SÉCURITÉ de l'information
Sécurité Informatique / Numéro 7 ////// Février 2010

Éditorial

Qualité de services et sécurité de l'information, deux nouvelles promesses des ASR[1]

JACQUES LAVIELLE
Responsable de la modernisation et de la qualité administrative
Membre fondateur du Club des pilotes de processus,
www.pilotesdeprocessus.org

Résinfo, fédération des réseaux d'Administrateurs Systèmes et Réseaux (ASR), vient de confirmer la dynamique, observée depuis plusieurs années, des réseaux des métiers exercés dans les unités de recherche. La publication, fin 2009, du Guide des bonnes pratiques organisationnelles pour les ASR, marque une avancée significative des ambitions de professionnalisation de ces métiers, prenant pour credo l'amélioration continue du service rendu aux clients des entités en charge du traitement des informations.

Adopter deux normes, ISO 20000 et ISO 27000, directement inscrites dans la filiation de la norme ISO 9001, revient à tirer le meilleur parti des principaux ressorts de la qualité. Désormais, ceux-ci guideront les bénéfices que l'on peut attendre du déploiement opérationnel de ce guide :

- l'orientation client, postulant que l'écoute et la satisfaction des exigences des bénéficiaires sont le moteur de l'amélioration ;
- l'implication du personnel, en faisant comprendre à chacun son rôle et son importance dans les progrès de l'organisation ;
- l'amélioration continue, au centre du système de management de la qualité ;
- l'approche processus.

Ce dernier concept, le management des processus, fonde, pour une large part, les exigences et préconisations énoncées par la norme ISO 20000, directement issues d'ITIL. Ce code des meilleures pratiques pour la fourniture de services informatiques fut publié dans sa version initiale en 1989, à l'initiative du gouvernement britannique qui souhaitait voir progresser la qualité des prestations de ses centres de traitement.

La production informatique est ainsi appréhendée au travers d'un ensemble de processus conduisant à garantir le niveau des services aux utilisateurs dans le cadre d'un engagement formalisé dans un contrat négocié.

A la différence de la vision procédure, centrée sur la description du chemin organisationnel à suivre, l'approche processus privilégie l'identification des buts à atteindre, les objectifs poursuivis, les compétences et les moyens associés ainsi que la mesure de leur efficacité.

En contribuant à l'introduction au CNRS de la culture du management par les processus, les ASR bénéficieront d'un langage et d'une grille de lecture de leurs activités communes, de nature à grandement faciliter la mutualisation de leurs expériences et de leur savoir-faire, voire le développement d'outils communs et innovants.

Autant d'atouts de nature à accompagner la mise en œuvre de la norme ISO 27000 relative à la sécurité de l'information dont on sait,

›››› *suite page 6*

1. **A**dministrateur **S**ystèmes et **R**éseaux

Guide de Bonnes Pratiques organisationnelles pour les ASR dans les unités de recherche

Olivier Brand-Foissac
ASR au Laboratoire de Physique Théorique d'Orsay- UMR8627

Laurette Chardon
ASR au Groupe de Recherche en Informatique, Image, Automatique et Électronique de Caen – UMR6072

Marie David
Coordinatrice SSI de la délégation régionale Alpes

Maurice Libes
ASR au Centre d'Océanologie de Marseille – UMS 2196

Gilles Requilé
ASR au Laboratoire de Mécanique et Génie Civil de Montpellier – UMR5508

Alain Rivet
Expert régional SSI, responsable Qualité – Système d'information du Centre de Recherches sur les Macromolécules Végétales de Grenoble, UPR 5301

Cet article est un résumé du Guide des Bonnes Pratiques organisationnelles des Administrateurs Systèmes et Réseau [1] (ASR), édité par RESINFO, dans lequel les thèmes abordés ci-dessous sont pleinement traités et développés. Il doit être considéré comme une introduction qui incite à sa lecture.
Le terme de « Guide » est défini dans plusieurs dictionnaires comme suit : « qui donne des conseils et accompagne ». C'est l'optique adoptée par les auteurs. De par leur fonction d'ASR de terrain, ils connaissent bien les problématiques du métier d'ASR dans les unités de recherche. Ils ont souhaité faire partager leur expérience.

