le principal mode d'archivage.
2.1.5	**Objectifs** de l'archivage/records management	Le records management a pour finalité de permettre à une entreprise ou un organisme de disposer à tout instant et dans des conditions optimales de l'information ou du document dont il a besoin pour conduire ses activités, répondre aux contraintes de l'environnement réglementaire, et construire et protéger une mémoire d'entreprise ou d'institution. Autrement dit, l'archivage/records management doit veiller : 1. à la conservation des documents/données utiles à l'entreprise 2. à la destruction des données périmées, d'abord pour des raisons légales, ensuite pour des raisons de bonne gestion.
2.1.6	Quelles sont les relations entre l'archivage et la législation sur la **protection des données** ?	La législation sur la protection des données personnelles impose la destruction, en général à court ou moyen terme, des données informatiques touchant à la vie privée des personnes, afin d'éviter tout risque d'utilisation ou de manipulation indue. Si ces données personnelles ont été archivées, le système d'archivage doit contrôler le processus de destruction. Le manquement à cette obligation de destruction est passible de sanctions, sous l'autorité de la Commission nationale informatique et liberté (CNIL) : www.cnil.fr Pour les archives publiques : les « renseignements individuels ayant trait à la vie personnelle et familiale » font l'objet d'une protection particulière, qui porte à cent ans le délai de libre consultation (art. L. 213-2 du Code du patrimoine).

2.1.7	Quel **périmètre documentaire** ou quel champ d'application, pour l'archivage ?	Le périmètre documentaire d'un système d'archivage / records management est constitué des documents/objets d'information ayant valeur de preuve, de témoignage ou de traçabilité, ou valeur documentaire dans le temps, que l'organisme aura décidé de préserver à titre de : ▪ obligation légale et réglementaire ▪ moyen de défense en cas de contentieux ▪ preuve de propriété intellectuelle ▪ preuve de savoir et savoir-faire ▪ document nécessaire à la reprise de l'activité en cas de sinistre (archives vitales) ▪ élément de construction et de maintenance d'une mémoire historique[1] ▪ document à contenu réexploitable Exemples : ▪ Les marchés publics ▪ Les dossiers médicaux ou dossiers de patient ▪ Une commande par mail ▪ Un fichier clients sous forme de base de données ▪ Des factures ….
2.1.8	Caractéristiques des documents/données gérées par l'archivage	Le document/objet d'information archivé est défini comme une information inscrite sur un support, et respectant les conditions suivantes : 1. il est figé, c'est à dire non modifiable, validé et/ou signé si nécessaire, et daté ; 2. il est accompagné de son contexte de production qui lui donne un sens (métadonnées). Il n'y a pas de restriction, ▪ ni sur sa forme et son niveau de granularité: message électronique, SMS, ouvrage, article de revue, base de données, flux de données, données d'un processus, extrait de document, etc. ▪ ni sur le support : papier, vidéo, microfilm ou électronique…

[1] La norme ISO 15489 exclut les archives historiques de son champ.

2.2 L'archivage et les autres aspects de la gestion de l'information

2.2.1	Archivage et **sauvegarde**	L'archivage s'attache à la conservation d'un objet logique en prenant en compte les aspects organisationnels et techniques liés à cette conservation de façon à restituer à un demandeur habilité les documents dont il a besoin dans le cadre de ses missions. La sauvegarde est une opération technique destinée à assurer la continuité de l'exploitation d'un système informatique en cas d'incident. voir le site de la SNIA (storage network industry association) www.snia.org
2.2.2	Archivage et **stockage**	L'archivage est un ensemble de processus tandis que le stockage est un outil technique mis en œuvre dans le cadre d'un système d'archivage. Les données archivées sont toujours stockées quelque part mais le stockage n'est pas chargé de la sélection ni de la lisibilité ou de l'intelligibilité des données.
2.2.3	Archivage et **GED** (gestion électronique de documents)	La gestion électronique de documents est une expression française très générique utilisée communément pour désigner la production et la gestion de documents numériques natifs ou issus de la numérisation en liaison ou non avec la gestion informatique des processus qui organisent les opérations. On parle alors de « GED workflow » ou de « document management ». Dans le sens de « document management », la GED s'oppose au records management : au sein de la GED, le document est placé sous la responsabilité de son créateur (de l'utilisateur). A partir du moment où sa validation et sa diffusion par une personne autorisée lui confèrent une valeur probante ou de référence au sein de l'organisme, le document devient un « record » et suit des règles communes d'archivage. Voir tableau GED/Archivage dans MoReq (chapitre 10)
2.2.4	Archivage et **ILM** (information lifecycle management)	L'ILM (*information lifecycle management - gestion du cycle de vie de l'information*) est une démarche de gestion de l'information qui vise à ajuster le choix du support à la valeur critique de l'information à chaque étape de son cycle de vie, afin d'optimiser les coûts de stockage. Les principaux aspects sont : le besoin de sécurité, le besoin de disponibilité de l'information, le besoin de pérennité. De ce point de vue, l'archivage apparaît comme un sous-ensemble de l'ILM ; l'archivage prend en charge le document dès que celui-ci ne doit plus être modifié.

2.2.5	Archivage et **durées de conservation**	Le besoin d'archiver est lié à la valeur de l'information et non à sa durée de conservation. Des documents peuvent être conservés pendant longtemps par un utilisateur sans être véritablement archivés, s'ils n'ont pas de valeur probante ou de valeur pour d'autres que leur auteur-utilisateur. Inversement, certaines données doivent être archivées même si leur durée de conservation est brève (quelques mois). Les règles d'archivage communes apportent des garanties sur la qualité de la conservation et de la restitution, et la maîtrise de la destruction à échéance.
2.2.6	Archivage et **gestion de contenu**	La gestion de contenu (« Content management ») se place dans une phase d'élaboration d'un document et dans un contexte d'évolutivité des sous-ensembles constitutifs de ce document. Le document, une fois finalisé (ainsi qu'éventuellement les versions intermédiaires importantes dans le cadre d'un processus décisionnel) pourra devenir une archive s'il entre dans les critères définis par le records management.
2.2.7	Archivage et **gestion des connaissances**	L'archivage est dédié à l'accompagnement du cycle de vie des documents et des données, avec un souci d'exhaustivité au sein du périmètre défini ; la gestion des connaissances (*knowledge management*) est dédiée à l'exploitation des contenus, avec un critère de pertinence de ces contenus par rapport à une action définie. La gestion des connaissances ne s'intéresse aux informations archivées que dans la mesure où elles sont immédiatement exploitables.
2.2.8	Archivage et **intelligence économique**	L'intelligence économique recouvre à la fois la gestion des connaissances internes de l'entreprise et la veille concurrentielle, technique ou commerciale. Elle est donc susceptible d'utiliser les archives comme ressource, d'une façon assez semblable à ce qui peut se passer avec la gestion des connaissances (ci-dessus). Les fonctions de collecte, en amont, et d'analyse, en aval, sont beaucoup plus développées pour la veille et l'intelligence économique mais on peut imaginer un plan de classement commun, voire des outils communs de capture, de conservation, d'accès et de restitution des documents ou informations rassemblées.
2.2.9	Archiviste, archiveur et records manager	Dans le langage courant (il n'existe pas de définition officielle de ces termes) : l'archiviste et le « records manager » gèrent l'archivage et conservation du contenu et du support ; l'archiviste gère en outre les archives historiques ; l'archiveur (tiers-archiveur souvent) gère la conservation, l'accessibilité et la lisibilité des documents et fichiers dont il a la charge, mais sans accéder aux contenus.

2.3 Recensement de l'information à archiver/conserver

2.3.1	Quels sont les **documents ou données qui sont concernés** par l'archivage ?	Ce sont les documents dont la non disponibilité présente un risque significatif pour l'entreprise. En priorité, les documents utilisés dans un contexte légal, réglementaire ou juridique à titre de preuve (*ad probationem*) ou pour validité d'un acte (*ad validitatem*). Les obligations dans ce domaine sont par nature dépendantes du droit national dans lequel les documents devront produire les effets juridiques attendus. En France, l'écrit sous seing privé[2], en tant que manifestation de la volonté, n'exige en principe aucun support matériel pour exister. Par exception toutefois, la formalisation d'un écrit constatant l'acte juridique peut être nécessaire, soit pour assurer la validité de l'acte lui-même, soit pour permettre la preuve. Pour définir l'information ou les documents à conserver, il convient donc de procéder à une analyse de ceux-ci dans leur contexte réglementaire de production.
2.3.2	Y a-t-il des documents dépourvus de valeur légale intrinsèque et qui doivent pourtant être archivés ?	Oui, les documents comportant l'explication d'une décision : ▪ informations sur lesquelles s'est appuyée une décision, ▪ critères de calcul de données fiscales ou financières. Ce peut être également : ▪ des documents provenant de l'extérieur adressés pour information, prouvant que l'entreprise avait ou n'avait pas connaissance de tel fait (voir les enquêtes officielles dans le secteur aéronautique – par ex. Columbia Accident Investigation Board), ▪ des documents apportant la preuve d'un savoir ou savoir faire (documentation permettant de prouver une antériorité en cas de dépôt de brevet), ▪ la documentation qui facilite la reprise d'une activité, après un sinistre. (exemple : certains documents de procédure).
2.3.3	Y a t-il des documents sans valeur juridique car non validés, à archiver ?	Il est bon de conserver des informations de traçabilité ou de mémoire, par exemple pour ne pas avoir à les refaire en cas de réactualisation du dossier : ▪ dossier de négociation commerciale non conclue, ▪ résultats de recherche pour un projet ou un brevet non abouti.

2 L'acte juridique a pour origine la volonté d'une ou plusieurs personnes. Il a pour objectif de produire des effets juridiques. Par exemple, un contrat de travail est un acte juridique résultant de la volonté d'un employeur et d'un salarié.

2.3.4	Quels sont les documents ou données **qui ne sont pas concernés** par l'archivage ?	Les documents ou données non fixés (non figés), non validés et donc dépourvus de valeur de preuve. Exemples : o documents préparatoires dépourvus de valeur de traçabilité ; versions non validées, copies de travail, o coupures de presse recueillies à titre d'information. Les documents que l'organisme aura décidé de ne pas conserver dans un système sécurisé, car jugés comme non essentiels à sa protection ou à la conduite de ses activités.

2.4 Organiser et structurer les documents à archiver : le plan de classement

2.4.1	Qu'est-ce qu'un **plan de classement** ?	Une organisation structurée et hiérarchique d'un ensemble de concepts ou d'objets. C'est un outil intellectuel qui permet aux documents et dossiers de trouver logiquement leur place les uns par rapport aux autres : ▪ regroupement dans une même classe de documents ayant des caractéristiques (métadonnées) communes comme par exemple un même contexte de production, des thématiques similaires, liés à une même activité de l'entreprise ou de l'institution, ▪ héritage des caractéristiques des niveaux génériques par les niveaux spécifiques. Il existe plusieurs types de plans de classement, selon : ▪ son objectif : pour optimiser l'automatisation de la gestion ou pour permettre au document d'être logiquement repérable et accessible ; ▪ son périmètre: pour toute l'entreprise ou l'institution, au sein d'une direction, etc. On peut distinguer, entre autres : ▪ le plan de classement documentaire défini pour un processus ou une activité métier, pour des besoins de gestion, de recherche et de consultation, dans un contexte de mutualisation. Il est basé sur des descripteurs renvoyant à des thèmes ou sous-activités (exemple : les rubriques « clôture de compte », « PEA »…dans un plan de classement du processus gestion de compte bancaire). C'est l'outil de gestion au quotidien de l'utilisateur et du producteur de documents ; ▪ le plan de classement par activité, préconisé par la norme ISO 15489 sur le records management, qui regroupe les documents en fonction de la

		responsabilité qu'ils engagent ; ▪ le plan de classement pour l'archivage est destiné faciliter la gestion, la conservation et la destruction des documents archivés par l'archiviste ou le records manager. Plusieurs types de plans de classement peuvent coexister au sein d'une entreprise ou d'une institution.
2.4.2	Un plan de classement est-il toujours **hiérarchique** ?	Il existe des méthodes non hiérarchiques de gestion de l'information (cf l'essor des "tags" sur internet). Certains estiment que l'on peut s'affranchir de la structuration *a priori* qu'est le plan de classement grâce à la technologie, l'organisation intellectuelle des documents archivés reposant uniquement sur les liens déclarés entre ceux-ci. On obtient ainsi un plan de classement « à la carte ». Cependant, pour les besoins d'archivage, la structure hiérarchique semble la plus adaptée dans la mesure où elle permet une vue d'ensemble du fonds, regroupé en grandes catégories intellectuelles qui peuvent être affinées selon les besoins. Par ailleurs la gestion est facilitée, dans la mesure où les niveaux spécifiques peuvent automatiquement hériter des caractéristiques de leurs "parents".
2.4.3	Pourquoi un plan de classement pour l'archivage ?	Compte tenu du nombre d'objets d'information à gérer (des dizaines ou des centaines de milliers) et compte tenu de leur hétérogénéité (forme, contenu, date, valeur juridique), l'organisation des objets d'information au sein d'un plan de classement permet la maîtrise des volumes, facilite l'automatisation de certaines décisions (quoi archiver et quelle durée ?), et des tâches (transfert, indexation, destruction…). Le contrôle du système en est ainsi allégé. Un plan de classement peut également faciliter l'accès à l'information (en partant du concept le plus général pour aller au plus détaillé). Dans cette finalité et pour les documents électroniques, il est évidemment concurrencé par la puissance des outils de recherche en texte intégral mais reste indispensable pour retrouver le contexte des résultats.
2.4.4	Caractéristiques d'un **plan de classement pour l'archivage**	Dans la mesure où l'archivage doit impérativement gérer la durée de conservation des documents/données, le plan de classement pour l'archivage doit prendre en compte les éléments structurants de la valeur d'archive : processus de production de l'information, rattachement à d'autres documents (amont et aval), confidentialité, valeur de preuve, caractéristiques de gestion au long du cycle de vie, fréquence d'utilisation, etc.
2.4.5	Plan de classement pour les archives papier ou électroniques ?	Le plan de classement est un outil de regroupement intellectuel des documents : il est donc indifférent à leur support. L'utilisation d'un plan de classement unique pour les archives papier et électroniques facilite la gestion de l'information.

2.4.6	Plan de classement et/ou plan de rangement	Le **plan de classement** structure de façon intellectuelle les documents et les dossiers entre eux. Son caractère intangible permet de classer un même document dans plusieurs dossiers. Le **plan de rangement** s'utilise principalement pour les fonds papier ou hybride (électronique / papier / objet). Il structure physiquement le fonds et indique la localisation "matérielle" du document (telle armoire, telle tablette, tel meuble de cartes et plans, tel hangar pour les carottes de forage par exemple, etc.) De façon à travailler aisément, il est vivement recommandé de distinguer le plan de classement (*classification scheme*) du plan de rangement (*filing plan*). Le plan de rangement peut s'inspirer éventuellement du plan de classement au niveau du dossier, mais certains documents peuvent trouver leur place dans un même dossier intellectuel sans pouvoir être rangés ensemble (par exemple, une carotte de forage, le rapport d'analyse et la maquette de couches sédimentaires qui en a été tirée).
2.4.7	Quel lien avec le tableau de gestion ou le référentiel de conservation si un archivage papier existe déjà ?	Le **tableau de gestion** des durées de conservation (modèle Direction des Archives de France) indique les durées de conservation et le sort final par type de document et/ou de dossier au sein d'un service. Il peut être structuré en fonction des rubriques du plan de classement bien que ce ne soit pas systématique. Outre l'indication des durées, le **référentiel de conservation** codifie les catégories de documents à conserver pour l'ensemble de l'entreprise, afin de faciliter le pilotage de l'archivage et l'évaluation de ce qui est conservé. La codification constitue une hiérarchie ; elle s'appuie de préférence sur le plan de classement.
2.4.8	Rôle du plan de classement en amont de l'archivage	Le plan de classement pour l'archivage ne sert pas seulement à gérer les documents et données archivés. Il sert aussi à encadrer la production de l'information qu'il faudra archiver, en permettant de distinguer dès la conception des documents ceux qu'il faudra archiver et ceux qui n'ont pas vocation à l'être.
2.4.9	Quel champ d'application du plan de classement pour l'archivage ?	Le plan de classement s'applique à toute l'entreprise ou l'institution, afin d'assurer la cohérence de la gestion de l'information au niveau global.
2.4.10	Quel **niveau de détail** du plan de classement pour l'archivage ?	Le plan de classement ne devrait pas être trop détaillé. En effet : - plus le plan est détaillé, plus sa maintenance sera difficile, du fait des nombreuses réorganisations ; - plus le plan est détaillé, plus il est lourd et long à faire accepter par tous les utilisateurs.

		En revanche, le plan global d'entreprise peut être complété de façon détaillée, dans chaque entité en fonction des spécificités d'organisation des équipes.
2.4.11	Existe-t-il plusieurs **modèles de plan de classement** pour l'archivage ?	Oui, plusieurs modèles de plans de classement existent. Ils diffèrent notamment par leur structure de base. On peut citer : o celui de MoReq : l'ossature du plan est constituée par les fonctions/activités conformément à la norme ISO 15489 ; le modèle des relations entre documents s'appuie sur une arborescence en 7 niveaux maximum (niveau, série, dossier, sous-dossier, document, pièce, extrait) dont 3 minimum, reflétant le processus de production de l'information depuis le domaine d'activité à l'élément documentaire le plus fin. (voir MoReq, 2.3, p 13) ; o le plan de classement lié au tableau de gestion construit sur la base de l'organigramme des services ; o des modèles basés sur la valeur juridique et fonctionnelle des documents, comme celui du Gouvernement du Québec ; le plan est construit autour de trois grands types de documents ; organisé autour de la distinction entre documents de référence, documents de transactions et dossiers, s'appuyant à la fois sur la forme et la valeur des documents o le référentiel de conservation s'appuyant sur les catégories de conservation de la méthode ARCATEG ©, créée par Marie-Anne Chabin (voir www.archive17.fr). Une catégorie est constituée par l'ensemble des documents procédant de la même activité et partageant la même durée de conservation pour la même raison. Ainsi, le nombre des catégories à gérer n'excède pas quelques dizaines. Ce classement a été notamment adopté par RTE – gestionnaire du Réseau de Transport Électrique. On peut imaginer d'autres modèles, basés sur les processus (plus précis que les activités) ; ou sur la confidentialité.
2.4.12	Qui prend les décisions de **gestion du plan de classement** pour l'archivage (arborescence, nombre de niveaux, règles de nommage) ?	Le « records manager » ou l'archiviste car il y a nécessité de centraliser. Les outils informatiques du système d'archivage électronique (SAE) doivent offrir les fonctionnalités de configuration nécessaires à l'administrateur.
2.4.13	Qui gère le plan de classement pour l'archivage ? (MoReq 3.1.1)	Les outils informatiques du système d'archivage électronique (SAE) doivent offrir les fonctionnalités de gestion du plan de classement
2.4.14	Quelle articulation entre le **plan de classement**	L'une des solutions pour le SAE est de ne pas tenir compte du plan de classement documentaire par processus. Les

	documentaire par processus/activité et le plan de classement pour l'archivage ?	utilisateurs auront alors à gérer deux outils. Une autre solution est de remplacer le plan de classement documentaire par processus par le plan d'archivage dès l'élaboration des documents. L'inconvénient : un changement de pratique des utilisateurs en général mal vécu. De plus, l'outil devant répondre à plusieurs exigences (gestion quotidienne du processus et gestion de l'archivage) peut devenir lourd à gérer. Une troisième solution est que le SAE utilise le plan de classement par processus/activité, comme ressource de cartographie organisée des documents en dossiers, par processus ou activité, pour toute l'entreprise, en l'adaptant à ses propres besoins. Cette adaptation peut se faire en minimisant les changements de pratique demandés aux utilisateurs : préciser dans le plan de classement par processus/activité quels documents archiver, et indiquant éventuellement les documents manquants. Ce plan sera l'outil unique de l'utilisateur. Pour le SAE, ce plan sera complété d'un outil de classement centré sur la gestion de la conservation : par grandes catégories de documents présentant des caractéristiques homogènes d'archivage (durée, événement déclenchant le calcul de la durée, sort final).

2.5 Les durées de conservation

2.5.1	Rôle de la **durée de conservation** ?	Attribuer à chaque document archivé une durée de conservation et un sort final est un des fondamentaux du records management pour pouvoir gérer la sortie du système à terme. Ces éléments peuvent être attribués à chaque document ou objet de données archivé mais peut aussi être attribués à tout un ensemble (toute une classe ou toute une catégorie) de documents ou d'objets, chaque élément de l'ensemble héritant de ses attributs. L'attribution d'une durée de conservation à chaque document ou objet de données archivé n'est pas acquise quand on parle aujourd'hui d'archivage ; cette approche est indispensable dans un guide d'archivage selon MoReq.
2.5.2	Quelles durées ?	Elles vont de 1 an à un siècle (façon de dire qu'il n'y a pas de limite dans le temps). Attention à la tendance de raccourcir les durées du conservation sous prétexte qu'on ne sait pas garantir la conservation des documents électroniques sur le long terme. Un même document peut être visé par plusieurs durées (selon le contenu et en fonction des services qui ont à utiliser le document).
2.5.3	Durée de conservation et **durée de vie des**	La durée de conservation est basée sur des contraintes juridiques ou fonctionnelles, en aucun cas sur des contraintes

	supports	techniques de conservation physique des supports. L'outil d'archivage doit permettre de gérer l'état des formats et des supports afin que la durée effective de l'enregistrement sur les supports corresponde à la durée de conservation du document, le cas échéant en utilisant un outil de conversion de format et/ou en réalisant des migrations technologiques visant les supports. La durée de conservation, les performances souhaitées, le niveau de sécurité technique ou juridique que l'on souhaite garantir ainsi que l'évaluation des risques inhérents à la perte d'une archive ou à l'incertitude quant à sa valeur probante représentent autant de facteurs qui influeront sur le choix du mode de conservation.
2.5.4	Durée de conservation et **délai de prescription**	La durée légale de conservation, attachée à un type de document (ou à un type de dossier ou à chaque rubrique du plan de classement), est énoncée dans les textes ou dans la réglementation en vigueur dans chaque pays. Les archives de valeur patrimoniale sont conservées au-delà, sans limitation de durée. *Nota bene* : de très nombreux documents ne sont visés directement par aucune durée légale de conservation. Le délai de prescription est lié à des actions juridiques qui peuvent être entreprises en fonction d'opérations spécifiques. Exemple : Construction immobilière : le bénéficiaire dispose d'un délai pouvant aller jusqu'à trente ans pour demander réparation s'il estime être victime d'une malfaçon ; dans le dossier lié à l'opération, il se trouvera des documents ayant leur propre durée de conservation (ex : factures conservées 10 ans) mais qu'il faudra éventuellement conserver plus longtemps pour répondre au délai de prescription de l'action tracée dans le dossier.
2.5.5	Comment évaluer la durée de conservation des documents ?	La probabilité est-elle forte – que survienne un contentieux concernant les documents ou qu'on ait des doutes sur leur intégrité ? – que l'enjeu soit important ? – que cela survienne longtemps après la création des documents ? – que les documents eux-mêmes aient un rôle décisif dans la résolution du contentieux ou la levée des doutes ?

