SÉCURITÉ INFORMATIQUE
numéro 58 décembre 2006
SÉCURITÉ DES SYSTÈMES D'INFORMATION

éditorial

Du bon usage des normes

La multiplication des normes aussi bien dans les domaines techniques que dans ceux relevant de l'organisation est une tendance lourde de nos sociétés. Désormais la Sécurité des systèmes d'information (SSI) fait l'objet de normes internationales, référencées ISO 27000. Peut-être faut-il y voir un signe de maturité de la SSI. En tout cas, cela devrait nécessairement influer sur la façon d'aborder la SSI. Il va devenir difficile de mettre en œuvre la sécurité et, surtout, de montrer que celle-ci est effective sans se référer aux normes en la matière.

L'expérience acquise pour la mise en œuvre des normes de qualité ISO 9000 pourra se transposer à la SSI d'autant plus facilement que les principes et la méthodologie utilisés sont très voisins. C'est pourquoi l'expérience du CERMAV, Centre de recherches sur les macromolécules végétales, qui, avec un appui très fort de la direction, s'est lancé dans une démarche qualité basée sur la norme, est riche d'enseignements. Elle est présentée dans l'article d'Alain Rivet.

D'un apport indéniable en matière de sécurité, les normes ne sont sûrement pas une panacée qui va résoudre tous les problèmes; il faut savoir les appliquer avec intelligence, comme nous le montre avec humour l'article de Laurent Bloch.

Les normes ne font souvent que reprendre, en les formalisant, des bonnes pratiques, des méthodologies éprouvées ou de simples principes de bon sens. Définir des procédures, les documenter et les faire appliquer, bâtir des indicateurs et des tableaux de bord, mesurer les écarts entre objectifs et réalisations, réitérer les processus en corrigeant leurs erreurs, étaient déjà ce que pratiquait le Monsieur Jourdain de la sécurité.

La Politique de sécurité des systèmes d'information (PSSI) du CNRS qui vient d'être signée et que nous présente l'article de Joseph Illand s'intègre dans cette logique de formalisation. Elle constitue un signal fort pour engager une démarche de sécurité.

Sans nécessairement aller jusqu'à l'étape ultime, qui est la certification, la démarche sous-jacente à ces normes ne peut-elle contribuer à l'amélioration de la sécurité des systèmes d'information ? C'est une réflexion qu'il nous faut avoir. Les articles de ce numéro donnent quelques éléments de réponses.

François Morris
Chargé de mission SSI au CNRS

La norme ISO 9001, outil d'organisation de laboratoire

Par Alain Rivet
Responsable qualité et système d'information du CERMAV

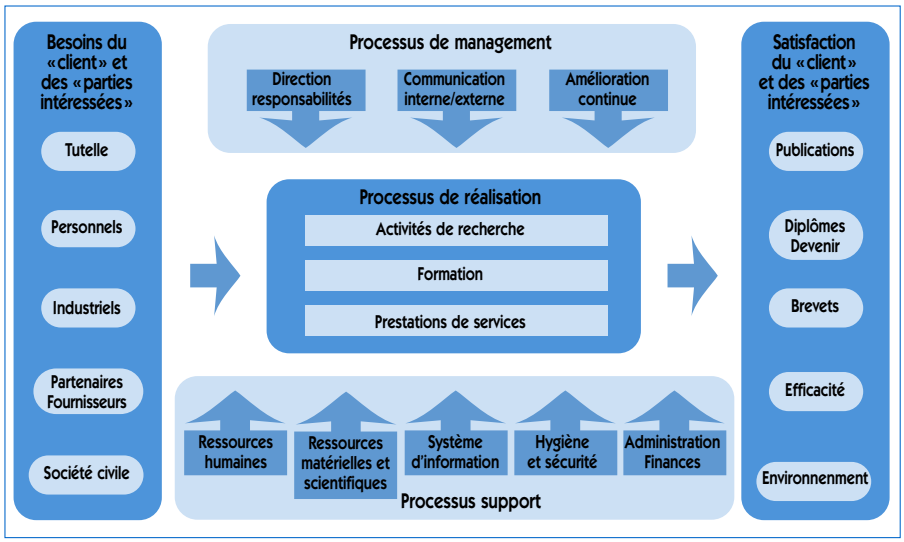
Longtemps associée au domaine industriel, la norme ISO 9001 relative au Système de management de la qualité (SMQ) est un concept récent dans le domaine académique, la qualité en recherche ayant longtemps opposé la créativité du chercheur à la notion de management. À travers l'expérience menée au Centre de recherches sur les macromolécules végétales (CERMAV), nous verrons comment la mise en œuvre d'un système de management de la qualité peut s'avérer un outil intéressant pour améliorer l'organisation et le fonctionnement d'un laboratoire et jouer ainsi un rôle fédérateur, important à prendre en compte dans la perspective de regroupement de laboratoires.