Introduction

Ce projet de Guide est né à l'initiative de RESINFO, à partir d'une réflexion générale liée aux différents contextes de travail de notre métier, dans lesquels on assiste à une intensification des tâches d'exploitation des systèmes informatiques et des réseaux et des responsabilités attenantes, la plupart du temps à moyens humains constants.
Son objectif vise à déterminer les pratiques et les processus à mettre en place sur le terrain, pour une meilleure organisation personnelle et de travail, afin d'améliorer la qualité et la fourniture de services, la sécurisation de nos

›››› *suite page 2*

serveurs et réseaux, la documentation de nos actions, la communication avec les utilisateurs, la prise en compte des évolutions technologiques, et *in fine* la lisibilité de nos activités d'ASR.
Notons que nous avons choisi dans un premier temps de ne pas développer les pratiques liées à l'utilisation de l'informatique et à ses conséquences sur l'environnement. En effet, le groupe ECOINFO de RESINFO a déjà réalisé un travail important sur ce thème. Le site ECOINFO (http://www.ecoinfo.cnrs.fr) fournit des recommandations concernant, entre autres, « les problématiques de la consommation énergétique et de la pollution liées à l'utilisation et au développement de l'outil informatique ». Cet aspect sera sans doute développé dans une seconde version de notre Guide.
Ce Guide des Bonnes Pratiques n'est pas un livre de solutions techniques toutes faites, de « recettes » ou de « trucs et astuces ». Les « FAQ » et les « HOWTO » comblent déjà ces besoins techniques depuis longtemps. Il n'est pas non plus un document administratif qui va dicter aux ASR une méthode d'organisation ou leur apprendre à travailler. Il s'agit plus modestement de s'initier à des méthodologies d'organisation issues du monde industriel ainsi qu'à des normes en matière de fourniture de service et de gestion de la sécurité. Nous abordons aussi quelques pratiques dans le domaine juridique visant à observer un comportement conforme aux règlements et terminons sur des notions de gestion du temps et de relations de l'ASR avec ses partenaires.
Les aspects de mise en œuvre pratique d'organisation de service et de démarche qualité extraits de ITIL [2] et ISO-20000 [3] que nous décrivons dans ce Guide sont jusqu'à présent peu intégrés dans nos habitudes de travail. Pour ne pas en rester à un stade théorique, nous donnons en annexe du Guide un ensemble de *références techniques* vers des logiciels ou vers de la bibliographie qui peuvent permettre aux ASR de mettre en place tel ou tel processus nécessité dans l'organisation de service. L'ASR reste de toute façon maître de ses choix techniques dans son propre contexte.
Ce Guide n'a pas la prétention d'apporter des solutions « magiques » à nos difficultés de travail mais plutôt de donner des pistes pour mieux s'organiser.

Les modèles ITIL et ISO-20000

Les recommandations sur l'organisation des services informatiques, exposées ci-après, sont issues d'une réflexion inspirée de l'approche de l'amélioration de la qualité des services informatiques décrite par ITIL [2] (*Information Technology Infrastructure Library*) et plus récemment par la norme ISO-20000 [3].
Il nous a semblé opportun de nous servir de ces référentiels normés qui fournissent un cadre dans lequel nous pouvons positionner les activités et méthodes existantes des services informatiques, tout en favorisant leur structuration. Cette norme formalise l'ensemble des activités d'une production informatique et correspond à une approche « orientée client » qui introduit la notion de « qualité de service » apportée aux utilisateurs.
Parmi les processus présents dans la norme ISO-20000, on va distinguer, d'une part, ceux relatifs à la fourniture de service qui décrivent les processus nécessaires pour fournir le service aux utilisateurs (gestion des niveaux de service, gestion de la continuité et de la disponibilité, budgétisation et gestion de la sécurité) et, d'autre part, les processus relatifs au support de service, destinés à mettre en place et assurer un service efficace et fonctionnel (gestion des configurations, gestion des changements, gestion de la mise en production, gestion des incidents et gestion des problèmes).
A ces processus « métier », s'ajoutent les processus qui accompagnent le modèle PDCA (pour Plan Do Check Act encore appelé roue de Deming), destinés à mettre en place les activités qui concernent l'amélioration continue (rôles et responsabilités de la Direction, gestion documentaire, gestion des compétences et de la formation, surveillance et mesures).

Transposition au contexte ASR dans une unité de recherche

Les auteurs ont donc cherché à replacer ce modèle d'organisation dans le contexte d'une unité de recherche et à le décliner en fonction du contexte et du périmètre de ces unités (taille, mono ou multi-site, diversité des recherches, collaborations internationales...). L'application de cette démarche qualité au métier d'ASR dans un laboratoire de recherche nous conduit à proposer un modèle d'organisation à travers les actions suivantes.

