# eSCM et SAS 70 : l'assurance vie du client

LIVRE BLANC


*A la mémoire de François RENAULT*

# eSCM et SAS 70 : l'assurance vie du client

Auteurs :

**Haissam Abdul-Wali**, Manager Sourcing, Logica Business Consulting.

**Eric Baussand**, Président, eSourcing partners.

**Thomas Estève**, Directeur Consulting, PWC.

**Marc Coen**, Directeur de mission, Timspirit.

**Marie-Noëlle Gibon**, Directeur de l'Innovation Technologique, des Systèmes d'Information et du Développement, Docapost.

**Mourad Kacir**, Responsable Audit SI Courrier, La Poste.

**Olivier Mauduit**, Associé, Deloitte.

**Laurence Molinier**, Senior Manager, Deloitte.

**Hubert Tournier**, Adjoint DOSI, Directeur du conseil, Groupement des Mousquetaires.

**Philippe Trouchaud**, Associé Consulting, PWC, Vice président de l'AFAI.

**Stéphane Wojewoda**, Consultant DOSI, Groupement des Mousquetaires.

**Serge Yablonsky**, Associé, Moore Stephens SYC, Président d'honneur de l'AFAI.

Publié par :

**l'Ae-SCM**
Association (loi de 1901) pour la promotion des bonnes pratiques de sourcing.
L'association Ae-SCM, qui regroupe clients, fournisseurs et sociétés de conseil a deux objectifs : faire connaître et faire adopter le référentiel eSCM, référentiel des bonnes pratiques du sourcing, élaboré par l'université américaine Carnegie Mellon. Le référentiel couvre l'ensemble des pratiques du cycle de vie des prestations externalisées et, pour en faciliter l'utilisation au sein des entreprises, les membres de l'Ae-SCM développent la boîte à outils nécessaire à sa mise en œuvre.

25, rue du Maréchal Foch
78000 Versailles, France.
www.ae-scm.com (contact : ae-scm@laposte.net)

et par :

**l'AFAI**
Association Française de l'Audit et du Conseil Informatiques
L'AFAI est le chapitre français de l'ISACA, organisation internationale qui regroupe 95 000 membres dans 75 pays. L'association rassemble plus de 800 professionnels autour des problématiques transversales liées à la gouvernance, au risque, à l'audit et la sécurité des systèmes d'information, ainsi qu'à la diffusion des meilleures pratiques associées. Elle a également une activité de formation tournée notamment vers la certification professionnelle. Sa spécificité : croiser les approches managériales, RH, sociologiques et juridiques.
164 bis, avenue Charles de Gaulle
92200 Neuilly-sur-Seine, France.
www.afai.fr

Créé et édité en avril 2011. Dépôt légal, avril 2011

# Sommaire


| | |
|---|---|
| **REMERCIEMENTS** | **6** |
| **PREFACE DU CIGREF** | **7** |
| **PREFACE DE L'AFAI** | **9** |
| **LE LIVRE BLANC EN QUELQUES LIGNES** | **10** |
| **ENJEUX ET PERSPECTIVES** | **12** |
| **MAITRISER LE SOURCING IT AVEC SAS 70 ET ESCM** | **14** |
| **RETOURS D'EXPERIENCE** | **15** |
| **CONCLUSION** | **34** |
| **ANNEXE A : APERÇU DU REFERENTIEL ESCM** | **35** |
| **ANNEXE B : APERÇU DU STANDARD SAS 70 ET DE LA NORME ISAE 3402** | **38** |
| **ANNEXE C : VUE D'ENSEMBLE ET COMPLEMENTARITE ESCM ET SAS 70** | **42** |
| **ANNEXE D : EXEMPLE DE LETTRE D'OPINION D'UN RAPPORT SAS 70** | **47** |
| **ANNEXE E : COBIT, ITIL, CMMI** | **49** |
| **GLOSSAIRE** | **52** |
| **REFERENCES ET BIBLIOGRAPHIE** | **54** |
| **WEBOGRAPHIE** | **55** |

## Remerciements

L'Ae-SCM et l'AFAI remercient pour leur aimable concours les personnes qui ont apporté leur témoignage et leur retour d'expérience publiés dans cet ouvrage :

**Jean-Pierre AGAZZI**, Associé, Commissaire aux Comptes, Responsable Global Accounting Advisory Services - Deloitte & Associés.

**Christian BARANOWSKI**, Responsable France de l'ensemble des démarches SAS 70 et Sécurité - Capgemini Outsourcing Services France.

**Christine BERGE**, Chef de projet Direction achat, Sanofi-Aventis.

**Michel DELATTRE**, Directeur des Systèmes d'Information du Groupe La Poste, La Poste.

**Sean ENNOR**, Head of Service Delivery, HR Access Employer Services.

**Savine GUILLEMIN**, Responsable Qualité SI, Sanofi-Aventis.

**Denis LARTIGUE**, Responsable du Contrôle Interne SI, Sanofi-Aventis.

**Franck MAHÉ**, Directeur de la sécurité, ADP.

**Laurent STRICHER**, DGA Systèmes d'Information / Secrétaire Général, Pôle Emploi.

**Daniel URBANI**, Directeur Général Adjoint Systèmes d'Information, Pôle Emploi.

## Préface du CIGREF

Dans un contexte économique incertain, les Directions des Systèmes d'Information (DSI) sont fortement sollicitées pour être plus efficientes. Les attentes des métiers sont claires : services avec qualité mesurée, respect des engagements, juste utilisation de ressources en fonction des objectifs fixés.

Cette démarche d'excellence permanente pousse les DSI à étudier toutes les opportunités pour assembler les composants technologiques et organisationnels qui offriront le meilleur équilibre d'ensemble. Les partenariats avec les sociétés de services trouvent de plus en plus souvent leur place dans les réponses des DSI.

L'externalisation croît sous l'effet conjugué de l'évolution radicale des offres - portée par la vague du cloud computing - et de la maturité croissante des DSI dans la relation qui les unit avec leurs prestataires de services.

Au-delà de ses aspects médiatiques et de ses acronymes barbares (IaaS, Saas, PaaS, Taas, etc…), le cloud computing propose des services « prêts » à l'emploi. Les phases de mise en œuvre sont raccourcies et les ressources engagées plus variables : le client ne paye que ce qu'il consomme. L'attractivité de ce type d'offre est indéniable pour les entreprises qui font face à des exigences de flexibilité et de productivité toujours plus pressantes.

Mais le service rendu doit être conforme aux attentes et aux engagements. La DSI doit être en mesure de fournir un support sans couture aux métiers. L'intégration des solutions internes et externes doit se faire dans un même continuum. La performance globale du SI doit être maîtrisée quelque soit l'origine des ingrédients qui la compose.

La relation entre tous les acteurs de la chaîne de services devient critique. Il faut dépasser le simple rapport client-fournisseur. Le respect des responsabilités respectives est le minimum requis. Il doit être complété par une solidarité opérationnelle qui le vrai signe de la maturité des acteurs et de leurs relations. Et c'est bien cette maturité qui représente le facteur clé de succès et donc l'objectif commun. La confiance réciproque entre les parties prenantes se construit sur des faits et se consolide dans les pratiques de la vie quotidienne.

