ISO 15489 pour mieux protéger les informations

La gestion des archives, à la fois outil de traçabilité et preuve recevable, se transforme avec ISO 15489 en records management de la mémoire de l'entreprise **Par Benoît Louvet, avocat-associé, LAMY & ASSOCIES – Paris/Lyon**

L'ensemble des organisations, entreprises comprises, sont aujourd'hui confrontées à des contraintes de plus en plus fortes en termes de traçabilité que ce soit au plan industriel, financier ou juridique. Les DSI et RSSI sont systématiquement impliqués sur ces projets.

La toute première étape est de mettre au clair toutes sortes de concepts relatifs au projet, des concepts entendus de-ci delà, voire lus : archivage électronique légal, ILM ou Information LifeCycle Management, GED, RM ou Records Management, MoReq, etc. ... Puis arrivé à ce stade de la réflexion, surgit naturellement le souci de la présence de référentiels. Des référentiels nécessaires notamment au moment de la mise en œuvre du projet de suivi au sein du SI. Ils sont indispensables pour répondre au mieux aux nouvelles exigences de traçabilité et de sécurité de l'information.

C'est dans un tel contexte qu'est apparue la norme ISO 15489. Pour appréhender au mieux le sujet, il devient alors impératif d'expliquer l'intérêt que peut représenter une telle norme, un standard totalement dédié aux records managements. Là, trois questions, toutes aussi importantes les unes que les autres jaillissent des esprits: quid de la norme ISO 15489? Quels avantages pourraient en tirer un RSSI? Enfin, comment se servir dans la pratique du référentiel proposé par le standard au moment de la mise en œuvre d'un projet ayant pour objectif la sécurisation des informations de l'organisation?

L'ISO 15489 est une norme internationale publiée en 2001 par l'ISO, l'organisation internationale de normalisation. Elle normalise la gestion des documents archivés à des fins de preuve. Elle a vocation à s'appliquer aux organisations du secteur privé comme à celles du secteur public.

L'ISO 15489 n'est pas un standard d'archivage pour archivistes. Il concerne la gestion des documents, ceux que l'organisation décide de conserver à des fins de preuve au sens large. En France, ces documents sont désignés archives courantes et intermédiaires par le code du patrimoine.

ISO 15489 Records management par le menu

La norme ne se chargera pas seulement de la phase d'archivage du document mais également de l'aspect de gestion de ce dernier et ce, pendant toute la duré de vie, allant de la création à l'élimination, dudit fichier. L'ISO 15489 concernera tous les documents indépendamment de leur support et de leur structure logique.

Le standard est constitué de deux composantes. La première se nomme ISO 15489-1 Information et documentation « Records management », Partie 1: Principes directeurs et la seconde, l'ISO/TR 15489-2 Information et documentation « Records management », Partie 2: Guide pratique. Si l'on considère l'ISO 15489 dans son ensemble, plusieurs points importants y sont traités dans le détail:

- Définition d'une politique de records management.

Il faut s'assurer de sa cohérence avec les autres politiques de l'organisation, en l'occurrence avec la stratégie de sécurité mise en place. Cette politique prendra notamment en compte l'environnement légal et réglementaire de l'organisation, entre autres, en matière d'obligation de conservation et d'archivage ou encore, par exemple, en matière d'informatique et libertés. Elle définira le périmètre documentaire, plus exactement celui des documents gérés. En suivant cette stratégie, l'organisation listera ses choix en matière de communication et d'accès aux documents. Et pour finir, elle édictera les règles de conservation.

Outils et responsabilités directes

- Responsabilités du records manager.

L'ISO 15489 invite à définir les fonctions de records manager, la chaîne de responsabilité du Records management et l'autorité archivistique.

- Outils du records management

La norme est peu détaillée sur ce point. Elle évoque le plan de classement des activités et le référentiel de classement et d'archivage des documents, les règles d'attribution des identifiants, les règles de localisation et les règles de description des documents. Elle cite également le plan de sécurité et la charte du Records management.

- Processus du records management

Ces processus concernent la conception et la mise en œuvre du système, la gestion des documents au sens du Records management et les processus d'audit et de contrôle.

Un suivi dès la naissance du document

Le records management se distingue également de l'archivage électronique légal, c'est-à-dire à finalité de conformité et de preuve. S'il traite notamment de la phase d'archivage stricto sensu des documents, le records management appréhende un document dès sa création ou son entrée dans l'organisation et en organise la gestion, plan méthodologique inclus. Mais attention, l'ISO 15489 n'a pas, en sa qualité de norme qui plus est internationale, vocation à édicter des règles à valeur juridique telles que, par exemple, des durées de conservation ou des règles tenant à la recevabilité de la preuve qui relèvent exclusivement de la loi ou des règlements des Etats.