- **Définir le périmètre d'action** : l'ASR doit, dans un premier temps, définir son périmètre d'action en spécifiant ses domaines d'intervention et/ou en

Zoom sur la démarche qualité en sécurité des systèmes d'information au CNRS

Le CNRS, depuis plusieurs années, s'est engagé dans une démarche qualité de la sécurité des systèmes d'information (SSI) au travers d'un certain nombre d'actions.
Le point de départ a été l'élaboration d'un document d'orientation de la sécurité des systèmes d'information du CNRS (Politique de Sécurité des Systèmes d'Information - PSSI du 15 novembre 2006).
Depuis, un réseau humain s'est organisé pour accompagner la démarche au sein des unités de recherche du CNRS : 100 coordinateurs régionaux ont été désignés auprès des délégations régionales à partir de 2007, parmi lesquelles 18 personnes certifiées ISO 27001 en 2008 (Lead Implementor).
Le dispositif des Chargés de Sécurité des Systèmes d'informations (CSSI) dans les unités sera terminé dans le courant de l'année 2010, finalisant ainsi l'organisation de la SSI au CNRS en trois niveaux, national, régional et local.
Pour accompagner la phase finale de ce dispositif organisationnel et plus particulièrement la prise de fonction des nouveaux CSSI, une formation en « management de la SSI » a été réalisée en région. De la conception du cours, des supports de cours, des TPs, de la « formation de formateurs » jusqu'à sa réalisation en région (plus de 400 heures de cours, 15 délégations), cela a été un lourd projet porté au cours de l'année 2009 :

- près de 500 CSSI et CRSSI ont été formés,
- plusieurs dizaines d'unités se sont déjà engagées dans la réalisation de leur PSSI locale.

L'effort déployé commence à donner des résultats, tout d'abord en mettant un terme à certaines expériences qui s'engageaient sur une méthodologie trop académique, sans appropriation par les utilisateurs eux-mêmes et qui risquaient de mettre en péril le déploiement ultérieur ; enfin en donnant aux CSSI des méthodes et des outils pour décliner la PSSI d'établissement dans les unités, tout en leur apportant une « culture du management » de la sécurité des systèmes d'information.

excluant ceux qui ne sont pas de sa responsabilité.

- **Mettre en place une gestion des configurations** : cette étape nécessite d'effectuer un inventaire de l'ensemble des composants aussi bien matériels (ordinateurs, équipements réseau...) qu'immatériels (documentations, licences, contrats...) du service.
- **Définir les niveaux de service** : la définition des niveaux de service doit permettre aux utilisateurs de connaître la nature et l'étendue du support offert par le service informatique. Chaque « niveau de service » sera associé à des objectifs réalistes visant à assurer un niveau de qualité satisfaisant pour les utilisateurs.
- **Définir la continuité de service** : associé à chaque niveau de service, l'ASR devra spécifier les exigences des utilisateurs en termes de continuité des services. Cet engagement établi en accord avec la Direction (et/ou une commission d'utilisateurs) sera évalué régulièrement.
- **Gérer les interventions** : il convient de prendre en compte de manière efficace toutes les demandes d'intervention qu'il s'agisse de celles émanant des utilisateurs, ou des changements à apporter aux éléments du système.
- **Gérer les dysfonctionnements** : l'objectif consiste, d'une part, à minimiser l'impact des dysfonctionnements du système d'information sur les services et, d'autre part, à prévenir leur réapparition.
- **Assurer les changements et la mise en production** : tout changement apporté au système d'information doit être maîtrisé afin de minimiser le risque d'incident potentiel lors de sa mise en place.

La gestion de la sécurité s'appuie sur un référentiel à lui seul (ISO-27001 Management de la sécurité). Il sert de base à la mise en place des politiques de sécurité au sein des unités et sera développé au paragraphe quatre. Adaptés à nos structures d'entités CNRS, Universitaires, EPST, EPIC..., les concepts ITIL/ISO-20000 peuvent être visualisés à travers la cartographie suivante (figure 1) :

