La mission d'un organisme de recherche consiste à produire et valoriser des connaissances, aussi, l'information qui est générée et transmise s'avère de nos jours un patrimoine essentiel de nos unités qu'il convient de préserver. Comme le rappelait un Fonctionnaire de Sécurité de Défense du CNRS : « Les entreprises, les laboratoires de recherche, les administrations regorgent d'informations dont la compromission peut nuire gravement aux intérêts de l'établissement, quand ce n'est pas aux intérêts nationaux (technologies innovantes, recherches duales, contrats industriels, données personnelles, données médicales… la liste est longue) » [12].

Les enjeux de la sécurité des systèmes d'information

La sécurité de l'information est définie comme la « protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ». Elle devient aujourd'hui une des problématiques majeures de nos unités.

Forts de ce constat, nous devons envisager la finalité de « protection du patrimoine scientifique » à travers des enjeux principaux :

- garantir la disponibilité de l'outil de travail pour l'ensemble des personnels de la structure ;
- garantir la confidentialité des informations, qu'elles soient professionnelles ou personnelles ;
- garantir l'intégrité des informations et des personnes ;
- assurer la protection des données sensibles de la structure (données scientifiques et techniques, données de gestion administrative, données individuelles) ;
- assurer la protection juridique (risques administratifs, risques pénaux, perte d'image de marque).

La mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) à travers la norme ISO 27001 [5] apparaît comme une réponse aux besoins de protection des données de nos unités de recherche dans un contexte de démarche qualité (PDCA).

[forum : annoter le chapitre]

La construction du Système de Management de la Sécurité de l'Information (SMSI)

L'apport des normes ISO 2700x

La norme ISO 27001 a été publiée en 2005 et est disponible en français depuis juillet 2007. Elle constitue le référentiel pour la mise en œuvre d'un système de management de la sécurité de l'information. La mise en place d'un SMSI est une démarche transverse qui concerne tous les métiers et activités d'une structure de recherche. Elle doit aider à la réalisation des objectifs communs dans un souci de gestion de la confidentialité, de l'intégrité et de la disponibilité du patrimoine informationnel.

La norme ISO 27001 [5]s'appuie sur une série de documents associés :

- ISO 27002 détaille les 133 mesures de sécurité listées dans l'annexe de l'ISO 27001 et regroupées en 39 objectifs de sécurité, eux-mêmes classés en 11 domaines (politique de sécurité, sécurité du personnel, contrôle des accès…). Les objectifs de sécurité présentent un but à atteindre et les mesures de sécurité présentent les activités permettant d'y parvenir et expliquent les actions à mettre en œuvre pour implémenter ces mesures ;

- ISO 27004 explique comment mettre en œuvre des indicateurs pour mesurer la pertinence du SMSI ;

- ISO 27005 est un socle important de la mise en œuvre du SMSI, puisqu'il décrit l'appréciation des risques de la sécurité de l'information de l'ISO 27001.

[forum : annoter le chapitre]

Les différentes étapes de mise en place du SMSI

On l'a vu précédemment, le SMSI s'appuie sur un modèle d'amélioration continue (appelé PDCA ou « Roue de Deming » [8]) qui conduit dans un premier temps à fixer les objectifs du SMSI (*Plan*), à le déployer (*Do*), puis à vérifier les écarts éventuels entre ce qui a été défini et ce qui est mis en œuvre (*Check*), enfin à mettre en place les actions qui permettront de corriger ces écarts et améliorer le SMSI (*Act*).

Etape de planification « Plan »

Dans cette étape on se doit de définir le périmètre que l'on va gérer dans le SMSI : périmètre géographique mais surtout périmètre en termes d'activités de la structure de recherche (périmètre d'activité de recherche, d'enseignement, d'administration, périmètre par métier, etc.). Il faut bien s'attacher à prendre en compte également les interfaces avec les fournisseurs, partenaires externes…

Il faut choisir et mettre en place une méthode d'analyse de risques pour déterminer, évaluer et couvrir les principaux risques qui peuvent peser sur le SI de l'unité . Cette méthode prendra en compte les étapes suivantes :

- l'étude du contexte, la définition des seuils d'acceptation des risques ;
- la cartographie et la classification des actifs primordiaux et actifs de soutiens ;
- l'identification des menaces, l'analyse des vulnérabilités ;
- l'identification des situations de risques, la classification des risques ;
- le traitement des risques retenus : la liste des risques couverts et non-couverts et le choix des solutions pour couvrir les risques ;
- la définition des coûts, bénéfices, impacts des solutions retenues ;
- l'acceptation des risques résiduels par la direction.

Pour terminer l'analyse on doit déterminer quelles sont les mesures de sécurité que l'on doit prendre pour couvrir les risques. On verra que ces mesures sont recensées dans un document particulier exigé par la norme appelée « déclaration d'applicabilité » (DdA).

Pour une structure déjà en place cette étape passe nécessairement, par un état des lieux de l'existant et surtout par un recensement des mesures qui sont déjà en place (on part en effet rarement de rien) : inventaire des documents existants et des mesures déjà appliquées. A quel degré sont-elles déjà conformes avec le SMSI ? Existe-t-il déjà une appréciation des risques ?

Certains écueils sont à éviter lors de cette phase importante de l'analyse des risques, notamment il est nécessaire de prendre en compte les ressources (financières, matérielles, humaines…) réellement disponibles, les freins psychologiques et surtout les réels enjeux

métiers de la recherche.

Etape du déploiement « Do »

Après l'analyse de risques, il est nécessaire de déployer les mesures de sécurité décidées dans le plan de traitement des risques et retenues dans la DdA.

Il est également nécessaire de former et sensibiliser les personnels. En effet rien ne sert de mettre en place des mesures si les personnels n'en sont pas informés et ne sont pas sensibilisés aux bonnes pratiques de sécurité. De même il ne sert à rien d'installer des outils de sécurité si ceux qui doivent les utiliser ne sont pas formés.

Enfin, il faut gérer le risque au quotidien par la détection et la réaction rapide aux incidents et la génération d'indicateurs au fil de l'eau.

Étape de vérification « Check »

C'est une étape fondamentale dans un SMSI puisqu'il s'agit de vérifier :

- qu'il n'existe pas d'écarts majeurs entre ce que le SMSI définit et ce qui est mis en œuvre en pratique ;
- que les mesures de sécurité qui couvrent les risques les plus critiques sont adaptées, efficaces et suffisantes.

Les indicateurs et les outils permettant ces contrôles sont multiples. Il peut s'agir par exemple de la liste des incidents de sécurité, des indicateurs de contrôle, des tableaux de bord sécurité, des rapports d'audits internes, des enregistrements de non-conformité produits par le SMSI, des revues de direction, etc.