Dans ce contexte, le référentiel eSCM est le précieux guide d'une relation réussie. Sa mise en œuvre progressive, depuis maintenant deux ans, au sein des DSI et avec leurs prestataires de service, atteste de la maturité croissante des parties prenantes. Comme tout référentiel, eSCM est un code de bonnes pratiques. Il délivre à ceux qui l'utilisent un véritable permis de piloter une offre conjointe de services, avec la maitrise nécessaire pour éviter les sorties de route, même quant les virages sont inattendus !

L'utilisation d'eSCM par le prestataire est pour la DSI un facteur essentiel de réduction du risque propre à la sous-traitance. Comment obtenir une assurance raisonnable que les prestations ne vont pas dériver et que la performance sera bien au rendez vous ? Comment vérifier que le niveau de contrôle interne des services du prestataire offre les garanties nécessaires? Comment prévenir plutôt que guérir ? Comment s'accorder sur des pratiques régulières de vérification ?

Le cadre eSCM offre aux acteurs un premier ensemble de réponses à ces questions. Le partage d'un même langage et la fédération autour d'une trentaine de pratiques établies sont les bases indispensables d'un dialogue et d'une cogestion réussis.

Ces réponses sont utilement complétées par la norme d'audit SAS 70. Elle permet aux DSI d'obtenir un engagement du prestataire sur ses pratiques de gestion de risque et les mesures de contrôle interne associées. La nécessité de produire un rapport SAS 70, qui peut être une obligation selon certaines réglementations financières, représente une évolution importante pour les acteurs de services.

La combinaison du référentiel eSCM et de l'application de la norme d'audit SAS70 représente une avancée considérable pour les DSI et leurs partenaires de services. Ils créent ainsi un nouvel espace de confiance, consolidant les pratiques de sourcing et de contrôle interne, et favorisant la cogestion maitrisée d'un service vers le client, le métier de l'entreprise.

Au delà d'un partenariat réussi, l'enjeu est bien la performance et la compétitivité de nos entreprises en termes d'excellence opérationnelle et, de plus en plus, d'innovation.

Je suis persuadé que cette contribution sera profitable à tous. Elle renforcera le rôle clé joué par SAS 70 et eSCM dans la gouvernance de nos entreprises.

Bruno MENARD
Président du CIGREF
Vice Pt SI Sanofi-Aventis

## Préface de l'AFAI

La confiance est aujourd'hui plus que jamais la première qualité recherchée dans les relations entre les personnes, les entreprises et les institutions. Notre profession a toujours eu un rôle majeur dans la chaîne de confiance, en accomplissant notamment des missions d'audit qui confortent les parties prenantes comme les tiers.

Dans le contexte de l'entreprise étendue et de l'externalisation de services, nos confrères américains ont mis au point une norme d'audit, SAS 70, pour qu'un seul auditeur puisse auditer pour le compte de tous les utilisateurs clients l'adéquation du contrôle interne mis en place par le prestataire et, par la même, s'assure de la continuité, au-delà des portes de l'entreprise, de la conformité aux bonnes pratiques de contrôle de ses processus externalisés chez son prestataire. Une norme similaire (ISAE 3402) a été définie au niveau international et sera transposée en France et dans le monde dès juin 2011.

Cette norme est indépendante du type de service fourni, ce qui lui ouvre un domaine d'application très vaste et très varié, en totale adéquation avec les différents acteurs de la chaîne de confiance.

Comme on le sait, un audit requiert deux référentiels : un premier référentiel méthodologique – c'est le cas de SAS 70 – et un référentiel de bonnes pratiques, spécifique au métier. Pour ce dernier, le choix du référentiel adapté au type de prestations, reconnu et exhaustif sans être hors sujet, est un exercice difficile. Par exemple, le référentiel général CobiT paraît s'imposer en matière de prestations informatiques, mais celui-ci est très large et couvre aussi bien l'organisation interne que les processus éventuellement externalisés. CobiT est exhaustif sur l'ensemble de la fonction informatique alors que l'externalisation ne couvre en général que des prestations de fourniture et d'exploitation de ressources.

C'est alors qu'eSCM révèle tout son intérêt pour l'auditeur, car il s'agit d'un référentiel international portant exclusivement sur l'externalisation de services informatiques et décrivant les bonnes pratiques tant du côté du prestataire que du côté de l'entreprise cliente, tout en couvrant l'intégralité du cycle de vie d'une externalisation de services.

L'utilisation conjointe de SAS 70 et d'eSCM offre aux auditeurs le cadre parfait pour évaluer la qualité des procédures et conforter ainsi la confiance indispensable aux bonnes relations entre les prestataires et les entreprises utilisatrices. Ce livre blanc, issu des travaux communs de l'Ae-SCM et de l'AFAI, explique de manière très concrète la manière d'utiliser ces référentiels et illustre par des exemples l'apport pour les entreprises. Nous sommes convaincus qu'il sera d'une grande utilité pour tous les professionnels de l'externalisation… ainsi que pour leurs commissaires aux comptes qui pourront aussi s'appuyer sur ces travaux d'audit externe pour leur analyse de risques et leur évaluation du contrôle interne de leurs clients !

François RENAULT
Président de l'AFAI

Serge YABLONSKY
Président d'honneur de l'AFAI
Expert comptable / Commissaire aux comptes

## Le livre blanc en quelques lignes

La place du SI comme vecteur de la performance de l'entreprise ne cesse de croitre. Délivrant des services stratégiques à forte valeur ajoutée ou optimisant les processus des entités pour les conduire vers l'excellence et faire que « tout marche tout le temps », le portefeuille des projets s'épaissit jour après jour et les moyens internes ne suffisent plus pour délivrer au moment opportun les services applicatifs attendus et créateurs de valeur.
L'industrie des services informatiques n'est pas en reste d'innovation dans ses offres, et le développement inéluctable d'un nouveau mode de consommation de ressources techniques et applicatives délivrées sous le nom générique d'offres Cloud Computing, est là pour témoigner du dynamisme du secteur.

Inéluctablement, l'externalisation progresse et les modalités de sourcing évoluent. Plus que jamais la relation Client-Fournisseur est au cœur des enjeux, et son développement vers un niveau de maturité croissant une garantie de succès pour les deux parties liées par un pacte mutuel de bonne fin.

Pour donner au Client les assurances nécessaires en ce sens, l'AFAI et l'Ae-SCM ont compris l'intérêt de marier le référentiel d'audit de l'externalisation qu'est SAS 70 avec le référentiel de gestion du sourcing qu'est eSCM, et ont souhaité travailler ensemble à la publication d'un premier Livre Blanc dédié à cette thématique .

Le premier chapitre de l'ouvrage donne une description des enjeux relatifs à l'externalisation des activités IT et fait un rapide rappel des contraintes, notamment réglementaires, et des risques auxquels sont soumises ces pratiques.

Le second chapitre expose en quoi les référentiels SAS 70 et eSCM sont de nature à aider les entreprises à maîtriser leur sourcing IT.