Le records management se différencie aussi de l'information de ILM également désignée gestion du cycle de vie de l'information. Concept créé par EMC, l'ILM signifie Information LifeCycle Management ce qui peut se traduire en français par la gestion du cycle de vie de l'information.

Concept initialement développé par un industriel du monde du stockage informatique, l'ILM consiste à optimiser les différents espaces de conservation dont dispose l'organisation par une allocation intelligente des informations à ranger en fonction de leurs caractéristiques et de différents autres paramètres.

ILM, une leçon du monde du stockage

Une information à laquelle l'organisation devra pouvoir accéder très rapidement et qui ne sera pas stockée comme une

BENOIT LOUVET

L'ISO 15489, standard totalement dédié au records management, n'est pas une norme d'archivage pour archivistes. Il concerne la gestion de documents conservés à des fins de preuve.

information archivée, une information considérée comme confidentielle ne sera pas non plus entreposée sur le même espace qu'une autre non-confidentielle. Cette optimisation nécessite que l'information soit classifiée, « étiquetée », on dira également qualifiée, dès sa création ou son entrée dans le système d'information. Née dans le monde du stockage et de son optimisation, l'ILM est aujourd'hui devenu un concept plus global de gestion de l'information non-structurée au travers de sa qualification systématique. Plus vaste dans son objet, le records management ne vise pas spécifiquement à l'optimisation des ressources de stockage mais partagera avec l'ILM le souci de qualifier l'information, au travers du document, pour mieux la gérer. Il est à noter que la notion d'ILM est aujourd'hui utilisée par certains dans un sens beaucoup plus large que le concept initial rappelé ci-dessus.

Le records management diffère pareillement de la GED acronyme de gestion électronique des documents appelée également GEIDE pour gestion électronique d'information et de documents existants. La GED est un système informatisé d'acquisition notamment par numérisation de documents papier, de classement, de stockage puis d'archivage des documents. Elle est basée sur le cycle de vie du document. Historiquement, le développement de la GED visait à favoriser l'accès et la circulation de l'information. Très orienté outils, notamment informatique, la GED n'intègre aucune exigence en matière d'archivage légal.

Si ces concepts se recoupent partiellement avec le records management sur plusieurs points, ils ont en commun l'imprécision de leurs frontières contrairement au records management que sa qualité de norme délimite clairement.

Enfin, L'ISO 15489 doit être bien différenciée de MoReq , autre référentiel qui lui est proche. MoReq signifie Model Requirements for the Management of Electronics Records, traduit en français par modèle d'exigences pour l'organisation de l'archivage électronique. MoReq énonce des spécifications essentiellement fonctionnelles pour l'archivage électronique à des fins de preuve à l'aide d'un système d'archivage électronique (SAE). Elaboré à l'initiative de la Commission européenne, MoReq a vocation à être utilisé par le secteur privé comme par le secteur public.

Une norme à l'aide des RSSI

L'ISO 15489 est bénéfique pour les RSSI à plusieurs titres. Tout d'abord, cette norme constitue un référentiel fort intéressant au stade de la conception d'une sécurisation de l'information dans une optique « info-centrée ». Par ailleurs, l'ISO 15489 devient également un outil fort utile sur le plan juridique au stade de la mise en œuvre d'un projet.

La mission traditionnelle du RSSI a été longtemps d'assurer la sécurité du système d'information. La sécurité des données d'entreprise était alors assurée au travers de celle du système. Si nul ne conteste la nécessité de sécuriser le système d'information, cette approche ne permet pas de répondre pleinement aux besoins de sécuriser le patrimoine informationnel de l'entreprise. C'est ainsi que notamment au travers de l'intelligence économique s'est développée une nouvelle approche dite « info-centrée », c'est-à-dire en considérant l'information comme l'élément pivot. Comme pour la sécurité du système, il s'agira de satisfaire aux trois règles de base: la disponibilité, l'intégrité et la confidentialité de l'information préalablement considérée comme devant être protégé pour différentes raisons.


Austin Van

ISO 15489 : records management

Un complément indispensable à 7799

Aucunement antagoniste mais complémentaires de la démarche traditionnelle de sécurité du système d'information, la norme ISO 15 489 s›inscrira de manière tout aussi complémentaire avec le référentiel que constitue la BS 7799 puis l'ISO 17799 pour le management de la sécurité des systèmes d'information.