Il faut garder à l'esprit, lors de cette étape, que les contrôles ne sont pas mis en place pour mesurer l'efficacité « théorique » du SMSI (celle décrite sur le papier), mais surtout l'efficacité des mesures appliquées.

La phase *Check* du SMSI doit permettre l'exécution des procédures de surveillance et de réexamen afin de détecter rapidement les erreurs à traiter et identifier rapidement les failles de sécurité et les incidents de sécurité.

Cette phase doit permettre de s'adapter aux changements :

- réexaminer à intervalles planifiés l'appréciation du risque ;
- s'adapter aux changements d'organisation, de techniques, d'objectifs de l'unité, de menaces, d'efficacité des mesures de sécurité, de réglementation…

Pour cela, il conviendra de mettre en place un suivi des améliorations possibles qui seront prises en compte lors de la phase *Act* suivante (entreprendre des actions correctives ou préventives).

Étape d'ajustement « Act »

Il s'agit de définir, lors de cette étape, les actions qui permettront de réaliser les corrections et les améliorations du SMSI, mises en évidence par les indicateurs lors de l'étape précédente, mais également de prendre en compte tout changement éventuel intervenu entre temps dans le système d'information (mise en place par exemple d'un nouveau matériel stratégique…) :

- un changement de périmètre (technique, organisationnel ou fonctionnel) ayant un impact sur le périmètre du SMSI ;
- de nouveaux risques (nouvelles menaces apparues, nouvelles vulnérabilités).

Les actions résultantes seront classées en trois catégories : actions correctives (sur incident ou écart constaté), actions préventives (sur une anomalie potentielle), actions d'amélioration (amélioration de la performance du processus existant).

Organiser la mise en place pratique d'un SMSI dans les unités de recherche

Etant donné l'importance des processus à mettre en place, il est à notre sens irréaliste à ce jour de vouloir mettre en place un véritable SMSI complet de type ISO 27001 dans nos unités de recherche. Nous allons donc, dans ces lignes, nous limiter à un SMSI « allégé » propice pour parvenir à la mise en place d'une Politique de Sécurité opérationnelle du Système d'Information dans l'unité (PSSI). En complément de l'aspect didactique du guide qui présente globalement le SMSI, pour conserver un aspect pratique nous mettrons l'accent sur la gestion du risque.

Engagement de la direction et lancement du SMSI

Tout d'abord, un SMSI est un acte de direction. Celui-ci doit donc émaner officiellement

de la direction d'une unité. Il est illusoire de vouloir initier un SMSI sur la seule base du bénévolat ou des compétences techniques ou organisationnelles d'un agent bien formé et volontaire.

Il convient que la direction définisse des dispositions générales claires en accord avec ses objectifs et qu'elle démontre son soutien et son engagement vis-à-vis de la sécurité de l'information en mettant en place et en maintenant une organisation propre à construire une politique de sécurité de l'information pour tout l'organisme.

Il est donc nécessaire que le Directeur d'Unité (D.U.) lance officiellement le démarrage d'une démarche SMSI et qu'il désigne un comité de pilotage. Ce groupe peut être composé de plusieurs membres représentatifs des différentes fonctions de l'unité par exemple : un membre de la direction (directeur adjoint par exemple), un personnel administratif, un personnel technique, des chercheurs et enseignants. Il va de soi qu'un représentant du service informatique, s'il existe, devrait y être présent.

Ce lancement peut passer par un document officiel et formel comme une autorisation de lancement de la part du directeur d'unité. Ce document rappellera qu'il est nécessaire de respecter :

- les dispositions législatives et réglementaires, les directives de niveau supérieur (ministérielles et interministérielles) ;
- les différentes recommandations des politiques SSI des tutelles.

Le document indiquera qu'il convient de lancer une analyse de risques permettant d'identifier ce qui doit être protégé dans le périmètre concerné, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité afin que l'unité se donne une politique de sécurité conforme à ses intérêts.

Étude du contexte et de l'environnement

Cette étape est importante car c'est sur elle que reposera le processus de gestion du risque. L'étude comprend trois parties successives :

- la présentation de l'unité : il faut d'abord présenter l'unité afin d'identifier ce qui est important pour son fonctionnement telles que sa structure, ses missions, son organisation et sa stratégie ;

- les contraintes : on s'attachera à analyser et à rappeler les différentes contraintes qui affectent l'organisation parmi lesquelles, par exemple, des contraintes réglementaires, budgétaires, calendaires (dates d'examens, de remise de rapports scientifiques…), politiques, fonctionnelles, ou encore culturelles (par exemple envisager le fait que certaines expérimentations scientifiques doivent pouvoir se faire en dehors des heures ouvrables…) ;

- le choix du périmètre : il doit servir à définir le périmètre géographique à sécuriser (les locaux, bâtiments…), mais également les actifs de l'unité (matériels, logiciels, personnels…) qui supportent l'information à sécuriser. Dans la norme ISO 27000, ces « actifs » sont de deux types :

- les actifs « primordiaux » représentent les fonctions essentielles de l'unité comme par exemple « acquérir des données scientifiques, rédiger des publications, assurer les commandes de l'unité… », ainsi que les informations nécessaires à l'accomplissement de la mission (résultats de recherches, contrats de partenariat, informations nominatives…) ;

- les actifs « de soutien » représentent l'ensemble des matériels (PC, serveurs, réseau…), logiciels (logiciels métiers scientifiques et administratifs), mais aussi les locaux ou encore les personnels (chercheurs, enseignants, administration…) qui supportent et manipulent les informations à sécuriser.

Ce périmètre peut être volontairement restreint lors de la mise en place du SMSI, il sera progressivement étendu lors des révisions ultérieures dans un processus d'amélioration de la qualité (démarche PDCA).

Cette étude préliminaire du contexte débouche sur une étude de l'appréciation des risques et plus globalement de gestion des risques que nous allons détailler.

[forum : annoter le chapitre]

La gestion du risque

Dans la mise en place du SMSI, la « gestion des risques » est un processus essentiel qui permet de définir des exigences de sécurité qui seront traduites en objectifs de sécurité qui à leur tour vont impliquer la mise en place de mesures de sécurité adaptées. Dans ce cadre,

plusieurs référentiels utiles à la mise en œuvre d'un tel système sont disponibles.

La gestion du risque comporte deux grandes étapes : l'appréciation des risques et le traitement des risques.

