SPECIFICATIONS DES SYSTÈMES D'ARCHIVAGE ÉLECTRONIQUE DANS LE DOMAINE DES SERVICES FINANCIERS

Les normes et réglementations relatives aux services financiers, qu'il s'agisse des banques, des assurances et des prestataires d'investissement ont été modifiées durant ces dix dernières années pour s'adapter au nouveau contexte d'une gestion des données et des documents dématérialisés.

La crise financière va accroître cette pression réglementaire. La Commission européenne a récemment publié une proposition de directive visant à harmoniser la réglementation des gérants de fonds alternatifs, notamment les Hedge Funds.

En France, les prestataires de services d'investissement (PSI) sont soumis au Code monétaire et financier ainsi qu'au règlement général de l'Autorité des Marchés Financiers.
Ces dispositions leur impose la mise en place d'un système d'archivage électronique, lequel participe directement au contrôle permanent interne, en particulier la sécurité de l'information, comme l'intégrité et, par conséquent, à la maîtrise du risque opérationnel.
Le recours aux normes, telle que la norme NF 42-013 sur l'archivage électronique, s'il est nécessaire, ne dispense pas d'une réflexion approfondie pour en faire un outil de conformité avec une approche des coûts et des risques.

Au-delà des risques économiques liés à la non conformité, notamment le pouvoir de sanctions de l'Autorité des marchés financiers, la croissance non contrôlée de la volumétrie des données milite également pour la mise en place d'un système d'archivage électronique permettant de gérer les durées de conservation et de désengorger les serveurs de production.

Exigences applicables à l'archivage électronique :

Les prestataires de services d'investissement doivent conserver les informations pertinentes relatives à toutes transactions sur instruments financiers qu'ils ont conclues, dans les conditions fixées par le règlement général de l'Autorité des marchés financiers[1].
Compte tenu de la généralisation des échanges sous forme électronique, les prestataires de services d'investissement doivent se doter d'un système d'archivage électronique répondant aux exigences posées dans le règlement général de l'Autorité des marchés financiers.
L'article 313-50 du Règlement général de l'Autorité des marchés financiers dispose que les enregistrements des prestataires de services d'investissement doivent être conservés sur un support

[1] C. mon. et fin., Art. L. 532-8.

3, avenue Pierre Grenier
92100 Boulogne Billancourt
+33 (0)6 13 21 61 56
info@vcm-conseil.fr
Siret : 50798089400020
Siren : 507 980 894
APE : 7022Z

qui permet le stockage d'informations de telle façon qu'ils puissent être consultés par l'Autorité des marchés financiers, sous une forme et d'une manière qui satisfont à un ensemble de conditions[2] :

- L'Autorité des marchés financiers doit pouvoir y accéder facilement et reconstituer chaque étape clé du traitement de toutes les transactions ;
- Il doit être possible de vérifier aisément le contenu de toute correction ou autre modification, ou l'état des enregistrements antérieurs à ces corrections ou modifications ;
- Il ne doit pas être possible de manipuler ou altérer les enregistrements de quelque façon que ce soit.

Recours aux normes :

La conformité d'un système d'archivage électronique aux exigences réglementaires nécessite, en pratique, d'avoir recours aux normes, d'application volontaire, en particulier la norme française sur l'archivage électronique[3], en cours de transformation internationale et dont la publication est envisagée en juillet 2012 sous le numéro ISO 14641.

Les normes permettent d'assurer une passerelle entre les exigences réglementaires et l'état de l'art. Le respect de la norme NF Z 42-013 s'impose désormais à l'externalisation des archives publiques électroniques[4]. Toutefois, l'application des normes n'emporte pas présomption de conformité à la réglementation, sauf exception[5].

Choix du support de stockage :

L'évolution des solutions d'archivage électronique, à l'instar des modifications apportées à la norme française sur l'archivage électronique, permet de substituer aux traditionnels supports physiques non réinscriptibles (Worm[6] physique), des supports logiques non réinscriptibles (Worm logique) voire des supports réinscriptibles.

La question se pose de savoir si le règlement général de l'Autorité des marchés financiers impose l'usage de supports non réinscriptibles ou si l'emploi de supports réinscriptibles est admissible au regard dudit règlement[7].

---

[2] Reg. gen. AMF, art. 313-50.
[3] NF Z 42-013: 2009 Archivage électronique. Recommandations 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.
[4] Arr. 4-12-2009 précisant les normes relatives aux prestations en archivage et gestion externalisée.
[5] Résolution du Conseil, du 7 mai 1985, concernant une nouvelle approche en matière d'harmonisation technique et de normalisation.
[6] Write Once, Read Many.
[7] Reg. gen. AMF, art. 313-50.