2.5.6	Quel contexte de création des documents/données et quelle réutilisation future ?	Y a-t-il ou non proximité entre le contexte de création des documents et le contexte de leur réutilisation – dans l'espace (même pays, même langue, etc.) ? – dans le temps ? – en termes institutionnels (même organisme, même réglementation, même communauté professionnelle, etc.) ? Plus la proximité sera grande, plus il y a de chances que la crédibilité des documents électroniques ne soit pas mise en doute ou puisse être vérifiée par d'autres voies (recours à des documents sur papier, témoignages, recoupements, etc.)
2.5.7	Durée de conservation des **copies** ?	Il y a nécessité de maîtriser l'existence de copies et de gérer les copies en même temps que l'original ou le document de référence, particulièrement en cas de destruction obligatoire à échéance de la durée de conservation : si l'original est détruit et que des copies subsistent, l'obligation de destruction n'est pas satisfaite. Dans certains cas, si la durée d'utilité pratique (valeur d'information) excède la durée de conservation légale, ou encore si le risque de remplacement de l'original par une copie est faible, il peut être envisagé de garder une copie numérique de substitution et de détruire l'original papier, de conservation plus coûteuse et d'accès plus difficile.

2.6 Les métadonnées

2.6.1	Qu'est ce que les **métadonnées** ?	Les métadonnées : dans le contexte du records management et de d'archivage, elles sont définies comme les 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 crées (définition de travail du Forum « Archivage des métadonnées »).
2.6.2	Des métadonnées pour quoi faire ?	Les métadonnées ont pour rôle de : ▪ gérer le cycle de vie (savoir combien de temps on doit conserver l'information, à quelles autres informations elle est rattachée, quand on peut la détruire), ▪ gérer les droits d'accès, ▪ gérer la recherche, ▪ gérer l'authenticité du document (valeur de preuve) ou simplement la fiabilité des données (valeur d'information) ?, ▪ assurer la traçabilité, ▪ exploiter le document dans son contexte.
2.6.3	Métadonnées ou attributs ?	Le mot « métadonnées », malgré son développement, semble surtout familier aux professionnels de l'information ; les

		informaticiens et les qualiticiens utilisent peu ce terme auquel il préfère celui d'attributs. Cette remarque pose le problème du vocabulaire commun entre informaticiens et archivistes ; de gros progrès ont été faits (au sein du groupe PIN[3] par exemple) mais il y encore de nombreuses incompréhensions (notions de volume, de classement, etc.) qui font que parfois des personnes très diplômées se trouvent totalement déstabilisées par un vocabulaire qui leur est étranger (insécurité intellectuelle).
2.6.4	Quelles exigences pour les métadonnées ?	MoReq propose une liste de 24 points très généraux ou très spécifiques – 16 obligations (doit) et 8 options (devrait) . Exemples : obligation ne pas limiter le nombre de métadonnées, sur les formats acceptés, sur la possibilité d'extraire des métadonnées au moment de la capture dans le SAE. L'héritage de métadonnées du plan supérieur est présenté comme une option. Le SAE doit accueillir des métadonnées par validation, par choix dans une liste de valeur ou par héritage.
2.6.5	Quelles métadonnées ?	Les exigences formulées par MoReq (section 12.1) demandent à être personnalisées : le SAE utilise les métadonnées qui permettent le bon usage des fonctionnalités définies dans le reste des spécifications ; le SAE comporte des fonctions pour la validation, l'héritage et les valeurs par défaut lors de la capture des métadonnées. MoReq donne des listes de métadonnées fonctionnelles pour chacun des niveaux de classement, sur 4 niveaux (plan de classement, dossier, sous dossier, document) mais les listes ne reprennent pas les valeurs héritées. D'une manière générale, il serait préférable de disposer d'une méthode plutôt que de listes : une typologie de métadonnées selon les tâches, par exemple pour l'indexation, la conservation, la restitution, l'exploitation – ces détails dépassent le cadre des spécifications de la version actuelle de MoReq.
2.6.6	Que reprendre de **MoReq** ?	Présentation des objets d'information dans une arborescence. Essai pour lister les métadonnées indispensables. Recommandations pour les fonctionnalités des logiciels (héritage).
2.6.7	Qu'est-ce qui manque à MoReq ?	Absence d'une démarche d'identification et de définition des métadonnées à mettre en œuvre. Rien sur la maintenance des métadonnées dans le temps et leur enrichissement ; or, le maintien et l'enrichissement des listes par de nouvelles métadonnées sont indispensables. Il y a des métadonnées appropriées à chaque moment du cycle de vie.

[3] Groupe de travail "Pérennisation des Informations Numériques" : http://vds.cnes.fr/pin/

		Voir : ▪ les travaux de l'AIIM sur les métadonnées (www.aiim.org) ▪ la Journée d'information AFNOR/CG46, mardi 7 juin 2005, Bibliothèque nationale de France http://www.bnf.fr/pages/infopro/journeespro/no-Afnor2005.htm ▪ les profils de métadonnées gouvernementaux du Québec (http://www.anq.gouv.qc.ca/conseil/crggid/crggid_outil.htm)
2.6.8	**Métadonnées de gestion documentaire ou métadonnées d'archivage** ?	Il y a des ambiguïtés entre métadonnées du système d'archivage et métadonnées du système de production : Ce ne sont pas les mêmes, mais certaines peuvent être communes. Les outils informatiques devront permettrent la récupération automatique de ces données communes. L'AIIM travaille à un rapprochement EDMS/ERMS (*electronic document management/electronic records management*). Voir aussi les travaux de l'UNCEFACT (United Nations Center for Trade Facilitation and Electronic Business) sur les échanges électroniques.
2.6.9	Quel recoupement entre **données et métadonnées** ?	La distinction entre données et métadonnées est parfois délicate dans la mesure où un certain nombre de données sont aussi des métadonnées (auteur, date…). D'un côté, pour certains documents structurés (Ex : base de données comptable, base de documents au format XML), dissocier les métadonnées du document apparaît à première vue comme inutile dès lors que le document contient toutes les données sur lui-même et sur son contexte de production. De ce point de vue, les métadonnées seraient appelées à disparaître en tant que telles. Par exemple, pour une base de données comptable, on pourrait ainsi considérer que les données d'un exercice constituent un seul objet et que toutes les données sont des métadonnées de description ou de gestion. D'un autre côté, on peut considérer que la traçabilité (nécessaire notamment en comptabilité) et la gestion de l'archivage consistent en métadonnées, *a priori* non présentes dans le document.
2.6.10	**La création de métadonnées est-elle contradictoire avec la recherche « plein texte » ?**	Structurer les métadonnées permet d'en contrôler la complétude (champ obligatoire ou non), la fiabilité (contrôle de format, contrôle de la valeur (valeur dans une fourchette, sur la base d'un vocabulaire contrôlé, …). De nombreux outils de recherche associent aujourd'hui recherche sur structure et recherche « plein texte ». Le choix du moteur de recherche devra tenir compte du corpus des documents exploités, ainsi que des types de questions

		posées. Ex : si la personne qui interroge un corpus d'archives cherche une information précise (une date, un identifiant, …) qu'elle connaît, une recherche sur structure est suffisante. Si les recherches portent aussi bien sur des éléments précis et connus, que sur des recherche d'information, une combinaison recherche sur structure + « plein texte » est souhaitée.
2.6.11	Quelles sont les relations entre les métadonnées et le plan de classement ?	Les métadonnées décrivent un document existant. Les rubriques du plan de classement constituent un cadre préexistant aux documents gérés. Le rattachement à une rubrique du plan de classement constitue l'une des métadonnées d'un dossier ou d'un document.
2.6.12	Quelle est la relation entre les métadonnées des outils de production (ERP, CRM…voire bureautique) et les métadonnées d'archivage ?	Les métadonnées de production et les métadonnées d'archivage ont des données communes notamment celles qui identifient le document (titre, auteur, etc.), et des données spécifiques destinées à la gestion de la production d'une part et la gestion de l'archivage d'autre part. Si les métadonnées d'archivage étaient un cumul de toutes les métadonnées utiles de tous les outils de production, la liste serait démesurée et pour partie inutile ; d'où l'opportunité de créer un modèle de métadonnées pour normaliser la structure.
2.6.13	Que dit **la norme ISO23081** ?	La norme ISO 23081 définit le cadre de structuration des métadonnées du « records management ». Ce modèle générique définit 5 classes de métadonnées comprenant chacune 6 rubriques. Les 5 classes sont : le document (record, y compris le format), les règles et politiques, les acteurs, les processus métier (activités métier), les processus Records management. Les 6 rubriques sont : identité, description, événements à venir, historique, relation, utilisation.
2.6.14	Qu'est-ce qu'un **jeu de métadonnées** ?	C'est la liste des métadonnées obligatoires ou optionnelles pour un type ou une catégorie de document.
2.6.15	Faut-il définir plusieurs jeux de métadonnées selon les types de documents/données gérés ?	Oui, si on veut automatiser la capture des documents à partir d'applications diverses et l'attribution de métadonnées à des documents de natures différentes.
2.6.16	**Comment organiser l'héritage de métadonnées ?**	Par le biais du plan de classement ou par une opération manuelle de lien, lors de l'archivage.
2.6.17	Faut-il détruire les métadonnées lors de la **destruction** des données ?	Cela dépend des besoins de traçabilité et des contraintes liées à la protection de la vie privée.

2.7 Exemple n° 1 - plan de classement par activité de la Commission européenne

Plan de classement de la Commission européenne basé sur ses activités, présenté au groupe de travail MoReq par Eric Pichon (le 15 décembre 2005)

Contexte
Dans le cadre de la réforme administrative et de l'avancée vers une "Commission en ligne", la Commission européenne met en place une nouvelle politique en matière d'archivage électronique et d'administration des documents ("e-Domec" : Electronic Archiving and Document Management in the European Commission) 4
L'une des premières réalisations de cette nouvelle politique a été la mise en place d'un plan de classement commun à l'ensemble de la Commission européenne.

Structure du plan de classement
Le plan de classement de la Commission européenne est une structure hiérarchique, basée sur les activités de la Commission Européenne. Le plan est divisé en 10 classes au sens de Moreq (10 rubriques principales subdivisées en sous-rubriques).
Le Secrétariat général a défini les trois premiers niveaux du plan de classement de l'Institution, appelés "nomenclature commune".
La nomenclature commune sert de base à la définition des niveaux suivants du plan de classement, appelés « niveaux spécifiques ». Ceux-ci sont définis et gérés par les DG en tenant compte de la spécificité de leurs activités. Ils se rattachent au dernier niveau de la nomenclature commune. Dans chaque DG, le/la Responsable de la gestion des documents (DMO, *document management officer*) est chargé(e) de la maintenance des niveaux spécifiques.

Rubrique/Dossier
La gestion du classement repose sur une distinction claire entre le plan de classement proprement dit et les dossiers qui s'y rattachent.
Les rubriques du plan de classement correspondent à des activités à vocation permanente. Les rubriques sont gérées uniquement par le Secrétariat général et les DMO. Un dossier correspond à une action précise ayant un début et une fin et est géré directement par les agents responsables de l'action en question.

Un document peut être classé dans plusieurs dossiers, tandis que chaque dossier doit être rattaché à une et une seule rubrique terminale (i.e. qui n'a pas de sous-rubriques) du plan de classement.

Extrait du plan de classement (rubrique 2 – niveaux supérieurs)

2	**Avenir de l'Union et questions institutionnelles**	
		Direction générale (DG) compétente
2.01	*Gouvernance et développement institutionnel*	
2.01.01	° Gouvernance	Secrétariat général (SG)
2.01.02	° Constitution	SG

[4] Décision 2002/47/ CE, CECA, Euratom de la Commission européenne sur l'administration des documents. Cette réforme a pour but d'assurer une meilleure efficacité dans la gestion des dossiers et une meilleure transparence vis-à-vis des organismes de contrôle et des citoyens.

2.01.03		°	Comitologie, subsidiarité et autres questions institutionnelles	SG
2.01.04		°	Mieux légiférer	SG
2.02		*Relations avec la société civile, transparence et information*		
2.02.01		°	Relations avec la société civile	SG
2.02.02		°	Gestion des subventions pour les organisations d'intérêt général européen	DG Education et Culture (EAC)
2.02.03		°	Transparence et accès aux documents de la Commission	SG
2.02.04		°	Déontologie	SG
2.02.05		°	Protection des données	SG
2.02.06		°	Archives historiques	SG
2.02.07		°	Rapport général et bases de données	SG
2.02.08		°	Multilinguisme	DG Traduction (DGT) DG Interprétation (SCIC)
2.02.09		°	Dialogue avec les religions et les courants humanistes	GOPA DG Conseil politique
2.03		*Élargissement*		
2.03.01		°	Négociations d'adhésion	DG ELARG, DG opérationnelles
2.03.02		°	Relations bilatérales et stratégie de adhésion	DG ELARG, DG opérationnelles
2.03.03		°	Instruments financiers pour les pays en phase de adhésion	DG ELARG, DG opérationnelles
			...	

2.8 Exemple 2 - Plan de classement par fonction du document (Gouvernement du Québec)

Contexte
Le gouvernement du Québec développe un Cadre de Référence Gouvernemental en Gestion Intégrée des Documents (CRGGID). Il s'agit de modèles génériques destinés à soutenir les activités de gestion documentaire des services gouvernementaux. Ce cadre est également proposé aux entreprises et aux citoyens.

Ce projet s'appuie sur les pratiques et outils existants, et cherche à établir une cohérence entre des outils différents, notamment le plan de classification des dossiers et le thesaurus thématique.

Structure du plan de classement

Le plan de classement général est composé de trois « facettes » : le Domaine/objet, le Processus/activité et le Type de document. Chacune des facettes a une structure hiérarchique, et représente une branche du plan de classement appelée « schème de classification ».

Le schème de classification Domaine/objet ou « domaine d'affaires » couvre 9 grands territoires de réalités sociales qui sont reconnues d'intérêt public (Des sources externes : canadienne, britannique, australienne, néo-zélandaise, ont été étudiées de manière comparative)

Catégories de domaine/objet	**Missions gouvernementales**
Ressources naturelles, agriculture, environnement	Économie et environnement
Économie, finances, industrie et entreprise	Économie et environnement
Loi, justice et droit	Gouverne et justice
Gouvernance, politique et administration publique	Gouverne et justice
Éducation et emploi	Éducation et culture
Information, culture et communication	Éducation et culture
Tourisme et loisirs	Éducation et culture
Santé et services sociaux	Santé et services sociaux
Soutien aux personnes, familles et communautés	Soutien aux personnes et aux familles

Extrait du schème de classification Domaine/objet

Gouvernance, politique et administration publique
- Gouvernance
  - Assemblée nationale
  - Élection
  - Législation
  - Relations internationales
  - Politique municipale
  - Politiques
- Administration publique

Ressources naturelles, agriculture, environnement
- Ressources naturelles
  - Pêcherie
  - Énergie
  - Foresterie
  - Mine
  - Territoire…
- Agriculture

Le schème de classification Processus/activité ou « plan de classification du ministère ou de l'organisme »
Cette facette est celle de la structure fonctionnelle des affaires. Structure hiérarchique destinée à classer les document dans les bons dossiers qui permet aussi de regrouper les documents papier et numériques, elle est généralement élaborée, mise à jour par l'unité administrative de gestion documentaire. .
Le calendrier de conservation qui regroupe les règles de conservation déterminées pour l'ensemble des documents et des dossiers s'appuie sur ce schème.

Une partie de cette structure est semblable dans tout ministère en raison de l'obligation de respecter des règles communes. On a identifié un groupe de 8 processus administratifs communs qui sont :

1. gestion des ressources humaines
2. gestion des ressources financières
3. gestion des ressources matérielles
4. administration et gestion
5. législation et réglementation
6. gestion des documents
7. communications

8. technologies de l'information

Pour les 8 processus identifiés une structure de noms de dossiers est proposée qui représente 4 étapes : 1) planification et évaluation des besoins, 2) acquisition des ressources, 3) gestion, utilisation et maintien des ressources, 4) renouvellement, disposition ou remplacement des ressources.

L'autre partie qui compose le Plan de classification est constituée des processus propres à un ministère donné.

Extrait du plan de classification Processus/activité

ADMINISTRATION ET GESTION

1. Planification administrative

Planification stratégique : Processus de prise de décision à long terme par lequel une organisation détermine ses choix stratégiques et les programmes d'action visant à assurer la mise en œuvre de ces choix.

- • Objectifs
- • Orientations

Planification des activités : Prévision des moyens à mettre en oeuvre pour atteindre les objectifs fixés par la planification stratégique (se limiter aux activités administratives générales à l'exclusion des objets de planification bien identifiés)

2. Organisation administrative

• Historique et constitution de l'organisation
• Mission et mandats
• Structure administrative
• Plan d'organisation
• Plan de délégation

3. Direction administrative

• Réunions administratives (statutaires)
• Comité (réunions thématiques)
• Cadre normatif (inclure décisions du Conseil des ministres, décrets, CT, politiques, directives, procédures)

4. Contrôle administratif

• Évaluation de programmes (contrôle de la qualité, etc)
• Rapports - bilans - statistiques
• Vérification interne
• Vérification externe

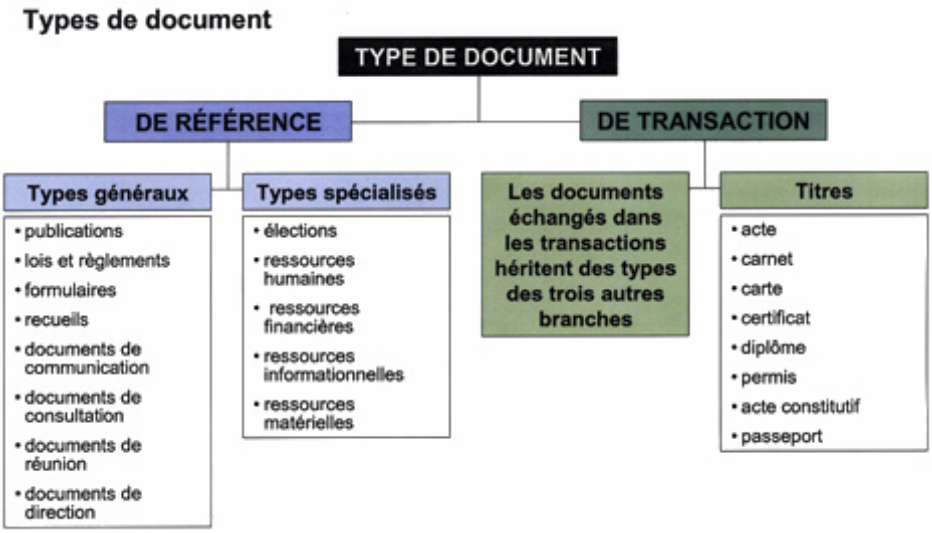
Le schème de classification Type de document

Cette facette est celle qui prend en compte la nature spécifique du document numérique. Elle distingue deux types de documents :

- **le document de référence** : document permettant d'acquérir une information générale pertinente quant à la réalisation d'un processus de travail.
  Par exemple, des études, des publications, des informations publicitaires, des spécifications techniques, des catalogues et des répertoires.
- **le document de transaction** : document établissant certaines informations relatives à un échange entre deux parties et liant par signature une responsabilité de portée juridique ou financière entre ces dernières.
  Par exemple, une déclaration de revenus ou une demande de renouvellement de permis de conduire soit sur papier, soit par service en ligne.

Pour ces documents dans le contexte numérique, l'attention est portée à la valeur probante.

Chacun de ces types de documents est subdivisé en catégories :



Pour les documents de transaction, une catégorie particulière « Titres », désignent les documents de transaction ayant une valeur juridique d'attestation.

Le plan de classement et la gestion des documents

La réflexion menée par le gouvernement du Québec aboutit à 3 profils de métadonnées qui correspondent à l'une des 3 classes d'objet suivantes : document de référence, document de transaction et dossier. Le dossier étant un regroupement de documents portant sur un sujet ou un thème donné. En général, un document est rattaché à un dossier, lequel est relié à un item du plan de classification Processus/activité.

Le cadre de référence CRGID impose que tout document ou tout dossier soit obligatoirement classé selon les trois « facettes » du plan de classement :
- l'attribut Type de document
- l'attribut Domaine/objet indique le sujet ou thème général de la ressource
- l'attribut Processus/classification qui indique la rubrique du plan de classification des dossiers.