Cette nouvelle approche de sécurité de l'information s'articule étroitement avec celles plus globales mais toujours « info-centrée » du records management et de la norme ISO 15489 qui traitent de la sécurité de l'information dans le cadre de la gestion des documents. Le records management s'intéresse notamment et dans le détail à la confidentialité des informations au travers des conditions d'accès aux documents et de leur communication. Il touche également de près à la préservation de l'intégrité des informations ne serait-ce que par sa finalité juridique précédemment évoquée. Le records management considère aussi la disponibilité au travers d›un certain nombre d'exigences concernant le système d'archivage électronique (SAE).

Enfin, le records management attache une importance particulière à la traçabilité des actions sur le document tel que les mouvements, les accès, les communications, etc.

Records management, ILM et GED se recoupent sur plusieurs points. Mais ILM et GED ont en commun l'imprécision de leurs frontières, au contraire du RM, que sa qualité de norme délimite clairement.


NSA

L'apport majeur de l'ISO 15489 et du records management sera les méthodes et référentiels de classement, d'« étiquetage » des documents au travers d'identifiants, et à travers eux, de l'information qu'ils contiennent. Cette approche permettra alors une gestion extrêmement fine du document notamment sur le plan de la sécurité. Il pourra par exemple être décidé qu'un compte rendu de réunion particulièrement sensible, ne pourra être communiqué qu'aux membres du comité exécutif de l'organisation, cette limitation ayant une durée de huit jours. Ce document devrait être immédiatement disponible pendant une année puis sera versé aux archives et conserver pendant cinq ans.

Par conséquent, si ce n'est pas là « le » cadre idéal, le records management peut devenir pour le RSSI l'occasion de développer, à l'aide du référentiel de l'ISO 15489, une sécurisation accrue des informations sensibles de son organisation.

Au stade de la mise en œuvre d'un tel système permettant d'accroître la sécurisation des informations sensibles de l'organisation, le référentiel que constitue l'ISO 15489 présente un fort intérêt au plan juridique.

Les organisations rencontrent en effet des difficultés fréquentes à déterminer et à exprimer à leurs fournisseurs et prestataires leurs besoins et exigences. Ainsi sera-t-il particulièrement important pour l'organisation, au-delà de la source d'inspiration méthodologique d'une norme comme l'ISO 15489, d'utiliser un tel référentiel également au plan juridique au stade de ses contrats avec ses fournisseurs et prestataires.

Il est important, par ailleurs, que l'organisation s'assure que les logiciels systèmes qu'elle envisage de retenir, par exemple, pour l'archivage de sa messagerie, pour les opérations de recherche sur celle-ci, soient bien conformes à la norme ISO 15489. Elle devra notamment veiller à ne pas se contenter des déclarations commerciales de l'éditeur et vérifier que celui-ci s'engage contractuellement sur la conformité de son logiciel avec la norme. Elle fera également attention à ce que les éditeurs s'engagent autant que possible sur les garanties d'évolution du logiciel qui devront suivre celles de la norme.

Plus généralement, l'organisation devra penser lorsqu'elle passera un contrat avec un ou plusieurs prestataires d'y inscrire expressément la conformité des livrables à la norme. À cet égard, le référentiel MoReq précédemment évoqué pourrait être également contractualisé comme exprimant les exigences fonctionnelles de l'acheteur.

Il faut cependant bien garder à l'esprit qu›une telle obligation contractuelle n'aura de valeur pour l'acheteur que dans la mesure où ce dernier pourra effectivement vérifier que son fournisseur ou son prestataire a satisfait à ses engagements. En l'occurrence, que les livrables sont bien conformes au référentiel et par conséquent que les objectifs notamment de qualité et de performance sont bien atteints. Or il existe un risque de blocage si les parties ne sont pas d'accord sur la conformité par exemple du logiciel ou des prestations livrées. C'est la raison pour laquelle se développent des référentiels normatifs assortis d'une certification par un tiers indépendant comme c'est le cas, par exemple, pour la nouvelle norme ISO 27001 concernant la certification du management de la sécurité des systèmes d'information. Dans le même esprit, le contrat pourra prévoir le constat de la conformité de la prestation par un tiers indépendant et que l'avis de ce dernier fasse foi entre les parties.

Cette présentation ne concerne que la norme ISO 15489 mais bientôt devrait naître une norme de certification concernant le records management. Elle est aujourd'hui en cours d'élaboration. L'intervention d'un tel standard de certification ne pourra que mieux favoriser le développement de cette approche au sein des organisations et développer par ce biais l'intérêt des RSSI. ❑

Le records management s'intéresse à la confidentialité des informations à travers les conditions d'accès aux documents et leur communication.

Une telle obligation contractuelle n'aura de valeur que dans la mesure où l'acheteur pourra vérifier que son prestataire a satisfait à ses engagements (conformité de son logiciel au référentiel).