3, avenue Pierre Grenier
92100 Boulogne Billancourt
+33 (0)6 13 21 61 56
info@vcm-conseil.fr
Siret : 50798089400020
Siren : 507 980 894
APE : 7022Z

Les exigences du règlement général relatives aux supports de stockage concernent :

- Le support de stockage ;
- L'intégrité ;

Et ce, sans omettre :

- Le droit à l'oubli dicté par la protection des données à caractère personnel.

L'application littérale du règlement général de l'Autorité des marchés financiers, par référence à la norme NF Z 42-013 / 2009, conduirait à ne retenir que les supports de stockage non réinscriptibles, à savoir le Worm physique, permettant une modification irréversible des enregistrements.

L'emploi de supports Worm logique, dont le caractère non réinscriptible est assuré par des dispositifs matériel et/ou logiciel intrinsèques a pour avantage de répondre aux besoins fonctionnels d'un système d'archivage électronique tout en interdisant la destruction, l'altération ou la modification de l'information.

Ces supports réinscriptibles non amovibles, compte tenu des dispositifs de protection embarqués, y compris contre la suppression, paraissent donc admissibles au même titre que le Worm physique, d'autant que, à la différence de ces derniers, le Worm logique permet de gérer l'exigence du droit à l'oubli, imposée par la loi Informatique et libertés, passée la durée de conservation initialement assignée[8].

Le recours aux supports dits réinscriptibles non Worm, au regard de la norme précitée, permet d'établir, sous réserve de se conformer à un ensemble d'exigences supplémentaires, la traçabilité de toute modification, c'est à dire l'intégrité des enregistrements, dès lors que la notion d'intégrité se limite à l'altération ou la modification mais non la suppression, intentionnelle ou non, d'une information.

Le choix du support de stockage peut être également guidé par d'autres considérations, comme les temps d'accès ou le coût total de possession.
L'exigence d'intégrité pourrait être appréciée par l'Autorité au cas par cas dans le cadre des enquêtes et ce, par application du principe de proportionnalité excipé du Règlement général de l'Autorité.

Dès lors, il pourrait être envisagé le recours à des supports de stockage réinscriptibles non Worm, sous réserve de répondre aux exigences de la norme NF Z 42-013 / 2009, c'est à dire de mettre en œuvre les moyens cryptographiques, qui y sont exigés, tout en précisant le niveau de sécurité acceptable au regard des exigences du règlement général de l'Autorité.

[8] En cas de recours au Worm logique, une attention particulière devra être apportée aux paramétrages de la solution de stockage, de sorte que l'enregistrement des données soit effectivement irréversible, même par le « super administrateur ».

Relevons néanmoins que la SEC[9] a, dès 2003, explicitement exclut le recours aux supports réinscriptibles.
Quoiqu'il en soit, il serait erroné de penser que la conformité d'un système d'archivage électronique dépend uniquement des supports de stockage.

Considérations techniques, organisationnelles et économiques :

Le système d'archivage électronique doit faire l'objet d'une description très complète (« dossier technique »), incluant la liste complète des matériels le composant, avec leurs numéros de série, leurs dates de fabrication, entre autres informations. De plus la totalité des procédures doivent être documentées et tracées. Ceci inclut des informations comme l'entrée dans le périmètre physique du système, le nettoyage des locaux, la maintenance des matériels, les accès physiques et logiques….

La rigueur de conception et d'exploitation demandée par la norme impose également de répondre préalablement aux questions suivantes :

- Quelles informations doivent être archivées ?
- Quelle source privilégier (e-mail, télécopie, courrier postal) pour un même document ?
- En cas de numérisation, est-il possible de supprimer les originaux ?
- Les versions successives des documents doivent-elles être archivées ?
- Comment déterminer les durées de conservation, notamment au regard des reports, suspension ou interruption de prescription ?
- Que doivent prévoir les conventions avec les partenaires ?
- Comment garantir la pérennité des archives ?
- Comment assurer l'intégrité à long terme des signatures électroniques ?
- Quels sont les risques à conserver et à ne pas conserver ?
- Le système d'archivage doit-il conserver les informations en ligne ?
- Si oui, quelles informations ont réellement besoin d'être en ligne ?
- De combien de temps dispose-t-on pour localiser une information ? Pour obtenir une copie fidèle de cette information ?
- La nécessaire duplication des informations archivées sur des supports distincts et distants se fait-elle sur les mêmes types de support ?
- Qui attribue les droits et définit les rôles du SAE[10] ?
- Comment est audité le SAE ?
- A quelles conditions une externalisation du SAE est envisageable[11] ?