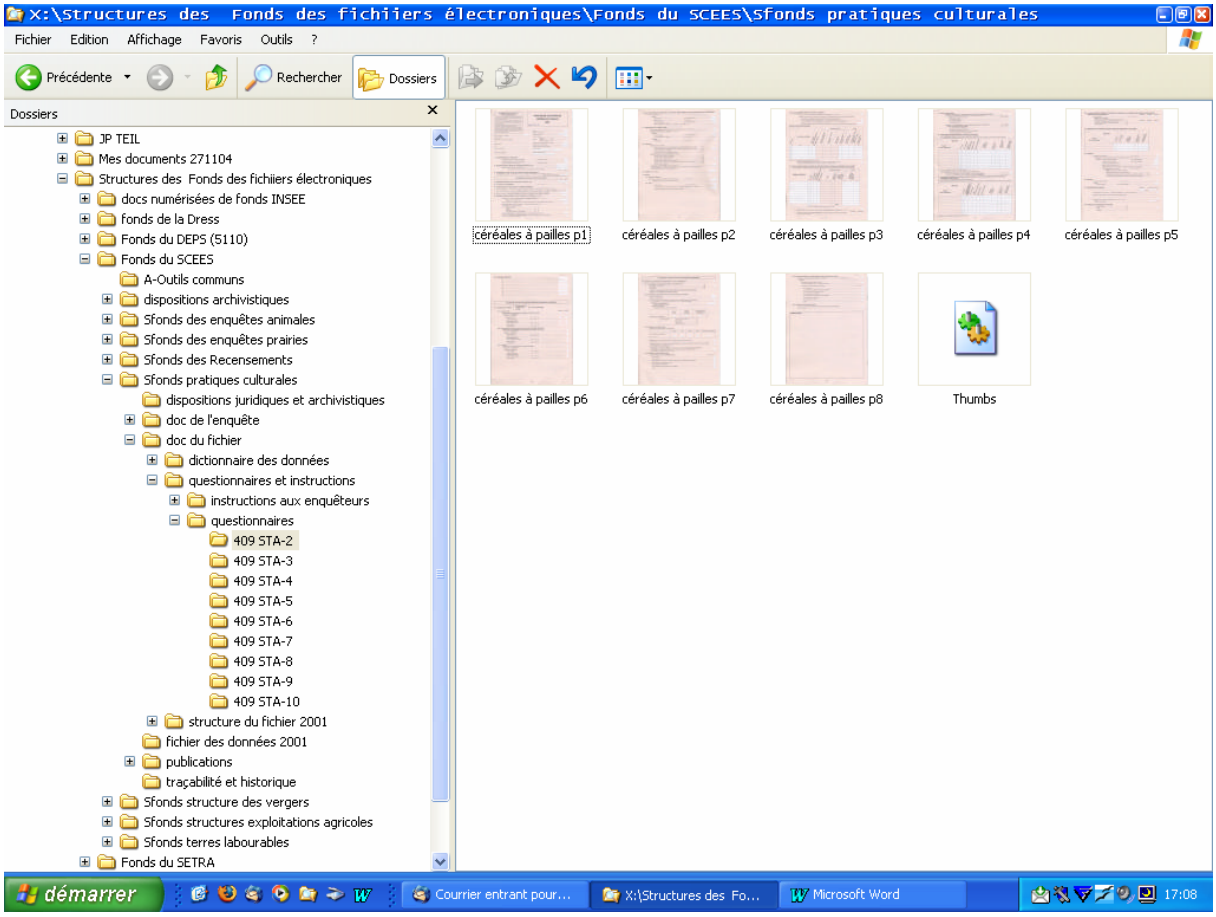
Relation entre le plan de classement et le Thesaurus

Le Thésaurus est une base sémantique pour décrire l'activité du gouvernement et classifier son information. Pour chaque terme on trouve une catégorie générale d'appartenance, une définition et les autres termes qui peuvent être ses équivalents et ses associés.
Le thesaurus fournit ainsi la documentation de tout élément du plan de classement.
Le plan de classement a une existence distincte du Thésaurus.

Annexes : Sources
Archives nationales du Québec : http://www.anq.gouv.qc.ca/conseil/crggid/crggid_outil.htm

2.9 Exemple 3 - Structuration des fonds au Centre des archives contemporaines (Fontainebleau)

Le plan de classement des fonds d'archives du CAC part du principe que s'agissant de fonds ouverts et donc en accroissement, de documents et fichiers de données, la représentation à la fois de la provenance, des activités concernées (ici les enquêtes de statistiques agricoles au niveau national) , des versements et de leurs compositions structurelles peut être avantageusement appréhendée par les différents acteurs (services producteurs, archivistes, chercheurs/lecteurs) depuis l'écran d'un poste de travail.
Dans cet exemple, on a déroulé une des branches de l'arborescence du versement de l'enquête statistique sur les pratiques culturales en 2001 en France.
La provenance n'est indiquée que partiellement puisque le niveau le plus haut, le ministère, n'apparaît pas ici. Mais cet exemple reste valable à ce niveau.
L'un des points importants de cette structuration est le nommage des différentes branches et des feuilles terminales qui doit être le reflet le plus fidèle possible des noms des activités, des fichiers, des dossiers et des documents en général utilisés par le service producteur. Un autre point, qui peut paraître déroutant, est le fait que ces arborescences sont dynamiques dans le temps par effet d'accroissement des fonds et parties de fonds. Il n'y a guère de retrait de branches puisqu'il s'agit de conservation historique dans la quasi totalité des cas.



2.10 Exemple n° 4 – Métadonnées pour les études du ministère de l'Equipement

Le projet de modélisation des rapports d'études avec la feuille de style Erélé, conduit par le Point d'Appui National Documentaire (PANDOC) du CETE Nord Picardie a pour objectifs :

- de mieux valoriser les rapports produits au sein du Ministère ;
- de constituer la mémoire du ministère.

Le document XML et les métadonnées qui en résultent doivent donc être adaptés aussi bien à la diffusion multi- supports qu'à l'archivage.

Le projet de modélisation des rapports c'est :

- un outil d'aide à la rédaction des rapports qui s'appuie sur l'utilisation d'une feuille de style Word ou Open Office intégrant les normes en matière de rapports et les contraintes de la charte graphique.
- un guichet de conversion qui permet de transformer un rapport, rédigé à l'aide de notre feuille de style au format HTML et / ou PDF.
- une valorisation pérenne des rapports dans les bases de données du ministère, qui restera accessible en ligne durablement sur l'Intranet.

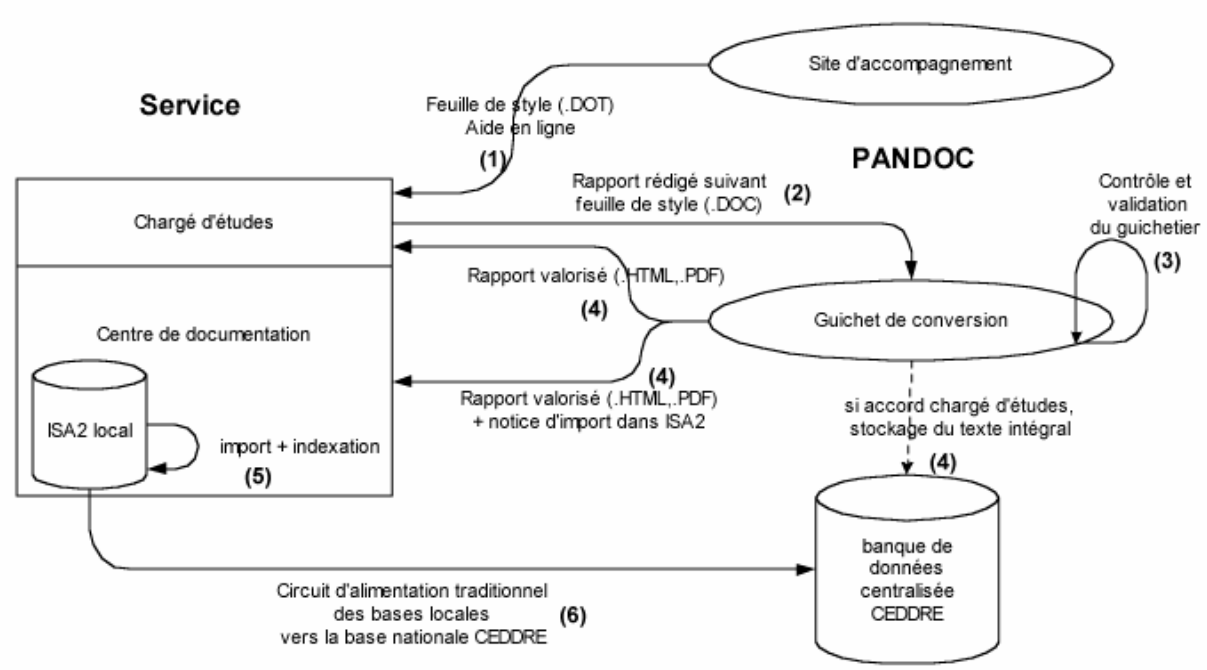
Les objectifs

Les objectifs sont d'une part de mieux valoriser les rapports, notamment au travers d'interfaces de recherches documentaires permettant la consultation en ligne du texte intégral, et d'autre part de constituer la mémoire du ministère.
Il s'agit de **mettre en place une chaîne entièrement numérique pour gérer les rapports** : de la production à l'archivage, en passant par la diffusion.
Au début de la chaîne, lors de la production du rapport, on utilise une feuille de style Word ou Open Office ad hoc. Conçue pour intégrer les contraintes de structure et de présentation des rapports du ministère, elle rend possible la création d'un document structuré.
A l'autre bout de la chaîne, on utilise un convertisseur, qui permet de transformer le document Word ou Open Office en un format pivot adapté à la diffusion multi-supports comme à l'archivage.

Feuille de style et chaîne de conversion

C'est l'utilisation d'une feuille de style adhoc qui rend possible cette conversion (basée sur des outils issus du monde des logiciels libres). Elle permet en effet en appliquant des styles à des parties de documents, de structurer typographiquement les rapports. A partir de cette structure superficielle, le convertisseur (sur le principe : à un style correspond une paire de balises) va produire un document XML au contenu réellement structuré, conforme au modèle.
Par ailleurs, la feuille de style constitue, en elle-même une aide à la rédaction : en intégrant d'une part une structure par défaut et d'autre part les contraintes de charte graphique, elle supprime la corvée de la mise en page, tout en laissant une assez grande liberté au rédacteur.
Cette chaîne de production (la feuille de style et le convertisseur) a vocation à être utilisée par l'ensemble des chargés d'étude du Ministère de l'Équipement pour la production de leurs rapports.

Utiliser la feuille de style c'est donc s'intégrer dans un processus de production, de diffusion, de valorisation et de conservation représenté ici :



récupérer la feuille de style sur le site d'accompagnement (le présent site Erele) puis rédiger le rapport en respectant la structure de la feuille de style.

- une fois le rapport terminé (ou durant la rédaction afin de contrôler la bonne utilisation de la feuille de style), le soumettre au guichet de conversion des rapports.
  Si vous le souhaitez vous pouvez éventuellement corriger les problèmes de structure (respect du modèle défini pour les rapports) vous-même ou passer la main à l'assistant chargé de la conversion.
- le guichetier contrôle la structure du fichier et valide le rapport.
- une fois le rapport validé par le guichetier, le chargé d'études récupère une version Word, une version HTML et une version PDF sur son poste.
- avec l'accord explicite du chargé d'études le Pandoc conserve un exemplaire électronique du rapport et envoie les versions HTML et PDF ainsi qu'une notice documentaire (format ISA2) pré remplie décrivant le rapport au centre de documentation dont dépend le rédacteur.
- le documentaliste intègre la notice ISA2 dans sa base documentaire et si l'accord a été donné la lie au texte intégral du rapport, désormais accessible, via l'interface web documentaire sur l'intranet du service.
  Il complète l'indexation de la notice.
- la notice est transférée dans la base de données des rapports et études du ministère : Ceddre où (si l'accord a été donné) le lien entre la notice et le texte intégral est fait.
  Le rapport est accessible, via l'interface web de recherche de la base Ceddre

Les métadonnées d'Erélé

La conversion du fichier Word formaté avec la feuille de style crée un fichier XML conforme à la DTD **DOCBOOK**. Certaines de ces métadonnées sont ensuite utilisées pour la création de notices bibliographiques conformes aux bases de données documentaires ISA2 du Ministère (D'abord les bases des centres de documentation puis CEDDRE qui centralise les données de ces bases).
Voici les métadonnées constituant le bordereau « documentaire » en tête des rapports constitués avec cette feuille de style :

Bordereau Documentaire

à rédiger par l'auteur du document
Le bordereau documentaire est inclus en tête du rapport. Il permet de mieux diffuser les informations sur les rapports à travers les banques de données et les cédéroms, les catalogues sur Internet et Intranet, les publications, les annuaires...

Informations du document	
Titre	

Numéro de Volume	
Sous-titre	
Numéro de fascicule	
Collection	
Sous-collection	
Mots-clés	
Mots-clés géographiques	
Autres informations bibliographiques	
Date du document	
Auteurs	
Auteur N°1	
Prénom	
Nom	
Rôle	
Qualité	
Nom de l'organisme d'affiliation	
Sigle de l'organisme d'affiliation	
Division de l'organisme d'affiliation	
Coordonnées de l'auteur	
Organisme Auteur	
Organisme Auteur N°1	
Nom de l'organisme	
Sigle de l'organisme	
Nom de la division	
Adresse	
Ville	
Région ou département	
Numéro de téléphone	
Numéro de fax	
Adresse mail	
Adresse du site web	
Organisme Auteur N°2	
Nom de l'organisme Point d'Appui National Documentaire	
Sigle de l'organisme PANDOC	
Nom de la division	
Adresse	
Organisme Commanditaire	
Organisme Commanditaire N°1	
Nom de l'organisme	
Sigle de l'organisme	
Nom de la division	
Adresse	
Code postal	
Ville	
Région ou département	
Numéro de téléphone	
Numéro de fax	
Adresse mail	
Adresse du site web	
Informations Contractuelles	
Statut du rapport	
Nature du rapport	
Conditions d'accès	
Date de révision des conditions d'accès	

Numéro de contrat	
Numéro d'affaire	
Numéro du chapitre budgétaire	
ISRN	
Programme	
Résumé	

Le tableau qui suit liste les métadonnées de DOCBOOK utilisées, et leur concordance avec les métadonnées utilisées par les bases documentaires :

ISA2	**Notes**	**DOCBOOK**
DOC_TITRE		bookinfo/title
		:
		bookinfo/subtitle
		(vol n°
		bookinfo/seriesvolnums
		)
		(fasc. n°
		bookinfo/volumenum
		)
DOC_AUTEUR	multivalué	bookinfo/authorgroup/author/surname
		(
		bookinfo/authorgroup/author/firstname
		)
DOC_AUTMORAL		bookinfo/authorgroup/corpauthor/affiliation/orgsigle
		;
		bookinfo/authorgroup/corpauthor/affiliation/orgname
DOC_SOURCE		bookinfo/publisher/address/city
		:
		bookinfo/publisher/publishername
		,
	les 4 derniers caractères	bookinfo/date
		.-
		bookinfo/pagenums
		bookinfo/pagenums/@unit
		, p.
		bookinfo/pagenums/@page-width
		x
		bookinfo/pagenums/@page-height
DOC_DL		bookinfo/keywordset/keyword
DOC_DIF	Libre, controlée, confidentielle	copyrights-legalnorice/@diffusion
DOC_AB		bookinfo/abstract
DOC_COMMENT		(
		bookinfo/bibliomisc
		; Etude réalisée par
		bookinfo/authorgroup/author/affiliation/orgdiv
		(
		lot/voltitle
		)
		)
EQ_LOCGEO		bookinfo/keywordset/keyword/@geo
EQ_FINANCEUR		bookinfo/contractsponsor
EQ_ISRN		bookinfo/biblioid[@otherclass='isrn'
DOC_PER_DPAR		bookinfo/date

DOC_DP	les 4 derniers caractères	bookinfo/date

2.11 Exemple n° 5 – Métadonnées pour les dossiers d'accréditation à la Haute Autorité de Santé (HAS)

Projet de métadonnées pour un compte rendu d'accréditation d'un centre de rééducation fonctionnelle (CRF). Le " compte rendu d'accréditation " résulte d'une procédure d'évaluation externe d'un établissement de santé (hôpital ou clinique), conduite par la HAS. Cette procédure vise à développer les actions relatives à la qualité et à la sécurité des soins au sein de chaque établissement. Ce compte rendu présente les résultats de la procédure engagée par l'établissement. Une liste de métadonnées est proposée pour un compte rendu d'accréditation.

Projet de métadonnées pour un compte-rendu d'accréditation.

Ex : CRF DIVIO

Liste des métadonnées de description à renseigner pour les fichiers :

- **Titre ou intitulé du document :** compte-rendu d'accréditation du centre de rééducation fonctionnelle DIVIO
- **Description brève du contenu et du contexte de production :** Le compte rendu d'accréditation contient les informations suivantes : la présentation de l'établissement de santé, le déroulement de la procédure d'accréditation et les conclusions du Collège de l'accréditation sur la situation de l'établissement. Ces conclusions mettent en évidence d'une part une synthèse selon les 10 référentiels, d'autre part une synthèse selon trois orientations stratégiques définies par le Collège de l'accréditation : la satisfaction des besoins du patient, la maîtrise des situations à risque et la dynamique de gestion de la qualité.
  Le " compte rendu d'accréditation " résulte d'une procédure d'évaluation externe d'un établissement de santé (hôpital ou clinique) conduite par la HAS. Cette procédure vise à développer les actions relatives à la qualité et à la sécurité des soins au sein de chaque établissement. Ce compte rendu présente les résultats de la procédure engagée par l'établissement.
  L'accréditation est un moyen pour inciter l'ensemble des professionnels des établissements de santé (soignants, médecins, personnels administratifs, agents d'entretien…) à analyser leur organisation et à améliorer la qualité de la prise en charge des patients. La procédure d'accréditation est obligatoire et intervient périodiquement sauf lorsque des situations obligent qu'elle soit renouvelée plus tôt.
- **Nom du service producteur :** Service certification
- **Auteur(s) :** Haute autorité de santé (HAS)
- **Expéditeur :** HAS
- **Destinataire(s) :** diffusion sur le site www.has-sante.fr, Service Archives de la HAS
- **Date de création, modification(s) :** 11.2003
- **Date de capture :** 24.10.2005
- **Format électronique :** pdf
- **Langage des données :** français
- **Logiciel de capture et version :** Acrobat reader 5.0
- **Support électronique d'origine :** Word
- **Indexation matière :** compte-rendu d'accréditation, centre de rééducation fonctionnelle, divio, dijon, Droits et information du patient, Dossier du patient, prise en charge des patients, Management de l'établissement et des secteurs d'activité, Gestion des ressources humaines, Gestion des fonctions logistiques, Gestion du système d'information, Gestion de la qualité et prévention des risques, Vigilances sanitaires et sécurité transfusionnelle, Surveillance, prévention et contrôle du risque infectieux, recommandations.

- **Situation dans le plan de classement de l'institution :** Dossier établissement/2001-2500/2032

Liste des méta-données de gestion à renseigner :

- **Service versant :** Service certification
- **Date de transmission des données** : 24.10.2005
- **Adresse de localisation :** Base base de données Archives
- **Support électronique de conservation** :pdf
- **Volumétrie :**172 Ko
- **Droits de reproduction** : oui
- **Communicabilité :** oui
- **Durée de conservation :** 8 ans
- **Année de révision :** 2014
- **Sort final :** Versement en archives historiques

2.12 Pour en savoir plus : le groupe Sedona (USA)

Au niveau américain et international

Aux USA, les contraintes d'archivage ont été renforcées par plusieurs facteurs : lutte contre le terrorisme, bonne gouvernance d'entreprise, scandales financiers du type Enron.

Elles sont déclinées dans tout un corpus de textes législatifs et réglementaires (Sarbanes-Oxley, Patriot Act, HIPAA, etc.). La France, quant à elle, ne dispose que de 2 ou 3 textes, mais il faut tenir compte de l'extraterritorialité et du risque pénal. Les textes légaux français ne précisent pas ou peu le contexte technique ou organisationnel de la conservation des documents électroniques. Il en était déjà de même pour les documents sur support papier. Cependant, quelques éléments de jurisprudence ainsi que des Instructions réglementaires commencent à apparaître dont il faudra tenir compte.

Le groupe Sedona et ses réflexions

Le groupe Sedona a publié 2 rapports pour éclairer cette problématique.

1er rapport en janvier 2004 « Recommandations & Principes pour la production des documents électroniques »

2e rapport en mars 2005 : « Bonnes pratiques pour la gestion des documents à l'âge électronique »

Deux idées forces ressortent :

1. la notion de « reasonableness » (il ne faut pas demander l'impossible),
2. il n'y a pas de politique générale, chaque entreprise doit définir sa politique [mais il y a sans doute des éléments communs].

Texte résumé et traduit par JY Gresser :

I. Principes relatifs à la production des documents :

- Toute organisation doit veiller à la bonne conservation des documents susceptibles d'être produits lors de litiges.
- Tous les coûts relatifs à la gestion, à l'archivage et à la communication des données doivent être rapportés aux enjeux réels.
- Les parties doivent se concerter le plus tôt possible à ce sujet et fixer de même les responsabilités et les droits de chacun.

- Toute demande de consultation doit être précise quant à la nature des données et documents demandés, de même que les réponses à ces demandes en ce qui concerne les limites du faisable.
- Tout ce qui est raisonnable peut être entrepris. Il n'est pas raisonnable de demander à quiconque d'archiver toutes ses données.
- Les parties sollicitées sont les mieux placées pour évaluer les procédures, méthodes et techniques adaptées à la conservation et à la restitution de leurs données et de leurs documents.
- C'est au demandeur de prouver que l'inadéquation des mesures prises par la partie adverse.
- La source des données et des documents réside dans les systèmes dédiés, qu'ils soient d'exploitation courante ou d'archivage, et « actifs », par opposition aux systèmes de secours.
- Une demande non-justifiée n'appelle aucune obligation de réponse.
- La partie sollicitée doit rester raisonnable dans ses refus.
- la partie sollicitée sera considérée comme de bonne foi sous réserve qu'elle utilise des techniques d'indexation, de recherche et d'échantillonnage (jugées suffisamment avancées).
- A moins de nécessité, il n'est pas nécessaire d'archiver les accords entre les parties ou les injonctions de la cour.
- Dans des limites raisonnables le coût de restitution est à la charge de la partie sollicitée. Sinon il est à la charge du demandeur.
- Les sanctions doivent viser les intentions frauduleuses ou les négligences (graves ou répétées).

II. Les recommandations relatives à la gestion de l'information et des documents archivés à l'ère de électronique

1. Toute organisation doit avoir une politique et des procédures d'archivage de l'information et des documents.
2. Cette politique et ces procédures doivent être réalistes et adaptées aux enjeux réels de l'organisation.
3. Une organisation ne doit pas tout conserver de ce qu'elle reçoit ou de ce qu'elle produit.
4. Politique et procédures doivent couvrir la création, l'identification, la conservation, la recherche, le sort final ou la destruction des informations ou documents archivés
5. Politique et procédures doivent prévoir la suspension ou l'arrêt des procédures ou opérations de destruction en cas de nécessité.

Extrait de The Sedona Guidelines Public Comment Draft 2004

3 Sécurisation de l'archivage

Un SAE s'intègre dans un système d'information. Il doit se conformer aux règles, procédures et outils de sécurité mis en œuvre par ce dernier.

La sécurité des SI est un sujet plus général. On peut supposer que beaucoup des points soulevés pour l'archivage sont ou seront traités par des approches globales au niveau de l'entreprise ou de son environnement.

Cela dit, les approches courantes sont loin de répondre à la totalité des besoins. Elles sont nécessaires mais non suffisantes.

Un des points essentiels est de pouvoir se situer dans la durée, ainsi : quelle pérennité assurer à l'authenticité documents, à leur intégrité, ainsi qu'aux métadonnées qui leur sont attachées.