Un risque est la conjonction de trois facteurs :

- une vulnérabilité d'un actif de soutien (matériel, logiciel, personnel humain…) : par exemple une salle serveur peut ne pas être climatisée ou ne pas posséder un contrôle d'accès ;
- la probabilité qu'un évènement menaçant (incendie, pirate…) exploite cette vulnérabilité : par exemple en l'absence de climatisation de la salle serveurs, l'augmentation de température engendrée par les machines hébergées peut occasionner une surchauffe, et le déclenchement d'un incendie ;
- un impact et des conséquences plus ou moins importantes résultant de la réalisation de cette menace : perte des données scientifiques et administratives de l'unité. En l'absence de sauvegardes, l'activité de l'unité est paralysée pour plusieurs semaines.

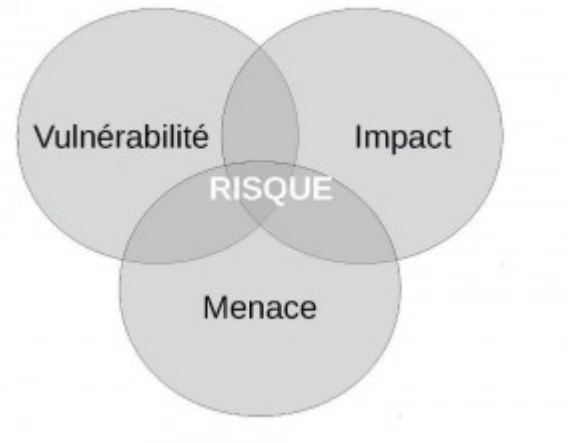

Figure 4 : Illustration des composants d'un risque en SSI

Un risque est qualifié en fonction de l'impact qu'il peut avoir et de sa probabilité ou vraisemblance d'occurrence. Pour analyser les risques on va passer par deux étapes :

- détermination / identification des risques : on détermine quels sont les principaux

risques qui pèsent sur les éléments du SI ;

- valorisation des risques : on calcule une valeur (un poids) pour chacun des risques en fonction de la probabilité d'occurrence d'une menace, de la facilité d'exploitation d'une vulnérabilité, et des impacts qui en découlent.

On sera donc amené à classer et à prioriser les risques selon la valeur calculée et d'en proposer un traitement.

Au final, le traitement des risques consistera à décider quelles mesures prendre ou pas pour diminuer ou éliminer le risque, en s'appuyant sur un référentiel de bonnes pratiques (le volet ISO 27002) associant objectifs et mesures de sécurité.

Pour chaque risque identifié, le traitement selon la norme sera ramené à quatre actions possibles :

- refuser le risque (*i.e.* supprimer au moins un des trois critères de définition d'un risque, voire supprimer la fonction générant le risque) ;
- réduire le risque (modifier les critères de vulnérabilité, la probabilité de réalisation des menaces, l'impact, jusqu'à un niveau de risque acceptable appelé risque résiduel) ;
- transférer le risque (transférer la fonction qui génère le risque à une autre unité) ;
- accepter le risque (par exemple si celui-ci est faible ou trop couteux à éliminer…).

[forum : annoter le chapitre]

Appréciation du risque

L'appréciation des risques consiste, d'une part, à les identifier, et d'autre part à les évaluer c'est-à-dire les exprimer avec une valeur qui caractérise leur importance.

Définition des échelles de valeurs

Avant de commencer l'analyse de risques proprement dite, il est important de se doter de diverses échelles de notation et d'évaluation qui seront nécessaires pour « quantifier » les risques et leur affecter une priorité (abaque).

Nous allons détailler successivement ces différentes échelles de valeur :

1. une échelle de valeur des actifs (quels sont les actifs les plus importants ?) ;
2. une échelle de vraisemblance des menaces (quelles sont les menaces les plus probables ou les plus vraisemblables ?) ;
3. une échelle de facilité d'exploitation des vulnérabilités ;
4. une échelle d'importance des impacts ;
5. un tableau de classification des risques.

[forum : annoter le chapitre]

Les niveaux de valorisation des actifs

Le CNRS, par exemple, propose dans le cadre de ses formations sur la mise en place de la Politique de Sécurité des Systèmes d'Information (PSSI) [6] au sein des unités de recherche, les cinq valeurs suivantes pour la valorisation des actifs :

- valeur négligeable (coefficient 0) : si cet actif vient à manquer, les effets ne sont pas décelables ;
- valeur faible (coefficient 1) : si cet actif vient à manquer, les effets affectent essentiellement des éléments de confort ;
- valeur significative (coefficient 2) : si cet actif vient à manquer, les effets affaiblissent la performance ;
- valeur élevée (coefficient 3) : si cet actif vient à manquer toute l'unité est impactée ;
- valeur critique (coefficient 4) : si cet actif vient à manquer les missions essentielles de l'organisme sont mises en danger.

[forum : annoter le chapitre]

Échelle d'estimation des menaces

On évalue les menaces à partir de leur vraisemblance (ou leur probabilité d'occurrence) dans le contexte de l'unité. La vraisemblance d'une menace se mesure à partir de scénarios d'attaques : types de menaces environnementales ou humaines, existence d'attaquants, motivations d'attaque…

On trouvera une liste de 42 méthodes d'attaques possibles dans le volet ISO 27005 ou dans la méthode Ebios [13] (comme par exemple, l'incendie, le vol, les écoutes réseau, etc.).

L'estimation des menaces peut ainsi s'évaluer sur une échelle à trois niveaux selon la vraisemblance ou probabilité d'occurrence : probabilité faible, moyenne et forte, notées de 1 à 3.

[forum : annoter le chapitre]

Échelle d'estimation des vulnérabilités (facilité d'exploitation)

Il convient dans un premier temps de répertorier les vulnérabilités présentes sur les actifs de soutien, puis pour chacune d'elles, de déterminer leurs facilités d'exploitation en tenant compte des mesures de protection existantes.

Pour chaque actif de soutien de l'unité on va estimer la facilité d'exploitation de leurs vulnérabilités :

- vulnérabilité très facile à exploiter (coefficient 1) : par exemple une salle serveur peut avoir comme vulnérabilité d'avoir une climatisation défectueuse ou de capacité insuffisante. L'augmentation de température qui peut s'ensuivre peut être un facteur de déclenchement d'incendie. Le déclenchement d'un incendie qu'il soit d'ordre environnemental ou intentionnel ne nécessite aucune compétence et est de ce fait facile à exploiter ;

- vulnérabilité moyenne (coefficient 2) : par exemple, le système de messagerie peut laisser passer certains documents comportant des virus. Les PC de l'unité ne sont pas tous équipés d'antivirus. Cette vulnérabilité est moyennement facile à exploiter du fait que certaines mesures antivirales sont déjà prises dans l'unité, et que l'unité a une architecture réseau sécurisée (réseau segmenté en vlan et filtres entre les réseaux) qui minimise les diffusions virales ;

- vulnérabilité difficile à exploiter (coefficient 3) : par exemple, le logiciel de gestion du service de noms (DNS) souffre d'un bogue de sécurité permettant de corrompre le cache des adresses IP de l'internet. Cette vulnérabilité potentiellement très dangereuse et spectaculaire nécessite toutefois des compétences très importantes relevant de spécialistes pour être exploitée.