ISO 9001 et qualité en recherche

Dans le domaine de la recherche, les premières démarches qualité furent initiées vers 1985 afin de répondre à des préoccupations sécuritaires pour être étendues par la suite aux domaines de la santé publique, de la sécurité des biens et des aliments. On observe, depuis les années 2000, une certaine généralisation des démarches qualité à l'ensemble des organismes de recherche. La mise en place récente de cahiers de laboratoire standardisés, outils essentiels d'une démarche qualité en recherche, en est un des exemples. Les enjeux pour les organismes de recherche sont multiples, à la fois scientifiques, de façon à garantir la maîtrise des résultats, mais aussi économiques et financiers, afin d'optimiser les ressources allouées, tout en répondant à une demande sociétale de plus en plus forte en termes de traçabilité et de transparence.
Les normes de la famille ISO 9000 de Système de management de la qualité (SMQ) sont des normes internationales de bonnes pratiques de management. Elles ne s'adressent qu'à l'organisation du laboratoire et non aux aspects techniques, le personnel restant l'expert scientifique de son travail. Cet aspect non directif permet ainsi une grande souplesse d'adaptation pour nos unités. S'agissant suite page 2

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

suite de la page 1



d'organisation, la qualité est l'affaire de tous, c'est donc une démarche participative qui va nécessiter un engagement des personnes et une implication forte de la direction.
Le CERMAV, unité propre de recherche du CNRS, UPR5301, s'est trouvé confronté dès 2002 à un certain nombre de difficultés fréquemment rencontrées dans les laboratoires de recherche : départs à la retraite, mise en place de l'ARTT, transmission essentiellement orale du savoir et existence d'un parc expérimental important (microscopie électronique, spectrométrie RMN, spectrométrie de masse…). Face à cette problématique, un SMQ, basé sur le référentiel ISO 9001, a été mis en place sous la coordination d'un comité de pilotage à travers trois groupes de travail : «Maîtrise documentaire», «Gestion des équipements» et «Capitalisation des connaissances», avec une volonté forte de la direction.

Aspects théoriques d'une démarche qualité

Revenons, au préalable, sur deux aspects plus théoriques de la démarche qualité que sont, d'une part, l'approche processus, qui correspond à la structuration des activités, et, d'autre part, la maîtrise documentaire, qui est une structuration des informations du laboratoire.

Approche processus

L'approche processus a consisté à décomposer le fonctionnement du laboratoire en un certain nombre de processus ou de grandes activités ; cela correspond à une nouvelle dimension de l'organisation par rapport à la représentation classique en organigramme. Les processus ainsi identifiés et présentés dans la figure ci-dessus se divisent en processus de management, processus support et processus de réalisation qui représentent les processus «cœur de métier» du laboratoire. L'ISO 9001 introduit la notion de «client», notion difficile à intégrer dans notre environnement, dont on va chercher à mesurer la satisfaction au moyen d'indicateurs. Ainsi, pour nos autorités de tutelle, la production scientifique du laboratoire (nombre de publications, facteurs d'impact) va représenter un indicateur du processus «Activités de recherche». En ce qui concerne le personnel doctorant, on va chercher à mesurer le fonctionnement du processus «Formation» par le suivi des carrières.

Maîtrise documentaire

Documenter les différents éléments du système est une exigence fondamentale d'un SMQ. Cette maîtrise documentaire associe, au sein d'une boucle de réactivité, un manuel qualité, des procédures qui décrivent l'organisation des activités (c'est le *Qui fait quoi ?*), des modes opératoires qui précisent en détail les étapes des procédures (c'est le *Comment ?*), des formulaires jusqu'aux enregistrements qui apportent la preuve de ce qui a été fait.
En matière de gestion documentaire, l'informatique apparaît comme un outil de choix, tant au niveau de la structuration des informations, en assurant l'unicité des documents, une accessibilité au moyen d'un navigateur, l'intégration d'outils complémentaires (agenda, réservations…), que de leur maintenance avec la possibilité de sauvegarder et mettre à jour aisément les informations. Au CERMAV, nous avons fait le choix d'associer refonte du site Intranet du laboratoire et démarche qualité dans une sorte de portail web fournissant un frontal d'accès aux ressources documentaires et applicatives internes du laboratoire.