La vocation de ce Livre Blanc est bien de partager avec le lecteur les retours « terrain » de mise en place d'eSCM et de SAS 70, dans différents environnements, tant dans les entreprises Fournisseurs que dans les entreprises Clientes. En vertu de quoi, l'essentiel de l'ouvrage leur est consacré. Un troisième regard vient utilement compléter les expériences des entreprises : c'est celui de l'auditeur, tierce partie de confiance entre le Client et le Fournisseur.

Chaque retour d'expérience suit un plan en quatre points : présentation de l'entreprise, genèse de la mise en place des démarches SAS 70 et eSCM, état du déploiement des autres référentiels utilisés, bilan des expériences faites et perspectives à venir.

Trois fournisseurs, œuvrant dans le BPO et l'infogérance, se sont prêtés à l'exercice : HR Access, ADP et Capgemini. Ces entreprises sont toutes internationales, les deux premières sont américaines et la dernière est française.

HR Access et ADP délivrent des prestations de sous-traitance en matière de gestion des ressources humaines (paie, gestion du personnel) ; ADP est aussi implanté dans les services de gestion dédiés au monde des constructeurs et des gestionnaires automobiles. Capgemini intervient dans le domaine de l'infogérance (des infrastructures notamment) et du BPO.

Côté Client, trois entreprises, aux profils et aux domaines d'activité bien différents ont accepté de témoigner sur leur expérience : Pôle Emploi, née de la fusion en 2008 de l'Unedic et de l'ANPE, Sanofi-Aventis, groupe mondial de l'industrie pharmaceutique, le Groupe La Poste, entreprise multiservices devenue Société Anonyme en 2010. Toutes trois partagent en commun d'avoir été parmi les entreprises pionnières en France dans le déploiement de eSCM. Seule, Sanofi-Aventis a fait de SAS 70 une exigence interne bien que limitée encore à des fins de conformité.
Deloitte, enfin, qui apporte sa contribution en tant qu'auditeur, rappelle la double responsabilité des cabinets d'audit et dans l'élaboration des rapports SAS 70 et dans l'usage qu'ils en font dans l'exercice de leur profession.

Pour conclure, on évoquera la nécessité du partage de bonnes pratiques de contrôle interne entre les acteurs, afin d'assurer, par une meilleure gestion des risques, l'atteinte des objectifs fixés et dans une perspective d'avenir, la pérennité de nos entreprises.

Les Annexes doivent permettre à chaque lecteur d'approfondir ses connaissances sur les différents référentiels évoqués dans le corps du Livre Blanc et leurs complémentarités : eSCM, SAS 70 et ISAE 3402, COBIT, ITIL, CMMI.

Un glossaire des principaux termes, les références bibliographiques des documents à consulter ainsi qu'une webographie des sites dédiés à ces thématiques sont fournis à la fin de l'ouvrage.

## Enjeux et perspectives

L'évolution rapide des technologies de l'information a permis l'émergence de nouvelles offres de solutions de services informatiques allant jusqu'à l'externalisation de processus métier (BPO). Selon la plupart des études menées auprès des entreprises, les 3 risques majeurs du sourcing IT sont :

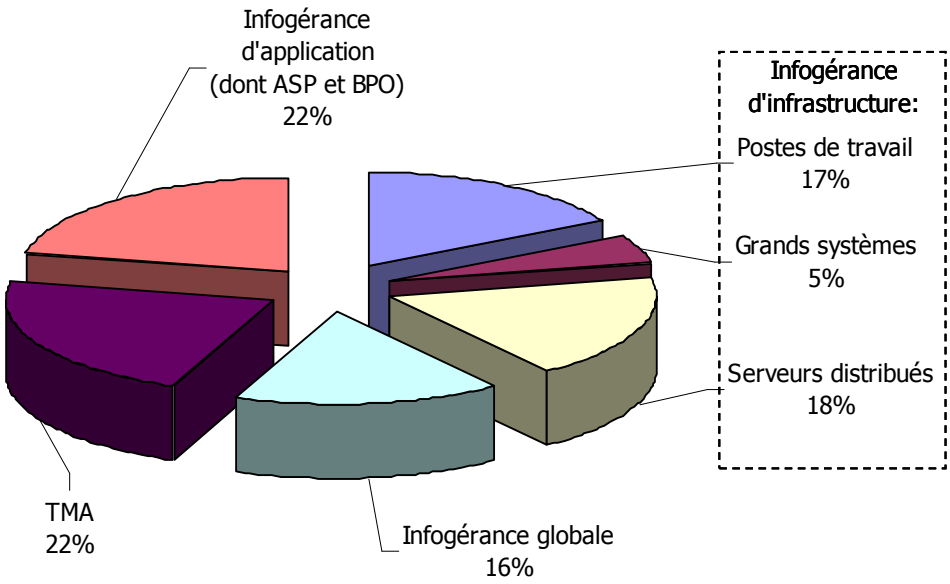
Des données confidentielles tombant entre les mains de la concurrence ;

- Des coûts d'externalisation plus importants que prévus ;
- Une érosion du savoir des ressources internes.

Selon d'autres études, 1/8 des contrats entre clients et fournisseurs de services aboutissent à des échecs en raison d'exigences non satisfaites.

A l'échelle européenne, la gestion défaillante de la relation client-fournisseur, couplée à l'absence de flexibilité durable dans les contrats d'outsourcing, représente un surcoût de 6,53 milliards d'euros par an. A l'échelle mondiale, les services des technologies de l'information, ont évolué de 6,4 % en croissance annuelle jusqu'en 2010 pour atteindre 855 milliards de dollars avec une croissance positive sur tous les segments du marché.

En France, le sourcing représente un marché de 8,64 milliards d'euros par an avec la répartition suivante [1] :




**Déclinaison du marché français de Sourcing IT**

A cette situation du marché de sourcing IT et des risques encourus viennent s'ajouter des contraintes liées au cadre légal et règlementaire. En effet, les services rendus par des tiers

[1] Pierre Audoin Consultants 2008

ayant un impact direct sur l'information financière ou sur les activités du client doivent faire l'objet de contrôles dans le respect de :

- La loi de sécurité financière pour les sociétés commerciales ;
- Le cadre de référence de l'Autorité des Marchés Financiers (AMF) publié en octobre 2010 ;
- La loi Sarbanes-Oxley pour les groupes cotés aux Etats-Unis.

Contrairement à la loi Sarbanes-Oxley, la loi de sécurité financière ne requiert pas à ce jour de rapport sur l'efficacité des contrôles mis en œuvre. Toutefois, l'AMF recommande aux émetteurs de rapports « d'entamer une démarche progressive d'évaluation leur permettant d'aboutir à une appréciation sur l'adéquation et l'efficacité de leurs procédures de contrôle interne ».

## Maîtriser le sourcing IT avec SAS 70 [2] et eSCM [3]

Les clients et les fournisseurs de services sont à la recherche de référentiels de bonnes pratiques et de standards d'évaluation visant la mise en place de relations durables de sourcing, la maîtrise des risques encourus et des réponses aux recommandations des autorités de tutelle que ce soit pour la loi de sécurité financière ou la loi Sarbanes-Oxley.