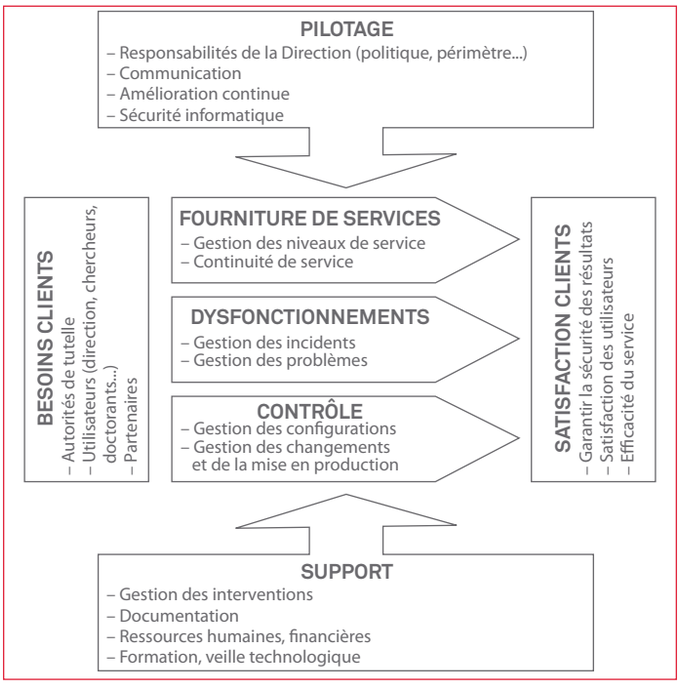

Figure 1. Cartographie des processus dans un laboratoire de recherche

Les processus de pilotage et de support complètent, dans cette cartographie, les processus métier représentés par la fourniture de services, la gestion des dysfonctionnements et le contrôle. La norme introduit la notion de « client » : autorités de tutelle, utilisateurs du service (Direction, chercheurs...) ou partenaires que l'on va chercher à satisfaire. Cette satisfaction va, par exemple, consister à garantir la sécurité des résultats de la recherche, répondre aux besoins des utilisateurs tout en améliorant l'efficacité du service.

La Documentation

Dans le cadre des processus d'amélioration continue, la documentation occupe une place très importante dans le suivi et la traçabilité de nos différentes actions (mise en place de nouveaux services, gestion des configurations, changements apportés au S.I., la résolution des incidents et problèmes, l'aide aux utilisateurs etc.). Dans l'ensemble des tâches qui jalonnent le métier d'ASR, il est donc nécessaire de rédiger les diverses documentations indispensables à la maintenance et à l'évolution du système d'information.

Un système documentaire centralisé, facilement accessible (CMS, Wiki...) riche en informations et bien organisé fera gagner du temps aux ASR. Pour des raisons de disponibilité, il est nécessaire d'assurer une redondance de cette documentation sensible sur support papier de manière à y avoir accès en cas de panne système. On distingue dans notre Guide deux grandes classes de documentation, celle destinée aux utilisateurs, la seconde à accès restreint réservée aux ASR, du fait des informations techniques confidentielles qu'elle peut contenir.

- **La documentation pour les utilisateurs** : ce sont les informations qui permettent aux utilisateurs de comprendre les règles et procédures à suivre pour accéder et utiliser correctement les services qui sont mis en place par le service informatique. Ce type de documentation peut permettre de rendre les utilisateurs autonomes et de ne pas déranger inutilement les ASR par des questions récurrentes.
- **La documentation technique destinée aux ASR** : ce sont les informations techniques propres au service informatique de l'unité, qui peuvent contenir des informations sensibles (architecture réseau, exploitation de services...). La qualité de ces documentations doit permettre de confier ou déléguer l'exploitation de certains services à d'autres ASR de l'équipe ou chargés transitoirement d'intervenir.

Les bonnes pratiques dans la gestion de la sécurité des systèmes d'information

La norme ISO-27001 [4] fournit un cadre normatif aux bonnes pratiques des ASR en matière de gestion de la sécurité du système d'information de nos unités. Elle spécifie les exigences relatives à la mise en œuvre des mesures de sécurité adaptées aux besoins de chaque organisme ou à leurs parties constitutives. En particulier, la norme ISO-27002[5] constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information.

En effet, la sécurité de nos systèmes d'information nécessite quelques pratiques d'administration et d'organisation de base que l'on retrouve dans les normes ISO-27001 et ISO-27002, de même que dans les politiques de sécurité (PSSI) d'établissement (dont la PSSI du CNRS [6]).