Le système d'organisation de l'unité de recherche CERMAV

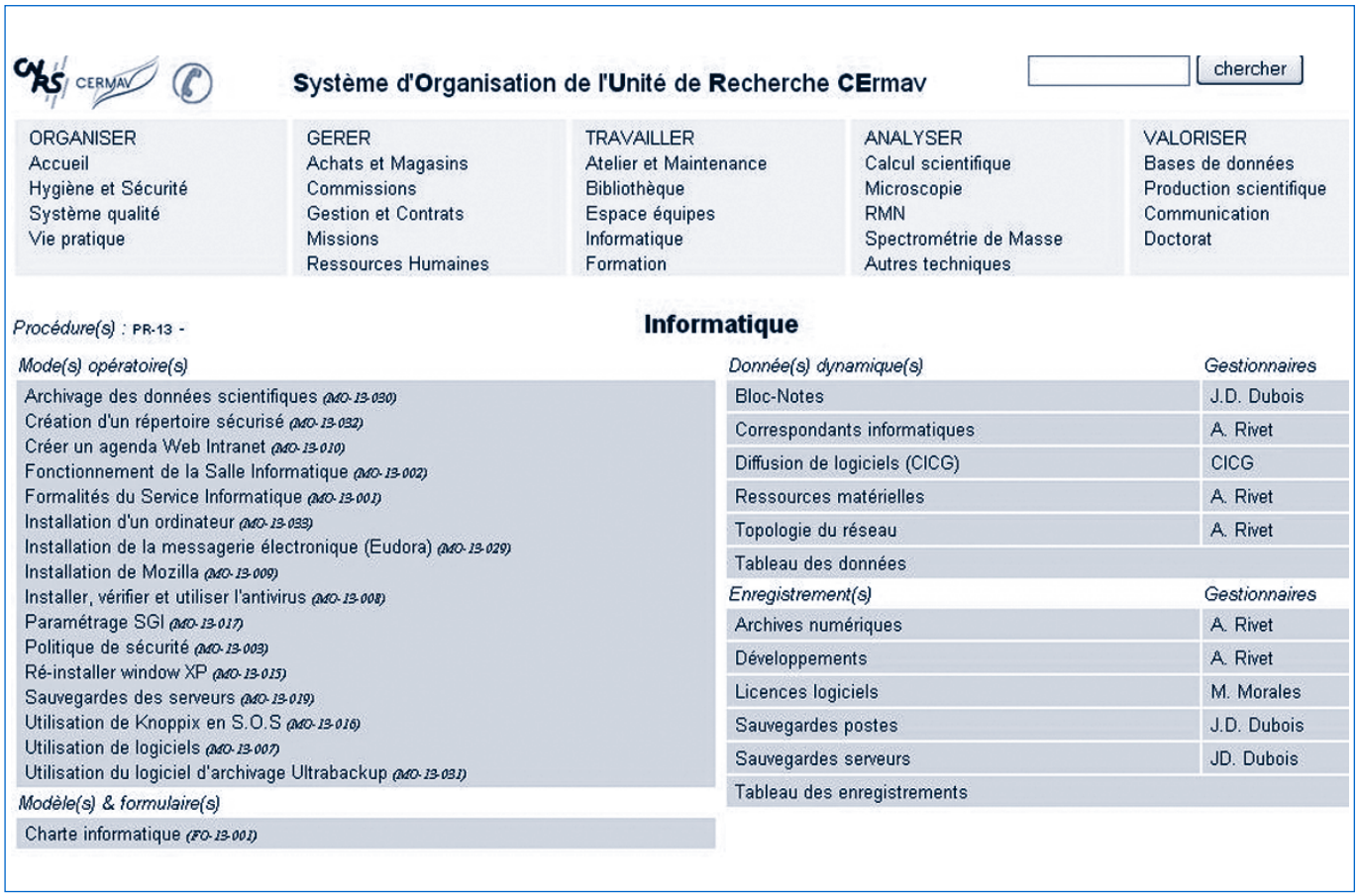
Le Système d'organisation de l'unité de recherche CERMAV (SOURCE) s'organise autour de cinq grands thèmes : organiser, gérer, travailler, analyser et valoriser, subdivisés en rubriques. Chaque page de l'interface web donne accès aux informations spécifiques de la rubrique : la documentation qualité (procédures, modes opératoires et formulaires), qualifiée de statique dans la partie gauche, et les informations dynamiques (données et enregistrements), dans la partie droite.