[forum : annoter le chapitre]

Établissement des critères d'impact

Il faut répondre à la question : à partir de quel niveau juge-t-on qu'un impact est assez important pour que le risque soit pris en compte ? Les niveaux d'impact peuvent être confondus avec les niveaux de valorisation d'un actif définis précédemment, à sa perte ou sa dégradation.

Cinq niveaux dans les critères d'impacts / conséquences :

- négligeables : les effets ne sont pas décelables (coefficient 0) ;
- faibles : les effets affectent essentiellement des éléments de confort (coefficient 1) ;
- significatifs : les effets affaiblissent la performance de l'unité (coefficient 2) ;
- élevés : toute l'unité est impactée (coefficient 3) ;
- critiques : les effets mettent en danger les missions essentielles de l'organisme (coefficient 4).

Par exemple :

- impact important (coefficient 3 à 4) : l'incendie de la salle serveur en raison de la défaillance d'une climatisation peut avoir un impact catastrophique pendant plusieurs semaines pour la poursuite des activités de l'unité ;
- impact moyen (coefficient 2 à 3) : en l'absence de dispositif de sauvegarde de données, la perte ou le vol d'un PC peut compromettre une expérimentation et les activités d'une équipe sans toutefois paralyser l'unité entière ;

- impact faible (coefficient 1) : dans des conditions de sécurité déjà présentes (présence d'antivirus sur la majorité des PC de l'unité, sensibilisation permanente des utilisateurs et filtrage sur les serveurs de messagerie) la contamination de quelques PC dans l'unité fera perdre tout au plus quelques heures à l'utilisateur et au service informatique.

Attention toutefois aux impacts « faibles » lorsque les événements sont multipliés à plus grande l'échelle : par exemple un virus qui impacte quelques PC dans une unité peut devenir un vrai fléau à l'échelle nationale lorsque plusieurs centaines d'unités sont concernées.

A titre indicatif, le volet ISO 27005 (2008) propose comme critères de mesure de l'impact de considérer les points suivants :

- niveau de classification des informations impactées ;
- réduction d'opérations, internes ou avec partenaires externes (empêche la réalisation complète d'une opération) ;
- perturbations de plans, dépassement de *dead line* (notamment si des actions sont en cours avec des partenaires extérieurs, grand projets, etc.) ;
- dommages à la réputation (des équipes de recherche, de l'unité, des tutelles).

[forum : annoter le chapitre]

Exemple d'évaluation de l'importance des risques

Avec ses 3 facteurs constitutifs (vulnérabilité, menace et impact), le risque peut donc être évalué à travers différentes formules (la norme n'impose pas de formule précise) reliant ces trois facteurs : Risque = fonction (impact, menace, vulnérabilité).

A partir de ces critères, on peut combiner ces trois facteurs par une formule qui permettra de donner une valeur à différents niveaux de risques.

L'abaque ci-après, proposé par le CNRS, équivaut à une formule :

Risque = (Menace + vulnérabilité + Impact) – 2

Dans ce tableau, le risque est ainsi maximal (valeur de 8) dans le cas d'un impact critique (4) avec de fortes probabilités de menaces (haute) et une vulnérabilité élevée (facile).

Vraisemblance de la menace		Faible (1)			Moyenne (2)			Forte (3)		
Exploitation de la vulnérabilité		Basse (1)	Moy. (2)	Elevée (3)	Basse (1)	Moy. (2)	Elevée (3)	Basse (1)	Moy. (2)	Elevée (3)
Impact (Valeur d'actif)	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tableau 3 : Abaque d'appréciation du risque

(Source : cours dispensés par la cellule sécurité du CNRS lors de formations en 2008 et 2009)

En fonction des coefficients que l'étude a permis d'affecter aux menaces et aux actifs de soutien, et donc du niveau de risque calculé, le tableau suivant permet de caractériser cinq zones d'évaluation du risque et plusieurs manières de le traiter.

0		Risques nuls (0)	Risques acceptables
1	2	Risques négligeables (1-2)	Risques acceptables
3	4	Risques significatifs (3-4)	Risques à traiter au cas par cas
5	6	Risques graves (5-6)	Risques à traiter systématiquement
7	8	Risques vitaux (7-8)	Refus du risque tant qu'il n'a pas été traité

Tableau 4 : Zones d'évaluation du risque

L'étape consiste, en fonction des objectifs internes de l'unité, à définir des seuils d'acceptation du risque, cela conduit par voie de conséquence à définir les risques qui seront traités en priorité.

[forum : annoter le chapitre]

Audit de sécurité auprès des experts métiers

Après que les abaques et les divers critères d'appréciation du risque aient été définis, il convient que le groupe de travail chargé de la SSI de l'unité mette en place une série d'entretiens auprès des experts métiers (chercheurs, administratifs, enseignants…) présents dans l'unité.

L'objectif de ces entretiens est de faire s'exprimer les différents experts métiers de l'unité et de comprendre leur besoins de sécurité en termes de disponibilité, confidentialité de leurs données et processus métiers.

Ces divers entretiens permettront d'analyser les besoins et de valoriser les actifs primordiaux et les actifs de soutien de manière globale et homogène au sein de l'unité.

Bien entendu, les écueils à comprendre et éviter sont souvent que chaque expert métier, non spécialiste de la SSI, peut avoir une vision partielle ou erronée de sa situation individuelle en terme de besoins de sécurité. La tendance étant alors soit de sous-estimer le

risque (« je n'ai pas de données sensibles », « je n'ai rien à cacher »), soit de le surestimer (« je ne peux supporter un arrêt de la messagerie plus d'une heure »). Le rôle de l'expert SSI au vu de son expérience peut être alors de dialoguer, faire comprendre les enjeux et trouver un compromis acceptable qui resitue les besoins dans le contexte général et permette de mieux cerner les objectifs de sécurité.

[forum : annoter le chapitre]

Traitement des risques

Traiter le risque c'est donc se référer aux procédures, codes de conduite, règles de sécurité, normes, standards et dispositifs techniques, ayant pour objectif la protection du système d'information de l'organisme.

Le traitement du risque va consister à décider si le risque est accepté, refusé, transféré ou réduit. La réduction du risque va entraîner la sélection de mesures de sécurité. Dans le cas où l'on veut réduire le risque, le choix de ces mesures passe par l'identification des objectifs de sécurité (que veut-on protéger et pourquoi ?) et le choix des mesures de sécurité adaptées.