Ces pratiques sont également basées sur une démarche par « processus » et intègrent le principe d'amélioration continue qui vise, après avoir mis en place des éléments de sécurité, à surveiller et réévaluer leur

efficacité. Nous parcourons dans notre Guide quelques bonnes pratiques essentielles dans le domaine de la sécurisation d'un S.I. :

- **Définition du périmètre sur lequel doit porter la sécurité du S.I.** : pour déterminer les exigences de sécurité de l'information de nos unités, il est nécessaire d'étudier au préalable le contexte et le périmètre de l'entité à sécuriser. Cette étude implique de bien connaître les spécificités de son unité (missions, enjeux, ...) et d'inventorier les différents actifs qui composent le S.I. de l'unité (matériels, logiciels, réseau, personnel, locaux, données, ...).
- **Appréciation des risques** : une analyse des risques qui peuvent peser sur les actifs de l'organisme (au travers de méthodes telles qu'EBIOS [7], MEHARI,...) permet d'identifier les objectifs de sécurité et les mesures à prendre, adaptées aux besoins de sécurité de l'unité. Elle sert de base à l'élaboration de la politique de sécurité du S.I. et permet de définir un plan d'action. Dans une analyse de risques, on identifie notamment les menaces et les vulnérabilités potentielles qui pèsent sur les actifs du système d'information. La documentation de la méthode EBIOS peut apporter une aide rigoureuse pour sélectionner les menaces et les méthodes d'attaques opportunes dans le contexte étudié. Ensuite, il faut s'attacher à identifier les impacts qui portent sur les besoins exprimés en termes de pertes de confidentialité, d'intégrité et de disponibilité.
- **Traitement des risques** : à partir de la liste des risques hiérarchisés, on peut définir quels sont les traitements à appliquer pour réduire ou éliminer ces risques et donc définir des objectifs de sécurité. Ces objectifs de sécurité constituent le cahier des charges des mesures de sécurité à mettre en œuvre pour l'environnement étudié. La norme ISO-27002 [5] propose une série de mesures à mettre en œuvre pour couvrir les risques révélés par l'analyse. Elle nous permet de lister les mesures de sécurité courantes qui constituent autant de bonnes pratiques dans le métier d'ASR.
- **Exemples de mesures de sécurité courantes** : nous explicitons dans le guide quelques pratiques courantes en matière de sécurité informatique qui sont fréquemment mises en place par les ASR dans la sécurisation du S.I. de nos unités de recherche telles que la sécurité physique des locaux, la sécurité du matériel et du câblage, la mise au rebut ou recyclage des supports informatiques, la protection contre les codes malveillants, la sauvegarde des informations, la gestion des journaux systèmes, la synchronisation des horloges, la sécurité du réseau et des échanges d'informations, les contrôles d'accès au réseau et aux systèmes, la gestion de parc et des moyens nomades, la télésurveillance, les mesures de l'utilisation des ressources (métrologie)...
- **Formation et sensibilisation à la sécurité du S.I.** : le personnel doit être régulièrement informé des pratiques de sécurité à suivre, des événements et alertes. Il est important pour l'ASR d'organiser des formations de sensibilisation au sein du laboratoire tant au niveau du personnel permanent que temporaire.

Bonnes pratiques liées aux aspects juridiques du métier d'ASR

Le travail des ASR est désormais en prise avec de nombreuses obligations et responsabilités de nature juridique. De nombreuses lois sont apparues ces dernières années concernant la sécurité des systèmes d'information comme la Loi pour la Confiance en l'Economie Numérique (LCEN) ou encore le renforcement du pouvoir de la Commission Nationale de l'Informatique et des Libertés (la CNIL). Il s'agit de cibler ce que doit retenir concrètement un ASR dans son travail quotidien pour être en accord vis-à-vis de la loi. Quelles sont les bonnes pratiques dans le contexte des responsabilités juridiques ? La réponse se décline principalement sous la forme de trois actions : informer, contrôler et agir.

- **Informer** : informer les utilisateurs et la Direction en leur transmettant une information claire par le biais de messages électroniques ou de notes de service écrites avec utilisation de mots clés comme « alerte », « conseil », « mise en garde » qui permettront en cas de litiges de prouver que l'ASR a bien réalisé cette tâche d'information et de sensibilisation.
- **Contrôler** : le contrôle vise la mise en place d'outils de surveillance et de métrologie pour vérifier le bon fonctionnement loyal et proportionné des services offerts (saturation réseau, informations de site web...).
- **Agir :** en situation de crise ou d'urgence (piratage, non respect des règlements...), l'ASR a le droit et le devoir d'agir et de prendre des mesures rapidement (déconnexion de machines, retrait de contenu illicite...) pour assurer la continuité du service et la protection des données dans le respect de la réglementation en vigueur.

Gestion du temps

Notre travail est souvent assujetti à un flot continu de requêtes diverses provenant des utilisateurs qui rentrent en concurrence avec les tâches incontournables d'administration. Il faut donc s'organiser au mieux pour répondre à cette situation ; savoir gérer son temps est un des moyens pour y parvenir. Cependant si notre charge de travail ne cesse de s'alourdir et que notre méthode « naturelle » d'organisation fonctionne moins bien, alors, une réflexion et une méthodologie s'imposent.