A travers l'exemple de la rubrique Informatique ci-après, un utilisateur pourra accéder à des modes opératoires généraux : «Fonctionnement de la salle informatique», «Politique de sécurité» ou Techniques : «Archivage des données scientifiques», «Installation de la messagerie électronique», et à la «Charte informatique» pour la partie formulaires. Au titre des données dynamiques, la liste des «Ressources matérielles», la «Topologie du réseau» sont, par exemple, disponibles, alors qu'au niveau des enregistrements l'utilisateur pourra retrouver les «Archives numériques» stockées au sein du service ainsi que la liste des licences des logiciels ou des sauvegardes.

De multiples informations sont ainsi disponibles au niveau de SOURCE et accessibles à l'ensemble du personnel du laboratoire, citons de manière non exhaustive :

- les modes opératoires d'utilisation des équipements techniques du laboratoire (microscopes électroniques, spectromètre de masse et RMN…) ;
- les comptes rendus du conseil de laboratoire et des différentes commissions,

suite de la page 2



Système d'Organisation de l'Unité de Recherche CErmav

chercher

ORGANISER	GERER	TRAVAILLER	ANALYSER	VALORISER
Accueil	Achats et Magasins	Atelier et Maintenance	Calcul scientifique	Bases de données
Hygiène et Sécurité	Commissions	Bibliothèque	Microscopie	Production scientifique
Système qualité	Gestion et Contrats	Espace équipes	RMN	Communication
Vie pratique	Missions	Informatique	Spectrométrie de Masse	Doctorat
	Ressources Humaines	Formation	Autres techniques	

Procédure(s) : PR-13 -

Informatique

Mode(s) opératoire(s)
Archivage des données scientifiques (MO-13-030)
Création d'un répertoire sécurisé (MO-13-032)
Créer un agenda Web Intranet (MO-13-010)
Fonctionnement de la Salle Informatique (MO-13-002)
Formalités du Service Informatique (MO-13-001)
Installation d'un ordinateur (MO-13-033)
Installation de la messagerie électronique (Eudora) (MO-13-029)
Installation de Mozilla (MO-13-009)
Installer, vérifier et utiliser l'antivirus (MO-13-008)
Paramétrage SGI (MO-13-017)
Politique de sécurité (MO-13-003)
Ré-installer window XP (MO-13-015)
Sauvegardes des serveurs (MO-13-019)
Utilisation de Knoppix en S.O.S (MO-13-016)
Utilisation de logiciels (MO-13-007)
Utilisation du logiciel d'archivage Ultrabackup (MO-13-031)
Modèle(s) & formulaire(s)
Charte informatique (FO-13-001)

Donnée(s) dynamique(s)	Gestionnaires
Bloc-Notes	J.D. Dubois
Correspondants informatiques	A. Rivet
Diffusion de logiciels (CICG)	CICG
Ressources matérielles	A. Rivet
Topologie du réseau	A. Rivet
Tableau des données	
Enregistrement(s)	*Gestionnaires*
Archives numériques	A. Rivet
Développements	A. Rivet
Licences logiciels	M. Morales
Sauvegardes postes	J.D. Dubois
Sauvegardes serveurs	JD. Dubois
Tableau des enregistrements	

les plannings de réservation (salles, équipements…);
- l'accès aux documents administratifs (demandes de missions, formation, accueil de personnel…);
- l'accès aux bases de données (personnels, publications, structures de molécules, images…);
- le suivi des cahiers de laboratoire.

Parallèlement à l'amélioration des circuits d'information du laboratoire, la mise en place d'un SMQ a également eu des impacts majeurs au niveau du personnel et de la gouvernance du laboratoire.

Sur le plan humain, on a observé :
- une mobilisation importante du personnel ITA autour de ce projet, qui a ainsi contribué à fédérer le personnel autour d'un objectif;
- une meilleure reconnaissance du travail du personnel ITA par la formalisation de leurs activités et de leurs savoir-faire;
- une sensibilisation des chercheurs initialement peu concernés par la démarche qualité : *«La qualité de notre travail est jugée par la communauté scientifique à travers les publications»*, qui commencent à appliquer des méthodes de management dans le cadre des projets doctorants.