Il s'agit dans ce chapitre d'aborder les aspects liés à la sécurisation juridique et technique spécifique du SAE en prenant pour hypothèse que celui-ci s'intègre dans un SI qui peut être celui d'une entreprise ou d'une organisation.

A ce titre, les points qui sont traités concernent plus particulièrement les moyens mis en œuvre pour respecter des obligations juridiques et réglementaires ainsi que ceux nécessaires pour protéger, assurer et contrôler l'accès aux documents, y compris en cas d'incidents majeurs.

L'objet de ce chapitre est de rappeler les points communs, et d'insister sur les éléments spécifiques. Il s'articule autour de 4 thèmes:

- Les grands principes,
- Les notions et exigences liées à la sécurisation des documents,
- Les processus (capture, conservation, restitution) et leur sécurisation,
- Les technologies (dans une perspective sécuritaire),

Il est complété d'une table de correspondance avec MoReq et de références (pour en savoir plus).

3.1 Sécurité ou sécurisation ?

3.1.1	Que faut-il entendre par **sécurisation** ?	La sécurisation consiste à appliquer à un échange électronique un niveau de sécurité qu'il ne possède pas en natif. Ces deux termes, sécurisation et sécurité, ne sont pas encore définis juridiquement. Un "référentiel général de sécurité", annoncé par l'ordonnance du 8 décembre 2005 est en cours d'élaboration, voir : http://synergies.modernisation.gouv.fr
3.1.2	La sécurisation pourquoi faire ?	1- Protéger documents ou archives (intégrité, accès) 2- S'assurer de la conformité des documents ou des processus mis en place aux obligations légales et réglementaires 3- Créer des espaces de confiance dans l'entreprise et au-delà. http://www.ssi.gouv.fr/fr/confiance/archivage.html)

3.1.3	L'entreprise/l'institution dispose-t-elle déjà d'une **politique générale de sécurité de l'information** (données, documents[5]) ?	La sécurité des systèmes d'information est un problème pour toute entreprise, quels que soient sa taille et son niveau d'utilisation des technologies informatiques. Sa traduction dans un plan de sécurité informatique diffère néanmoins en fonction des pratiques de l'entreprise. Bâtir une politique adaptée, économiquement viable et conforme à la réglementation en vigueur suppose de pouvoir répondre aux points suivants y compris pour les documents : - Quelles sont les priorités en matière de protection ? - Quels sont les risques (externes, internes) ? - Quels sont les facteurs de risque ? La couverture de l'infrastructure de sécurité pouvant aller au-delà de l'entreprise vers les partenaires, fournisseurs ou sous-traitants, en particulier les « tiers archiveurs », les dispositifs mis en place doivent pouvoir fonctionner, être contrôlés et audités tout au long du processus ou de la chaîne d'échanges entre les parties concernées.
3.1.4	**Sécurité du SI** et archivage	Les éléments de sécurisation de l'archivage tels que le contrôle d'authenticité, l'intégrité et la traçabilité sont souvent extérieurs à la problématique de la sécurité des systèmes d'information tels que l'entendent les RSSI (responsable sécurité des systèmes d'information). La sécurité de l'archivage est toutefois une notion présente dans MoReq et indispensable à la mise en œuvre d'un système d'archivage électronique au sens du records management.
3.1.5	Les principes et systèmes généraux s'appliquent-ils à l'archivage électronique ?	Rappel : un SAE s'intègre dans un système d'information et dans un service informatique en se pliant aux règles, procédures et outils de sécurités mis en œuvre par ce dernier. Ceci est nécessaire mais non suffisant pour la conservation « de confiance » de documents électroniques à valeur probante.
3.1.6	Quel est le **niveau de sécurité** requis pour le système d'archivage ?	Le système d'archivage, partie intégrante du système d'information de l'entreprise, est au minimum aussi sécurisé que celui-ci. Il peut l'être davantage, notamment en ce qui concerne la confidentialité et l'horodatage, ou le cas des documents faisant l'objet d'une législation spécifique comme ceux classifiés « Défense ».
3.1.7	À quel moment du cycle de vie gérer la **sécurité attachée aux**	La sécurité des documents renvoie d'une part à l'identification et à l'intégrité (art. 1316-1 du Code

[5] Les informaticiens définissent au mot « document » le sens très général de « données sur un support ».

	documents ?	civil), d'autre part à la confidentialité de l'information. Ces besoins doivent être pris en charge pendant tout le cycle de vie du document, tant au plan juridique qu'au plan archivistique. La sécurité est indissociable de la **conservation.** Le degré (l'indice) de **confidentialité** est une métadonnée au moment de la capture. Les évolutions de la confidentialité (ouverture ou restriction) sont prises en compte lors de l'archivage et au cours de la phase de conservation (voir ci-dessous).
3.1.8	Quels sont les **acteurs** de la sécurisation ?	Tous les agents de l'entreprise qui créent, éditent, valident les documents (ou l'information). Selon MoReq, ces agents sont « classés », et dotés d'un « profil ». Il existe aussi des agents qui ont un rôle spécifique dans la sécurisation : administrateur(s) du système ou de la sécurité ; auditeurs. Certaines des responsabilités ou fonctions peuvent être dévolues à des « tiers ».
3.1.9	Quels sont le rôle et l'importance du **tiers de confiance** ?	Un « tiers de confiance » peut-être une « autorité » ou un « opérateur ». « L'autorité » est le porteur de la responsabilité juridique contractuelle vis à vis du donneur d'ordre. L'« opérateur » est le garant technique de des opérations qu'il réalise (collecte et conservation). Les tiers de confiance, peuvent couvrir des fonctions variées comme (liste non exhaustive) : - Tiers archiveur, - Tiers horodateur, - Tiers certificateur, - Tiers de validation.
3.1.10	Quels **instruments** pour les administrateurs et les auditeurs ?	Les contrôles (3.2.21) sont effectués sous la responsabilité d'un **administrateur** (ce qui peut constituer une différence entre un SAE et un système de GED). Ils sont plus ou moins automatisés et peuvent s'appuyer sur des outils de gestion des flux (angl. *workflow*). Les rapports (et alertes) sont à destination des contrôleurs et auditeurs divers (gestion, financier, données personnelles etc.). Les outils tels que le guide des procédures, les

		historiques, la base de données des traces (transactions, accès), etc.

3.2 Les notions et exigences liées à la sécurisation des documents

3.2.1	Quels sont les **aspects fonctionnels** de la sécurisation de l'archivage ?	Ce sont : - *L'identification ;* - *L'authentification ;* - *La signature électronique (authentification et scellement/validation) ;* - *La gestion des habilitations ou des autorisations (profil groupe d'autorisations fonctionnelles*[6]), la validation des opérations ;* - *L'historisation (historique*), la traçabilité ;* - *La sauvegarde,* - *La restauration.* Ces fonctions sont des instruments au service de la « sécurité juridique », qui repose notamment sur : - l'imputabilité, l'authenticité, - l'intégrité, la lisibilité, - la traçabilité, Ces fonctions s'appuient elles-mêmes sur des technologies adaptées (voir 3.5).
3.2.2	De quelle **identification** parle le MoReq?	De celle des documents et non de celle des acteurs. L'identification des acteurs est incluse dans la notion de « profil d'utilisateur».

[6] L'astérisque indique que les termes figurent dans le glossaire de MoReq.

3.2.3	Qu'est-ce qu'un **« acte authentique** » ?	En droit français l'expression «acte authentique » renvoie aux actes établis par les officiers publics et ministériels (notaires, huissiers) qui revêtent les signes de validation réglementaires propres à assurer l'imputabilité et la portée juridique des actes. Définition élargie depuis la loi du 13 mars 2000 : *L'acte authentique est celui qui a été reçu par un officier public ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises. Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'État.* Des pièces annexes peuvent être rattachées à un acte authentique. Il peut s'agir, par exemple, de documents annexés à un procès-verbal de constat. Ces pièces peuvent être d'origine électronique ou converties sous forme électronique par un processus de numérisation garantissant leur reproduction à l'identique. L'acte authentique s'oppose à la notion d'acte sous seing privé. A la différence d'un acte sous seing privé, l'acte authentique fait pleine foi de son origine et s'impose à la conviction du juge, sauf à considérer la procédure d'inscription de faux en écriture publique. Les systèmes d'archivage des actes authentiques sur support électronique des huissiers de justice et des notaires sont réglementés et organisés par décret.
3.2.4	Comment un document qui n'est pas un « acte authentique » peut néanmoins présenter un **caractère d'authenticité** ?	L'**authenticité** est définie par la norme ISO 15489 comme le caractère d'un document dont on peut prouver : 1. qu'il est bien ce qu'il prétend être, 2. qu'il a été effectivement produit ou reçu, par la personne qui prétend l'avoir produit ou reçu, et 3. qu'il a bien été produit ou reçu au moment où il est prétendu l'avoir été. Ainsi, du point de vue archivistique, un document sans être un acte authentique (acte sous seing privé, simple courrier voire copie) peut présenter un caractère d'authenticité. Pour éviter toute ambiguïté, il est préférable de parler de l'authenticité des documents archivés que de documents ou d'archives authentiques.

3.2.5	Quelle relation entre la notion d'**original** et la notion d'authenticité ?	Les deux notions ne se recouvrent pas. La notion d'original renvoie au processus de création du document (un original est la rédaction première du document validé et s'oppose à la copie) tandis que la notion d'authenticité renvoie à la valeur du document. L'original est plus facilement jugé authentique qu'une copie mais un faux en écriture est un original tandis qu'une copie peut être authentifiée.
3.2.6	Dans quelles conditions est établi un acte authentique sur **support électronique** ?	Les systèmes informatiques établissant les actes authentiques sur support électronique doivent être agréés. La conservation (archivage) doit être assurée au sein d'un minutier central établi et contrôlé par les organes représentatifs des huissiers de justice ou des notaires. Voir le décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires et Décret n° 2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice.
3.2.7	Pourquoi est-il nécessaire de contrôler l'authenticité au moment de l'archivage ?	Le système d'archivage peut maintenir l'authenticité du document, il ne peut apporter de l'authenticité à un document qui ne serait pas authentique à l'entrée dans le système.
3.2.8	Comment l'archivage peut-il préserver la « **valeur probante** » d'un document numérique ?	La garantie de préservation du statut d'origine du document numérique constitue l'enjeu majeur de la conservation. Les textes juridiques concernant l'écrit sous forme électronique font de la bonne conservation du document électronique l'une des conditions essentielles de sa « valeur probante ». Devant le juge se posent les questions de la recevabilité et de la force probante des documents électroniques archivés. A ce titre, l'article 1316-1 du Code civil précise que l'écrit sous forme électronique doit, pour être « admis en preuve au même titre que l'écrit sur support papier », être «établi et conservé dans des conditions de nature à en garantir l'intégrité ». Aucun texte ne précisant les critères permettant de juger de cette intégrité, il est donc nécessaire de garantir que celui à qui incombe la preuve disposera bien, au moment opportun, des moyens requis pour accéder à un document archivé et qu'il pourra démontrer l'authenticité et l'intégrité de celui-ci devant le juge pendant tout le cycle de vie.
3.2.9	Que faut-il entendre par **intégrité** ?	Au sens de la norme ISO 15489, l'intégrité d'un document renvoie au caractère complet et non altéré de son état.

		Il convient de distinguer l'intégrité technique (identité au bit près) et intégrité du point de vue informationnel dans laquelle la portée du contenu n'est en rien altéré même si la présentation a pu subir des modifications (couleur, polices de caractères,etc.). Le Droit français ne donne pas de définition de l'intégrité.
3.2.10	**Q**u'est-ce qu'une signature numérique ?	La norme ISO 7498-2 définit la signature numérique comme des "données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant[7] à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)".
3.2.11	**Q**u'est-ce qu'une signature électronique **?**	Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil. Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes : - être propre au signataire, - être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, - garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable. Une "signature électronique qualifiée" est une signature fondée sur un « certificat qualifié » et créée par un dispositif sécurisé de création de signature. (Extraits de l'article 2 de la Directive 1999/93/EC)
3.2.12	Quelles sont les particularités d'une **signature électronique** pour l'archivage ?	La signature électronique d'un document dans son sens juridique fournit une information dans la mesure où elle manifeste le consentement du signataire au contenu du document (Code civil. Art 1516-1). Elle peut aussi être considérée comme un « sceau » permettant d'attester que le document n'a pas subi d'altération.

[7] Il serait plus juste de dire fournissant des éléments de preuve et de protection…

3.2.13	Faut-il garder (archiver) les **moyens d'authentification** ?	Ce serait souhaitable mais paraît impossible sur le long terme : disparition des acteurs, obsolescence des matériels, des logiciels et/ou des applications (voir développement sur la signature électronique). Pour la conservation dans le temps, on peut admettre que l'authentification du document soit attestée par une métadonnée que le système devra tracer et stocker tout au long de la vie du document.
3.2.14	A quoi servent les **conventions de preuve** en matière de documents électroniques ?	En l'absence de dispositions légales expressément applicables à la conservation électronique de documents ou de jurisprudence sur l'applicabilité du régime juridique des copies de document à la conservation électronique, il est possible de recourir à des conventions de preuve pour faciliter la preuve et les échanges. Une convention de preuve permet aux parties de décider contractuellement d'accepter certains modes de preuve et de reconnaître la valeur probatoire des écrits électroniques qu'elles échangent et par là même les modalités de conservation de ces actes pour leur attribuer une force probante. NB : la valeur de ces conventions peut être cependant soumise à l'appréciation d'un juge.
3.2.15	Que faut-il entendre par « **confidentialité** » ?	La consultation d'un document peut être restreinte à certaines personnes ou fonctions préalablement définies. La notion de confidentialité traduit le niveau de sensibilité des informations contenues dans un document ; en fonction du niveau de sensibilité, une opération de marquage doit être réalisée et des règles suivies quant à la création, à l'enregistrement, à la diffusion, à la reproduction, à la conservation et à la destruction. La notion de confidentialité est à relier à la notion d'habilitation et, notamment, de droits d'accès. NB : dans certains cas le plan de classement peut se fonder sur des critères de confidentialité.
3.2.16	Comment gérer l'évolution de la **confidentialité** dans le temps ?	La confidentialité se gère par un rapprochement entre les habilitations (droits d'accès) des utilisateurs et le marquage des documents (voir métadonnées appelées « indices de sécurité »). La sophistication des uns et des autres peut varier d'un système à l'autre, et selon le contexte (voir le cas des données de santé). L'évolution peut se faire dans le sens d'une restriction (survenance d'un contentieux) ou dans le sens d'une ouverture (publication d'un brevet) : un « garant documentaire » est utile pour suivre les évolutions.

3.2.17	Quelles sont les particularités des droits d'**accès** pour l'archivage ?	Les droits d'accès d'un document peuvent varier dans le temps. Ainsi un document peut être considéré comme confidentiel lors de sa création, et perdre ce caractère au bout de quelques années (exemple : projet de fusion d'entreprises). Les droits d'accès sont personnels (nominatifs) ou attribués par fonction, activité, etc. Deux aspects sont à considérer : 1. l'historique des droits d'accès (qui a eu le droit d'accéder à l'information tout au long de son cycle de vie) ; 2. l'historique des accès. Cette « traçabilité » peut constituer un élément de preuve (qui a eu accès à l'information et quand). Les modalités de définition et de gestion des droits peuvent aussi varier au court du temps. Ainsi pour les archives patrimoniales, les droits sont d'abord donnés à des personnes ou des groupes à travers des profils, bases de connaissances, puis par les règles de communicabilité définies dans la loi et le code du patrimoine pour la conservation au titre des archives historiques.
3.2.18	Droit d'**accès ou** « droits d'**usage** » ?	Au-delà de l'accès à l'information, archivée ou non, se pose la question de la réutilisation que peut en faire l'utilisateur. La notion de droit d'usage vise à gérer ce qu'un utilisateur est autorisé à faire des contenus numériques auquel il a lui-même accès : usage personnel, droit de les diffuser, obligation de retransmettre l'information, etc. Les éléments descriptifs de ces droits peuvent faire partie des métadonnées. Voir : http://www.hub2b.com
3.2.19	Quel est le rôle de l'annuaire d'entreprise dans la gestion des droits d'**accès** aux informations archivées ?	Relier une fonction (ou un usage) à une information : Exemple : le service du personnel a accès aux dossiers du personnel, la Direction Générale a accès à toutes les informations (Ces points sont à préciser dans la charte ou les procédures d'archivage).
3.2.20	Quelles fonctions **piloter et contrôler**?	D'une manière générale, TOUTES les fonctions mises en place doivent être **pilotables & contrôlables** (3.2.8 et 3.2.9) tant au niveau d'un document individuel ou d'un processus particulier qu'à un niveau plus global (gestion des flux ou des stocks d'archives).

3.2.21	Quels éléments faut-il particulièrement contrôler?	Des éléments aussi divers que : • Les durées de conservation • Les accès et les profils d'accès, l'ouverture des documents, les impressions, • Les exigences légales de traçabilité et de sécurité, • La modification et le rangement des documents, • L'exécution du transfert, de l'export ou de la destruction, • La capture, • La saisie des métadonnées, • Le chiffrement et le déchiffrement, • L'accessibilité des données historisées, • La traçabilité « physique », le contrôle des mouvements, acheminements, « entrées - sorties » et accès physiques, • Le vocabulaire des termes et relations issues d'un thésaurus (conformité à ISO 2788 ou 5964), • L'administration (contrôles administratifs), • Les dossiers, • Les documents auto-modifiables, • Les messages électroniques • L'assurance qualité.
3.2.22	À quel moment aborder les **contrôles ?**	Il serait, comme partout, souhaitable que contrôles et sécurité soient pris en compte dès l'amont (dès la configuration du SAE).
3.2.23	Selon quels critères mettre en œuvre ces contrôles ?	Ces critères sont surtout liés aux risques dus à la conservation et au mode de stockage, risques de type ; - financier, - juridique, - image, - opérationnel, etc. Voir NF Z 42-013 (révision en cours) pour la prise en compte des niveaux d'exigences minimales et complémentaires.
3.2.24	**Q**ue faut-il entendre par **traçabilité** ?	La notion actuelle de traçabilité, sans être définie officiellement, couvre l'imputabilité, l'auditabilité, l'associabilité et la socialisation des risques (assurabilité). C'est une qualité du système ou de l'application permettant de suivre les évolutions fonctionnelles ou techniques au cours du cycle de vie du document et montrant le respect des caractéristiques sécuritaires exigées. Elle repose sur la possibilité de suivre les événements intervenus sur une information, un

		produit ou un service depuis sa création jusqu'à la fin de son cycle de vie. **L'identifiant unique du document en est un élément clé dont la maîtrise doit être assurée sur tout le cycle de vie.**
3.2.25	Quelle articulation entre **traçabilité et horodatage** ?	L'horodatage contribue à la traçabilité en permettant d'établir la chronologie précise des événements tracés.

3.3 Processus de capture et de destruction, et leur sécurisation.

3.3.1	**Q**u'est-ce que la **capture** ?	MoReq définit la capture comme le processus « d'enregistrement, de classement, d'ajout de métadonnées et de stockage d'un document dans un système d'archivage ».
3.3.2	**Q**uels sont les **objets** qui peuvent être **capturés** ?	Tout objet dématérialisé mais bien formé techniquement, identifiable et accompagné de ses métadonnées elles aussi bien formées; si cet objet entre dans le cadre d'un accord entre émetteur et récepteur. Dans le cas particulier des flux d'impression, il faut pouvoir archiver aussi bien en mode page qu'en mode ligne. Certains flux peuvent aussi produire simultanément des documents papier et des documents numériques (factures en format PDF par ex.) .
3.3.3	**Présentation et/ou contenu ?**	Dans certains projets, il peut être intéressant de séparer la conservation des contenus de celle des formats de présentation. Ex. Le projet de l'association EDIFICAS sur la modification des règles fiscales concernant la conservation des données : pouvoir produire des données comptables même si l'on n'a pas le programme d'origine ; pouvoir revenir sur les écritures d'origine.
3.3.4	**Quels types de capture ?**	La capture des données (documents) comme des métadonnées peut être : • automatique : une routine d'extraction est programmée et exécutée sur la base de la localisation des fichiers (dans tel répertoire), des caractéristiques des données (dans une base de données), du nommage des fichiers, de leur date, etc. • semi-automatique : le processus est déclenché manuellement puis les opérations sont automatiques en fonction des tâches prédéfinies ;

		• manuelle : le fichier est acheminé manuellement vers le SAE ; les métadonnées sont saisies par l'utilisateur.
3.3.5	**Capture ou versement ?**	Il s'agit de la même notion vue selon deux points de vue « géographique » : 1. Celui du SAE, les documents sont « capturés » dans le système 2. Celui de l'application cliente (de l'archivage) ou de l'utilisateur, les documents sont « versés » dans le SAE.
3.3.6	À quel moment capturer les données ?	La capture des documents dans le SAE peut se concevoir à deux moments : 1. au moment même où le document est validé 2. à un moment ultérieur, dès lors qu'entre le moment de la validation du document dans l'application native et le moment du transfert dans le SAE), l'intégrité technique et juridique est gérée.
3.3.7	Comment contrôler la **qualité** du document à archiver ?	La qualité du document AVANT l'archivage est importante dans la mesure où la technologie ou la performance du système de conservation ne pourront en cas redonner à un document archivé la valeur d'authenticité, de fiabilité ou d'intégrité qui lui ferait défaut à l'entrée dans le système. La qualité du document présenté à l'archivage relève d'abord de procédures métier, de procédures qualité au sens ISO 9000 ou de normes techniques (voir ISO 12029). Les procédures d'archivage permettent de préciser les caractéristiques formelles des documents à archiver et de définir les métadonnées obligatoires. Voir le chapitre 2. La pertinence des documents à archiver est ensuite gérée par les procédures d'archivage : sélection des documents en fonction de leur valeur de conservation et association des règles appropriées. Par ailleurs, lors de la capture, le système d'archivage doit vérifier que les métadonnées obligatoires sont renseignées et qu'elles sont conformes aux tables ou modèles déclarés.
3.3.8	Peut-on capturer des documents électroniques par des **processus automatisés** ?	Il est recommandé d'automatiser au maximum la capture des métadonnées pour éviter la lourdeur des ressaisies : lecture du document, récupération des caractéristiques du fichier, etc. Voir aussi la notion d'héritage des métadonnées (chapitre 2, rubrique métadonnées) Pour le transfert d'archives d'un producteur vers un service d'archives publiques, voir aussi le Standard

		d'échange de la direction des Archives de France : https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/a103_archivage_elect/public/standard_d_echange_d/folder_contents
3.3.9	Peut-on gérer de manière groupée (**traitement par lot** ou de masse) ?	Oui, grâce au rôle fondamental du plan de classement (structuré et hiérarchique) et de sa mise à jour Le système d'archivage doit permettre l'automatisation de la gestion des durées et du sort final : pilotage et visibilité d'ensemble, alerte sur les documents dont les durées sont arrivées à échéance.
3.3.10	Comment automatiser la capture des métadonnées ?	Une partie des métadonnées peut être capturée automatiquement à deux conditions : 1/ si les métadonnées figurent dans le document à une place définie préalablement (cf feuille de style) et sont techniquement extractibles ; 2/ si un indice (une métadonnée spécifique) permet d'aller chercher d'autres métadonnées dans des tables déclarées dans le système.
3.3.11	Quels **contrôles** après la capture ?	Après la capture, il est particulièrement important de contrôler : 1. l'intégrité du document, 2. les métadonnées, 3. le format, 4. la lisibilité.
3.3.12	Comment contrôler les **durées de conservation** ?	Le contrôle de l'échéance de la durée de conservation se fait en comparant la durée de conservation attachée au document avec la date de départ de cette durée. Ce contrôle doit être automatisé autant que possible, ce qui suppose que le système connaisse la date de départ de la durée lorsque celle-ci est différente de la date de création du document (date de fin de validité d'une délégation de signature par exemple). Voir chapitre 2, rubrique « durée de conservation ».
3.3.13	Traitement des **« ressources » associées** aux données (polices, formules) ?	Ceci est lié aux conditions de restitution (de lisibilité) des données ou documents archivés. Le document ne sera pas reproductible si on n'a pas accès à certaines ressources. D'une manière générale, ces ressources doivent être amalgamées aux données. Il s'agit d'un problème complexe car les ressources liées à la forme d'un document peuvent, avec des changement de formats et d'évolution des logiciels,

		varier au cours du temps.
3.3.14	Que signifie « **destruction** des données » ?	Destruction du contenu, du support, d'éventuelles copies ? Il convient de distinguer : ▪ la suppression des données du système actif ▪ la destruction complète et irréversible des données ▪ le contrôle de l'existence de copies dans d'autres applications de l'entreprise. Au sens archivistique, c'est au terme de la durée de conservation, la suppression des documents concernés. Pour la CNIL par exemple, c'est, au terme prévu, détruire (faire disparaître physiquement) l'original et ses copies afin que nul ne puisse réutiliser ultérieurement les données. Voir le chapitre 2
3.3.15	Peut-on détruire les documents originaux après numérisation ?	Le choix de la destruction après numérisation des documents papier dépend d'une part de la valeur probante des documents, d'autre part du risque attaché à la disparition de l'original. Attention : la loi française ne reconnaît pas la qualité d'original à un document numérisé (cf article 289bis du Code Général des Impôts par exemple). Toutefois, la norme NFZ 42-013 procure un cadre technique offrant aux copies numériques une garantie raisonnable quant à leur valeur probante. On ne peut cependant généraliser. Chaque opération de numérisation doit comporter une étude d'opportunité et de risque. NB : un document qui a valeur patrimoniale, ne doit pas être détruit. Le numériser (pour diffusion) ne peut conduire à sa destruction.