Exemple de risque refusé :

- Risque de perte de données scientifiques issues d'expérimentation et de missions scientifiques. Ces données sous-tendent l'activité de publication du laboratoire et sa renommée scientifique :

- vulnérabilité : climatisation trop ancienne et insuffisante dans la salle serveurs et absence de moyens de sauvegarde, plusieurs interruptions de la climatisation en été ;

- menace : élévations fréquentes de la température en salle serveurs, menace d'incendie ou de dégradation des disques supportant les données scientifiques ;

- Objectif de sécurité : on veut obtenir une disponibilité, une confidentialité et une intégrité élevée des données scientifiques acquises en missions ou d'expérimentation. On ne peut supporter la perte de données. Ces données doivent être sauvegardées sur un média externe et restituées en cas de problème.

Exemple de risque transféré :

- Réception importante et fréquente de virus et de spams par la messagerie électronique. Le service informatique du laboratoire en sous-effectif investit trop de temps dans la maintenance du serveur de messagerie de l'unité. Dans la conjoncture actuelle, il n'y a pas de valeur ajoutée à ce que l'unité conserve un serveur de messagerie en interne. La direction décide de « transférer » le risque et demande à ce que le service de messagerie soit pris en charge par l'organisme hébergeur.

Le traitement du risque dépend en effet des objectifs de sécurité que l'unité s'est fixée. Les objectifs de sécurité expriment la volonté de couvrir les risques jugés inacceptables sans préjuger des solutions pour y parvenir. Ils découlent logiquement de l'appréciation des risques.

Un exemple d'expression d'objectifs de sécurité concernant la disponibilité des données pourrait être : « Eviter les dommages dans les locaux comportant les données essentielles de l'unité ». Nous trouvons l'expression d'un tel objectif dans l'annexe A.9.1 de l'ISO 27001 :

- [A.9.1] Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur les informations de l'organisme.

A.9 Sécurité physique et environnementale
A.9.1 Zones sécurisées
Objectif: Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur les informations de l'organisme.

Figure 5 : Premier extrait de l'annexe de l'ISO 27001

L'objectif de disponibilité des données de l'unité est également exprimé dans le maintien des moyens de traitement de l'information. L'annexe A.10.5 est un objectif nécessaire pour mettre en place des mesures de sauvegarde des informations :

- [A.10.5] Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.

A.10.5 Sauvegarde *Objectif:* Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.		
A.10.5.1	Sauvegarde des informations	*Mesure* Des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

Figure 6 : Second extrait de l'annexe de l'ISO 27001

Les mesures de sécurité qui découlent de ces objectifs donnés en exemple sont :

- les zones sécurisées seront protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel habilité est admis ;
- des mesures de protection physique contre les dommages causés par les incendies doivent être conçues et appliquées ;
- des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

L'annexe de la norme ISO 27001:2005 représente les mesures de sécurité génériques qui couvrent les risques. Ces mesures sont détaillées dans le document ISO 27002.

Pour déterminer les mesures de sécurité appropriées à chacun des risques identifiés, on pourra utiliser l'annexe A de l'ISO 27001. Ce document qui associe les objectifs de sécurité et les mesures associées comporte 133 mesures structurées en 11 chapitres, couvrant l'essentiel des domaines de la sécurité.

Ce catalogue de mesures s'avère très utile et permet d'être sûr de ne pas oublier une mesure importante même si toute latitude est autorisée pour mettre en place des mesures de sécurité non mentionnées. La norme ISO 27002 [5] est en fait un véritable « guide de bonnes pratiques » en matière de SMSI et présente en détail les 133 mesures précédentes accompagnées de recommandations concrètes d'experts en sécurité.

Une fois le traitement du risque mis en œuvre, il conviendra de déterminer les risques résiduels qui subsistent une fois les mesures de sécurité appliquées de façon à les prendre en compte dans la réactualisation de l'analyse des risques.

[forum : annoter le chapitre]

Déclaration d'applicabilité

La dernière étape de la gestion des risques, dans sa phase de « traitement » consiste à dresser un tableau récapitulatif reprenant l'ensemble des 133 mesures de l'Annexe A de l'ISO 27001.

L'ensemble de ces 133 mesures sera consigné dans un document intitulé Déclaration d'Applicabilité (DdA ou SoA pour *Statement of Applicability* en anglais) qui contient pour chaque objectif de sécurité, les mesures de sécurité retenues, les raisons de leur sélection mais également les mesures de sécurité non retenues et les raisons de leur mise à l'écart. Pour la réalisation de ce document, aucune mesure n'est à priori obligatoire même si les exigences de la norme ISO 27001 et les obligations règlementaires ou statutaires rendent plusieurs mesures incontournables.

La DdA est le document fondamental demandé par la norme auquel il est nécessaire d'aboutir pour mettre en place un SMSI. Il représente la synthèse des mesures de sécurité nécessaires pour sécuriser l'unité. Il s'appuie sur l'ISO 27002 qui est un guide de bonnes pratiques en matière de mesures de sécurité. Pour chacune des 133 mesures de sécurité apportées par la norme ISO 27002, la DdA permet d'indiquer les raisons de la sélection des mesures ou de leur rejet.

Ainsi les mesures de sécurité qui peuvent être sélectionnées seront le fait des exigences de sécurité suivantes :

- imposées par la norme ISO 27001 ;
- imposées par les contraintes légales et réglementaires, par exemple, présentes dans la PSSI de la tutelle ;
- imposées par le contexte ou les bonnes pratiques : certaines mesures sont évidentes ;
- issues de l'appréciation des risques ;
- déjà mises en place.

[forum : annoter le chapitre]

Bénéfice de la démarche SMSI

Au vu des éléments précédents, le projet de mise en place d'un SMSI permet de mobiliser l'ensemble des acteurs de la structure de recherche autour d'un projet commun. Chaque acteur, depuis l'utilisateur final, jusqu'à la direction de la structure, en passant par l'équipe informatique, prend sa part de responsabilité dans la sécurité de l'information.

Cette implication ne s'obtient concrètement que par l'engagement fort de la direction qui doit s'affirmer de manière claire et visible. En retour, la mise en place d'un SMSI apporte à la direction de l'unité des règles de bonne conduite, l'aidant à gérer ses objectifs et à répondre à des questions simples mais fondamentales (où se trouvent les informations sensibles de ma structure ? Sont-elles bien conservées ? Sont-elles bien protégées eu égard aux contextes et enjeux scientifiques ?…).