Au niveau de la direction du laboratoire, le SMQ a permis :
- une disponibilité accrue des informations et un meilleur suivi des activités du laboratoire par la direction, qui dispose ainsi, à tout moment, des données nécessaires à l'élaboration de rapports;
- une meilleure visibilité vis-à-vis de nos partenaires industriels pour qui la démarche qualité apparaît comme un gage de professionnalisme.

Par ailleurs, le SMQ va offrir un cadre idéal pour mettre en place à l'avenir une Politique de sécurité du système d'information de l'unité auprès d'un personnel déjà sensibilisé avec le suivi des anomalies, l'élaboration de tableaux de bord et la mise en place d'audits. De telles actions contribuent déjà au processus d'amélioration continue, un des principes essentiels de la démarche qualité, mené au CERMAV.

Je terminerai par les remarques du comité d'évaluation du CNRS qui mentionnait dans son rapport sur l'évaluation du laboratoire en novembre 2005 :
«La mise en place du système qualité de gestion des activités du CERMAV est un excellent atout. La démarche est originale et très bien menée. Il faut vraiment féliciter le CERMAV pour cette initiative. Ce système "SOURCE" peut être considéré comme un outil au service de la recherche, au CERMAV aussi bien que dans d'autres organismes qui voudraient s'en inspirer. C'est aussi un élément rassembleur, présenté, à juste titre, comme un pas supplémentaire vers l'unité du CERMAV. Il faut remarquer à cette occasion l'importante implication des ITA et, aujourd'hui, des étudiants dans la réalisation de ce qui n'était qu'à l'état d'ébauche lors de la précédente évaluation. Les étudiants semblent particulièrement bénéficier de cette organisation structurée qui les aide à établir des interactions scientifiques et autres leur permettant de mieux exploiter la richesse du CERMAV.» ■

Contact :
Alain.Rivet@cermav.cnrs.fr,
Site :
http://www.cermav.cnrs.fr
Référentiels utiles :
http://www.utc.fr/qualite-recherche/referentiels/referentiels.htm

Le management de la sécurité de l'information

Laurent Bloch, RSSI de l'INSERM

Le domaine de la sécurité informatique voit depuis quelques années éclore des normes comme champignons après une pluie d'été : nous nous intéresserons plus particulièrement ici à la norme IS 27001, consacrée aux Systèmes de management de la sécurité de l'information (SMSI).

L'ISO a entrepris d'encadrer par des normes les systèmes de management, et pour ce faire a commencé par en donner une définition, qui fait l'objet de la norme IS (pour International Standard) 9000 ; un système de management est un système qui permet :
- ***d'établir une politique ;***
- ***de fixer des objectifs ;***
- ***de vérifier que l'on a atteint les objectifs fixés.***

L'idée cruciale, au cœur de cette problématique, est que le système de management repose sur un référentiel écrit, et qu'il est donc vérifiable, au moyen d'un audit qui consistera à comparer le référentiel à la réalité pour relever les divergences, nommées écarts ou non-conformités.

Description de la norme IS 27001

Le SMSI a pour but de maintenir et d'améliorer la position de l'organisme qui le met en œuvre du point de vue, selon les cas, de la compétitivité, de la profitabilité, de la conformité aux lois et aux règlements, et de l'image de marque. Pour cela, il doit contribuer à protéger les actifs *« assets »* de l'organisme, définis au sens large comme tout ce qui compte pour lui. Pour déterminer les mesures de sécurité, dont une énumération devra être fournie lors d'une étape de planification, la norme IS 27001 s'appuie sur le catalogue de mesures et de bonnes pratiques proposé par la norme IS 27002 (ex-17799), *« International Security Standard »,* plus volumineuse et au contenu plus technique.

IS 27001 impose une analyse des risques, mais ne propose aucune méthode pour la réaliser : l'auteur du SMSI est libre de choisir la méthode qui lui convient, à condition qu'elle soit documentée et qu'elle garantisse que les évaluations réalisées avec son aide produisent des résultats comparables et reproductibles. Un risque peut être accepté, transféré à un tiers (assurance, prestataire) ou réduit à un niveau accepté.