3.4 Autres notions liées à la conservation et à la restitution des documents électroniques

3.4.1	Qu'est-ce qu'un **format ?**	1 : Un élément de langage spécifiant la représentation, sous forme de caractères, des objets désignant les données sur un support d'information. 2 : Une structure définie de données contenues sur un support magnétique ou autre, établie selon des règles qui régissent le stockage, l'affichage, la manipulation, l'impression ou la transmission de ces données → Source : www.granddictionnaire.com
3.4.2	Quels sont les **formats de fichiers** adaptés à l'archivage **?**	Les formats appropriés pour l'archivage doivent être pérennes, publics, largement diffusés, reconnus pour leur fiabilité (forte probabilité d'assurance d'évolution et non pas de rupture ou de disparition). Les principaux formats recommandés sont : Pour les document textes : - PDF 1.4 (PDF/A-1), voir ISO 19005-1 - OpenDocument (ODT), RTF, TXT - HTML et XML valides Pour les images* : - PNG, TIFF, GIF, JPG Pour le son - FLAC, MP3 Pour la vidéo : - MPEG Pour les documents textuels ou graphiques il faut privilégier cependant les formats qui ne détruisent pas une partie de l'information en la compressant : GIF plutôt que JPG, FLAC plutôt que MP3, …)[8] Attention aux appellations des formats qui peuvent recouvrir plusieurs réalités : le bon HTML et le mauvais HTML (ex: le HTML de Microsoft utilise des balises non définies dans les recommandations du Worldwide Web Consortium W3C).
3.4.3	Qu'est-ce que la **conversion ?**	Action de transférer des documents d'un support vers un autre ou d'un format vers un autre (voir norme ISO 15489).
3.4.4	Qu'est-ce que la **migration ?**	Action de transférer des documents d'un système à un autre en préservant leur authenticité, leur intégrité leur fiabilité et leur exploitabilité (voir norme ISO 15489). **Pour les migrations, voir la norme OAIS (ISO 14721)**
3.4.5	Faut-il **convertir avant ou après**	Il est préférable que la conversion intervienne avant la capture, notamment lorsqu'il s'agit de présenter

[8] Sur les formats avec ou sans perte : http://www.twixo.org/flac/lossy-lossless/

	la capture ?	les données dans un format conforme aux exigences de l'archivage. La conversion peut néanmoins être opérée après la capture lorsque, par exemple, celui qui archive n'a pas les équipements nécessaires pour effectuer la conversion. La conversion doit dans ce cas être tracée.
3.4.6	Faut-il **archiver une signature** électronique ?	L'archivage d'une signature électronique ne présente d'intérêt que dans la mesure où, lorsque l'on accède au document conservé correspondant, il doit être démontré que le signataire était en droit d'effectuer cette signature au moment où le document a été établi.
3.4.7	Comment résoudre le problème de la conservation des documents électroniques signés ?	Pour que cette vérification soit possible et ait toute sa portée il faut donc disposer d'une chaîne de certification opérationnelle et connaître les délégations du signataire. Les révocations des certificats tous les deux ou trois ans et l'absence quasi systématique d'informations sur les délégations des signataires rendent l'archivage des signatures électroniques inopérant. La validation de la signature au moment de la capture du document (dans la mesure où celle-ci intervient dans un délai rapproché) et la conservation de cette information en tant que trace est une opération plus efficace et judicieuse. Voir ci-dessus 3.2.14. Voir l'étude de Jean-François BLANCHETTE, « La conservation de la signature électronique : Perspectives archivistiques », Rapport remis à la Direction des archives de France, Ministère de la culture, 2004, 39 p
3.4.8	Que faut-il entendre par **pérennité** ?	La pérennité est la caractéristique des objets qui possèdent la faculté de se conserver dans le temps. La pérennité concerne soit les documents (contenu et support), soit les formats et les supports. La pérennisation est le processus qui permet d'assurer la pérennité. Voir norme OAIS (ISO 14721) sur la pérennisation des données numériques.
3.4.9	Comment choisir un format pérenne de conservation des documents numériques ?	Un format pérenne pour la conservation d'un document électronique doit en permettre la restitution fidèle au document d'origine tout au long de la période de conservation indépendamment d'un environnement système ou applicatif spécifique. Dans ces conditions le choix devra privilégier les formats disposant d'une normalisation internationale et permettant de préserver le contenu et la

		présentation du document lors de sa conversion si celui-ci n'est pas directement créé dans le format d'archivage. Les caractéristiques intrinsèques d'un format d'archivage sont les suivantes : • Non propriétaire • Libre d'accès et de droits • Excluant les liens dynamiques avec des éléments externes • Incluant les polices d'affichage des caractères • Disposant d'algorithmes de compression d'image normalisés ou standard L'adoption de formats réputés pérennes lors de la mise en place d'un système d'archivage n'exclut pas la nécessité d'effectuer périodiquement des opérations de migration lorsque les formats deviennent obsolètes mais réduit fortement la fréquence de ce type d'opération.
3.4.10	Pourquoi doit-on envisager de **migrer** les documents numériques archivés ?	L'archivage de documents électroniques, comme tout projet informatique, doit prendre en compte l'évolution des technologies et des environnements ainsi que les incidents courants d'exploitation tels que par exemple la dégradation des supports. Trois types de migration peuvent être envisagés : 1. migration faisant suite à l'évolution ou à la dégradation de l'environnement d'exploitation, 2. migration résultant de l'évolution ou de la disparition d'un format utilisé dans la solution d'archivage, 3. migration combinant les deux premiers types. Il convient de tenir compte du fait que la migration impliquant un changement de format peut potentiellement induire une perte d'intégrité du document. Dans tous les cas les conditions opérationnelles d'une migration devront être précisées de façon à préserver, autant que faire se peut, l'intégrité et l'authenticité du document. Voir le site d'InterPARES www.interpares.org
3.4.11	Que signifie « **restitution** » ?	En fonction de la finalité (besoins de production, de preuve ou de contrôle), la restitution pourra prendre plusieurs formes : • Fourniture du document ou d'une copie sur un support amovible • Impression du document • Affichage du document sur écran La restitution doit s'effectuer dans le cadre d'une procédure définie : • Contrôle de l'habilitation du demandeur à effectuer la requête de restitution.

		• Contrôle de la disponibilité et de la maîtrise de l'ensemble des procédés externes de restitution par le demandeur. Cette étape vise à s'assurer de l'absence d'altération entre la sortie du système d'archivage et la réception par le destinataire final. • Lecture sur son support de stockage et transcription conformément au mode de restitution choisi. • Accusé de réception. Dans une perspective de bonne gestion, il est souhaitable que le demandeur accuse réception du document communiqué et puisse notifier la bonne fin des opérations.
3.4.12	Que signifie « **lisibilité** » des documents ?	La lisibilité désigne la possibilité d'avoir accès, au moment de la restitution du document par tout moyen technique approprié, à l'ensemble des informations qu'il contient.
3.4.13	Comment garantir cette lisibilité ?	Garantir la lisibilité d'un document suppose, *a minima*, que l'environnement technique en vigueur permette d'accéder au fichier contenant le document et implique de disposer, dans cet environnement, des logiciels interprétant le format dans lequel le document a été codé de façon à en produire une restitution, sur écran ou imprimée, intelligible pour un humain.
3.4.14	Impact des environnements sur les logiciels de restitution et sur le choix du format d'archivage	Tous les environnements, quels qu'ils soient, restreignent les possibilités de restitution. Ce point est à examiner soigneusement, au cas par cas.
3.4.15	Impact de la **migration** sur l'**intégrité**	S'il s'agit d'une migration de support, cette opération doit être sans effet sur l'intégrité. Les fichiers migrés doivent être identiques octet par octet aux fichiers avant migration. Les migrations impliquant un changement de format portent atteinte, au sens strict, à l'intégrité du document. Cependant, tout en modifiant le contenu binaire du fichier, le contenu informationnel ne doit pas être atteint pour que le document conserve sa vocation en tant qu'archive. En revanche une migration de format peut ne pas être sans effet sur la présentation du document (polices différentes, alignement, couleurs, etc.). Dans tous les cas, les sceaux ou signatures électroniques sur des documents migrés ne s'appliquent plus. L'opération de migration a été explicitement prévue dans les décrets « Actes authentiques » 2005-972 et 2005-973 et dispose que la nature d'original d'un

		acte est conservée après migration.
3.4.16	**Q**ue signifie « **réversibilité** » ? Comment peut-on y répondre ?	La clause de réversibilité, dans un contrat d'externalisation ou lors de l'acquisition d'un système, définit les conditions selon lesquelles le fournisseur du service ou du système redonnera à son client la maîtrise de ses données ou de ses applicatifs. Dans le contexte d'un SAE, pour que cette clause soit applicable, il convient de définir dès la mise en place du service ou du système les conditions techniques et procédurales de l'opération de transfert des archives vers le donneur d'ordre ou vers un nouveau sous-traitant. Si cette opération n'est pas possible *a priori*, il convient de prévoir contractuellement qu'elle devra être mise en place sur simple demande du donneur d'ordre.
3.4.17	Que signifie « **interopérabilité** » ?	L'interopérabilité peut être la caractéristique : • d'un objet, pouvant être traité dans plusieurs environnements, Ce peut être le cas des identifiants, des certificats ; • d'un outil, capable de communiquer avec les autres composantes d'un système d'information, ou avec d'autres systèmes ; • de deux systèmes susceptibles de communiquer et d'opérer ensemble. NB : L'interopérabilité n'a de sens que si l'on sort de la "juridiction" de la "source". Il existe différents niveaux d'interopérabilité : technique, fonctionnelle, opérationnelle etc., parfois qualifiés de termes spécifiques comme « portabilité », « multi-acceptance », « certification croisée ».
3.4.18	**Q**uels sont les besoins d'interopérabilité ?	L'interopérabilité et le partage des ressources sont importants pour la continuité et la pérennité de tout service. C'est le cas de l'archivage dans le cadre de l'Administration. Si les données ne sont accessibles qu'à un seul utilisateur (ou un petit nombre d'utilisateurs au sein d'une même structure), l'interopérabilité n'est pas nécessaire, ni souhaitable (cf Minutier électronique des notaires ou des huissiers de justice)

3.5 Technologies et moyens techniques

3.5.1	Quelles **technologies** pour quelles **exigences**?	Rappel (voir 3.2.1) : la « sécurité juridique » repose sur *la garantie d'imputabilité, d'authenticité, d'intégrité, et de lisibilité, dans le temps (pérennité)*. Cette garantie fait appel à des fonctions telles que *l'identification , l'authentification ; la gestion des habilitations ou des autorisations, la validation des opérations , l'historisation, la traçabilité ; la sauvegarde, la restauration.* Le choix et l'utilisation de certaines technologies est critique, ainsi : - Formats (lisibilité, pérennité), - Support de stockage (lisibilité, pérennité, intégrité, sauvegarde, restauration), - Chiffrement, certificat, signature électronique (imputabilité, intégrité), - Système de capture (intégrité), - Horodatage (traçabilité).
3.5.2	La **technologi**e est-elle neutre ?	Les technologies de production de l'information ne sont pas neutres. Exemple : une déclaration d'échange de biens (DEB) ne présente pas la même sûreté juridique selon qu'elle est : établie sous forme papier transmise par EDI transmise par messagerie électronique. Selon la technologie utilisée, diverses mesures doivent être mises en oeuvre pour garantir l'authentification et l'intégrité, obligatoires dans tous les cas (cf. arrêté du 4 janvier 2002 portant approbation du cahier des charges pour la transmission par voie informatique de la déclaration d'échanges de biens).
3.5.3	Comment effectuer la **réception des dispositifs** sécuritaires ?	Cette réception peut se fonder sur différents référentiels de l'Administration, des normes, des guides de bonnes pratiques. Selon la référence utilisée, elle peut donner lieu à « certification », « accréditation », «labellisation » ou à un simple rapport. Une fois le SAE mis en place et opérationnel, il est conseillé de procéder à des audits périodiques.
3.5.4	**Q**u'entend on par **chiffrement** ?	Une technique cryptographique visant à assurer la confidentialité d'un document ou d'un fichier à

		l'encontre des personnes non autorisées.
3.5.5	A quoi sert le chiffrement ?	Notamment à apporter de la confidentialité, donc de la sécurité à la transmission et/ou à la conservation d'un objet électronique. Attention : pour la conservation à long terme, le chiffrement peut devenir une entrave (notamment à la migration) et perdre de sa nécessité. Il paraît en général préférable de mettre l'accent sur le contrôle d'accès et l'authentification des utilisateurs plutôt que sur le chiffrement. Toutefois, le chiffrement peut s'avérer le seul moyen d'une confidentialité efficace vis à vis des indiscrétions de toutes natures, y compris « internes ». Le chiffrement est aussi un instrument de préservation de l'intégrité des données échangées, y compris des données de sécurité (identifiants, certificats, signatures électroniques).
3.5.6	**Q**uels sont les risques du chiffrement ?	Perte de l'algorithme, dégradation ou perte des clés, modifications du contenu ayant pour conséquence de rendre illisible le document.
3.5.7	Concurrence entre la **solution « chiffrement » et la solution « coffre-fort »** : où mettre les verrous ?	Le « coffre-fort électronique »[9] est une application ou un service visant à assurer la confidentialité par chiffrement d'un document ou d'un fichier et d'autres services connexes, comme le contrôle d'accès et l'horodatage.
3.5.8	Qu'est qu'un **certificat** ?	Fonctionnellement, un certificat se définit comme un objet informatique logique lié à une entité. Il peut s'agir d'une clé publique signée par une Autorité de Certification. L'ensemble bi-clé/certificat permet d'utiliser des fonctions cryptographiques (cryptographie asymétrique) permettant notamment des opérations d'authentification, de signature numérique et de chiffrement. (Glossaire ADAE) La Directive européenne sur la signature électronique en fait une « attestation électronique qui lie les données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne. » Un « certificat qualifié » est un certificat fourni par un prestataire de services de certification satisfaisant à certains niveaux d'exigences.
3.5.9	Comment gérer les **certificats**?	La durée de vie d'un certificat est généralement de deux ans. A l'issue de cette période il est nécessaire d'émettre un nouveau certificat.

[9] « coffre-fort électronique »® est une marque déposée par CDC-Arkhinéo – Caisse des dépôts et Consignation ; l'expression « coffre-fort électronique » est toutefois largement utilisée.

		En cas de perte ou de compromission, un certificat doit être révoqué. Les conditions d'usage et les modalités de gestion d'un certificat sont définies dans la politique de certification émise par l'Autorité de Certification.
3.5.10	**C**omment choisir entre **« archivage en ligne »** et « stockage distant » ?	Cette question relève de l'ILM (Information Lifecycle Management) : arbitrage entre l'archivage en ligne plus facilement accessible mais plus cher et l'archivage distant plus économique mais avec un accès plus long. Le choix tient aux besoins des utilisateurs.
3.5.11	Qu'est-ce qu'une **plate-forme** d'archivage ?	Un ensemble de services et d'équipements permettant l'archivage dans une perspective mutualisée. Il peut y avoir mutualisation, dans certaines administrations ou dans différents services d'une grande entreprise.
3.5.12	Quelles sont les différences entre **sauvegarde** et archivage ?	Les finalités et les moyens sont différents. La sauvegarde est un procédé informatique qui permet de figer un environnement complet afin de pouvoir redémarrer une ou plusieurs applications en cas d'incident. Les opérations de sauvegarde et de restauration font partie de plans de reprise d'activité adaptés à la nature et à la gravité des incidents. L'archivage est un ensemble de procédures et d'outils qui gèrent des objets figés et signifiants en fonction de leur valeur propre, selon des règles de conservation et d'accès prédéfinies. Voir aussi chapitre 2
3.5.13	Quels sont les différents **supports** d'archivage ?	On distingue deux grandes catégories : - Supports amovibles - Supports fixes Les supports peuvent être de type non réinscriptible (WORM) ou réinscriptible. Pour les applications d'archivage, les supports de type WORM sont préférables mais non indispensables. Il existe des supports WORM pour lesquels l'impossibilité d'effacer et de réenregistrer est obtenue par des moyens physiques ou logiques. Ces supports peuvent être des disques magnétiques, des bandes magnétiques, des disques optiques (UDO, DVD-R, CD-R, etc.)

3.5.14	Fragilités dues aux **plates-formes techniques** et accroissement des risques	On entend par « plate-forme technique », les éléments matériels et logiciels (systèmes d'exploitation, utilitaires) sur lesquels sont développées les fonctions spécifiques du SAE. En l'état actuel de la technique, ces plates-formes sont « perméables » aux attaques de toutes sortes. Le moment d'extrême fragilité se situe au lancement, à l'ouverture ou à la reprise des opérations du SAE, que cela se fasse quotidiennement ou à une autre périodicité. Ceci rend d'autant plus indispensables les contrôles et le recours à des outils de détection des anomalies de toutes natures. Voir aussi le point 4.3 dans le chapitre suivant.
3.5.15	Comment rendre **pérenne** les informations de toutes applications informatiques ?	La première action consiste à insérer une clause standard dans les cahiers des charges concernant l'acquisition ou le développement de toute application informatique. Cette clause standard dans les cahiers des charges doit couvrir : - le choix des données à conserver champ par champ ; - la définition d'un format d'échange de données ; - le principe d'export des données dans le format d'échange défini. De fait l'application doit pouvoir exporter automatiquement les données choisies et ainsi garantir la possibilité d'un archivage électronique pérenne.
3.5.16	Qu'est-ce que la gestion de la **continuité** ?	« Une approche globale qui comprend la politique, les règles et les procédures pour garantir le maintien ou la reprise des opérations spécifiées d'une façon planifiée en cas de perturbation. Son but est de réduire au minimum les conséquences opérationnelles, financières, légales, de réputation et autres conséquences substantielles résultant d'une perturbation. » (voir Forum tripartite pour en savoir plus)
3.5.17	Quels sont les liens entre le SAE et la continuité ?	La problématique de la continuité s'applique au SAE. En sens inverse le SAE peut être un composant important d'une politique de continuité.

3.6 Table de correspondance avec MoReq

Le tableau suivant liste les sections de MoReq où sont abordés les différents aspects de la sécurisation.

	MoReq	**Ce guide**
Chap. 4	Contrôles et sécurité	3.1.3 3.1.4 3.1.6 3.1.7
4.1	Accès	3.2.18 3.2.19 3.2.20
4.2	Historique des évènements*	3.2.1
4.3	Sauvegarde et restauration	3.2.1 3.5.12
4.4	Traçabilité des mouvements	3.2.24
4.5	Authenticité* (défini dans le glossaire, chap. 13)	3.2.4 3.2.5
4.6	Indices de sécurité*	3.2.18 3.2.19 3.2.20
	Éléments liés	
Chap. 7	Identification (chap. 7)	3.3.8 3.3.9
Chap. 9	Fonctions d'administration (chap. 9)	
Chap. 10	Dans Autres fonctions (chap. 10)	
10.5	Signature électronique (10.5)	3.2.11 3.2.12 3.2.13
10.6	Chiffrement (10.6)	3.2.21 3.5.4 3.5.5
10.7	Filigranes numériques (10.7)	
10.8	Interopérabilité et ouverture (10.8)	3.4.17 3.4.18
Chap 11	Dans Exigences non fonctionnelles	
11.3	Disponibilité du système	
11.5	Environnement législatif et réglementaire	
11.6	Externalisation et recours à des tiers	
11.7	Conservation à long terme et obsolescence technologique	
Chap.12	Dans Les métadonnées	
12.9	Métadonnées concernant l'utilisateur	3.3.10
12.10	Métadonnées concernant les profils	
Chap. 13	Dans Modèle de référence	
13.1	Glossaire	
13.4	Modèle de contrôle d'accès (matrice)	

3.7 Pour en savoir plus

Le modèle OAIS

Modèle de référence pour un Système ouvert d'archivage d'information (OAIS) : standard CCSDS, CCSDS 650.0-B-1 (F).