Concrètement, les clients et les fournisseurs de services cherchent des solutions pour :

- Améliorer l'efficacité du dispositif de contrôle des activités de sourcing IT ;
- Démontrer l'assurance raisonnable de la qualité du dispositif de contrôle interne mis en œuvre dans le cadre d'un contrat de sourcing IT tout en étant conforme au cadre légal et règlementaire.

De façon complémentaire et cohérente, le référentiel eSCM et la norme SAS 70 constituent une réponse à ces 2 préoccupations.

D'une part, le référentiel eSCM a été élaboré pour permettre aux clients et aux fournisseurs de services l'amélioration continue et la mise en place durable et bénéfique de relations de sourcing.

Ce référentiel regroupe un ensemble de bonnes pratiques de sourcing IT nécessaires à la réussite d'une relation de sourcing. Les fournisseurs de services tirent avantage d'eSCM pour améliorer leurs aptitudes en matière de :

- Gestion de la relation client-fournisseur ;
- Gestion des risques ;
- Pilotage de la performance ;
- Gestion de la connaissance et des ressources humaines ;
- Contractualisation, conception, déploiement et transfert du service ;
- Fourniture et réversibilité du service.

D'autre part, la norme SAS 70 fixe les standards d'évaluation du dispositif de contrôle interne d'un fournisseur de services et permet l'émission d'un rapport unique à destination des parties prenantes (régulateurs, clients, auditeurs des clients, prospects et audit interne du fournisseur de service).
En ce sens, le rapport type SAS 70 constitue :

- Une opinion indépendante et reconnue par la profession sur le niveau de maîtrise des activités de contrôle d'un fournisseur de services ;
- Une réponse au nombre croissant d'audits externes commandités par les clients ;
- Un élément discriminant et favorable au choix d'un fournisseur de services.

[2] Statement of Audit Standard n° 70
[3] eSourcing Capability Models

# Retours d'expérience

La mise en place d'eSCM et de SAS 70 ne doit pas être vue comme un exercice théorique mais plutôt comme une volonté affirmée de l'entreprise d'adresser et de piloter ses risques liés à l'externalisation de certaines de ses activités souvent clefs.

Dans ce cadre, l'expérience prend souvent le pas sur la théorie. Nous avons donc souhaité que certaines entreprises, et leurs auditeurs, puissent partager la manière dont elles ont appréhendé cette problématique et leur vision de l'apport effectif d'une telle approche.

## HR Access

### La personne interviewée

Sean ENNOR, Head of Service Delivery - HR Access Employer Services.

### HR Access en quelques mots

HR Access, leader des solutions de gestion des ressources humaines et d'externalisation, propose une gamme complète de services pour la gestion du personnel, la paie et la gestion des talents. HR Access est implanté dans 54 pays et permet aux entreprises de réduire leurs coûts et de gagner en efficacité.

HRa Employer Services est une gamme complète de solutions d'externalisation allant du Processing au Business Process Outsourcing, qui couvre la gestion administrative, la paie et la gestion des talents. La suite applicative HRa Suite 7, au cœur des solutions d'externalisation, regroupe toute l'expertise et l'innovation de HR Access depuis plus de 35 ans. Elle est déployée sur une plateforme propriétaire unique qui satisfait aux normes technologiques et sécuritaires les plus exigeantes. Des équipes professionnelles et expérimentées, supportent et guident les entreprises au quotidien pour assurer les meilleurs processus et pratiques métiers.

### SAS 70

HR Access Employer Services a lancé un projet de préparation à la certification SAS 70 en novembre 2008, couvrant les services RH et Paie délivrés en France et en Espagne et allant du « Processing » au « Business Process Outsourcing ».
Le rapport de Type I a été émis en juillet 2009 et le premier rapport de Type II en janvier 2010.

HR Access s'inscrit actuellement dans une dynamique récurrente, avec la publication d'un rapport annuel de Type II.

Les motivations principales de lancement du projet ont été les suivantes :

D'une part, le SAS 70 est reconnu sur le marché comme une preuve de l'assurance qualité des services offerts par un prestataire ;
D'autre part, pour certains des clients et prospects d'HR Access, la certification SAS 70 était une condition « sine qua non » pour l'externalisation de leurs services RH et Paie chez HR Access.

Ce projet stratégique figure parmi les principales priorités de l'entreprise ; il a bénéficié du soutien de la Direction Générale d'HR Access et d'importants investissements ont été effectués. HR Access a mis en place une équipe interne dédiée avec un chef de projet désigné et deux interlocuteurs en France et en Espagne. Il est vrai qu'à l'époque l'entreprise ne maîtrisait pas la norme SAS 70, toutefois le chef de projet avait une expérience de 4 ans dans la mise en place et la maintenance de dispositifs SAS 70.

HR Access a aussi fait appel à des consultants externes experts en contrôle interne et SAS 70. Enfin, les équipes opérationnelles ont été aussi sollicitées, en fonction du besoin, pour mettre en place et améliorer les processus et contrôles existants.
Lors de la phase de conception et de déploiement des contrôles, une certaine réticence des équipes opérationnelles s'est fait ressentir. En effet, prouver la valeur ajoutée des contrôles fut une tâche compliquée, en particulier au regard de la charge de travail que certains d'entre eux engendrent au jour le jour.

De plus, l'objectif était d'obtenir un rapport SAS 70 unique qui traduise une approche unifiée des Offres de Service, basée sur l'alignement des processus et ce malgré les barrières linguistiques et culturelles.

Aujourd'hui, le dispositif de contrôle a mûri et se trouve dans une phase de maintenance et d'amélioration continue. Des avantages certains sont déjà perceptibles :

La mise en place de contrôles a clairement contribué à la croissance de l'organisation ;
Les clients et les commissaires aux comptes éprouvent plus de confiance et le nombre d'audits externes est nettement moins élevé;
En outre, le projet SAS 70 a permis de construire des processus forts de contrôles dont l'efficacité opérationnelle est régulièrement vérifiée ;
Enfin, l'alignement des processus entre eux au sein des différents sites a permis, dans un 1er temps, de mieux mesurer et comparer des processus similaires à travers l'organisation ; ceci devrait permettre de devenir plus efficace plus rapidement.

Actuellement, le management opérationnel reconnait l'utilité des contrôles mis en place par le projet SAS 70.

**eSCM**

Lors du lancement du projet SAS 70, HR Access connaissait l'existence du référentiel eSCM et avait lu plusieurs articles intéressants à ce sujet. Bien que la norme SAS 70 fût considérée comme un impératif, les complémentarités entre eSCM et SAS 70 ont été identifiées dès le début du projet, avec une vision à long terme pour assurer la coexistence de la norme SAS 70 et du référentiel eSCM.

SAS 70 est certes une norme d'audit reconnue, mais ne fournit pas de bonnes pratiques concernant la manière de concevoir et d'implanter les contrôles. Par conséquent, pendant les phases de conception et de déploiement, eSCM a servi de boîte à outils pour certains domaines ou pratiques. Cela a permis d'avoir une vision focalisée sur l'externalisation et orientée performance et non plus limitée au contrôle interne et à l'audit.

