Normes et référentiels : suivez les guides !

Compte-rendu de la rencontre « Autour d'un verre » du 14 janvier 2010 avec les cinq auteurs des derniers guides relatifs aux normes et référentiels

Alain Guercio

Au moment même où la nouvelle édition du « Guide des certifications SI » d'ADELI (Martine Otter, Jacqueline Sidi, Laurent Hanaud) sortait chez Dunod, un autre ouvrage sur ce thème était publié par Eyrolles : « Le Guide commenté des normes et référentiels » de Gilles Teneau et Jean-Guy Ahanda.
Cette première rencontre « Autour d'un verre » de l'année 2010 était donc l'occasion d'une aimable confrontation des points de vue sur les normes, les référentiels et les certifications.

L'élaboration d'un guide requiert une collecte, un approfondissement et un tri d'une somme considérable d'informations.
C'est aussi l'occasion de prendre du recul sur ce fonds documentaire et – pourquoi pas ? – d'essayer de se projeter dans l'avenir à partir des évolutions constatées.

C'est ce qu'ont fait les cinq auteurs de nos deux guides.

Les 3 périodes

Selon Laurent Hanaud, l'évolution de la qualité des systèmes d'information passe par trois périodes successives : la période de la technique, la période de la facilitation, la période de la régulation.
La période de la technique arrive aujourd'hui à un haut niveau de maturité.
La période de la facilitation fait encore l'actualité.
Les conditions d'émergence de la période de la régulation se mettent en place : celle-ci va rapidement imposer ses vues, et ses contraintes.

La période de la « technique » ou de l'efficacité

Par définition « être efficace », c'est atteindre le but. Avant de parler de qualité, il faut savoir faire.
La période de la « technique » est donc la première, celle où l'on cherche à faire, et à mieux faire.

C'est la période des méthodes : méthodes de conception, méthodes de réalisation, méthodes de conduite de projet…
Les membres d'ADELI connaissent bien cette période de la « technique » puisque le but initial de notre association était de promouvoir la « Logique Informatique » objet des travaux de Jean-Dominique Warnier.
Comme dans l'industrie, la qualité des SI a cherché d'abord à faire reconnaître la qualité du produit livré par l'informatique : le logiciel.

Lorsqu'on sait faire – du moins suffisamment pour s'engager - l'objectif de faire reconnaître la qualité fournie s'impose : c'est le principe de la certification.
D'énorme progrès ont été réalisés sur la qualité du logiciel et sa mesure, mais sont restés insuffisants. Il a donc fallu faire certifier des systèmes, des organisations… comme d'ailleurs dans les « métiers » où la certification ISO 9001 se généralisait.

La période de la « facilitation » ou de la reconnaissance

La période de la facilitation cible la ressource - et notamment l'organisation - qui va faire, et non plus le produit qui est en le résultat.
Une certification exige trois composantes :

1. un référentiel commun ;
2. un modèle d'évaluation ;
3. un dispositif de reconnaissance.

Les premières certifications d'organisations informatiques s'appuyaient naturellement sur l'ISO 9001.
Pour maîtriser les difficultés rencontrées dans ce monde qui était bien loin du modèle industriel, l'idée d'une approche par palier a émergé. Des modèles comme CMMI ont vu le nombre de leurs adeptes croître fortement.

Face à la complexité des organisations et des situations de travail, les individus restent importants. La certification de personne s'est développée d'abord pour les situations complexes comme les projets : PMI, Afitep, Prince 2… ou encore ITIL qui a fait sa percée spectaculaire dans le monde de la production informatique où - de manière surprenante - il n'y avait rien.

Aujourd'hui, la tendance est au panachage. Panachage entre les domaines différents de certification : la qualité, le développement, la sécurité, le management de projet(s)…
Gageons que la production s'invitera bientôt.