Cette norme définit un vocabulaire et un ensemble de concepts permettant d'appréhender de façon globale et complète, la question de la conservation à long terme de données sous forme numérique. Elle définit deux modèles complémentaires : un modèle d'information et un modèle fonctionnel détaillé. Elle propose également une classification des types de migration et des différents modes de coopération possibles entre centre d'archives.

Norme OAIS version anglaise (janvier 2002)
Reference Model for an Open Archival Information System : Recommendation for Space Data System Standards, CCSDS 650.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, January 2002. [Equivalent to ISO 14721:2003.].

Version anglaise de l'OAIS (ISO 14721) à l'adresse :
hypp//www.ccsds.org/publications/archive/650x0b1.pdf

Version française de l'OAIS (ISO 14721) à l'adresse :
http://vds.cnes.fr/pin/documents/projet_norme_oais_version_francaise.pdf

Le standard d'échange de données pour l'archivage

Cas du transfert d'archives publiques aux Archives Nationales : Standard d'échange de données pour l'archivage, publié par la DAF / DGME :

https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/a103_archivage_elect/public/standard_d_echange_d/folder_contents

Le standard d'échange de données pour l'archivage vise à faciliter l'interopérabilité entre le système d'information d'un service d'archives et les systèmes d'informations de ses partenaires (producteurs, utilisateurs...). Il fournit un modèle pour les différentes transactions qui peuvent intervenir : transfert, communication, destruction.
Il préconise un format qui assure le transfert (automatique si nécessaire) d'archives d'un service versant à un service d'archives.

Le standard d'échange s'adresse plus particulièrement :
- aux producteurs d'archives publiques tels les ministères, les services déconcentrés de l'Etat, les collectivités territoriales, les établissements publics ;
- aux services publics d'archives, en vue de normaliser la réception et la communication d'archives numériques et de favoriser ainsi les portails de consultation multi-sites ;
- aux éditeurs de logiciels qui souhaiteraient se conformer à un cadre normatif pour le développement de leur module d'archivage ;
- aux éditeurs de logiciels de gestion et de description des archives papiers ;
aux prestataires de services d'échanges œuvrant pour des producteurs d'archives publiques et pouvant être amenés, à la demande de ces producteurs, à transférer des documents à des services publics d'archives ;
- aux tiers-archiveurs ;
- aux services d'archives étrangers.

Référentiels de sécurité et d'interopérabilité

La circulaire du 21 janvier 2002 a défini un cadre d'interopérabilité des systèmes d'information publics commun aux administrations de l'Etat.

> Le Référentiel Général d'Interopérabilité (RGI) spécifie l'ensemble des règles dont le respect s'impose à tous pour faciliter les échanges et rendre cohérent l'ensemble constitué des systèmes d'information du service public…L'ordonnance téléservice prévoit une durée de trois ans pour une mise en conformité des téléservices.
> Le Référentiel Général de Sécurité (RGS) spécifie l'ensemble des règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et entre les autorités administratives.
> Chaque version du RGS : Référentiel Général de Sécurité définira les services et les niveaux de sécurité correspondant aux besoins des autorités administratives.
> La PRIS est un référentiel documentaire qui définit des exigences pour différentes fonctions de sécurité. Il concerne les produits de sécurité et les prestataires de services de confiance utilisés dans le cadre des échanges dématérialisés entre usagers et autorités administratives ainsi qu'entre autorités administratives…

Voir : http://synergies.modernisation.gouv.fr

Authenticité des actes

Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires et Décret n° 2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice

Droits d'accès et droits d'usages

http://www.hub2b.com

Les formats

Présentations sur différents thèmes relatifs aux formats numériques faites devant le groupe de travail PIN (Pérennisation de l'information numérique) : http://vds.cnes.fr/pin/pin

Thèmes:

- Critères applicables aux formats
- Répertoire de formats
- Format WARC
- Formats Audio et Vidéo
- Format d'image
- Format XML

Voir: http://vds.cnes.fr/pin/pin_formats.html

Comment conserver des documents électroniques signés ?

Voir étude de Jean-François BLANCHETTE, « La conservation de la signature électronique : Perspectives archivistiques », Rapport remis à la Direction des archives de France, Ministère de la culture, 2004, 39 p texte : http://www.archivesdefrance.culture.gouv.fr/fr/circulaires/rapport_signature%e9lectronique_archivage1.pdf

Continuité

Principes directeurs en matière de continuité d'activité, Le Forum tripartite / Joint Forum (Comité de Bâle sur le contrôle bancaire, Organisation internationale des Commissions de valeurs, Association internationale des superviseurs en assurance
voir : http://www.bis.org/press/p060829.htm

4 Le projet d'archivage électronique

Le projet d'archivage électronique est un projet à forts enjeux pour l'entreprise ou l'organisme ; il doit donc être préparé, comme tous les projets majeurs, avec le plus grand soin.

Garantir l'accès à l'information, assurer la traçabilité des documents en réponse aux exigences juridiques sans cesse croissantes, organiser la conservation et la pérennité des documents électronique, autant de motivations fortes conduisant les décideurs à la création d'un système d'archivage électronique. Ce SAE devient d'autant plus une nécessité que les informations électroniques sont de plus en plus nombreuses : les échanges pour courrier électronique se sont développés ces dernières années jusqu'à la banalisation, les transferts de fichiers via intranet ou internet (voire extranet) se sont amplifiés. Cette évolution touche l'ensemble des collaborateurs d'une entreprise ou d'un organisme.

Cependant, le développement des échanges électroniques n'est pas toujours suivi de procédures ni de règles de conservation et on constate fréquemment un stockage individuel de ces informations, stockage qui a plusieurs conséquence néfastes : le non partage de l'information et donc risque de perte de l'information ainsi qu'une redondance importante, la même information, le même document pouvant être stocké par de nombreuses personnes différentes : c'est le cas par exemple des comptes rendus de réunions gardés potentiellement par tous les destinataires.

Un archivage électronique, en centralisant les informations, doit faciliter la pérennité ainsi que l'accès partagé par toutes les personnes autorisées et de ce fait permettre un gain de temps, par une recherche rapide. De plus, la centralisation, en évitant des redondances, doit permettre de désencombrer la mémoire des postes de travail.

Un projet de SAE peut se mener par étapes mais il doit s'inscrire dans une vision d'ensemble sur les plans stratégique, organisationnel et technique. Il est donc nécessaire de déterminer les acteurs impliqués dans ce processus ; le groupe devra être désigné avec soin en gardant bien présent à l'esprit que ce projet est l'affaire de tous et pas uniquement du service informatique ou de l'archiviste / records manager.

Ce n'est que par une étroite collaboration entre la direction générale, la direction juridique et la direction informatique que se projet pourra aboutir.

Avant tout il faudra garder présent à l'esprit quelles sont les informations à faire entrer dans le périmètre de l'étude et de mettre toujours en regard les bénéfices obtenus avec les coûts induits par un archivage électronique.

Cette analyse, du point de vue technique, gestionnaire et archivistique, ne doit pas faire oublier le point de vue humain Un SAE conduit à un véritable changement dans l'entreprise et ce sont des habitudes de travail, souvent bien ancrées chez les collaborateurs (seul le papier est considéré comme archives), qu'il faut changer.
Un tel projet ne pourra donc aboutir qu'avec eux et non malgré eux.

4.1 Le contexte et les acteurs

4.1.1	Quels sont les **événements déclencheurs** du projet d'archivage / records management ?	Bien souvent un problème de gestion ou une perte de documents… La mise en place d'un plan d'urbanisation des systèmes d'information. La gestion de documents standardisés issus d'une procédure. Cette gestion impliquant de lourds volumes d'archives papier. Pallier au manque de place dans les magasins de stockage

		papier comme informatique (local archives versus baie de stockage). Optimiser la gestion des espaces de stockage informatique. Établir des rapports sur l'état de la gestion de documents comme un risque inhérent à l'entreprise. Améliorer les relations clients / fournisseurs / partenaires (impact sur la gestion et le partage des documents, plates-formes d'échange de données). Environnement externe : impact des lois de sécurité financière, filiales à l'international, fusions/acquisitions, activités réglementées (ex : aéronautique). Environnement interne : contentieux, développement du *risk management*, demandes des utilisateurs, accompagnement des modifications de structure et des modes de changement, mise en place de projet de *knowkedge management* (gestion des connaissances).
4.1.2	Quels sont les **résultats** attendus ?	Créer un système d'archivage électronique viable remportant l'adhésion de tous les acteurs concernés. Aspect normatif / juridique / règlementaire. S'assurer du respect des contraintes légales, normatives et réglementaires. Obtenir une politique commune dans une entreprise voire dans un groupe. Connaître et maîtriser le patrimoine documentaire. Tracer l'information. Faciliter la gestion quotidienne des documents. S'assurer de la validité de l'information. Rationaliser les coûts.
4.1.3	Qui sont les **acteurs** du projet ?	Archiviste / records manager, chef de projet informatique, professionnel du secteur d'activité concerné, qualiticien, documentaliste, knowledge manager, juriste.
4.1.4	Quel est le rôle de la **direction générale** ?	Elle soutient fortement le projet par des actions de communication (ex : note de cadrage signée par le directeur général). Le soutien de la hiérarchie permet l'adhésion au projet. C'est une phase primordiale qui permet aussi de légitimer le projet archivage par rapport à d'autres projets jugés plus « cœur de métier ». La maîtrise d'ouvrage est le garant du projet ; elle impulse la dynamique, oblige les partenariats (ex : métier / informatique), donne les moyens. Elle soutient le projet dans la phase d'implémentation, quand il y a des résistances au changement. Les « sponsors » du projet doivent appartenir à la direction générale. *A priori*, le directeur informatique, le directeur financier et le directeur juridique sont des sponsors potentiels.
4.1.5	Quel est le rôle de la **direction**	Elle apporte les compétences techniques informatiques, l'expertise informatique

	informatique ?	Elle connaît l'environnement informatique et technique dans lequel évolue la société ainsi que les possibilités du système. Elle joue le rôle de maître d'œuvre et apporte la technique et les outils ; elle joue également un rôle de conseil sur les outils et les règles du SI et un rôle de garant des règles et standards du SI (sécurité, annuaire, réseau, qualité du code fourni...) Elle fédère les différents projets informatiques tels que la GED et évite les redondances dans les systèmes proposés. Elle veille à l'intégration du SAE aux activités techniques de l'entreprise.
4.1.6	Qui est le **chef de projet** ?	On peut distinguer deux profils de chef de projets : l'archiviste est le chef de projet opérationnel et l'informaticien est le chef de projet informatique. Ils assurent la coordination, le développement et la promotion du projet. Dans ce cas de figure, l'archiviste est le Maître d'ouvrage et le chef de projet informatique le Maître d'œuvre. Le chef de projet est en général interne (meilleure connaissance du fonctionnement et du fonds documentaire) ; il peut être extérieur (accent mis sur la méthode en toute indépendance). Exemples dans deux grandes entreprises privées : ▪ le chef de projet est le responsable Groupe Gestion documentaire & Archivage (aussi appelé garant documentaire) pour la phase avant-projet ; à l'issue de cette phase, le chef de projet peut être changé et la composition de l'équipe redimensionnée ; ▪ comme il n'y a pas d'archiviste, le chef de projet maître d'ouvrage est rattaché à un des services de la direction informatique ; la maîtrise d'oeuvre est sous-traitée.
4.1.7	Comment est constitué le groupe projet ?	Deux comités sont crées : le comité de pilotage et le comité opérationnel. L'**équipe projet** comprend des informaticiens, archivistes spécialistes GED, qualiticiens, documentalistes, juristes, experts en management de projet, responsable sécurité informatique, représentant du knowkedge management et pôle utilisateurs. Le **Comité de pilotage** regroupe des représentants de tous les métiers, ainsi que la direction juridique, direction des risques, direction Qualité, direction informatique qui sont les garants du projet. Il est important que les professionnels de l'information et les techniciens « cœur de métier » soient présents.
4.1.8	Qui sont les **acteurs extérieurs** ?	Le projet peut nécessiter de recourir à des prestataires : ▪ dans les domaines du conseil en organisation (experts fonctionnels en records management notamment) pour apporter un éclairage extérieur sur le métier, ▪ les tiers archiveurs (voir chapitre précédent).
4.1.9	Quels liens entre le projet d'archivage et les projets de **gestion des**	Liens possibles au niveau : du plan de classement,

	connaissances ?	du plan de nommage des fichiers. Tenir compte de l'essor des logiciels de gestion de contenu qui intègrent dans leurs outils des modules de records management / archivage. Lien indispensable entre le *records management* ET le *knowledge management* (clubs de réflexion et de retours d'expérience) Les projets d'archivage électronique permettent de développer le *knowkedge management* au sein d'un organisme (il est clair que les documents archivés sont un des supports de connaissance). L'approche *knowkedge management* permet une structuration de l'information, suggère une notion de priorisation, un autre point de vue sur les outils de partage et de traçabilité de l'information. Le cycle de vie des documents concerne le *knowkedge management* et le *records management*. Le records management permet une meilleure gestion des connaissances dans le temps et assure, via les notions de processus records management et de rôles & responsabilité, que seuls des documents importants seront conservés et les autres seront détruits. voir chapitre 2 (2.2.7)
4.1.10	Quels liens entre le projet d'archivage et les projets de **gestion de la sécurité** ?	Le système d'archivage doit s'intégrer aux pratiques favorisant la fiabilité et l'intégrité des données capturées dans le système. Pour la restitution des données les droits d'accès seront issus du LDAP. Deux exigences liées à la sécurité : la protection des données et le respect de la réglementation. Liens indispensables : un projet d'archivage électronique sous-entend la maîtrise d'œuvre à l'informatique pour la question des « outils », tout projet informatique doit avoir un représentant/responsable de la sécurité informatique qui dépend du département Protection industrielle. Voir chapitre précédent

4.2 Le déroulement du projet

4.2.1	Quelles sont les **étapes du projet** d'archivage ?	En mode projet classique, il y a forcément une phase avant-projet qui a deux temps forts : 1. l'analyse fonctionnelle 2. l'état des lieux Ce sont deux impératifs qui permettent d'analyser les clients, les acteurs, le périmètre, la connaissance des collections documentaires. La démarche permet également de décrypter les contraintes de gestion documentaire et d'archivage issues des réglementations / certifications métiers. Les résultats de cette phase avant-projet sont : 1. la définition du macro-processus, des sous-processus, des procédures, des standards et fiches d'instruction afférentes (politique d'archivage) 2. l'analyse des fonctions 3. l'audit du système existant 4. le « business model » 5. le plan Qualité 6. le plan de conduite du changement 7. le plan de migration des données 8. le rapport Risques 9. rapport de l'étude et de l'évaluation des solutions 10. le bilan économique Cette méthodologie, lourde mais très structurante, permet notamment de vérifier que tous les acteurs du projet sont en phase. Ensuite, on débouche sur la rédaction de la politique d'archivage avec la validation des propositions de procédures liées à un macro-processus et rédaction du référentiel d'archivage toujours selon un approche processus.
4.2.2	Comment définir et mettre en œuvre les **outils et procédures** nécessaires ?	Rédiger les spécifications des outils à mettre en place : cahier des charges en relation avec la charte d'archivage. Rédiger une procédure pour implémenter ces outils dans le système existant (articulation avec les autres éléments du système d'information, arriéré à traiter ou non) ; ces procédures devront être expliquées à l'ensemble des personnes concernées.
4.2.3	Le choix d'une **solution**	La solution technique fait appel au processus classique d'appel d'offres. Choisir au maximum une solution transparente pour l'utilisateur (capture et métadonnées automatiques).

		Les utilisateurs ne doivent pas être dépendants de l'informatique pour l'utilisation d'une telle solution. Pour diminuer les risques, si le projet fait appel à un intégrateur externe, éviter de choisir le logiciel d'abord. Lancer un appel d'offres vers les intégrateurs qui leur demande de choisir le produit dans une liste définie.
4.2.4	Comment vérifier la **qualité du système** ?	Établir la liste des points à vérifier pour la sécurité et le fonctionnement du système d'archivage. Relever tous les incidents relatifs à une recherche d'information difficile ou infructueuse ; analyse de chaque incident, proposition d'actions correctives. Analyse à faire très régulièrement (tous les 6 mois ou 1 an). MoReq2 (attendu pour 2008) inclura une procédure de test pour les logiciels d'archivage / records management.
4.2.5	Quel est l'intérêt d'un ou plusieurs **sites pilotes** pour le déploiement du projet	Un site pilote permet de tester des solutions et de les améliorer ce qui permet de proposer à l'ensemble de l'entreprise une solution testée et optimale. Une telle solution sera apte à donner confiance à l'ensemble des acteurs qui adhèreront plus facilement à de nouvelles techniques et procédures. Le site pilote permet de tester la validité du processus d'archivage, son intégration aux processus métiers, tester les campagnes de conduite du changement, tester les outils d'audit. Le pilote permet d'amorcer la pompe, afin de susciter l'intérêt des autres sites/acteurs de l'entreprise.
4.2.6	Quelle **communication** autour du projet et pourquoi ?	Politique d'archivage ou au minimum note de cadrage signée du directeur général. Le soutien officiel de la direction aide à lever les réticences. Il rassure et permet d'avoir l'adhésion des décideurs et des utilisateurs – en lien avec le choix de site pilote. Ne pas hésiter à faire appel au service Communication de l'organisme. Un tel système est l'affaire de tous et ne peut fonctionner correctement qu'avec la collaboration de tous les acteurs. La conduite du changement est indispensable. Il faut prévoir une équipe dédiée à la conduite du changement, établir des visuels (logo...), construire des campagnes de sensibilisation au RM, des formations utilisateurs.
4.2.7	Quelles actions de **formation** aux procédures et aux outils ?	La formation est un impératif dans la conduite de changement ; elle permet d'assurer la pérennité du système sur le long terme. Construire des campagnes de sensibilisation sous forme de formation en ligne, avec questionnaire. Les formations en classe suivent les campagnes de sensibilisation. Formation à prévoir dans le budget initial. Eviter au maximum de miser sur la transmission interne des connaissances en ne formant qu'un petit groupe (manque de temps et de

		compétences pédagogiques des formateurs internes pressentis). Déterminer qui s'en charge : les membres du groupe projet ou d'autres intervenants ?
4.2.8	Quels sont les avantages et les contraintes d'une **externalisation** du stockage ?	Avantages : • se recentrer sur son cœur de métier, • bénéficier de l'expertise technique et spécifique du prestataire, de sa veille permanente sur l'évolution des pratiques et de la technologie, • bénéficier d'un coût inférieur permis par la mutualisation des moyens. Contraintes : • exigence dans la sélection et le suivi par des audits permanents du prestataire sélectionné, Cf guide de l'externalisation mis en ligne sur le site de l'AAF ?: http://www.archivistes.org/IMG/GUIDE_externalisation_2006.pdf • étudier le coût de la création d'un bâtiment sécurisé par rapport à une externalisation. Une fois l'externalisation mise en place, risque pour l'entreprise qui voudrait récupérer l'intégralité de ses archives de payer le prix fort.
4.2.9	**Audit** du système	Il s'agit de repérer les dysfonctionnements du système ; ces dysfonctionnements peuvent être signalés par les utilisateurs et/ou par le responsable de l'archivage. Audit à effectuer régulièrement.
4.2.10	Audit des procédures	Analyser les difficultés survenues dans la recherche d'information (information non fiables, informations indûment détruites, temps de recherche ou d'accès anormal, etc.) pour corriger aussi bien le plan de classement, les durées de conservation, les métadonnées, les fonctionnalités du système, les procédures.
4.2.11	Audit de la qualité des données	Avoir une vision globale des types d'information qui composent le flux et le stock. Prendre en compte la notion de document vital, c'est à dire de document indispensable pou l'activité de l'organisme (Contrats, statut de société…).

4.3 Clés du succès et risques du projet

4.3.1	Clé : **soutien hiérarchique**	La légitimité et l'implication du comité de pilotage sont capitales. Sans le soutien de la direction rien ne peut se faire. Sensibiliser les dirigeants par rapport aux coûts/risques en cas de non protection, perte des données d'entreprise.
4.3.2	Clé : adhésion des	Sans l'adhésion des utilisateurs le projet aura de grandes

	utilisateurs	difficultés à s'imposer. Nécessité de communiquer régulièrement afin que chacun soit au courant de l'avancement du projet et puisse dans la mesure du possible y collaborer.
4.3.3	Clé : classement des données/documents en fonction des **risques**	Définir des priorités. Voir chapitre 2. Voir MoReq, chapitres 3 (Plan de classement), 5 (Conservation et sort final) et 8 (Recherche, repérage et restitution).
4.3.4	Risque : solution technique qui ne répond pas à tous les **besoins**	Insister sur l'importance du cahier des charges, renforcer le rôle de l'informatique.
4.3.5	Risque : difficulté d'évaluer le **retour sur investissement**	Ce risque tient au cycle de vie des documents, certains documents nécessitent une « période de test » pour découvrir leurs valeurs (archivage « purgatoire »). Rechercher des histoires vécues qui montrent la « souffrance » des utilisateurs (perte financière, temps passé).
4.3.6	Risque de **concurrence** avec d'autres projets	Communiquer et faire intervenir des membres du groupe dans d'autres projets pour rappeler la dimension transversale.
4.3.7	Risque de contournement du projet avec d'autres outils	Tendance des entreprises à utiliser les outils existants en les modifiant. D'où intérêt du cahier des charges techniques pour voir si les outils sont compatibles.
4.3.8	Risque du projet d'archivage et la **méthodologie EvRP**	Les préconisations Moreq s'intègrent à l'évaluation globale des risques demandée aux entreprises (méthodologie EvRP - Evaluation des Risques Professionnels, recommandée par l'INRS). Selon l'INRS, chaque entreprise doit suivre une méthode globale et transversale pour repérer, classer et manager les risques inhérents à ses activités (méthodologie EvRP). L'ensemble des préconisations que contient Moreq s'intègre justement à ces exigences au niveau du système d'information.
4.3.9	Risques que les données soient endommagées	Diminuer les mouvements physiques des documents. Dupliquer les données du SAE.
4.3.10	Risques que les données soient divulguées	Cahier des mouvements des documents à sécuriser. Traçabilité des accès.
4.3.11	Risques qu'une information n'ait pas été capturée et soit perdue	Déterminer en amont un audit régulier. Respect des procédures de versement / capture. Voir aussi la norme NFZ 42-013 « conception et exploitation du système informatique en vue d'assurer la conservation et l'intégrité des documents stockés ».