Un exemple de méthode d'analyse de risque utilisable dans le cadre d'IS 27001 est la méthode EBIOS® (Expression des besoins et identification des objectifs de sécurité), qui *« permet d'apprécier et de traiter les risques relatifs à la Sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI ».* On pourra consulter le site consacré à EBIOS : **http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html**

L'ISO prépare une norme d'analyse de risques, IS 27005. Pour un inventaire commenté de toutes ces normes, on se reportera avec profit à la présentation (**http://www.hsc.fr/ressources/presentations/emiae-intro27001/img0.html**) qu'en a faite Hervé Schauer, consultant en sécurité.

Élaboration et mise en place du SMSI

La norme IS 27001 précise la démarche qui doit être suivie pour élaborer et mettre en place le SMSI : disons que l'organisme désireux de se voir certifier devra :
- définir le champ du SMSI ;
- en formuler la politique de management ;
- préciser la méthode d'analyse de risques utilisée ;
- identifier, analyser et évaluer les risques ;
- déterminer les traitements qui seront appliqués aux différents risques, ainsi que les moyens d'en vérifier les effets ;
- attester l'engagement de la direction de l'organisme dans la démarche du SMSI ;
- rédiger le *« Statement of Applicability »* (SOA), qui sera la charte du SMSI et qui permettra de le soumettre à un audit.

Suivi et application du SMSI

Ici, la norme précise que, une fois le SMSI formulé, il faut faire ce qu'il stipule, vérifier que c'est fait, identifier les erreurs dans son application, les failles qui s'y manifestent, les modifications du contexte de nature à nécessiter sa mise à jour ou sa modification.

Analyse critique de la norme IS 27001

Ainsi que tout RSSI devrait le faire, j'ai suivi une formation pour devenir responsable d'audit pour les Systèmes de management de la sécurité de l'information (SMSI), autrement dit *« Lead Auditor IS 27001 »,* et j'ai obtenu la certification correspondante. Voici les impressions que j'en ai retirées.

Comme pour la plupart des normes similaires, au premier rang desquelles IS 9001, les idées à la base d'IS 27001 semblent de bon sens : il est sain de réfléchir aux risques auxquels l'entreprise est exposée, d'élaborer un référentiel de mesures à prendre pour s'en prémunir, de vérifier régulièrement l'application de ces mesures, de réviser le référentiel, etc.

Mais, comme presque toujours, la norme en fait trop, et comme les ressources dévolues à la démarche SSI seront de toute façon limitées, celles qui seront absorbées par le processus administratif très lourd, nécessaire à suite page 5

suite de la page 4

l'application de la norme, seront perdues pour l'action SSI pratique sur le terrain. Il faut en effet prendre à la lettre le titre de la norme : il ne s'agit pas de sécurité, mais de management de la sécurité, c'est-à-dire des processus de contrôle du travail réel, qui, lui, doit bien être fait par des gens quelque part.
Selon un participant à une réunion consacrée à IS 27001, il y a trois raisons qui peuvent pousser à se soumettre à la norme :

- un obligation légale : les lois Sarbanes-Oxley et leurs semblables européennes peuvent engendrer une obligation de ce type, mais cela ne concerne guère les établissements de recherche publics ;
- une obligation contractuelle : on peut imaginer qu'un laboratoire doive s'y soumettre à l'occasion d'un contrat industriel ;
- une obligation morale, ce qui reste à l'appréciation de chacun, mais place assez haut le seuil financier de la paix avec sa conscience.

Il est frappant de constater que la vérification formelle de conformité à une norme telle qu'IS 27001 peut presque être effectuée par un auditeur dépourvu de compétence technique : il suffit de lire les documents obligatoires et de vérifier que les mesures mentionnées ont bien été appliquées, ce qui doit être écrit dans un autre document, une feuille de tableur en général.