Nous avons, dans ce guide, essayé de donner quelques pistes pour permettre aux ASR d'adopter une méthode de gestion du temps si le besoin s'en fait sentir, ou encore d'affiner celle utilisée en fonction des principes que nous avons développés. Pour cela, nous avons synthétisé la méthode de trois auteurs :

- « Getting Thing Done », de David Allen [8]
- « Admin'sys, gérer son temps » de Thomas Limoncelli [9]
- « Question de temps » de François Delivré [10]

Cinq grands principes se dégagent à la lecture de ces ouvrages.

- Tout d'abord, adopter une méthode de gestion du temps, c'est avant tout prendre conscience objectivement de nos moments les plus productifs dans la journée, de nos tendances « naturelles » et habitudes, de nos aspirations et de la façon dont nous occupons réellement nos journées.
- Le second principe met en lumière le fait que la majeure partie du stress naît d'une mauvaise gestion des engagements pris ou acceptés. Il est irréaliste de penser qu'une méthode de gestion du temps nous permettra de prendre en compte tous ces engagements. Une méthode de gestion du temps nous invite plutôt à lister tous les projets que l'on souhaite réaliser, puis elle nous amène à choisir consciemment certains d'entre eux, à mettre en place des critères de choix et donc renoncer ou différer.
- Le troisième principe est de déterminer à quel niveau de « définition » se situe un projet. Un projet naît suite à une

réflexion, à une discussion informelle avec des collègues. Ce stade de « remue-méninges » est très ouvert, sans aucune limite technique ou temporelle. A ce niveau, le projet est encore flou, il n'a pas de contours bien définis. Son déroulement ne peut donc pas vraiment être planifié. Il faut donc poursuivre la réflexion jusqu'à ce qu'il mûrisse pour le découper en sous-projets plus concrets que l'on pourra planifier.

- Le principe suivant consiste en la prise en compte de nos tendances « naturelles » à sous-estimer des délais, donc à ajouter beaucoup trop de tâches dans une journée, à se disperser, à commencer « plein de choses » et à ne jamais les finir ... Un lien dans les fiches de références du Guide vous permet de lire un résumé du livre de François Délivré [10].
- Enfin, un dernier principe consiste à définir les priorités. Qu'est-ce qui est prioritaire ? Par rapport à quoi et à qui ? C'est une notion délicate dont la signification change au cours du temps (durée, impact pour le laboratoire...) en fonction du nombre de tâches à effectuer ou selon le demandeur. Ce Guide propose quelque pistes pour permettre de réfléchir à définir ses propres priorités, particulièrement lors de journées très chargées.

Ces ouvrages montrent, à travers les exemples fournis, que la meilleure gestion du temps que l'on peut adopter est forcément personnelle. Elle nécessite de s'approprier et personnaliser les différents éléments des méthodes rencontrées.

Les formes de communication de l'ASR

Dans une unité de recherche les ASR sont en relation avec plusieurs catégories d'interlocuteurs. Il y aura donc lieu d'établir plusieurs formes de communication adaptées à chacune (formes écrites, orales, dialogues, écoutes, négociations...). On peut distinguer :

- **Les relations avec les structures de Direction**. L'ASR doit bien sûr fournir des éléments permettant de définir la politique informatique de l'unité en liaison avec les objectifs scientifiques. Ce type de communication permet d'améliorer la « lisibilité » et la crédibilité du Service Informatique au sein des unités, et permet d'afficher les missions du service, son organisation, ses moyens, les priorités à suivre, ses actions et réalisations, etc. Cela peut se traduire par exemple par la participation à des « commissions informatiques » ou par la rédaction de rapports annuels ou lors des évaluations quadriennales.
- **La communication avec les utilisateurs**. Il s'agit là d'un rôle essentiel qui consiste d'abord à être « à l'écoute » pour comprendre et prendre en compte les besoins et problèmes afin de proposer des solutions ; il s'agit aussi souvent de traduire en besoins fonctionnels ce qu'expriment les utilisateurs pour les reformuler en termes de « solutions techniques ». Il faut rendre toutes les informations accessibles pour simplifier/faciliter l'utilisation de l'outil informatique, prévenir les pratiques qui pourraient porter atteinte à la sécurité du S.I. et accueillir les nouveaux entrants.
- **La communication interne au service**. Il convient de permettre la transmission de l'information au sein du service sur les modifications et évolutions apportées à tel ou tel équipement ou configuration et donc de pouvoir assurer la continuité des fonctions en cas d'absence de certains personnels. Cela nécessite une structuration écrite (quels que soient le média et la forme) des informations pour assurer leur transmission et la traçabilité du fonctionnement des installations. Ceci s'applique bien sûr même si l'ASR est seul dans sa fonction, afin que son remplacement en cas de départ et/ou d'absence puisse se faire sans interruption des services essentiels à l'unité.
- **La communication avec les partenaires et les fournisseurs**. Un grand nombre de nos unités sont hébergées par des tutelles différentes et sont souvent amenées à travailler avec des partenaires extérieurs. Il est donc nécessaire de mettre en place une communication appropriée auprès, par exemple, des structures locales d'hébergement. Il est aussi indispensable d'assurer des liaisons avec les services s'occupant de la sécurisation du S.I. avec lequel l'unité est reliée. Enfin l'ASR est souvent la personne qui est en contact avec les fournisseurs, chargée des achats informatiques et des négociations financières ou encore de la rédaction des appels d'offre des marchés publics.