Des initiatives visant à améliorer le modèle de service de HR Access en s'appuyant sur eSCM sont actuellement en cours ; il s'agit d'une première étape ayant pour but d'élargir le périmètre déjà couvert par le projet SAS 70.
Les autres référentiels SI
En ce qui concerne l'usage d'autres référentiels, HR Access fait appel à son propre modèle adapté du modèle CMMI pour les développements. En matière de gestion de service IT, HR Access a recours aux bonnes pratiques du référentiel ITIL. De surcroît, HR Access examine encore les possibilités d'obtention de la certification ISO 9000.

**Conclusion**

Il n'y a pas de réponse unique, les différents référentiels (ou standards cités) sont absolument indispensables pour réussir à opérer dans le marché dans lequel se trouve HR Access. Il est donc nécessaire de mettre en place SAS 70, même si cet outil ne fournit ni les bonnes pratiques ni une approche orientée service. eSCM a l'avantage d'être un référentiel qui permet d'accueillir d'autres référentiels et normes tels qu'ITIL ou SAS 70 ; il met de plus l'accent sur la relation client-fournisseur. L'adoption de nouvelles pratiques d'eSCM est un projet qui se poursuit dans la durée et reste une action continue d'amélioration.

## Capgemini

**La personne interviewée**

Christian BARANOWSKI, Responsable France de l'ensemble des démarches SAS 70 et Sécurité - Capgemini Outsourcing Services France.

**Capgemini en quelques mots**

Capgemini est l'un des leaders mondiaux du conseil, des services informatiques et de l'infogérance. Implanté dans plus d'une trentaine de pays, Capgemini aide ses clients à innover, à se transformer et à devenir plus performants.

Le Groupe offre un large éventail de compétences qu'il sait mettre en œuvre de manière cohérente. En coopération avec ses clients, Capgemini contribue à l'élaboration de leur orientation stratégique, à sa mise en œuvre et les aide à tirer le meilleur parti de la technologie. Pour eux, il prend en charge la gestion de leurs processus opérationnels et de leurs infrastructures informatiques.

En associant ses compétences en matière d'entreprise, de technologie et de gestion des opérations, Capgemini propose des services véritablement intégrés, ce qui constitue son expertise la plus précieuse. Capgemini propose à ses clients une gamme complète de prestations organisées autour de quatre métiers :

- Le Conseil en stratégie et transformation ;
- L'Intégration de systèmes et applications informatiques ;
- L'Infogérance qui prend en charge totalement ou partiellement l'infogérance de transformation et l'externalisation des fonctions de support "Business Process Outsourcing", dans un ensemble de services appelés "Outsourcing Services" ;
- Les Services Informatiques de Proximité.

**SAS 70**

En France, une telle démarche a été initiée en octobre 2005, avec la production d'un premier rapport « Type 1 » en janvier 2006 et d'un premier rapport « Type 2 » au titre de la période janvier – août 2006.

Afin de répondre au mieux aux besoins et contraintes de ses clients, Capgemini a délibérément choisi une double approche :

- Un rapport multi-client couvrant tant les activités d'Infrastructure Management que les activités d'Application Management ;
- Des rapports dédiés pour les clients en faisant la demande.

La genèse de ce projet réside dans la forte demande des clients côtés aux Etats-Unis et soumis à la réglementation Sarbanes Oxley. C'est donc sans expérience particulière en France sur cette thématique que Capgemini est monté rapidement en compétence grâce notamment à sa cellule dédiée aux Etats-Unis en charge de la coordination mondiale des démarches « SAS 70 ».

Dans le contexte particulier de l'infogérance (se caractérisant notamment par des équipes au service de plusieurs clients avec chacun leurs particularités) et au-delà des difficultés inhérentes à la « revisite » des processus (efforts de vulgarisation, documentation des processus ajustés afin que tous les collaborateurs puissent s'y appuyer au mieux et au service de ses clients), Capgemini a su dès la première année dégager une valeur ajoutée dans la mise en œuvre d'une telle démarche.

Il est important de mettre en avant les trois aspects suivants :

- Uniformisation des pratiques ;
- Accentuation de l'importance d'une traçabilité continue et pertinente des opérations ;
- Communication en interne sur la valeur ajoutée des « bonnes pratiques » et plus largement de nos activités.

Après cinq années de recul, le bilan est globalement très positif pour Capgemini. Au-delà de la mise en place d'une offre spécifique à destination de ses clients soumis à des enjeux forts de maîtrise de leur contrôle interne et de la valeur ajoutée importante dans le gain de nouveaux clients (et notamment deux acteurs du CAC40), cette démarche a notamment imposé une continuité et une amélioration continue dans la rigueur de mise en œuvre des processus de Capgemini.
Elle a été un apport méthodologique précieux et complémentaire aux méthodes de travail en interne. Elle a par ailleurs permis de transformer l'activité managériale au travers d'une responsabilisation de tous, et en particulier des managers, à l'importance du contrôle interne et de la pérennité de son efficience.

Cependant, il faut toutefois noter que cette démarche est encore aujourd'hui trop vécue comme une contrainte tant en interne que par les clients de Capgemini. Dans ce cadre, et pour vaincre les dernière réticences, l'enjeu actuel est donc de rendre plus dynamique les matrices de contrôles afin d'apporter davantage de confort dans l'exécution quotidienne de bonnes pratiques.

**eSCM et les autres référentiels SI**

Dans le cadre de l'amélioration continue des processus et de la satisfaction client, Capgemini s'est penché sur eSCM. Toutefois, le niveau de connaissance chez Capgemini reste aujourd'hui encore modeste. En l'absence d'écho à date chez les clients de Capgemini, le choix de déployer ce référentiel reste à déterminer. Capgemini s'appuie actuellement sur d'autres référentiels parmi lesquels ITIL, CMMi (pour les activités d'Application Management), ISO 9001 (pour la production de services) ainsi que diverses normes tant au niveau sécurité que sectorielles (par exemple NDA) toujours en échos aux enjeux et contraintes de nos clients.

**Conclusion**

L'élaboration de l'ensemble des normes et standards, dont font partie SAS 70 et eSCM, renforce le métier de Capgemini avec une progression constante.

De plus en plus, les relations client-fournisseur se trouvent apaisées par l'utilisation de ces référentiels de par l'apport d'un vocabulaire commun mais sous réserve d'un échange essentiel sur la compréhension que chacun peut en avoir. Et le point principal est sans doute là : les référentiels normatifs restent souvent peu pratiques à utiliser dans la mise en œuvre et demandent un investissement important de tous et particulièrement dans un contexte de diversité de la maturité des clients et de leur compréhension.
Néanmoins, le SAS 70 est sans conteste un élément clef pour tous dans la maîtrise des processus et garantit un apport constant de valeur mutuel.

## ADP

**La personne interviewée**

Franck MAHÉ, Directeur de la sécurité - ADP.