Le deuxième domaine d'intérêt concerne le fait d'impliquer l'ensemble des métiers de la structure dans la gestion des risques qui pèsent sur le patrimoine informationnel. On l'aura compris, la sécurité n'est pas qu'une affaire de technique, mais aussi et surtout de politique, d'organisation et de comportement.

Par cette démarche et des pratiques qui en découlent, l'ASR trouve sa légitimité dans la bonne prise en compte des mesures de sécurité à déployer et à accompagner. Il sera renforcé dans son rôle de « force de proposition » pour conduire ce projet et n'aura sans doute plus le sentiment d'être isolé dans son unité en mettant en œuvre, de par ses décisions personnelles, des mesures de sécurité le plus souvent techniques qui ne couvrent qu'une partie des risques potentiels.

Enfin, faire connaître auprès des tiers et de ses partenaires sa nouvelle gouvernance concernant la protection de son patrimoine et le respect des contraintes réglementaires pourra apporter plus de confiance et de professionnalisme dans les relations réciproques.

[forum : annoter le chapitre]

5. Exemples de mesures de sécurité courantes

Voici ci-après, quelques pratiques générales en matière de sécurité informatique qui sont fréquemment mises en place dans la sécurisation du SI de nos unités de recherche.

Sécurité physique des locaux

L'objectif est d'empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux dans lesquels résident les informations de l'unité. Les locaux contenant des informations sensibles et des moyens de traitement de l'information (salles serveurs, secrétariat de direction ou d'enseignement…) doivent donc être protégés physiquement des accès incontrôlés ou malveillants (contrôle d'accès par carte ou code).

Pour se protéger des menaces d'ordre environnemental, il convient également de mettre en œuvre des dispositifs de détection et d'alerte de température élevée, d'incendie ou d'inondations ou d'autres formes de sinistres provoqués soit accidentellement soit par malveillance.

[forum : annoter le chapitre]

Sécurité du matériel et du câblage

On protégera les matériels sensibles (routeurs, serveurs…) des pertes d'alimentation électrique par un système de secours bien dimensionné, ainsi que d'éventuelles surchauffes par des moyens de climatisation adéquats et bien dimensionnés.

Afin de garantir une disponibilité permanente et un bon fonctionnement en cas de panne, le matériel sensible qui nécessite un fonctionnement continu doit être placé sous contrat de maintenance.

Les accès aux câbles réseaux transportant des données doivent être protégés contre toute possibilité d'interception de l'information, ou de dommage. Les câbles ou concentrateurs réseaux doivent être hors de portée immédiate et donc protégés dans des gaines ou des armoires de répartition.

[forum : annoter le chapitre]

Mise au rebut ou recyclage

Les matériels, les informations ou les logiciels ne devraient pas pouvoir être sortis des unités sans autorisation préalable au vu d'une procédure formelle. En cas de mise au rebut ou de revente de PC, il convient de vérifier que les données ont été effacées des disques de manière efficace. Un simple formatage n'étant bien entendu pas suffisant pour effacer les données de manière pérenne, des méthodes sont préconisées [14].

Les supports qui ne servent plus doivent être mis au rebut de façon sûre. Il n'est pas conseillé pour des raisons environnementales de même que pour des raisons de sécurité du

SI de se débarrasser des PC et des supports amovibles dans des bennes non spécialisées, ni sans avoir au préalable correctement effacé les supports (magnétiques, etc.).

[forum : annoter le chapitre]

Procédures de sécurité informatique liées à l'exploitation

5.4.1 Protection contre les codes malveillants : virus et autres « malwares »

La plupart des attaques via le réseau tentent d'utiliser les failles du système d'exploitation ou des logiciels d'un PC. Les attaques recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parvenir à s'y introduire.
C'est pourquoi il est fondamental que les ASR mettent à jour les logiciels des serveurs et des postes clients afin de corriger ces failles.

Suite aux avis de sécurité qui émanent des CERT et CERTA [15], l'ASR doit veiller au maintien du niveau de sécurité au cours du temps par l'application récurrente des correctifs logiciels (*patchs*) sur les serveurs en exploitation dans l'unité.

Il est également dans ses fonctions, de veiller à ce que chaque poste du réseau local soit équipé d'un antivirus régulièrement mis à jour. L'ASR doit donc mettre en place des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants.

5.4.2 Sauvegarde des informations

La sauvegarde des informations est un processus essentiel permettant de garantir la disponibilité des données et la continuité de l'activité du laboratoire en cas d'incident. Une politique de sauvegarde (fréquence, fenêtre de sauvegarde…) doit être élaborée pour protéger les données de l'unité et ces informations de sauvegarde doivent être communiquées aux utilisateurs. Une sauvegarde régulière des données des utilisateurs ainsi qu'un processus de restauration, testés au préalable, doivent être mis en place. Les droits d'accès à ces sauvegardes doivent faire l'objet d'une attention particulière.

Des copies de ces sauvegardes doivent être réalisées sur des supports externes (robot de bandes, disques externes…) et placées dans des locaux (ou coffres) sécurisés et distants. Ces copies de sauvegardes doivent aussi être testées régulièrement conformément à la politique de sauvegarde convenue.

5.4.3 Journaux systèmes – les logs

Les journaux systèmes produits par nos serveurs informatiques permettent la surveillance du contrôle d'accès à nos systèmes et réseaux. Ils permettent de faciliter les investigations ultérieures et sont en outre également exigés dans le cadre de la collecte de preuve par les autorités juridiques compétentes.

Les journaux systèmes qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant la période légale pour surveiller l'exploitation du système. La politique de gestion des traces du CNRS a fait l'objet d'un document disponible sur l'intranet du CNRS [16].

Il est important de protéger les serveurs qui conservent les informations journalisées contre des accès non autorisés ou des actes de malveillance qui pourraient s'opposer au maintien de la preuve.

En raison du nombre de serveurs présents dans nos unités, il convient de mettre en œuvre des moyens pour faciliter l'exploitation transversale de ces journaux provenant de multiples serveurs. Par exemple la centralisation des journaux systèmes sur un serveur unique et dédié, permet de concentrer la sécurisation des *logs* sur un seul point d'accès, de mieux réguler la période d'archivage légal et surtout, de permettre la consultation simultanée des journaux de plusieurs serveurs [17].

5.4.4 Synchronisation des horloges

En cas d'analyse des journaux informatiques, pour retracer la chronologie d'un événement ou d'une anomalie, il est essentiel que les horloges des différents systèmes de traitement de l'information (serveurs, routeurs, PC utilisateurs…) de nos unités de recherche soient synchronisées à l'aide d'une source de temps précise et préalablement définie.