Recommandations sur les compétences

Dans le contexte d'une unité de recherche l'ASR, souvent isolé, doit faire preuve de compétences et de savoir-faire dans un grand nombre de domaines simplement pour répondre aux diverses missions qui lui sont confiées. Il est donc crucial qu'il dispose de moyens et méthodes pour maintenir, améliorer et faire évoluer ses connaissances. Nous proposons quatre voies complémentaires permettant à l'ASR de suivre les évolutions technologiques et de s'adapter à son contexte.

- **L'auto-formation** : expérimenter « sur le tas » est une manière de progresser et d'acquérir des connaissances et un savoir-faire nouveau. Une bonne pratique va consister à « formaliser » ces nouvelles connaissances en conservant la trace réutilisable de ses expérimentations (cf. chapitre sur la documentation). Se former sur internet, avec des articles ou avec des ouvrages de librairie est aussi une source importante d'acquisition et d'approfondissement de nos compétences.
- **La formation professionnelle (ex formation continue)** : trois niveaux sont à considérer en terme de formation : l'adaptation au poste, l'évolution du métier et l'acquisition de nouvelles compétences. Nos tutelles disposent de structures de formation financées annuellement et la plupart du temps d'un service de Formation Permanente avec des conseillers relayés par des correspondants dans les laboratoires ou services. Il est nécessaire que l'ASR définisse ses besoins de formation chaque année (le cadre du PFU, s'il existe dans l'unité, est adapté à cela).
- **La veille technologique** : elle permet de se faire une idée des évolutions en cours dans son domaine et d'être en mesure d'anticiper pour proposer des modifications d'architecture informatique et réseau au sein de l'unité. Plusieurs méthodes complémentaires sont accessibles : s'abonner à des revues spécialisées, à des lettres de « news » techniques, assister à des séminaires proposés, par exemple, par les constructeurs ou les fournisseurs, participer à des congrès techniques nationaux JRES (http://www.jres.org) ou salons techniques, etc.
- **Les relations de métier** : l'ASR souvent isolé dans son unité ne l'est certes pas à l'échelle régionale ou nationale. Trouver

des conseils auprès de collègues permet de capitaliser un savoir-faire collectif. Parmi ces moyens, de nombreuses listes thématiques de messagerie ont été créées par la communauté. Les communications entre collègues ASR permettent le partage des connaissances et la capitalisation globale des savoir-faire. Parmi ces moyens, les « Réseaux de métiers » fonctionnant en région permettent des rencontres et proposent des formations sur des thèmes d'actualité. On trouvera sur le site de RESINFO (http://www.resinfo.org) les coordonnées de ces réseaux de terrain.

Conclusion

L'ambition de ce Guide est de fournir aux ASR en poste, mais aussi aux nouveaux entrants, quelques principes de base dans l'organisation de leur travail quotidien et de formaliser un ensemble de comportements qui font consensus dans la communauté des ASR. Comme M. Jourdain faisait de la prose sans le savoir, chacun de nous n'a, bien sûr, pas attendu la sortie des normes ISO, sur lesquelles nous nous appuyons dans ce Guide, pour mettre en place certains principes d'organisation de service, ainsi que des outils afin d'assurer le bon fonctionnement et la sécurité de nos infrastructures informatiques.

Cependant nous avons utilisé les normes ISO dans l'optique générale de donner un cadre référentiel à nos pratiques de terrain, ce qui permet de rendre compte de la meilleure façon de nos activités et contribue, à terme, à améliorer la qualité du service.