**ADP en quelques mots**

Créé en 1949, le groupe ADP capitalise aujourd'hui près de 60 ans d'expertise au service des entreprises à travers le monde, et se concentre sur ses deux activités principales « Employer Services » (services de gestion des ressources humaines) et « Dealer Services » (services de gestion pour les constructeurs et les gestionnaires automobiles). ADP totalise un chiffre d'affaires de 8,9 milliards de dollars. L'activité « Employer Services » représente 7,8 milliards de dollars dans plus de 60 pays. 52 millions d'employés dans le monde reçoivent ainsi un bulletin de paie réalisé par un système d'information ADP.
En France, ADP concentre son activité dans un seul domaine : les Ressources Humaines (Employer Services). ADP prend en charge tout ou partie des tâches du département des Ressources Humaines des entreprises et s'engage contractuellement sur le service. Ce panel de services mobilise les compétences de 2 000 personnes dans toute la France pour servir au quotidien 9 200 clients représentant mensuellement 2,5 millions de salariés. Ceci représente un chiffre d'affaires de 275 millions d'euros.

**SAS 70**

Le projet SAS 70 d'ADP Europe a démarré en 2004. La mise en œuvre d'une démarche SAS 70 chez ADP résulte d'une demande des clients et de l'impact normatif aux Etats-Unis, plus particulièrement pour les clients soumis au Sarbanes-Oxley Act. La démarche a donc été top-down, à l'initiative de la maison mère ADP Inc. située aux USA. Outre la demande des clients et l'aspect normatif, ADP voit dans la démarche SAS 70 une opportunité d'amélioration de ses processus et de son contrôle interne couplée à un instrument marketing et commercial pour approcher de nouveaux clients. A titre d'exemple, une petite plaquette indiquant qu'ADP possède des rapports SAS 70 est disponible sur le site du groupe et visible par les clients et prospects.

25 rapports SAS 70 type 2 sont produits annuellement auxquels s'ajoute un rapport portant sur l'offre transverse GlobalView.

100 à 150 clients sont demandeurs d'un ou plusieurs rapports, toutefois les rapports sont également remis à d'autres clients qui ne les demandent pas explicitement.

Aujourd'hui, la démarche SAS 70 mobilise une équipe de coordination d'une dizaine de personnes et environ une centaine de personnes sont sollicitées directement lors des audits sur les processus métiers et informatiques, et ce à l'échelle mondiale. La production annuelle des rapports SAS 70 est considérée comme un projet chez ADP et gérée comme tel avec une direction, des objectifs et des jalons à respecter.

La démarche SAS 70 n'a pas induit de changements dans l'organisation mais a nécessité la mise en place de fonctions de pilotage dédiées au SAS 70.

Comme indiqué précédemment, la mise en œuvre d'une démarche SAS 70 contribue à l'amélioration permanente des processus métiers et informatiques du groupe et constitue un atout commercial et marketing. C'est également un vecteur de transparence et de confiance vis-à-vis de l'extérieur. Néanmoins, les clients souhaitent de plus en plus une approche personnalisée et demandent à ADP de remplir des questionnaires ou exercent leurs clauses d'audit pour satisfaire leurs besoins de contrôle interne et de conformité.

En interne, la démarche SAS 70 est souvent méconnue en dehors de la sphère Finance, ce qui devrait changer avec la mise en œuvre des nouvelles normes ISAE 3402 et SSAE 16 qui requièrent la mise en place d'un système d'autoévaluation et une attestation de la direction sur son dispositif de contrôle interne.

L'adoption des nouvelles normes ISAE 3402 et SSAE 16 va contribuer à impliquer davantage les différents acteurs de l'entreprise dans l'amélioration du contrôle interne, puisque ceux-ci vont devoir s'auto-évaluer et s'engager formellement sur le sujet. Néanmoins, il convient d'appréhender le coût du dispositif d'autoévaluation à mettre en œuvre car celui-ci existe forcément.

La Direction de la Sécurité, dans sa fonction de coordinateur du projet SAS 70, assure le lien entre le management des pays audités dans le cadre des SAS 70 et les auditeurs.

Cette Direction conçoit donc la relation avec ses auditeurs comme un partenariat, qui permet également de former, de sensibiliser et de faire évoluer les collaborateurs d'ADP sur le terrain du contrôle interne. Charge à l'auditeur d'expliquer son métier et ses objectifs afin que l'audité comprenne le fondement de ses travaux et puisse en retirer des bénéfices.

**eSCM et les autres référentiels SI**

eSCM n'est pas utilisé au sein d'ADP. ADP utilise des référentiels tels que Cobit, ITIL et ISO 2700x, certains de ses sites/fonctions étant titulaires d'une certification. Le nombre de sites ou fonctions certifiés a vocation à s'étendre dans les années à venir.

**Conclusion**

ADP voit des synergies possibles entre ces référentiels qui partagent des critères communs. Il convient de ne pas les prendre tels quels mais de sélectionner dans chacun d'eux ce qui convient le mieux à l'entreprise afin de maximiser les bénéfices que l'on en retire.

## Pôle Emploi

**Les personnes interviewées**

Laurent STRICHER, DGA Systèmes d'Information / Secrétaire Général- Pôle Emploi.
Daniel URBANI, Directeur Général Adjoint Systèmes d'Information - Pôle Emploi.

**Pôle Emploi en quelques mots**

Le Pôle emploi est né par la loi du 14 février 2008 de la fusion du réseau des ex-Assédic et de l'ANPE, et a été lancé opérationnellement le 5 janvier 2009. La mission de la DSI est d'assurer l'évolution et le maintien en conditions opérationnelles du Système d'Information. Elle est organisée par métiers de Pôle emploi, composée de 1400 collaborateurs repartis sur une vingtaine de sites en France. Elle est structurée autour de 2 processus : Fabrication (ou conception de service) et Services et comporte un service d'achats informatiques.

**eSCM**

Pour mener à bien sa mission et assurer la réalisation de son plan de charge, la DSI de Pôle Emploi doit faire appel à la sous-traitance. Une politique de sourcing a ainsi été définie et mise en œuvre, alignée sur les stratégies métiers. Elle a permis d'identifier notamment les activités à sous-traiter.
C'est dans ce contexte que le Pôle Emploi a lancé en 2008 un marché majeur portant sur 12 lots de maîtrise d'œuvre, couvrant l'ensemble du cycle en V de la fabrication d'un service (à la fois métiers, techniques et de Tierce Maintenance Applicative). L'enjeu de cet appel d'offres était de travailler avec des fournisseurs organisés en centres de services et mettre fin à l'assistance technique (professionnalisation de la relation avec le fournisseur).
Le référentiel eSCM a été utilisé pour déployer ce marché d'un montant de plus de 100 Millions d'€ sur 4 ans et a permis la structuration de la démarche, et plus particulièrement : la définition de la stratégie, les compétences requises pour la mener à bien, le pilotage de la transformation et la gestion des achats.
Le projet de déploiement a été structuré en reprenant en partie les « domaines » du modèle eSCM. La complétude de ce référentiel a permis une couverture large des problématiques dans un délai court.