5.4.5 Sécurité du réseau – Echange des informations – Contrôle d'accès réseau

Les réseaux de nos unités de recherche doivent être gérés et contrôlés de manière adéquate pour garantir la protection contre des menaces aussi bien externes qu'internes. On veillera surtout à contrôler l'accès physique au réseau, segmenter le réseau local en différents réseaux virtuels et à rendre illisibles notamment les informations en transit, par des moyens de chiffrement des protocoles :

- contrôle d'accès réseau : il est nécessaire d'empêcher les accès non autorisés aux services qui sont disponibles sur le réseau (partages de dossiers, imprimantes, accès intranet, web, etc.). L'ASR doit s'assurer de ne donner accès qu'aux services pour

lesquels les utilisateurs ont spécifiquement reçu une autorisation. Des méthodes d'authentification appropriées doivent donc être utilisées pour contrôler l'accès des utilisateurs distants. Il peut être nécessaire d'avoir recours au standard 802.1x. pour contrôler l'accès aux ports du réseau interne au moyen d'une identification et authentification. La mise en place d'annuaires centralisés tels que *Active Directory* ou LDAP ou encore un serveur RADIUS représente un élément fondamental pour permettre cette authentification ;

- cloisonnement des réseaux : il est particulièrement efficace de séparer les flux réseau issus des différents services d'information de nos unités. La segmentation du réseau de l'unité en réseaux logiques virtuels (VLAN) est donc une bonne mesure à prendre pour séparer des flux réseau de différentes entités administratives (le réseau des chercheurs, le réseau des étudiants, le réseau de secrétariats, le réseau des serveurs…). Cette différenciation des flux permet, par la suite, de leur appliquer des mesures de sécurité différentes. Dans le processus de segmentation du réseau, il est fortement recommandé de regrouper et d'isoler les services devant être visibles de l'extérieur dans une zone réseau « semi ouverte » ;

- contrôle du routage réseau : le réseau hébergeant le SI doit être protégé des tentatives d'accès illicites provenant de l'extérieur comme de l'intérieur de nos unités. Des mesures de routage des réseaux doivent être mises en œuvre afin d'éviter que des connexions réseau non souhaitées ne portent atteinte à la politique de contrôle d'accès des applications métier de nos unités. Les flux d'entrée, et de sortie, du réseau doivent également être protégés par un ensemble de filtres
(ACL dans le jargon) qui permettent d'interdire des accès réseau vers des ressources ou des services non contrôlés.

5.4.6 Protection des transferts de données : chiffrement

L'objectif des mesures cryptographiques est de protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des algorithmes utilisant des clés de chiffrement. Aussi, il faut les utiliser pour protéger les flux d'information liés à des services sensibles. Par exemple, la messagerie électronique ou les accès intranet ou tout autre service demandant une identification doivent être protégés de manière adéquate par des protocoles sécurisés reposant sur SSL, comme IMAPS, SSTPS, SASL pour la messagerie ou HTTPS pour le web.

Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information devrait être mise en œuvre. Cela revêt un caractère obligatoire pour les

données classifiées « sensibles ». On consultera à cet effet le document de recommandations du CNRS en la matière [18].

Il est important pour les ASR de connaître le fonctionnement de l'Infrastructure de Gestion de Clé (IGC) de leur structure lorsqu'elle existe et l'utilisation que l'on peut faire des certificats délivrés (signature et chiffrement des messages électroniques, certification de machines serveurs…).

Dans le cas du CNRS, par exemple, l'ASR se rapprochera des Délégations Régionales (DR) pour connaître les modalités d'obtention et d'utilisation des certificats électroniques du CNRS, ainsi que celles pour devenir Autorité d'Enregistrement (AE) afin de fournir des certificats électroniques aux utilisateurs de son unité. Il est, à ce propos, nécessaire de connaître l'Autorité d'Enregistrement en place pour la DR. On trouvera de nombreuses documentations à ce sujet sur les sites des IGC [19].

5.4.7 Exigences relatives au contrôle d'accès aux systèmes d'exploitation

Il est du ressort des ASR de maîtriser par des dispositifs techniques ou procéduraux, l'accès à l'information présente dans nos unités. Il est donc nécessaire de mettre en place une politique de contrôle d'accès de manière à empêcher les accès non autorisés aux systèmes d'exploitation.

Une procédure formelle de création (et de suppression) des comptes informatiques des utilisateurs destinée à accorder ou à supprimer l'accès à tous les systèmes et services d'information doit être définie. Après création des comptes, il est nécessaire de gérer correctement l'attribution et l'utilisation des privilèges.

L'accès aux ressources informatiques ne doit donc être possible qu'après identification et authentification des utilisateurs et doit être adapté aux droits et aux profils des utilisateurs (chercheurs, administration, enseignement, etc.).

L'ASR attribue un identifiant et un mot de passe unique à chaque utilisateur et met en place le système d'authentification adéquat, pour vérifier l'identité déclarée par l'utilisateur lors des entrées en session.

Les utilisateurs doivent pouvoir changer leur mot de passe à partir d'un processus formel contrôlé de manière à empêcher l'utilisation de mots de passes trop faibles (utiliser des mots ne figurant pas dans un dictionnaire et difficiles à retrouver à l'aide de programmes).

Il est important de faire adhérer les utilisateurs à ces mesures qui peuvent paraître

contraignantes, mais qui figurent parmi les mesures de base permettant d'assurer la sécurité de l'accès au système d'information des unités.

Dans certains contextes (salles d'enseignements ou applications sensibles…) les sessions inactives devraient être déconnectées après une période d'inactivité définie.

5.4.8 Gestion de parc et des moyens nomades – Cybersurveillance

L'administration des postes de travail de nos unités est normalement placée sous la responsabilité de l'ASR. Selon la réglementation en vigueur actuellement, il a donc toute latitude pour mettre en place des outils de gestion et de surveillance du parc informatique. Ainsi, une vérification du niveau de sécurité des postes nomades (présence d'un antivirus à jour par exemple) doit être mise en place avant l'accès au réseau local. Les postes de travail et moyens nomades doivent par ailleurs être protégés par des mots de passe robustes.

En cas de télémaintenance sur un PC avec des outils de prise en main à distance tel que VNC, les ASR doivent avertir le propriétaire du poste et respecter la législation.

5.4.9 Mesure de l'utilisation des ressources : outils de métrologie

L'utilisation des ressources systèmes ou du réseau doit être surveillée et ajustée au plus près. La sécurité du système d'information implique une surveillance de l'utilisation du réseau et des serveurs tout en respectant la réglementation en vigueur (cf. les aspects juridiques du métier d'ASR dans ce guide). Cela consiste notamment à respecter le principe de proportionnalité qui est d'adapter les moyens de surveillance aux enjeux de sécurité et d'avoir pour principe d'informer les utilisateurs et les partenaires sur les moyens de surveillance mis en place. Dans le respect de ce cadre, l'ASR a toute latitude pour mettre en place divers outils de métrologie réseau et de journalisation des accès aux serveurs.