4.4 Les contraintes

4.4.1	**Rigueur**	Un système d'archivage des données électroniques exige, comme tout système s'appuyant sur l'informatique, de la rigueur. L'approximatif qui pouvait faire fonctionner, tant bien que mal, un système classique papier, n'a plus sa place dans l'environnement électronique. Rien ne peut reposer sur la mémoire humaine.
4.4.2	Travail en **amont**	Avant toute mise en place d'un tel système, l'organisme doit avoir rédigé un cahier des charges précis. Les procédures doivent être, rédigées, approuvées par l'ensemble des acteurs et validées par la direction. La mise en place d'un SAE demande une analyse initiale de la situation et des problèmes inhérents à l'entreprise ou l'organisme tant sur le plan technique qu'humain, cette dernière composante étant trop souvent négligée.
4.4.3	Renforcement du service ou de la **mission Records management / Archivage**	Un service ou une mission *ad hoc* doit avoir les moyens intellectuels et financiers pour pouvoir : • contrôler les données capturées et leurs métadonnées quand celles ci ne sont pas automatiques, • assurer une veille juridique afin que l'organisme soit toujours en conformité avec la législation qui peut être amenée à changer rapidement dans un domaine relativement nouveau, • contrôler la bonne adéquation du SAE avec les besoins et contraintes de l'organisme.
4.4.4	**Changement** de mentalité	Rigueur et procédures sont les pré-requis minimum pour un tel système. C'est dans bien des cas un véritable changement des mentalités qu'il faut gérer et accompagner. Chacun est responsable des données qu'il produit. Dans un SAE, l'archivage est l'affaire de tous et le service Archives a une place centrale.
4.4.5	**Nécessité de solutions à long terme**	Des solutions à court terme peuvent entraîner une multiplication des serveurs, une disparité des logiciels ayant pour conséquences • Une duplication des données • Une disparité des données • Un coût de maintenance et de consultation élevé
4.4.6	Quels sont les dysfonctionnements que le système d'archivage ne peut pas résoudre ?	Un système d'archivage est difficilement rétroactif : il prend prioritairement en compte les documents/données nouvellement créés et quelques années d'antériorité (2, 3 voire 4 ans) mais ne résout par les problèmes des documents créés il y a dix ans et qui ont été mal archivés. Une reprise du stock peut être envisagée mais une reprise complète peut présenter un coût prohibitif. Voir les risques.

4.5 Les coûts

4.5.1	**Investissements initiaux**	Ces investissements correspondent à ceux nécessaires à la création de la plate-forme d'archivage électronique : 1. Le serveur d'archivage, hébergeant les applicatifs, et équipé de disques permettant le stockage des documents fréquemment consultés, dont l'accès doit être immédiat (archives en ligne). 2. Des supports WORM logiques ou physiques, dimensionnés à la volumétrie estimée (capacité, durabilité et fiabilité annoncée des supports). Ces supports pourront être conservés dans un robot (librairie automatisée ou Juke-box) ou dans des systèmes spécialisés (voir les produits EMC, IBM, NetApp, etc.), pour constituer des archives devant rester rapidement consultables. Le robot sera également dimensionné en fonction du nombre de supports, et donc de la capacité de stockage nécessaire (nombre de slots). Les archives dont la consultation est évaluée comme occasionnelle, pourront être stockés sur des supports hors Juxe-box (archives hors ligne). 3. Les applicatifs permettant d'assurer les fonctions principales suivantes : • versement par capture ou archivage volontaire • restitution / consultation (incluant les programmes associés) • suppression et destruction • gestion des médias de stockage • gestion du plan de classement et des règles d'archivage • gestion de la sécurité (tracabilité, confidentialité) • administration et exploitation. 4. Les prestations initiales de conception et de mise en place de la plate-forme comprenant : • analyse des spécifications et des niveaux de services nécessaires • installation, configuration et le déploiement de la solution • formation, transfert de compétence • assistance, accompagnement lors de la mise en place • suivi de projet et la maîtrise d'œuvre.
4.5.2	Les coûts de **maintenance technique**	Administration et contrôle du bon fonctionnement de la plate-forme Contrôle d'intégrité et migration des supports Assistance technique des utilisateurs Veille technologique permanente Maintenance annuelle des logiciels Maintenance annuelle des matériels
4.5.3	Le bilan financier global	Il est globalement difficile d'évaluer le coût d'un archivage électronique.

		Au delà des coûts directs, le bilan financier devra prendre en compte les paramètres suivants: • les bénéfices financiers attendus par la diminution de certains coûts administratifs, par la gestion électronique de certains documents et des flux documentaires associés ; • les coûts indirects liés aux risques de la non mise en place d'un système d'archivage électronique (amendes et sanctions, coûts des systèmes palliatifs…).
4.5.4	Evaluer les risques et les coûts d'un **non archivage**	Nécessité d'un retour d'information sur ce que coûte le fait de ne pas retrouver l'information / les documents : ▪ cas des contentieux, ▪ cas de documents notariés à refaire, ▪ impact des procédures « discovery » (procédure officielle de recherche d'information). Prendre en compte le coût des externalisations de stockage quand elles se font sans maîtrise de l'information externalisée (pas d'inventaire, pas de délai contractuel, etc.) Sur ces aspects, il est judicieux de s'assurer de l'appui du contrôle de gestion et de celui de la direction de l'audit.

4.6 Les bénéfices

4.6.1	**Rapidité** de recherche	Un système d'archivage des données électroniques permet un accès (sous réserve des droits) rapide à l'information car il n'y a plus de dépendance physique entre le chercheur et le document qui peut être consulté où que l'on se trouve.
4.6.2	Traçabilité des consultations	Les métadonnées liées à un SAE permettent de savoir à tout instant qui a consulté le document. Ces métadonnées sont à prévoir dès la conception du système.
4.6.3	**Centralisation** des informations	Un SAE permet une concentration des informations en un point donné et évite les déperditions d'informations classiques dues à un archivage anarchique et laissé au bon vouloir de chacun.
4.6.4	Partage de l'information sous contrôle	La centralisation des informations permet un meilleur partage entre tous les partenaires ayant accès à cette information
4.6.5	**Sécurité**	Les informations centralisées peuvent être sauvegardées et dupliquées plus facilement.
4.6.6	Gain de place physique	Un SAE sécurisé permet de se dégager des impressions papier qui gonflent le volume des informations à archiver.
4.6.7	Eliminations (exécution) plus simples	Il est facile de supprimer des fichiers électroniques, sous contrôle. La destruction du papier est un processus simple mais lourd qui a un coût et qui prend du temps.
4.6.8	Comment évaluer les coûts et bénéfices du projet ?	Rédiger une grille d'évaluation des coûts matériels : équipements, logiciels, supports, coût de maintenance (matérielle et logicielle, migration). Evaluer les coûts humains : réalisation et maintenance du plan de classement et des listes de métadonnées ;

		administration du système ; audit et formation aux outils. Etude des risques attachés à chaque ensemble cohérent de documents/données. Distinguer les gains pour les employés et les gains pour l'entreprise.
4.6.9	Bénéfices du projet **pour les employés** ?	Pour les employés, le processus RM permettra de: • Sécuriser les archives durant les changements de postes. Assurer la continuité de l'information • Savoir où trouver les documents recherchés, n'importe quand, quel que soit le créateur • Accélérer le processus de recherche (contrats, courriels, factures…) • Gérer les archives facilement • Améliorer l'efficacité de leur travail journalier
4.6.10	Bénéfices du projet **pour l'entreprise** ?	Pour l'entreprise, le processus RM permettra de: • Être en conformité avec la législation et les règlements et standards de l'entreprise, • Faciliter la gestion des risques jusqu'à la destruction des archives. Remplir les obligations législatives et réglementaires, • Fournir une protection et un support en cas de contentieux, • Améliorer le traitement des réclamations clientèle par un meilleur accès à l'information ; impact en termes d'image, • Maintenir la mémoire de l'entreprise.
4.6.11	**Exemples** de bénéfices quantitatifs	• Réduction des pertes fiscales: les récupérations de TVA qui ne peuvent être prouvées, dues à un archivage insuffisant • Réduction des coûts de contentieux (paiements, avocats), grâce à des archives faciles à rechercher associées à des procédures d'archivage bien pensées • Réduction des amendes douanières, fiscales, de licence et de visa, liées à des pratiques d'archivage inadéquates • Réduction des coûts de l'impact de pertes catastrophiques d'un établissement, spécialement dans les endroits éloignés • Réduction des temps de recherche durant une investigation judiciaire • Réduction des coûts de stockage des archives papier • Réduction des coûts grâce à l'externalisation du stockage des archives papier • Réduction des coûts de stockage électroniques, spécialement dans les systèmes de sauvegarde

4.7 Pour en savoir plus : Méthodologie DIRKS

Méthodologie DIRKS, guide, extraits

voir http://www.records.nsw.gov.au/recordkeeping/dirks-state-records-act_4230.asp
(trad. Marie-Anne Chabin ; NB : le mot « archivage » traduit « recordkeeping »).

1.Contexte et objectif

1.1. Finalité de l'archivage

Une bonne administration a besoin d'un bon archivage. Un bon archivage contribue à une gestion responsable et efficace par la création, l'organisation et la conservation d'une trace pertinente, précise, fiable, accessible et durable des activités et des décisions administratives.

[…]

Autrefois, les bonnes pratiques d'archivage étaient plus ou moins une seconde nature chez les fonctionnaires. Le service public d'hier, avec l'importance donnée aux procédures, à la hiérarchie, au recours à des agents de classement et autres secrétaires, assurait que l'on créait et archivait de bons documents. En ce début de XXIe siècle, de telles certitudes sont ébranlées. Maintenant, les administrations mettent l'accent sur les flux d'information par-dessus les procédures et la hiérarchie.

[…]

Au cours des dernières années, la diffusion des systèmes électroniques a exacerbé la dérive vers des pratiques d'archivage ponctuelles ou non-conformes. L'adoption du traitement de texte, de la messagerie électronique et des applications multimédia ont conduit à une situation où la preuve des décisions administratives et des relations contractuelles est souvent stockée sur des disques durs, dans des boîtes de messagerie ou des dossiers partagés d'individus ou de groupes de travail. Cette forme d'archivage ne satisfait pas aux exigences d'une preuve complète, précise, fiable, accessible et durable de l'activité administrative. De plus, de telles pratiques présentent des risques inacceptables pour la capture et la gestion de la preuve. Non seulement, des individus peuvent détruire des document sans réfléchir vraiment aux besoins de conservation de ces archives, mais encore on risque de perdre de grandes quantités d'archives à chaque mise à jour de logiciel ou de matériel.

Heureusement, si la technologie contribue au problème, elle offre aussi des moyens de le résoudre. La solution réside dans la conception et la mise en œuvre de systèmes qui garantissent la production de documents complets et précis et leur archivage pendant la durée requise par les besoins de gestion des affaires, la reddition des comptes, ou pour un intérêt collectif plus large. L'apparition des archives électroniques a forcé les professionnels de l'archivage à rendre compatibles les principes fondamentaux et les composantes d'un bon archivage avec les contraintes de l'environnement électronique.

Au sein de cette communauté professionnelle, un consensus s'est fait jour sur les éléments essentiels d'un cadre théorique et pratique pour un archivage moderne et de bonnes pratiques.

Index

FIN DU DOCUMENT

Apprivoiser MoReq

Recueil de définitions

Introduction

Ce recueil présente un ensemble de définitions préexistantes correspondant aux principales notions développées dans le Guide.
Le choix des entrées a été fait en tenant compte de l'hétérogénéité des destinataires du guide sur le plan des métiers, des domaines, et du niveau de connaissance des concepts et techniques de la gestion de l'information.

Une notion peut être accompagnée de définitions multiples quand les termes ont une connotation un peu différente selon leur domaine d'utilisation :

- documentation et archives,
- droit,
- technologies informatiques.

Certaines définitions s'appliquent non pas au terme d'entrée, mais à des termes du même champ lexical.

Ce travail terminologique devra être poursuivi pour aboutir à un glossaire du domaine des archives.

Sources

Les sources principales sont les normes, les études et travaux de groupes de réflexion institutionnels et des ressources terminologiques.
Les références des quelques sources ponctuelles sont précisées à la suite des définitions.

a) Domaine de la documentation et des archives

- Norme NF ISO 15489 -1 Avril 2002 - Information et documentation « Records Management » - Principes directeurs : www.afnor.fr
- Norme NF Z42-013 Décembre 2001, Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes (homologuée) : www.afnor.fr
- Norme NF EN 82045-1 Mars 2002 - Gestion de documents - Partie 1 : principes et méthodes : www.afnor.fr
- MoReq : Mars 2001 —- Model Requirements for the management of Electronic Records - MoReq Specification –DLM-FORUM INSAR Information Summary on Archives supplement VI - Modèle d'exigences pour l'organisation de l'archivage électronique - Traduction française – Trad. Marie Anne Chabin, novembre 2004,
- Archivistique - Terminologie Direction des archives de France DAF : http://www.archivesdefrance.culture.gouv.fr/fr/archivistique/index.html
- Abrégé d'archivistique Association des archivistes français AAF, Paris, 2007-Glossaire

1. La maîtrise du cycle de vie du document numérique, Présentation des concepts. Glossaire Rapport établi par le groupe de travail DGME/SDAE - APROGED– version 3 du 22 mai 2006, (mise à jour 2006)
   http://www.adij.asso.fr/medias/cycle_de_vie_document_numerique_v3_1_(2).pdf ou
   http://www.aproged.org/Portals/0/Cycledeviedocumentnum%c3%a9rique.pdf

b) Domaine des technologies de l'informatique

- Glossaire - Termes relatifs à la sécurité des systèmes d'information, Direction centrale de la sécurité des systèmes d'information (DCSSI) : - http://www.ssi.gouv.fr/fr/glossaire/index.html#c
- CSTIC - Commission Spécialisée de Terminologie et de Néologie de l'Informatique et des Composants Electroniques : http://www.ensmp.net/cstic/
- Guide de l'horodatage, Fédération nationale des tiers archiveurs (FNTC), Collection Les Guides de la Confiance, Novembre 2004 : www.fntc.org
- Charte d'éthique et de conformité des services de tiers archivage, Fédération nationale des tiers archiveurs (FNTC), 2001 : www.fntc.org
- Documents par le MINEFI/DSI : Charte d'éthique et de conformité des services de tiers archivage, etc.. Les références de ces documents sont indiquées à la suite des définitions concernées.
- Dictionnaire informatique, Infoclick solution informatique - http://www.infoclick.fr/dico/index.html

c) Domaine du droit

- Glossaire V0.31, ADAE - Projet Adèle 121: https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/adele_121_gestion_de/public/adele_121_-_glossair/view
- Vocabulaire juridique, Gérard Cornu, PUF, 8ème édition, 2000.

d) Ressources terminologiques

- Trésor de la langue française (TLF) : http://www.atilf.fr/
- Grand dictionnaire terminologique (GDT) - Office Québécois de la langue française - www.granddictionnaire.com
- Wikipédia : http://fr.wikipedia.org/wiki/Accueil

Entrées

1. Accès
2. Acte authentique
3. Acte juridique
4. Administrateur
5. Archivage
6. Archives
7. Archives définitives ou historiques
8. Attribut
9. Authenticité
10. Capture
11. Certificat / Certificat numérique / Certificat électronique
12. Charte d'archivage
13. Chiffrement / Déchiffrement
14. Classement
15. Conservation
16. Conversion
17. Cryptographie
18. Cycle de vie du document
19. Destruction
20. Document
21. Droits d'usage
22. Enregistrement
23. Espace de confiance
24. Exploitabilité
25. Externalistion
26. Externalisation des Archives
27. Fiabilité
28. Format
29. Granularité
30. Horodatage
31. Identifiant
32. Indexation
33. Intégrité
34. Interopérabilité
35. Lisibilité
36. Marquage
37. Métadonnées
38. Migration
39. Nommage
40. Pérennité
41. Plan de classement
42. Plate-forme
43. Profil (d'accès)
44. Records Management (RM)
45. Ressource
46. Restauration
47. Réversibilité
48. Sauvegarde
49. Sceau ou Empreinte ou Condensat
50. Scellement numérique
51. Signature électronique
52. Sort final
53. Stockage
54. Tiers archiveur
55. Tiers de confiance
56. Traçabilité
57. Transfert
58. Valeur de preuve ou Valeur probante
59. Valeur documentaire
60. Valeur patrimoniale
61. Versement

Définitions

1 Accès

- Droit, modalités et moyens de rechercher, d'exploiter ou de retrouver l'information
(Equivalent anglais : access)
Source : ISO 15489-RM

- Au sens juridique du terme : droit par un particulier d'opérer une démarche auprès d'un service public pour la défense de ses intérêts
Droit d'accès « au dossier » : Droit pour l'intéressé, ou parfois seulement son conseil d'avoir connaissance des pièces de la procédure qui le concerne (suivant des modalités variables : consultation, copie, etc…)
Droit d'accès « aux documents administratifs. Droit d'avoir communication de documents administratifs non nominatifs, reconnu à toute personne, à titre de liberté publique, comme moyen de garantir son droit à l'information.
Source : Vocabulaire juridique - Gérard Cornu

2 Acte authentique

- L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises. Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat.
Source : décret 2005-972

3 Acte juridique

- Opération juridique (*negotium*) consistant en une manifestation de la volonté (publique ou privée, unilatérale, plurilatérale ou collective) ayant pour objet et pour effet de produire une conséquence juridique (établissement d'une règle, modification d'une situation juridique, création d'un droit, etc). Exemple : arrêt municipal édictant une réglementation de police ; décision nommant un fonctionnaire.
Source : Vocabulaire juridique - Gérard Cornu

4 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.
Source : MoReq

5 Archivage

- Transfert de *documents* qui ont cessé d'être d'utilité courante dans un local de *stockage* ou dans un *service d'archives* compétent pour les recevoir. Le verbe correspondant est archiver.
Source : Terminologie DAF

- « Maîtrise de l'archivage »
Forme abrégée « Archivage »
Démarche d'organisation et de contrôle de la production, de la conservation et du sort final des informations liées à l'environnement réglementaire et aux besoins de traçabilité
(Equivalent anglais: records management)
CR de la réunion du 15 septembre 2006, document CSTIC numéro 115, p.6.

- « Archivage électronique » : action de recueillir, de classer et de conserver des informations à des fins de consultation ultérieure. L'archivage est une fonction en soi, qu'il ne faut confondre ni avec la

sauvegarde ni avec la gestion électronique des documents. Les données archivées nécessitent un support adapté, fiable, résistant au temps et suffisamment sécurisé.
(Equivalent anglais : electronic archiving)
*Source : FNTC - Charte des tiers archiveurs***Archives**

- Documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité.
(Code du patrimoine du 20 février 2004 Titre II chapitre II)
Source : Terminologie DAF

- « Documents d'archives / documents » :
Supports d'information 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
(Equivalent anglais : records)
Source : ISO 15489-RM

- « 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.
Source : MoReq

- « Documents d'archives » : Ensemble constitué d'un support et de l'information qu'il porte, utilisable comme preuve ou à des fins de consultation
Source : Abrégé AAF

7 Archives définitives ou historiques

- Document ayant vocation à être conservés indéfiniment
Source : Abrégé AAF

- Documents qui, ayant subi des tris, ne sont plus susceptibles d'élimination, par opposition aux archives courantes ou intermédiaires, et qui sont conservés pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, et pour la documentation historique de la recherche.
Source : Terminologie DAF

8 Attribut

- Des attributs sont associés à la plupart des éléments contenus dans l'EAD. Les attributs permettent de qualifier les éléments. On leur donne une valeur selon le contexte dans lequel ils apparaissent.
Source : Terminologie DAF

- Qualificateur d'un individu, d'un rôle ou d'un objet (par exemple : adresse, âge, profession, fonction d'une organisation, etc. .
Source : Glossaire ADAE - projet Adèle

Voir aussi Métadonnées

9 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.
Source : MoReq

- Un « document authentique » est un document dont on peut prouver :

qu'il est bien ce qu'il prétend être, qu'il a été effectivement produit ou reçu par la personne qui prétend l'avoir produit ou reçu, et qu'il a été produit ou reçu au moment où il prétend l'avoir été.
Source : ISO 15489-RM

- « Authentique »

1/ - Qualité de l'objet ou du document (œuvre, écrit, etc.) dont l'auteur ou l'origine sont attestés, notamment sur la foi d'un certificat.
2/ - Qualité (spécialement force probante) dont est revêtu un acte du fait qu'il est reçu ou, au moins, dressé par un officier public compétent, suivant les formalités requises.
Source : Vocabulaire juridique - Gérard Cornu

10 Capture

- La finalité de l'intégration des documents dans le système d'archivage est de :

- établir un environnement reliant le document, son producteur et le contexte d'activité économique, qui l'a engendré,
- placer le document, avec son environnement, dans un système d'archivage, et
- relier ce document à d'autres documents d'archives.

(Equivalent anglais : capture)
Source : ISO 15489-RM

- Enregistrement, classement, ajout de métadonnées et stockage d'un document dans un système d'archivage.
Source : MoReq

11 Certificat / Certificat numérique / Certificat électronique

- Déclaration formelle confirmant les résultats d'une évaluation, et le fait que les critères d'évaluation ont été correctement utilisés. [ITSEC[10]]
Source : DCSSI : Glossaire sécurité des systèmes d'information

- Fonctionnellement, un certificat se définit comme un objet informatique logique lié à une entité.

Il s'agit d'une clé publique signée par une Autorité de Certification. L'ensemble bi-clé/certificat permet d'utiliser des fonctions cryptographique (cryptographie asymétrique) permettant notamment des opérations d'authentification, de signature numérique et de chiffrement.
Source : Glossaire ADAE - projet Adèle

- Fichier électronique attestant qu'une clé publique appartient à l'entité qu'il identifie (personne physique ou morale ou entité matérielle). Il est délivré par une autorité de confiance : l'Autorité de certification. En signant le certificat elle valide le lien en l'entité et le bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Source : Ministère de l'économie, des finances et de l'industrie (Délégation aux Systèmes d'information). Politique de Certification - type Entreprise – Juin 2003

[10] ITSEC : Critères d'évaluation de la sécurité informatique définis et publiés par la Commission des communautés européennes en 1991

12 Charte d'archivage

- Document qui regroupe les procédures et qui explique les contraintes légales, organisationnelles ainsi que techniques en cause dans ces procédures.