Les auteurs de ces normes semblent croire que l'univers peut être décrit de façon adéquate par un tableau de cases à cocher, analogue à un questionnaire à choix multiples : on se demande pourquoi les grands nigauds nommés Aristote, Descartes, Newton, Kant et Einstein n'y ont pas pensé, ils se seraient épargné bien de la fatigue cérébrale, ainsi qu'aux étudiants des siècles suivants !
Il est aussi possible de noter que ces procédures d'évaluation ne sont pas uniquement construites en fonction des buts à atteindre, mais aussi, sinon surtout, en fonction de ce qui, dans les processus étudiés, se prête bien à l'évaluation, parce que, par exemple, il est facile d'y adapter une métrique.
Le mot de la fin sera que les règles de sécurité complexes seront simplement inappliquées, parce que trop difficiles à comprendre. Si l'on doit appliquer la norme IS 27001, il faudra sérieusement se poser la question du périmètre de cette application : les systèmes de management à périmètre trop grand ne résistent pas aux audits et perdent rapidement leur certification. ■

laurent.bloch@auteuil.inserm.fr
Laurent Bloch vient de publier avec Christophe Wolfhugel aux Éditions Eyrolles un livre intitulé *Sécurité informatique - Principes et méthode*.

BRÈVES

En cette année 2006, deux types d'incidents ont fait l'actualité dans notre environnement : la compromission de serveurs web dynamiques et l'attaque par force brute de serveurs SSH. Ils feront sans doute aussi l'actualité 2007. Mais, en plus, il faudra aussi s'attendre à de nouveaux risques potentiels liés à l'utilisation de nouveaux outils.

Outils d'indexation et de recherche

Le CERTA vient de publier une note d'information traitant de ce sujet (http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009.pdf). Ce document, en décrivant les fonctionnalités, l'installation et l'utilisation de ces logiciels ainsi que les menaces liées, met l'accent sur les effets néfastes tant sur le matériel (consommation excessive de ressources) qu'au niveau applicatif (intégrité du SI, fuite d'informations confidentielles, nominatives…) engendrés par l'utilisation des outils d'indexation et de recherche.
Six recommandations sont proposées, que nous vous conseillons de suivre.

Supports de stockage USB (http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006.pdf)

Interface de connexion, l'USB (Universal Serial Bus) offre actuellement des possibilités aisées de connexion des équipements informatiques : souris, support de stockage mais aussi support d'application (USB 3). L'utilisation de ces derniers dans un contexte nomade présente des risques aussi bien pour le périphérique que pour l'hôte (installation de rootkits, vol d'information…). Aussi, que ce soit pour l'utilisateur ou l'administrateur, certaines précautions doivent être prises, celles-ci sont clairement détaillées dans le document du CERTA.

Dans les publications du CERTA, nous avons également retenu une note d'information traitant d'un sujet d'actualité

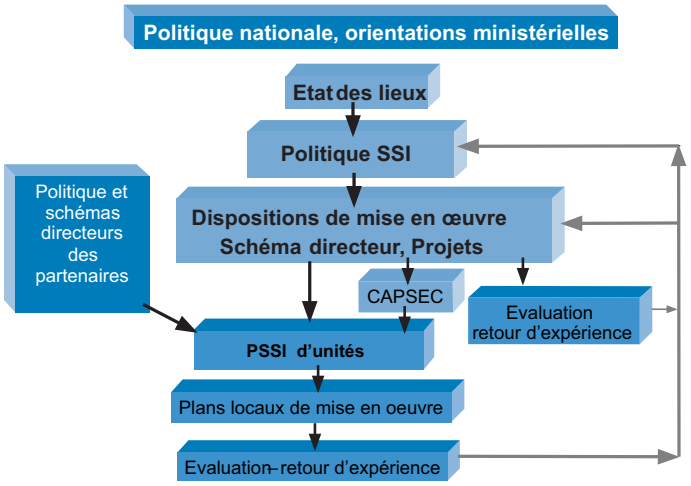
Cartes postales électroniques (http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-002.pdf)

Grâce à Internet, il est désormais facile et peu coûteux d'envoyer une carte de vœux. Cependant, l'envoi de carte postale électronique, pas seulement de vœux, est un vecteur de propagation des virus, chevaux de Troie ou autres contenus malveillants. En ces périodes de fêtes, la vigilance et la sensibilisation des utilisateurs sont de rigueur. La note du CERTA donne quelques précautions à prendre lors de la réception de tels messages et conseille aux webmestres, dont les sites proposent des cartes postales, de vérifier l'intégrité des fichiers qu'ils proposent.
Contact : Marie-Claude Quidoz UREC
marie-claude.quidoz@urec.cnrs.fr

Une PSSI pour le CNRS

Joseph Illand, fonctionnaire de sécurité de défense du CNRS

Schéma de déclinaison de la PSSI au sein du CNRS



Arnold MIGUS, directeur général du CNRS, a signé le 15 novembre dernier le document de «Politique de sécurité des systèmes d'information» (PSSI) du CNRS.