Panachage aussi entre les certifications de « système » organisationnel et d'individu : l'entreprise sera conforme ISO 20000 et le personnel sera certifié ITIL.
Panachage entre différentes entités juridiques, comme dans le cadre d'eSCM qui balise la relation client-fournisseur.
Panachage entre les référentiels informatiques et les référentiels « métier » comme dans le secteur de la Banque et de la Finance, précurseur de la troisième vague de certification.

La période de la régulation, ou de la conformité

Certains signes ne trompent pas : parmi les populations certifiées dans des domaines informatiques (ITIL, CMMI, Prince 2…) on rencontre de plus en plus d'avocats.

Il est vrai que les vagues d'externalisations massives des entreprises génèrent des contrats extrêmement pointus. Par exemple, il faut cadrer toutes les situations où le « métier » aura besoin d'un support, et même parfois penser à l'escalade : au support du support…

Mais une autre vague, bien plus haute, arrive.
En France, elle prend la forme d'un acronyme à trois lettres : LSF. La Loi de Sécurité Financière a été votée en 2003 et a d'abord transformé la COB (Commission des Opérations de Bourse) en AMF (Autorité des Marchés Financiers).
Cette transformation s'est accompagnée d'un cadre de référence transformant les « bonnes pratiques » de gouvernance d'entreprise en textes législatifs.

Contrairement à la démarche américaine (la SOX : Sarbanes Oxley Act), la LSF ne s'applique pas qu'aux entreprises cotées en Bourse et ne se limite pas à la transparence des données comptables.
La LSF impose de mettre en place un contrôle interne à la mesure des risques de toute nature encourus par l'entreprise.
Son guide d'application, édité en 2005, intègre dans le périmètre du contrôle interne tous les processus « amont » par rapport à la production des données comptables.
On voit bien que c'est l'ensemble du système d'information qui est impacté, et se doit donc d'être auditable. Ce qui est nouveau pour les DSI, c'est que les processus de maîtrise du SI en font partie.

Imaginez que la production ait adopté ITIL : le processus de gestion de configuration et celui de gestion des biens (« assets ») impactent la comptabilité.

Par exemple, il faut savoir si la période d'amortissement démarre à la date de livraison ou à celle de mise en service.
Quand on avait un mainframe, on le savait. Quand on a des dizaines de « blades » en rack, c'est plus subtil…

Vous avez dit NRMM ?

L'objectif du « Guide commenté des normes et référentiels » est de pouvoir réunir dans un même ouvrage quatre grands thèmes qui sont les normes, les référentiels, les méthodes et les modèles ainsi que le savoir-faire pour les utiliser à bon escient au sein de l'entreprise.

Les auteurs – les hôtes d'ADELI et conférenciers du jour - sont Gilles Teneau, responsable du pôle ITIL au sein de SOGETI, et Jean-Guy Ahanda, consultant en direction de projet et qui possède également une solide expérience dans l'industrie.

La collecte

Cet ouvrage est complémentaire au « Guide des certifications SI » car il ne se limite ni aux référentiels de certification, ni au monde des SI. Néanmoins, si ce guide fait aussi une place à l'industrie et aux services, il est vrai qu'un certain nombre de NRMM (Normes, Référentiels, Méthodes, Modèles) se rencontrent dans l'univers de l'informatique.

La première étape de construction de l'ouvrage est la collecte. Alors qu'ils maîtrisaient déjà les « outils du consultant » et ceux du monde de la qualité, les auteurs ont quand même surpris de la profusion !
Il a donc fallu faire des choix.
Par exemple, ils se sont limités aux NRMM « génériques », par opposition à ceux d'un secteur particulier comme l'alimentaire ou l'automobile.

Ils n'ont pas retenu de NRMM trop « informatiques », comme les méthodes agiles (« et pourtant, je m'appelle Gilles … alors les méthodes à Gilles » … ;-)

Et puis, ils se sont aperçu que certains NRMM étaient partout : le PDCA, les cartes mentales, le RACI…

La classification

Devant la confusion des termes, le premier travail a donc été de clarifier ce catalogue.