[forum : annoter le chapitre]

Sauvegarde et archivage

Quelle que soit l'unité de recherche concernée, il y a production et utilisation d'informations sous forme de données numériques. Une des fonctions de l'ASR est de proposer des dispositifs qui permettent d'assurer une préservation de ces données en cas de perte accidentelle ou autre. La duplication de ces données par stockage redondant sur des supports différents de ceux de l'équipement utilisé (poste de travail fixe, mobile, serveur, …) est un des principes de base. Elle nécessite la mise en place de techniques et de procédures de stockage et de restauration spécifiques au type de donnée concernée.

Ces recommandations sont notamment issues de la norme NF-Z-42-013 (2001) [20] qui fournit des spécifications relatives à la conception et l'exploitation de systèmes en vue d'assurer la conservation et l'intégrité des documents stockés, dans le domaine de l'archivage électronique. Y sont abordées diverses recommandations d'organisation et de bonnes pratiques concernant la gestion des supports WORM (*Write Once Read Many*) mais qui peuvent aisément être transposées à d'autres types de sauvegarde et d'archivage.

Il convient donc de distinguer clairement les deux finalités :

- la sauvegarde, quelle que soit sa forme et son usage, est destinée à mémoriser des données évolutives de manière à en conserver la persistance et pouvoir les restituer en cas d'accident. On peut couramment considérer que les données stockées sont régulièrement modifiées (écrites, effacées) ;

- l'archivage, en revanche, consiste à rendre accessible en lecture des données immuables (archives de documents administratifs, données de mesures expérimentales, résultats de simulations coûteuses à produire, etc.), bien que leur classification puisse évoluer dans le temps (métadonnées associées).

La durée de rétention, les modes d'accès et souvent les volumes, sont fondamentalement différents, ce qui suppose que des supports, des nommages, des lieux d'hébergement adaptés et une gestion des risques devraient leur être appliqués (notamment en cas de risque de perte accidentelle et en cas de sinistre). Le critère le plus important qui distingue ces deux aspects sera la durée du cycle de vie.

La quantité d'informations traitées dans nos unités a une nette tendance à augmenter. Tant pour les sauvegardes que pour l'archivage, certaines techniques comme la déduplication, pourront, à fonctionnalité constante, réduire le volume des données et les coûts d'infrastructure.

La norme propose par exemple des méthodes d'identification des supports ainsi que des processus d'enregistrement de leur chaînage. A intervalle régulier, des copies de sécurité doivent être effectuées (fréquence et nombre dépendant de la criticité des données, de la durée de vie des supports dans l'environnement de conservation…) et stockées loin des originaux. D'une manière générale, les sauvegardes et archivages doivent être systématiquement vérifiés et régulièrement testés. Il peut arriver que des supports deviennent illisibles, dans ce cas les systèmes d'écriture/lecture doivent être vérifiés et une copie de sécurité régénérée et identifiée.

Cependant, l'archivage pose des problèmes particuliers propres à la longue durée de rétention des données. Typiquement, on peut trouver actuellement des supports garantis au moins 30 ans (magnéto-optiques notamment). En revanche, les matériels et logiciels permettant d'exploiter ces supports survivent rarement au-delà de 10 ans. Il en va de même de la possibilité d'exploiter les formats des informations stockées sur ces supports. C'est un paradoxe de l'archivage électronique : conserver des données pendant de longues durées en s'appuyant sur des technologies rapidement obsolètes. Quelques règles simples de bonnes pratiques nous permettront de minimiser les risques liés à ce paradoxe tout en respectant disponibilité, intégrité et confidentialité des données.

[forum : annoter le chapitre]

Imposer des standards indépendants des applications et des environnements informatiques

Ne pas perdre de vue que la lecture, le décodage ou la transcription doivent rester pérennes durant toute la durée de conservation. Privilégier les formats ouverts (soit libres, soit dont les caractéristiques sont publiées) est un gage de pérennité (XML, HTML, PDF/A sont les plus cités en ce qui concerne les documents texte). L'interopérabilité consistant à pouvoir transférer les données d'un système à un autre devrait s'imposer à tout système d'archivage.

L'obsolescence rapide de la plupart des supports impose (en particulier pour les données conservées plus de 5 ans) d'envisager dès l'origine la migration en tenant compte des formats logiques mais aussi du temps nécessaire et de l'indisponibilité éventuelle occasionnée.

[forum : annoter le chapitre]

Respecter la législation

Les données peuvent faire l'objet de restrictions d'accès, voire de déclarations (données personnelles, etc.). L'archivage est autant concerné que le stockage, d'une manière générale, par ces aspects juridiques. Certains documents notamment administratifs doivent être probants. Il conviendra d'assurer l'intégrité de ces documents tout au long de leur durée de conservation (Code Civil Art.1316-1 [21]).

[forum : annoter le chapitre]

Pérenniser les données descriptives

L'augmentation du nombre et du volume de données va de pair avec les données descriptives (métadonnées) permettant de les situer (origine, dates, etc.), de les retrouver (classification, indexation, etc.), éventuellement d'en mémoriser les accès (données protégées ou sensibles) et de s'assurer de leur intégrité (signature, empreinte, chiffrement…).

La sauvegarde des systèmes de gestion des données descriptives fait partie intégrante de l'archivage des données elles-mêmes. Ainsi, une base de données d'index ou de mots-clés permettant la recherche de documents dans un thésaurus d'archive est à sauvegarder, simplement pour maintenir opérationnel l'accès aux documents, voire parce que la reconstitution d'un tel index peut s'avérer un processus long et complexe.

[forum : annoter le chapitre]

Analyse de risques et politique d'archivage

Conserver les données sur le long terme, les retrouver et les restituer avec fidélité dans un format intelligible tout en sécurisant leur accès constituent les objectifs de l'archivage électronique. Une analyse de risques portant sur les données d'archivage ainsi que sur les moyens d'y accéder permettra de définir une politique de sauvegarde propre à l'unité.

La politique d'archivage doit conduire à :

- définir les objectifs du système (services rendus) ;
- préciser l'ensemble des intervenants et leurs responsabilités ;
- définir les fonctionnalités (versement, stockage, administration) ;
- préserver l'environnement sécuritaire associé en lien avec la politique de sécurité du système d'information.

Elle permet de transformer les exigences en différents niveaux de service eux-mêmes traduits en architecture technique et en processus.