On pourrait penser que ces recommandations/pratiques de base concernant la formation, la documentation sont évidentes dans le cadre de notre métier, cependant il apparaît qu'elles ne sont pas toujours suivies ni acceptées par nombre d'ASR. En effet on ne prend pas toujours forcément le temps de documenter nos actions, les changements apportés au S.I., ni de gérer de manière un peu plus rationnelle le temps consacré à nos diverses tâches.

Nous pensons qu'un guide des bonnes pratiques organisationnelles du métier d'ASR peut être un document adapté pour rappeler ces nécessités en termes de pratiques de base du métier. D'autre part, les méthodes de gestion du temps que nous décrivons sont relativement peu connues ou peu suivies dans notre métier et adaptées à nos besoins et personnalités, elles peuvent être des outils de perfectionnement et de confort.

Nous insistons aussi sur le fait que le fil conducteur de l'ensemble des méthodes abordées est « l'écrit ». En effet, que ce soit pour la formalisation des procédures, la documentation, la communication, les rapports d'activités, la gestion de parc, la configuration des équipements, la gestion des traces..., il est indispensable de consigner par écrit ces informations afin qu'elles soient, confidentielles ou non, transmissibles ou consultables et si besoin partagées.

Ce Guide est une base qui se veut évolutive, nul doute que nous aurons besoin d'y revenir pour le modifier et le faire évoluer dans les années qui viennent, en intégrant par exemple les pratiques liées aux économies d'énergie dans l'utilisation de l'outil informatique.

»»» suite de l'Éditorial, page 1

au travers des premières expérimentations déjà réalisées au CNRS, que sa maîtrise implique une bonne compréhension des objectifs poursuivis par le management des risques sur le système d'information : prévention des risques très en amont des phases de développement des projets, identification et évaluation des risques en production, élaboration de plans d'actions en réduction et contrôle des risques, communication et reporting à la Direction.

Gageons que la mise en œuvre de ces démarches de progrès contribue, dès aujourd'hui, à renforcer les ASR dans le cercle vertueux d'un progrès collectif capitalisant sur des succès, parfois simples mais rapides.

Jacques.Lavielle[à]cnrs-dir. fr

La fédération du réseau métier d'ASR RESINFO et les réseaux régionaux ou thématiques qui le constituent sont une des possibilités pour partager nos expériences. Cette nécessité d'échange de pratique est une « piste » importante à retenir pour donner une suite à ce guide, le maintenir à jour et pouvoir répondre d'une manière efficace à nos missions. Le Guide des Bonnes Pratiques [1] est disponible sur le site web de RESINFO (http://www.resinfo.cnrs.fr/spip.php?article41).

Il revient donc à chacun de nous de l'enrichir et de le faire évoluer par l'apport de nos « bonnes pratiques » quotidiennes mises à l'épreuve des différentes situations d'exercice de notre métier. Toute participation est, à cet effet, la bienvenue ! ■

Contact pour le groupe des auteurs :
marie.david[à]dr11.cnrs. fr

Bibliographie et Références

[1] Guide de Bonnes Pratiques organisationnelles pour les Administrateurs Systèmes et Réseaux dans les unités de recherche : http://www.resinfo.cnrs.fr/spip.php?article41
[2] ITIL : Information Technology Infrastructure Library - http://www.itilfrance.com/
[3] ISO 20000-1 Technologies de l'information – Part 1 - Gestion des services & Part 2 – Code of practice http://www.iso.org/
[4] ISO 27001 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences - http://www.iso.org/
[5] ISO 27002 : Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la gestion de la sécurité de l'information – http://www.iso.org/
[6] PSSI CNRS : http://www.sg.cnrs.fr/fsd/securite-systemes/documentations_pdf/securite_systemes/PSSI-V1.pdf
[7] EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité - http://www.ssi.gouv.fr/site_article45.html
[8] S'organiser pour réussir : la méthode GTD (Getting Things Done), David Allen, Leduc.s Editions, 2008
[9] Admin'sys Gérer son temps, Thomas Limoncelli, Eyrolles, 2006
[10] Question de temps, François Délivré, InterEditions, 2007

SÉCURITÉ DE L'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 cedex 16
Tél. : 01 44 96 41 88
Courriel : joseph.illand[à]cnrs-dir. fr
http://www.sg.cnrs.fr/fsd

Rédacteur en chef :
Robert Longeon
Chargé de mission SSI du CNRS
Courriel : robert.longeon[à]cnrs-dir. fr

Impression : Bialec, Nancy (France) - D.L. n° 73287
ISSN 1257-8819