Les normes (N), on connaît. Elles suivent des procédures formelles d'élaboration et de diffusion, gérées en France par l'AFNOR.

Les référentiels (R) peuvent recenser des « bonnes pratiques » ou/et formaliser des « exigences », surtout dans le cadre d'une certification. Un référentiel est alors bien identifié et géré en version, comme une norme.

Le terme de méthode (M) a été réservé à des outils assez sophistiqués, alors que celui de modèle (M) est utilisé pour les outils simples.

On reconnait volontiers que ces concepts de NRMM sont encore un peu flous, et il arrive encore à nos auteurs et à leur éditeur de commettre des lapsus. Mais le premier pas, et les auteurs sont ouverts à toutes propositions complémentaires.

Cette classification va devenir indispensable car l'articulation de plusieurs NRMM sur un même périmètre devient une pratique courante, et à juste titre.
Par exemple, quand une organisation adopte ITIL (R), il n'est pas rare qu'elle s'intéresse aussi à la sécurité (via la Norme ISO 27000).
Comme le préconise l'ItSMF, elle va peut-être élaborer un BSC (Balanced Score Card) qui est une méthode (M).
Pendant cette étude, elle va mettre en œuvre le modèle (M) SWOT : la fameuse matrice Strengths (forces), Weaknesses (faiblesses), Opportunities (opportunités), Threats (menaces).

Les évolutions

Au fur et à mesure que les organisations adoptent ces NRMM, elles comprennent l'intérêt des approches d'amélioration continue.
L'industrie est très en avance dans ce domaine qu'on appelle le KAIZEN.
Les approches LEAN (élimination du Muda) structurent la « chasse au Gaspi ».
Le TQM – pour Total Quality Management – est une démarche d'excellence, au même titre que l'EFQM.
Les modèles comme le PDCA, les 5S – pour Seire (Trier), Seiton (Ranger), Seiso (Nettoyer), Seiketsu (conserver en ordre), Shitsuke (formaliser et impliquer) – ou les 5P (les « 5 Pourquoi » pour chercher les causes)… sont de plus en plus mobilisés dans les entreprises, et notamment hors des ateliers de l'industrie : dans tous le secteur des services.

L'évolution majeure que l'on constate provient de l'importance accordée aux individus et à leur participation dans l'application des NRMM.
Il est heureux que la norme ISO 26000 sur la responsabilité sociétale des entreprises (RSE) arrive bientôt à maturité.

Questions-Réponses-Débats

Processus d'élaboration des lois et des normes

Il est vrai que parfois, le processus d'élaboration juridique oublie que les normes existent, et qu'elles peuvent déjà être imposées.

Aux États-Unis, le FISMA - Federal Information Security Management Act – est une loi qui vise à sécuriser les biens et les informations.
Elle s'applique d'abord aux administrations.
Elle s'étendra rapidement à l'ensemble de leurs fournisseurs. Elle deviendra ensuite une référence… à gérer en cohérence avec l'ISO 27000 (sécurité) !

La multiplicité des contraintes qui s'imposent aux entreprises, multinationales notamment, est une facette du problème. « Êtes-vous en règle avec la loi ? » est la première question des audits de conformité.
Bien sûr, il faudra savoir répondre.

Prolifération versus Utilisation

Parmi la multitude des NRMM existantes, beaucoup présentent quelques décennies d'existence : 5S, 5P, PDCA, RACI…
En parle-t-on parce que c'est la mode ?
Est-ce rassurant ?
Les applique-t-on vraiment ?

Que les organisations les appliquent à la lettre n'est pas très important. L'essentiel est qu'elles en retiennent une « vision », une ligne directrice.
Par exemple, le CobIT est à l'origine un outil pour les auditeurs, on en fait un référentiel de gouvernance.
L'eSCM donne une vision sur le positionnement relatif d'un client et de son fournisseur (et inversement).