En effet, en 6 à 9 mois, les centres de services étaient opérationnels sur l'ensemble des lots. Cependant il n'a pas été exigé des prestataires l'utilisation ou la connaissance du référentiel eSCM, bien que cela soit désormais mentionné dans les cahiers des charges. eSCM a également été utilisé pour accompagner l'évolution des métiers de la DSI : passage du mode « faire » au mode « faire faire » (gouvernance, pilotage des fournisseurs, relation plus étroite avec le métier, etc.). Ainsi, 250 personnes ont déjà été formées sur cet aspect dans le cadre de cette démarche de transformation. De plus, pour pouvoir comparer les prestations des divers prestataires, une dizaine d'indicateurs communs ont été définis (fin 2009). Le choix de ceux-ci a été inspiré des pratiques eSCM. Le référentiel eSCM-CL a été utilisé pour définir le référentiel des achats de la DSI, mais celle-ci fait appel aussi à d'autres référentiels ou standards. Par exemple :

- Le référentiel des emplois internes de la DSI unifiée a été réalisé en s'appuyant sur le référentiel CIGREF ;
- Le système qualité a été construit en s'appuyant intégralement sur ITIL pour la définition du processus « services ».

**Les autres référentiels SI**

D'autre part, les deux DSI ex-Unédic et ex-ANPE étaient certifiées ISO9001/2000 avant la fusion. Dans le prolongement et pour mettre l'accent sur l'apport des référentiels métiers SI, la DSI de Pôle emploi vise la certification ISO 20000 pour début 2011 et dans le même temps, celle-ci sera aussi complétée par une certification ISO 27001 relative à la Sécurité. Ces deux certifications complémentaires marqueront un progrès sur l'évolution du service en général et la relation fournisseur en particulier (suivi, conformité avec les règles de sécurité…).

Au-delà de ces certifications collectives, il y a une vraie promotion des certifications individuelles ; celles-ci sont encouragées et mesurées au niveau des indicateurs de performance. L'accent est mis principalement sur ITIL et plus récemment sur quelques modules de CMMI :

- En effet, le référentiel interne de gestion de projet (« Conduite de Projet Unifié ») a été défini en tenant compte des recommandations CMMI, référentiel très structurant en termes de gestion de projet. Environ 200 personnes ont déjà été formées ;
- La deuxième étape (en cours) est de définir le référentiel de gestion des exigences, sur la base des recommandations CMMI également.

**SAS 70**

SAS 70 est, en revanche, peu, voire pas connu au sein de Pôle Emploi qui ne demande pas à ses fournisseurs de disposer d'un rapport SAS 70. Le contrôle des prestataires et des services offerts se fait moyennant le modèle de Gouvernance et des procédures documentées. Néanmoins, l'idée, d'avoir un processus de contrôle interne vis-à-vis des prestataires, est jugée intéressante et porteuse de professionnalisation et de rationalité dans la relation client-fournisseur.

**Conclusion**

Les Centres de Service sont bel et bien en place, mais leur fonctionnement reste cependant à optimiser. Le référentiel eSCM est à nouveau utilisé dans le cadre de cette opération d'optimisation. Il s'agit en premier lieu d'obtenir les gains attendus en termes de qualité, de coût et de délais. Il s'agit aussi de poursuivre les évolutions en interne :

- Consolidation de la gouvernance et du pilotage stratégique des centres de services ;
- Installation de nouvelles fonctions dans l'organisation et accompagnement du changement pour les équipes internes ;
- Evolution des compétences nécessaires au pilotage des centres de services …
- … et renforcement sur les activités internes à forte valeur ajoutée (relation client, contrôle / qualité, …)

Ces évolutions internes sont le résultat du projet GPEC (Gestion Prévisionnelle des Emplois et Compétences) que mène actuellement la DSI. Le projet GPEC nécessite de revisiter la stratégie de sourcing. Ceci va potentiellement amener une refonte des centres de service existants. Dans ce cadre, l'usage du référentiel e-SCM servira de ligne guide pour la mise en place des nouveaux centres de service.

## Sanofi-Aventis

**Les personnes interviewées**

Christine BERGE, Chef de projet Direction achat - Sanofi-Aventis.
Savine GUILLEMIN, Responsable Qualité SI - Sanofi-Aventis.
Denis LARTIGUE, Responsable du Contrôle Interne SI - Sanofi-Aventis.

**Sanofi-Aventis en quelques mots**

Sanofi-Aventis est un groupe mondial de l'industrie pharmaceutique qui recherche, développe et diffuse des solutions thérapeutiques pour améliorer la vie de chacun. Sanofi-Aventis a pour ambition de devenir un leader mondial et diversifié de la santé centré sur les besoins du patient. Le Groupe s'appuie sur trois axes pour atteindre ses objectifs et assurer une croissance pérenne :

- Accroître l'innovation en Recherche et Développement ;
- Saisir les opportunités de croissance externe ;
- Adapter le Groupe aux enjeux à venir.

Sanofi-Aventis possède des atouts fondamentaux dans le domaine de la santé avec cinq plateformes de croissance : les marchés émergents, les vaccins humains, la santé grand public, la prise en charge du diabète et les produits innovants.

**eSCM**

La contribution des SI à la réussite de l'entreprise implique une approche industrielle en matière de gestion des services IT, notamment lorsqu'ils sont externalisés. C'est dans ce contexte qu'eSCM a été utilisé.

Afin de suivre et d'évaluer les activités SI externalisées, un référentiel d'exigences, inspiré des bonnes pratiques eSCM, a été mis en place pour encadrer le suivi des phases de transition, d'exploitation et de réversibilité du contrat. Cette approche a facilité le suivi des relations avec les prestataires en fixant des règles claires dès le début de la relation. Avant même la contractualisation, les prestataires sont challengés sur ces exigences et doivent démontrer leur apport au regard des aspects économiques, de conception de services, de fourniture et de transfert de services et de contribution à l'innovation. Le modèle est adapté à chaque contexte d'appel d'offres. Il permet notamment aux chefs de projet une meilleure maîtrise et une anticipation de la phase de production des prestations. En outre, il nourrit une réflexion commune aux achats et aux SI sur l'exploitation optimale du contrat dans la durée.

Pour ce qui relève des activités de SI maintenues en interne, le référentiel eSCM a servi dans la mise en place d'offres d'insourcing. A titre d'exemple, la DSI de Sanofi-Aventis a lancé en 2008 un programme visant à structurer son Centre de Services Partagés à partir des bonnes pratiques en matière de gestion de services issues d'ITIL et des bonnes pratiques de sourcing issues d'eSCM. Ce programme s'est fixé pour objectif l'industrialisation des activités de réalisation et de maintenance de solutions spécifiques reposant sur tout un panel de

technologies (SAP-ABAP, JAVA/J2EE, Microsoft .Net, ORACLE Forms). Bien entendu, cette harmonisation s'est accompagnée de l'optimisation du rapport coût / qualité de service.

La mise en place de cette nouvelle structure de Centre de Service a permis d'identifier et de développer de nouveaux rôles et métiers, désormais reconnus au sein de la fonction SI du Groupe. La communication, notamment sur l'interaction entre les différents acteurs, est un facteur clé de réussite et reste, dans ce cas comme dans de nombreux projets, un axe de progrès identifié. Aussi, ce qu'il convient de souligner est l'approche pragmatique offerte par eSCM. Dans les faits, la prise en main du référentiel eSCM a été progressive et Sanofi-Aventis a pu l'adapter à la réalité opérationnelle. Cette démarche d'appui sur le référentiel eSCM a permis de renforcer l'efficacité du Centre de Service. Elle a aussi été utile pour explorer d'autres activités SI pouvant bénéficier du référentiel eSCM.