Ce document marque un engagement fort de la direction générale du CNRS sur les points essentiels que sont les enjeux, l'organisation et les grands arbitrages d'orientation en matière de sécurité des systèmes d'information.

Le texte rappelle le contexte propre au CNRS et replace la SSI dans le contexte de la protection du patrimoine scientifique. Il définit l'organisation interne de la fonction SSI, aux niveaux national, régional et local, et l'organisation des relations avec les autres tutelles d'unités mixtes de recherche.

Un chapitre important est consacré aux principes de mise en œuvre de la PSSI. Ce chapitre définit les orientations essentielles qui doivent servir de guide aux responsables de la SSI, qu'ils soient en position hiérarchique (directeurs d'entité) ou en position fonctionnelle (responsable ou expert SSI).

La PSSI a vocation à être déclinée et adaptée sur le terrain en «PSSI d'entités», sous la responsabilité des directeurs d'entités, en intégrant les orientations nationales et les particularités de chacune de ces entités.

Une PSSI qui s'inscrit dans une démarche de pilotage et de communication

La PSSI du CNRS se veut la clé de voûte d'un dispositif de pilotage et de mise en œuvre.

Elle apporte un éclairage et un cadrage de l'action des acteurs de terrain (responsables hiérarchiques et acteurs «fonctionnels» de la SSI).

C'est aussi un document à vocation de sensibilisation, d'information et de communication sur l'organisation et les grands choix du CNRS en matière de sécurité des systèmes d'information, document à destination interne mais aussi externe (notamment dans le cadre du partenariat avec les autres tutelles).

Au niveau des entités du CNRS, la PSSI va trouver sa concrétisation dans l'élaboration et la mise en œuvre des «PSSI d'entités», sous la responsabilité des directeurs d'entité et avec l'appui des acteurs spécialisés en matière de SSI. Ces PSSI devront intégrer orientations nationales et particularités locales.

Pour les unités mixtes, la PSSI locale doit tenir compte également des politiques et schémas directeurs propres aux autres tutelles. La PSSI du CNRS est alors un document de référence et de dialogue avec les autres tutelles.

Une démarche souple et adaptable

Le CNRS a volontairement retenu de faire du document de PSSI un document assez court, sans entrer dans un formalisme excessif. En ce sens, le CNRS s'est inspiré du *Guide pour l'élaboration d'une politique de sécurité de système d'information* proposé par la DCSSI, sans s'y conformer à la lettre et en renvoyant vers le schéma directeur de la SSI les développements les plus techniques.

C'est un document évolutif et sa révision est prévue selon une périodicité annuelle.

Une démarche concertée

Le projet de PSSI a été élaboré par un groupe de travail constitué des représentants des principaux acteurs impliqués en PSSI au CNRS. Les travaux ont donné lieu à de nombreux échanges intermédiaires, où sont intervenus d'autres acteurs apportant leur contribution aux réflexions (personnels UREC, coordinateurs et correspondants SSI, délégués régionaux…).

Une démarche suivie d'effets

La signature de la PSSI du CNRS ouvre un chantier, dont les premières étapes sont la mise en place des instances de pilotage national, le réajustement du dispositif d'animation régionale et la redéfinition des responsabilités dans les entités.

Le dispositif sera alors en ordre de marche pour engager les démarches de mise en schémas des orientations, directives et méthodologies au niveau national et pour lancer, dans les laboratoires, le processus de constitution des «PSSI d'entités».

La publication prochaine d'une nouvelle charte «utilisateurs», intégrant évolutions législatives récentes (loi CNIL, LCEN…) et jurisprudence, s'inscrit également dans cette nouvelle démarche. ■

joseph.illand@cnrs-dir.fr

SÉCURITÉ INFORMATIQUE
numéro 58 décembre 2006
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
JOSEPH ILLAND
Fonctionnaire de sécurité de défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris XVI
Tél. 01 44 96 41 88
Courriel : Joseph.Illand@cnrs-dir.fr
http://www.sg.cnrs.fr/fsd

Rédacteur en chef de ce numéro :
FRANÇOIS MORRIS, CNRS/IMPMC et UREC
Courriel : francois.morris@impmc.jussieu.fr

ISSN 1257-8819
Commission paritaire n° 1010 B 07548

Conception et réalisation : La Souris 01 45 21 09 61