ITIL certifie des individus, l'ISO 20000 certifie des organisations. Comme cette dernière, ITIL v2 représente l'usine, la chaîne de production informatique. Par contre, ITIL v3 est orienté « service », c'est plus compliqué. Toutes ces approches sont complémentaires.

Parfois, il est préférable pour les spécialistes de ne pas trop parler de tout çà, de ne pas les mettre en avant. Ils risquent de passer pour des théoriciens, des « extra-terrestres ».
Surtout en cette période de crise où il est préférable de rester concret. On lance donc des actions en s'inspirant de tel NRMM et on obtient des résultats. En s'appuyant sur des réussites, on peut faire de la pédagogie et présenter des explications.

Le vrai danger vient souvent de l'intérieur. Comme l'acheteur qui veut formaliser toutes les « exigences » grâce à un référentiel (ou plusieurs !). Inversement, comme le commercial qui s'engage un peu vite sur les certificats obtenus, ou – probablement - ceux en cours d'obtention…
On aura progressé quand on aura démystifié la certification : c'est-à-dire quand on s'interrogera d'abord sur le périmètre réellement certifié.
Quand la combinaison d'un « technicien de surface » est barrée de la mention « certifié ISO 9001 » : de quoi parle-t-on ?

Le business des certifications

Les certifications font effectivement l'objet d'un marché : les référentiels, les formations, les audits de certification et de renouvellement.
Il peut même y avoir une certaine concurrence : sur le management de projet, il y ceux qui sont PMI et ceux qui sont Prince 2, ou autre.
Sur la production des services, il y a ITIL mais CMMI-SVC (Services) arrive à grands pas.
Il y a une offre de NRMM reconnus, mais il y a aussi une demande : pour certains, être certifié ITIL (3 jours de formation et un QCM), c'est mieux que d'avoir réussi son baccalauréat !

Quelles sont les motivations des organisations ?

Les entreprises veulent des guides pour déployer les processus. Elles cherchent bien sûr des « Quick Win » et du retour sur investissement, mais elles sont en recherche d'une plus grande valeur.
On ne parle pas seulement de la valeur au sens de la création de valeur de Porter. On parle aussi de la valeur sociale.
Souvenez-vous du rapport d'Antoine Riboud « Modernisation, mode l'emploi ». En 1987, il écrivait : « Avec les nouvelles technologies, ce sont les hommes qui feront la différence ».

Et n'oublions pas la 3ème vague qui arrive à grands pas ! Actuellement, les sujets de RSE et LSF sont encore une affaire de spécialistes. Demain, ce réglementaire devra être intégré aux processus de l'entreprise.

Aujourd'hui, les règlements du CRBF (Comité de Réglementation Bancaire et Financière) sont élaborés entre professionnels de la banque et de la finance. Demain, la LSF s'appliquera à toutes les sociétés anonymes, cotées ou pas.

Contrairement à la SOX aux États-Unis, la LSF exige de prendre en compte les processus « amont ». En bref, le périmètre concerne quasiment toute l'entreprise, et la loi exige de clarifier les modalités d'audit des fournisseurs. Imaginez l'impact dans le secteur pharmaceutique où 70% des budgets passent en sous-traitance !

Aujourd'hui, on parle d'exigences de référentiel mais la qualité n'est pas toujours au rendez-vous ; on s'en arrange, et c'est parfois « un peu n'importe quoi ».
Demain, on devra être certifié et c'est la responsabilité juridique de l'entreprise qui sera engagée. Gageons que les acheteurs vont monter en poids et en compétence.

L'élaboration des normes internationales (ISO)

160 pays travaillent sur les normes ISO. Néanmoins, la moitié de ces pays ne participe à aucun groupe de travail, et notamment en Afrique. Plus de 25% des groupes de travail sont menés par les délégations de pays développés.