[9] 17 CFR Part 241 34-47806 SEC Interpretation Electronic Storage of Broker-Dealer Records.
[10] Il conviendra de s'interroger sur le rôle du RCCI, eu égard à ses attributions dans le cadre du contrôle permanent interne, lequel concerne, en particulier, l'intégrité de l'information.
[11] Instruction AMF 2008-03, art. 27.

3, avenue Pierre Grenier
92100 Boulogne Billancourt
+33 (0)6 13 21 61 56
info@vcm-conseil.fr
Siret : 50798089400020
Siren : 507 980 894
APE : 7022Z

La réponse à ces questions doit, in fine, se traduire dans une politique d'archivage électronique, puis dans le cahier des charges du SAE.
Il est possible de définir plusieurs types d'architecture pour des SAE normalisés :

- Une architecture adaptée à l'archivage de documents originellement sur support papier ;
- Une architecture adaptée à l'utilisation de supports amovibles ;
- Une architecture adaptée à l'archivage de documents nativement électroniques ;
- Et bien entendu, des architectures adaptées à des SAE hybrides assurant la gestion de documents physiques et numériques.

Il est bien évidemment difficile de donner un schéma d'architecture universel pour un SAE normalisé, puisqu'il faudra également tenir compte de l'architecture des applications informatiques dans lesquelles il viendra s'intégrer.
Quelque soit le type d'architecture choisi, la définition et la mise en œuvre d'un système d'archivage électronique conforme aux normes s'inscrit dans le cadre d'un véritable projet système d'information réglementaire. Celui-ci doit être préparé avec bienveillance.

Le business case de ce type de projet doit mettre en évidence les coûts détaillés des phases de conception et d'exploitation mais aussi les risques associés. Ces risques ne sont pas seulement économiques. Ils peuvent aussi être structurels, techniques et révélés de nombreux impacts sur les systèmes adjacents de ces sociétés prestataires de services financiers.
Quand aux gains, comme dans tous projets règlementaires, ils sont essentiellement qualitatifs en réponse aux exigences requises par l'Autorité des marchés financiers et la norme en vigueur.
La mise en œuvre d'un système d'archivage électronique est un projet complexe et couteux en fonction du mode de stockage retenu. En phase d'implémentation, le suivi analytique des dépenses engagées comme la gestion des risques doivent permettre d'éviter tout dérapage économique.

Perspectives :

La montée en puissance de ce qu'il convient d'appeler le « Cloud Computing » et le « Cloud Storage » nécessite une attention particulière, eu égard aux nombreuses problématiques posées par l'externalisation, au regard du règlement général de l'AMF et des exigences de la norme sur l'archivage électronique. Dans quelle mesure ce tiers pourra répondre aux exigences réglementaires et normatives et apporter les garanties nécessaires aux prestataires de conserver la maîtrise sur le contrôle interne ? Et le coût proposé par ce tiers, une fois ces exigences remplies, sera-t-il compétitif par rapport à des solutions internes, dont certaines peuvent être relativement peu onéreuses ?

Pour pouvoir répondre à toutes ces questions, il est clair qu'il faut bien distinguer ce qui est du domaine de l'archivage réglementaire et ce qui est du domaine du référentiel informationnel de l'entreprise. Une solution excellente pour ce référentiel peut s'avérer désastreuse pour l'archivage réglementaire, et réciproquement. Mais la force de l'information numérique est de pouvoir faire cohabiter deux solutions optimales, en totale transparence pour l'utilisateur.

3, avenue Pierre Grenier
92100 Boulogne Billancourt
+33 (0)6 13 21 61 56
info@vcm-conseil.fr
Siret : 50798089400020
Siren : 507 980 894
APE : 7022Z

L'élaboration d'un référentiel de bonnes pratiques spécialement adapté aux exigences de conservation des enregistrements à la charge des prestataires de services d'investissement pourrait être envisagée, le cas échéant, en concertation avec l'Autorité des marchés financiers, compte tenu des projets déjà réalisés dans ce secteur.

En toute hypothèse, la mise en œuvre d'un système d'archivage électronique implique une véritable gestion de projet, de l'analyse préliminaire à l'audit de suivi, en associant compétences juridiques, organisationnelles et techniques.

Philippe BALLET (Alain Bensoussan Avocats - www.alain-bensoussan.com)
Michel THOMAS (SERDA – www.serda.com)
VCM Conseil - 2009