Source : Abrégé AAF

13 Chiffrement / Déchiffrement

- Chiffrement » : transformation cryptographique de données produisant un cryptogramme.
- Déchiffrement » : opération inverse d'un chiffrement réversible.

[ISO 7498-2]
Source : DCSSI : Glossaire sécurité des systèmes d'information

14 Classement

- Identification systématique et classement des activités et des documents d'archives en catégories suivant l'organisation logique d'un système de classification et en accord avec ses principes, ses méthodes et ses règles.

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.
(Equivalent anglais : classification)
Source : ISO 15489-RM

Voir aussi Plan de classement

15 Conservation

- Actions et tâches concourant à la pérennité technique et intellectuelle des documents authentiques

(Equivalent anglais : preservation)
Source : ISO 15489-RM

- « Conservation matérielle » : Une des fonctions fondamentales d'un service d'archives consistant à garder physiquement les documents qui lui sont confiés
- « Conservation préventive » : ensemble des mesures prises par un service d'archives pour assurer la conservation matérielle des documents qui lui sont confiés en vue d'assurer leur sauvegarde

Source : Abrégé AAF

16 Conversion

- Action de transférer des documents d'un support à un autre, ou d'un format à un autre.

(Equivalent anglais : conversion)
Source : ISO 15489-RM

Voir aussi Migration

17 Cryptographie

- Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur contenu ne passe inaperçu et/ou d'empêcher leur utilisation non autorisée.[ISO 7498-2]

Source : DCSSI : Glossaire sécurité des systèmes d'information

18 Cycle de vie du document

- Période qui s'étend de l'idée conceptuelle jusqu'à la destruction logique et physique d'un document.

Source : ISO CEI 82045

19 Destruction

- Action d'éliminer ou de supprimer des documents, de façon irréversible
(Equivalent anglais : destruction)
Source : ISO 15489-RM

- Procédure réglementée qui consiste à soustraire un dossier ou un ensemble de dossiers du versement auquel il appartient, ou bien encore à soustraire des documents du dossier auquel ils appartiennent, car ils sont dépourvus d'utilité administrative et d'intérêt historique
Source : Abrégé AAF

20 Document

- Tout écrit ou enregistrement considéré comme une unité
(Equivalent anglais : document)
Source : ISO 15489-RM

- Ensemble composé d'un support et des informations enregistrées sur ce support
Source : NF Z42-013

- Quantité structurée et fixe d'informations qui peut être gérée et interchangée en tant qu'unité entre les utilisateurs et les systèmes. [ISO/CEI 8613-1, modifiée*]*
Note : cette unité peut ne pas être nécessairement perceptible à l'homme. L'information est habituellement stockée sur un support.
Source : ISO 82045-1 gestion documentaire

- Du latin : *documentum*, de *docere* : instruire, enseigner.
1/ - Ecrit contenant un élément de preuve ou d'information. Comp. Pièces, archives, *instrumentum*, écritures. V. Dossier, papier, registre, journal, commencement de preuve par écrit, note.
2/ - Terme étendu à d'autres supports d'information. Ex. Enregistrement, films, objets saisis.
Source : Vocabulaire juridique - Gérard Cornu

21 Droits d'usage

- Droit réel permettant à une personne de se servir de la chose d'autrui et d'en percevoir la portion de fruits nécessaire à ses besoins et à ceux de sa famille.
- Fait d'utiliser quelque chose pour sa consommation, pour ses besoins.
Source : Citation tirée de la rubrique « Usage » du Trésor de la langue française

22 Enregistrement

- Action de donner un identifiant unique à un document au moment de son archivage
(Equivalent anglais : registration)
Source : ISO 15489-RM

- Inscription intégrale ou par extrait sur un registre et par extension sur tout support durable, destinée à garder trace d'une opération (correspondance, entrées et sorties de documents)
Source : AFNOR Dictionnaire des archives, Paris 1991

23 Espace de confiance

- Ensemble de composants fonctionnels et techniques permettant de fournir à une personne les outils et les ressources nécessaires pour effectuer des opérations et des transactions électroniques.
Un espace est dit de confiance quand il répond à des critères de sécurité considérés comme suffisants par la Maîtrise d'Ouvrage concernée.
Source : Glossaire ADAE - projet Adèle

24 Exploitabilité

■ Un document utilisable est un document qui peut être localisé, récupéré, communiqué et interprété. Il convient qu'à chaque communication, le document soit relié à l'activité ou à l'opération à l'origine de sa création. Il convient que les liens contextuels des documents portent les informations nécessaires à la compréhension des opérations qui les ont crées et utilisés. Il est recommandé de pouvoir replacer un document dans le contexte d'activités ou de fonctions élargies. Il convient de maintenir les liens entre les archives qui documentent une succession logique d'actions.
(Equivalent anglais : Useability)
Source : ISO 15489-RM

25 Externalistion

■ L'externalisation, aussi appelée *outsourcing*, désigne le transfert de tout ou partie d'une fonction d'une entreprise vers un partenaire externe. Elle consiste très souvent en la sous-traitance des activités non essentielles et non stratégiques (celles qui ne sont pas productrices de revenus) d'une entreprise. Il s'agit d'un outil de gestion stratégique qui se traduit par la restructuration d'une entreprise autour de sa sphère d'activités : ses compétences de base et son cœur de métier (core business en anglais)…….
L'externalisation diffère de la simple prestation extérieure de services, et de la simple sous-traitance, dans la mesure où il y a :
- pilotage étroit par l'entreprise donneuse d'ordre,
- engagement du prestataire externe.

Source : Wikipédia

Voir aussi Tiers de confiance et Tiers archiveur

26 Externalisation des Archives

■ Avoir recours à la sous-traitance pour la conservation de ses propres archives
Source : Abrégé AAF

■ L'externalisation est définie comme l'action pour toute institution de confier le stockage et la gestion de tout ou partie des ses archives à une société tierce.
Source : Manuel d'externalisation AAF section entreprise

Voir aussi Tiers archiveur

27 Fiabilité

■ Un document fiable est un document dont le contenu peut être considéré comme la représentation complète et exacte des opérations, des activités ou des faits qu'il atteste, et sur lequel on peut s'appuyer lors d'opérations, d'activités ou de faits ultérieurs. Il est recommandé que les documents soient créés au moment de l'opération ou du fait qu'ils relatent ou juste après, par des personnes qui ont une connaissance directe des faits ou par des outils courants dans la conduite des affaires.
Source : ISO 15489-RM

28 Format

■ Structure définie de données contenues sur un support magnétique ou autre, établie selon des règles qui régissent le stockage, l'affichage, la manipulation, l'impression ou la transmission de ces données. [Office de la langue française, 2001]
Source : Dictionnaire terminologique québécois

■ 1 : Élément de langage spécifiant la représentation, sous forme de caractères, des objets désignant les données sur un support d'information.
2 : Structure définie de données contenues sur un support magnétique ou autre, établie selon des règles qui régissent le stockage, l'affichage, la manipulation, l'impression ou la transmission de ces

données
Source : Dictionnaire terminologique québécois

29 Granularité

- Degré de fragmentation d'une entité donnée (mémoire, disque, fichier, champ, etc.) en unités plus petites, dans un but de protection ou pour la gestion.
Note(s) : Par exemple, on dira que la granularité d'un champ est plus fine que celle d'un fichier pris globalement.
Source : Dictionnaire terminologique québécois

- Taille minimale d'un élément pouvant être manipulé par un système. La granularité d'un logiciel de réplication de base de donnée peut être par exemple un champ. La granularité d'un programme est un facteur essentiel de ses performances sur une machine parallèle (plus elle est petite, plus le programme sera efficace)
Source : Dictionnaire informatique Infoclick

30 Horodatage

- Opération qui consiste à dater un document électronique de façon fiable.
Source : Dictionnaire terminologique québécois

31 Identifiant

- Remplacé par « Cote » : Ensemble de symboles (lettres, chiffres, signes) servant à classer chaque « article » dans son fonds ou sa série
Source : Dico AFNOR

- Remplacé par « Cote » : La cote est une combinaison de symboles (lettres, chiffres, signes) destinée à identifier chacun des articles conservés dans un service d'archives.
Source : Circulaire AD 98-8 de la DAF, 1998

- Information permettant d'identifier une entité (exemple : une personne ou une application) (par exemple : NIR, NUMEN, n° matricule, RNE, n° de passeport, etc.).
Source : Glossaire ADAE - projet Adèle

- Tout nom, caractère ou indicatif caractérisant une donnée et permettant de l'identifier ou de la reconnaître comme telle dans toute technique de recherche.
Source : Dictionnaire terminologique québécois

32 Indexation

- Action de définir des points d'accès pour faciliter le repérage des documents et/ou des informations.
Source : ISO15489-RM

- Opération destinée à représenter par les éléments d'un langage documentaire ou naturel des données résultant de l'analyse du contenu d'un document ou du document lui-même
Source : Abrégé AAF

33 Intégrité

- L'intégrité d'un document renvoie au caractère complet et non altéré de son état.
Source : ISO15489-RM

- Caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification

Source : NF Z42-013

- 1/:propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée. [*ISO 7498-2]*
- 2/ l'intégrité du système et de l'information traitée garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est à dire à la garantie de son origine et de sa destination. [IGI nç900]

Source : DCSSI : Glossaire sécurité des systèmes d'information

- Protection contre l'altération accidentelle ou volontaire d'un message émis.

Source : http://www10.finances.gouv.fr/fonds_documentaire/minefi/services/securite/teleprocedures/html/html/glossaire.htm

34 Interopérabilité

- Faculté que possèdent des services ou des composants hétérogènes de fonctionner conjointement. L'une des conditions fondamentales permettant la communication entre ces services et ces composants est l'utilisation de langages et de protocoles communs.

Par exemple, les protocoles SOAP ou XML sont normalisés et permettent aux différents services web d'échanger des informations selon les mêmes règles et les mêmes méthodes

Source : Glossaire ADAE - projet Adèle

- Aptitude des équipements terminaux (informatiques et de télécommunication) à fonctionner d'une part, avec le réseau et d'autre part, avec les autres équipements terminaux permettant d'accéder à un même service.

Source : Rapport du groupe de travail présidé par M. Francis Lorentz sur le Commerce électronique : Une nouvelle donne pour les consommateurs, les entreprises, les citoyens et les pouvoirs publics. - extraits du glossaire établi par AFCEE/EDIFRANCE, Observatoire du commerce et des échanges électronique)

- L'interopérabilité est le fait que plusieurs systèmes, qu'ils soient identiques ou radicalement différents, puissent communiquer sans ambiguïté et opérer ensemble.

Source : /Dématérialisation et archivage électronique/, Jean-Marc Rietsch, Marie-Anne Chabin et Eric Caprioli, Dunod, 2006, p. 104.

35 Lisibilité

- La lisibilité est l'aptitude d'un texte à être lu rapidement, compris aisément et bien mémorisé. La lisibilité est "une aptitude du texte à se faire comprendre" (Source : Bourque, 1989). On peut distinguer la lisibilité matérielle et la lisibilité intellectuelle : en anglais on a les mots "legible" / "readability" ; en français on peut opposer lisable-inlisable et lisible-illisible. La lisibilité matérielle doit être au service de la lisibilité intellectuelle.

Source : http://www.alsace.iufm.fr/web/former/formcont/2nddegre/res_peda/pao/i_lisibilite.htm

36 Marquage

- Marquage des supports de stockage avec le numéro de série du lecteur-enregistreur :

Lorsque cette option a été retenue, lors de l'écriture de chaque document, en plus de l'horodatage, le numéro de série du lecteur enregistreur tel qu'il est fourni par le constructeur de ce matériel doit être inscrit sur le support de stockage avant ou après l'écriture du document sur le support..

Source : NF Z42-013

37 Métadonnées

- Données décrivant le contexte, le contenu et la structure des documents ainsi que leur gestion dans le temps
- (Equivalent anglais : metadata)

Source : ISO 15489-RM

■ (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)).
Source : MoReq

■ Ensemble des informations renseignant la structure d'un groupe de données ; les métadonnées exercent la fonction de médiateur entre l'utilisateur et l'information qu'il recherche ; elles permettent également de définir les caractéristiques d'évolution dans le temps d'un document -(Source : Circulaire du 2 Novembre 2001 relative à la gestion des archives dans les services et établissements publics de l'Etat paru au JO du 4 Nov 2001)
Source : Terminologie DAF

■ Informations descriptives à propos d'un document. Ce concept est surtout utilisé lorsque le document lui-même n'est pas structuré et ne possède pas de données descriptives intrinsèques
Source : Abrégé AAF

38 Migration

■ Action de transférer des documents d'un système à un autre en préservant leur authenticité, leur intégrité, leur fiabilité et leur exploitabilité
(Equivalent anglais : migration)
Source : ISO 15489-RM

Voir aussi conversion

39 Nommage

■ Activité qui consiste à attribuer des noms uniques à des entités de réseau ou à des utilisateurs.
Note(s) : L'utilisation des termes affectation d'un nom et désignation convient davantage, lorsqu'il s'agit d'attribuer un nom à une seule entité ou à une seule personne. L'affectation d'un nom à un organisme, c'est-à-dire sa désignation, est une activité de nommage. [Office de la langue française, 2001]
Source : Dictionnaire terminologique québécois

40 Pérennité

■ Capacité à garantir l'intégrité des données archivées sur une longue durée.
(Equivalent anglais : durability)
*Source : FNTC - Charte des tiers archiveurs***Plan de classement**

■ 1/ Système qui fixe l'organisation des archives courantes et intermédiaires en usage dans les bureaux, permettant de les ranger de les classer et de les retrouver.
■ 2/ Ordre dans lequel les archives définitives d'un fonds, d'une série ou d'un versement ont été classées et ordonnées dans un service d'archives. A ne pas confondre avec cadre de classement
Source : Abrégé AAF

■ Structure hiérarchique et logique permettant le classement et le repérage de documents ou d'ensembles documentaires.
Source : Définition moissonnée sur le Web

Voir aussi classement

42 Plate-forme

■ Ensemble constitué par un système d'exploitation et un ordinateur (donc une architecture matérielle donnée).
Source : Dictionnaire informatique Infoclick

43 Profil (d'accès)

■ Groupe d'autorisations fonctionnelles allouées à un ensemble d'utilisateurs prédéfini. [Source : spécifications fonctionnelles PRO (Annexe 1 référence [2])]
Source : MoReq

■ Profil applicatif (PA)
Identifiant permettant d'attribuer des droits dans le cadre de l'accès aux ressources d'une application
Source : Glossaire ADAE - projet Adèle

44 Records Management (RM)

■ (Terme anglais toléré en français) Champ de l'organisation et de la gestion en charge d'un contrôle efficace et systématique de la création, de la réception, de la conservation, de l'utilisation et du sort final des documents, y compris des méthodes de fixation et de préservation de la preuve et de l'information liées à la forme des documents
(Equivalent anglais : records management)
Source : ISO 15489-RM

■ Ensemble des mesures destinées à rationaliser la production, le tri, la conservation et l'utilisation des archives courantes et intermédiaires.
Source : Abrégé AAF

45 Ressource

■ Moyens dont on dispose, possibilités d'action.
Source : Petit Larousse Illustré1981

46 Restauration

■ Représentation tangible d'un document électronique dont peut disposer un utilisateur.
Source : MoReq

■ Ensemble des techniques employées pour remettre en état, renforcer et ralentir la dégradation des documents fragilisés ou endommagés.
Source : Abrégé AAF

■ (Influence de l'anglais. *restoration* « rétablissement »)
Remise d'un système dans des conditions de fonctionnement antérieures à une interruption. Logiciel de tests de fonctionnement de restauration. Restitution de fichiers sauvegardés.
Il convient ici, de préciser le type de restauration :

- restauration/restitution sur incident technique : (crash disque, crash serveur) automatique, prévue dans le contrat, permet au système de re-fonctionner, aux utilisateurs (applications comprises) de retrouver leurs fichiers dans l'état le plus proche (selon les stratégies de sauvegarde) de l'état où ils les ont laissés.
- restauration/restitution d'archives : archives techniques : audit ; archives juridiques : sur commission rogatoire ; archives système : dernier mode de bon fonctionnement connus en cas de dysfonctionnement (Système d'Exploitation et applicatifs) ; archives des bases de données applicatives _Exemple : revenir à état des absences, des notes après destruction ou modifications non désirées (malveillance, erreur humaine...)_ ; archives personnelles : récupération de la version J-4 ou S-3 ou M-6 ou A-1 ou d'un fichier effacé par erreur.

Source : Glossaire ADAE - projet Adèle

47 Réversibilité

■ Caractère d'une restauration dont les résultats peuvent être annulés par un autre traitement
Source : Abrégé AAF

48 Sauvegarde

■ Copie de sécurité destinée à protéger de tout incident un ensemble de données mises en mémoire, ou sur support numérique. "Faire une sauvegarde". [Petit Robert]
Source : Glossaire ADAE - projet Adèle

■ La sauvegarde est une opération technique destinée à assurer la continuité de l'exploitation d'un système informatique en cas d'incidents.
Source : SNIA (storage network industry association) www.snia.org

■ Transfert sur un support distinct d'informations en mémoire en vue de les protéger ou de les mettre en sécurité en cas d'anomalie de fonctionnement du système d'information et permettant de le remettre dans un état de référence.
(Equivalent anglais : backup)
*Source : FNTC - Charte des tiers archiveurs***Sceau ou Empreinte ou Condensat**

■ Ensemble de bits associés à un message pour s'assurer de son intégrité. L'empreinte est obtenue par une fonction de hachage. Toute modification du message entraînera une empreinte différente qui révèlera la modification par comparaison avec la première empreinte.
Source : NF Z42-013

50 Scellement numérique

■ Fonction mathématique permettant d'obtenir l'empreinte sceau (ou sceau) à partir d'un message de façon à en garantir l'intégrité.
Source : NF Z42-013

51 Signature électronique

■ Donnée ajoutée à une donnée ou à un ensemble de données et garantissant l'origine de cette ou de ces données, c'est-à-dire certifiant l'authenticité de l'émetteur
Source : NF Z42-013

■ La signature électronique permet, à l'aide d'un procédé cryptographique, de garantir l'intégrité du document signé et l'identité du signataire.
Source : DCSSI : Glossaire sécurité des systèmes d'information

■ Signature électronique sécurisée - Une signature électronique qui est liée de manière unique au signataire, qui est créée par des moyens que le signataire est en mesure de maintenir sous son seul contrôle, et qui est liée à la donnée signée de telle manière que tout changement ultérieur est détectable.
Source : FNTC – Guide de l'horodatage

■ Art 1er. – Au sens du présent décret, on entend par :
1/ Signature électronique : Donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil.
2/ Signature électronique sécurisée
Une signature électronique qui satisfait, en outre, aux exigences suivantes :
- être propre au signataire,
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif,

- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.
Source : Décret n°2001-272 du 30 Mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique).

52 Sort final

■ Destination concrète des documents correspondant à la mise en œuvre des décisions de conservation, de destruction ou de transfert des documents, telles qu'elles sont explicitées dans la charte d'archivage ou un autre outil de référence
Source : ISO 15489-RM

53 Stockage

■ Action d'enregistrer sur un support numérique en vue d'une utilisation ultérieure.
Source : Glossaire ADAE - projet Adèle

54 Tiers archiveur

■ Personne physique ou morale qui se charge pour le compte de tiers d'assurer et de garantir la conservation et l'intégrité de documents électroniques
Source : NF Z42-013

■ « Tiers archivage » (Equivalent anglais : archiving third party service) : ensemble comprenant, la fourniture d'un système d'archivage électronique et des prestations associées, à un client entreprise ou organisation
« Tiers archiveur » (Equivalent anglais : archiving third party) : Personne physique ou morale qui se charge pour le compte de donneur d'ordre, d'assurer le service de tiers archivage.
Source : FNTC - Charte des tiers archiveurs
Voir aussi Externalisation

55 Tiers de confiance

■ Organisme habilité à mettre en œuvre des signatures électroniques reposant sur des architectures d'infrastructure à clés publiques ou PKI (Equivalent anglais : Public Key Infrastructure).
Source : Wikipédia

■ « Tiers horodateur » : Tiers de confiance composée d'une entité ou de plusieurs entités intervenant dans la fourniture et la gestion de contremarques de temps.
Source : FNTC – Guide de l'horodatage

56 Traçabilité

■ Fait de créer, d'enregistrer et de préserver les données relatives aux mouvements et à l'utilisation des documents
(Equivalent anglais : tracking)
Source : ISO 15489-RM

■ Aptitude à retrouver l'historique, l'utilisation ou la localisation d'une entité (activité, processus, produit, etc.) au moyen d'identifications enregistrées (ISO 8402:1994)
(Equivalent anglais : traceability)
*Source : FNTC - Charte des tiers archiveurs***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]).]
Source : MoReq

58 Valeur de preuve ou Valeur probante

- Qualité des documents d'archives qui leur permette de servir de preuve.

Source : Terminologie AAF

59 Valeur documentaire

- Remplacé par « Valeur secondaire » ou « Valeur primaire »

« Valeur primaire » : Qualité que possède chaque document parce qu'il a été produit ou reçu par une personne physique ou morale, publique ou privée, dans l'exercice de ses activités à des fins administratives, légales, financières ou probatoires. La valeur primaire des documents est étroitement liée au processus administratif qui leur a donné naissance et à leur utilisation site DAF.
« Valeur secondaire » : Par opposition à valeur primaire, quantité et qualité d'un document d'archives appréciée en fonction des informations de portée scientifique et historique qu'il contient et du motif de sa production
Domaine Archives
Source : Terminologie DAF

60 Valeur patrimoniale

- Remplacé par « Intérêt patrimonial » : Valeur d'un document au regard d'une part, de sa présentation matérielle, de sa forme et/ou de son contenu et, d'autre part, de la mémoire d'un pays, qui détermine sa conservation définitive.

Note : Cette définition s'applique aussi bien à un organisme ou à une personne
Domaine Archives
Source : Terminologie DAF

61 Versement

- Action de transférer la conservation physique, la propriété ou la responsabilité de documents

Source : ISO 15489-RM

- Opération matérielle et intellectuelle par laquelle la responsabilité de la conservation d'archives passe de l'administration à un service de pré archivage ou à un service d'archives. Ce terme désigne aussi, par extension, les documents ainsi transférés

Source : Abrégé AAF

FIN DU DOCUMENT