Les normes sont souvent faites par et pour les économies développées.
Par certains côtés, ce peut être une forme de protectionnisme. On arrive parfois à des aberrations où les pays en voie de développement ne peuvent commercer avec leurs voisins à cause des normes internationales qu'ils ne peuvent pas appliquer, et qui n'ont pas toujours d'intérêt dans leur contexte …

Il n'est pas sûr que la norme ISO 26000 (Responsabilité Sociale des Entreprises) atténue ce phénomène.
Bien que l'on prévoie déjà des mesures transitoires « de passage » pour certaines régions.
La normalisation représente un enjeu. Par exemple, la Chine intervient sur la norme ISO 26000. Cette norme défend les droits de l'Homme, mais elle n'est pas applicable aux États … ouf !
Il est admis que des domaines comme la santé ou l'alimentation sont particuliers.
Le risque Zéro n'existe pas, et les pratiques des États sont différentes. Par exemple, en cas d'incident aux USA, la FDA (Food and Drug Administration) n'hésite pas à bloquer l'usine d'abord, pour enquêter ensuite. Une pratique qui incite à la vigilance.

L'empilement des normes : plus qu'hier et moins que demain

Appliquer successivement plusieurs normes ou référentiels sur le même domaine et sur une même organisation est une pratique encore beaucoup trop récente.
On ne peut pas encore parler de capitalisation. Néanmoins, on peut constater que l'effort à produire pour adopter un référentiel est bien moindre quand l'organisation en connait déjà un autre.

Il existe un domaine assez mûr sur ce point : le couplage des audits QSE (Qualité, Sécurité, Environnement).
Les normes ISO 9001 (Qualité) et ISO 14001 (Environnement) ont été construites pour s'intégrer ensemble. Cela apporte de la simplification, de la cohérence et donc de la compréhension : elles obligent à revenir sur le métier.
Le plus difficile semble toutefois de trouver de bons auditeurs.

On ne doit pas confondre ce phénomène avec l'utilisation d'une boîte à outils. La majeure partie des NRMM sont des outils qu'un bon « bricoleur des organisations » doit savoir mettre en œuvre.
Peut-on envisager qu'un bricoleur génial puisse « normer » une organisation ? Si on veut tout « normer » il faudra aussi distribuer des certificats de bricolage !

Les audits de certification forment aussi un business. Les auditeurs savent qu'ils doivent faire des remarques et soulever des non-conformités, mais pas trop non plus … Ils reviendront l'année prochaine et valoriseront les efforts accomplis par le client.

La logique de l'audit interne n'est pas la même que celle de l'audit externe.
L'obtention du « papier » ne doit pas être confondue avec la véritable démarche qualité. Il ne faut pas perdre de vue qu'il faut surtout valoriser ce que l'organisation fait de bien.

Les normes doivent aider les entreprises à progresser, même si les exigences sont parfois difficiles à atteindre. Par exemple, l'ISO 20000 génère de fortes exigences en matière de gestion de configuration. C'est très compliqué à mettre en œuvre, mais on doit mesurer les progrès.

La norme ISO 9001 est probablement un des référentiels les plus aboutis, notamment depuis la version 2000.
Beaucoup d'autres s'y appuient avec pertinence.
À l'origine, son objectif était de donner confiance au client. On parle bien d'assurance qualité.

Avec l'empilement d'autres normes, on ne comprend plus rien. Les experts, eux-mêmes, s'y perdent. Alors les opérationnels … En termes de résultat, on obtient quoi : la défiance.

« Trop de normes tue les normes ».

L'ISO 26000 (RSE) frôle ce risque.
Elle ferait déjà 300 pages, et ce serait surtout de la philosophie.
Elle sera invendable aux décideurs, surtout en PME.
Heureusement, car on ne voit pas non plus comment l'auditer…▲

alain.guercio@e-media-management.com