**Les autres référentiels SI**

En matière de gestion des services IT, Sanofi-Aventis a lancé un programme d'harmonisation des processus d'exploitation des services informatiques. Ce programme concerne, à l'échelle de plusieurs continents, près de 2500 personnes ayant des activités portant sur les systèmes d'information (applications métier, infrastructure SI, production informatique, etc.). Le premier retour d'expérience de l'usage partagé d'un référentiel comme ITIL s'est traduit par une amélioration de la réactivité et de la qualité des échanges lors de la conception des processus. Il est toutefois encore trop tôt pour établir un retour d'expérience complet dans la mesure où la phase de déploiement est actuellement en cours.

En matière de gouvernance et de contrôle des SI, Sanofi-Aventis a construit son référentiel de contrôle interne à partir du cadre de référence COBIT tout en l'adaptant aux risques d'entreprise. C'est ce référentiel de contrôle interne qui sert dans l'activité d'audit interne pour donner, à l'équipe dirigeante, l'assurance de l'atteinte des objectifs d'entreprise et la maîtrise des risques encourus.

**SAS 70**

En fonction des enjeux liés aux contrats d'outsourcing, Sanofi-Aventis s'appuie sur des rapports SAS 70 (type II) à la fois sur les aspects de conformité mais aussi sur des aspects plus spécifiques par rapport à l'analyse de risques internes. En effet, dans le cadre du respect de la loi Sarbanes-Oxley, le SAS 70 permet de fournir une appréciation de l'intégrité, la confidentialité et la disponibilité des SI faisant l'objet d'un contrat d'externalisation.
A titre d'exemple, Sanofi-Aventis a lancé un appel d'offres concernant l'infogérance d'une partie des SI représentant environ 15 % du budget global d'infrastructure SI. En demandant un rapport SAS 70 dont le périmètre d'évaluation est aligné au référentiel d'exigences de l'appel d'offres, Sanofi-Aventis dispose d'une évaluation fiable et indépendante sur l'efficacité des contrôles en place chez les soumissionnaires.

**Conclusion**

Le rôle du référentiel eSCM a été fondamental dans le renforcement des relations client-fournisseur. Ce renforcement s'est traduit par une amélioration de la qualité des services

rendus aux clients internes et une meilleure évaluation du suivi. L'usage des pratiques eSCM à permis une dynamique bénéfique et durable à la fois sur les activités SI vis-à-vis des fournisseurs externes mais aussi vis-à-vis des acteurs internes à l'entreprise. La démarche portant ses fruits, elle a été proposée aux autres familles d'achats. L'usage de rapports SAS 70 reste encore limité à des fins de conformité à la réglementation. Toutefois, on constate, en fonction des sujets à traiter, un intérêt grandissant à disposer d'une évaluation fiable et indépendante sur l'efficacité des contrôles en place chez les soumissionnaires et les prestataires.

## Groupe La Poste

**La personne interviewée**

Michel Delattre, DSI du Groupe la Poste

**La Poste, en quelques mots**

Le groupe La Poste est une entreprise de services multi-métiers qui a réalisé en 2009 20, 5 milliards de CA dont 53,8% avec les activités Courrier, 24,3% les services financiers et 21,7% les activités Colis-Express

Chacun des 3 métiers possède sa propre DSI. Une 4ème DSI, adressant les fonctions support (RH, Finance, Siège, ..), vient compléter le dispositif. Le cadre de cohérence de l'ensemble est assuré par une DSI Groupe. Les DSI s'appuient sur 2 entités transverses pour, d'une part, la gestion des infrastructures et des services réseau et pour, d'autre part, le support aux utilisateurs et la gestion des postes de travail.
Les DSI de La Poste font appel à divers types de contrats d'infogérance principalement pour l'hébergement de leurs infrastructures, le développement et la gestion d'une partie de leur patrimoine applicatif.

Le Groupe La Poste doit répondre aujourd'hui aux besoins d'évolution de ses services générés notamment par le développement d'une économie de plus en plus numérique En tant que support de la stratégie du Groupe, les DSI et le SI sont au cœur du développement de l'entreprise.

**eSCM**

L'adoption d'eSCM a été amorcée au sein de la DSI du Courrier, fin 2006, dans un contexte de forte transformation du métier requérant le lancement de nombreux projets et la nécessaire augmentation de ses capacités de développement.

Le défi pour la DSI consistait à « fournir les bonnes ressources au bon moment » et faire les arbitrages entre les services à réaliser avec les équipes internes et ceux à sous traiter ponctuellement ou durablement. Il fallait adapter, en conséquence, la politique de sourcing IT : la DSI a, alors, identifié que le référentiel eSCM pouvait être un accélérateur de sa mise en œuvre et un guide pour sa pratique au quotidien.

Le déploiement d'eSCM, au sein de la DSI du Courrier, s'est déroulé en 3 phases :

- Une première étape a permis de définir une politique de sourcing cohérente et en ligne avec les besoins du métier en choisissant les activités à externaliser, puis de remplacer les contrats existants à engagements de moyens par des contrats à engagements de résultats ;
- Une deuxième étape visait à professionnaliser et industrialiser les pratiques internes ;
- La troisième étape (en cours) est orientée sur l'application de pratiques plus opérationnelles dans la gestion des fournisseurs au quotidien.

Cette initiative est considérée comme un succès. Elle a permis de mettre en place le cadre de gouvernance nécessaire à la gestion d'une relation équilibrée client-fournisseurs, ce qui a eu un impact positif sur l'optimisation des coûts et l'amélioration de l'agilité. Il est intéressant de noter que les fournisseurs ont réellement joué le jeu.

Cette première expérience, sous l'impulsion de la DSI Groupe, a fait tâche d'huile dans les autres DSI du Groupe, et notamment au sein de la Banque Postale, née en 2006 : celle-ci a pu intégrer, dès sa création, les principes de gouvernance d'eSCM dans ses activités de Sourcing. Le Colis, lui aussi a été conquis par la démarche.

**Les autres référentiels SI**

La Poste, comme nombre de ses consœurs, a investi dans l'implémentation des référentiels dédiées à ses activités SI : le référentiel des emplois du CIGREF pour la GPEC, CMMI pour le Développement, ISO 2700X pour la sécurité des SI et ITIL pour les opérations.

Un des rôles, en effet, de la DSI Groupe est de faire connaître, de promouvoir et d'aider au déploiement de ces référentiels, de capitaliser sur l'expérience des différentes DSI. Cette action est principalement basée sur :

- La mise en place de communautés d'utilisateurs internes permettant un partage d'expériences, la mise en commun de bonnes pratiques choisies ;
- La formation des équipes.

Le groupe La Poste a généralisé l'utilisation d'ITIL à la fois dans le pilotage des activités de la production mais aussi en intégrant certaines bonnes pratiques dans les appels d'offres en complément de celles tirées d'eSCM. 407 personnes (soit près de 78% de la population concernée au sein de la DSI Transverse et de la DSI Courrier) sont certifiées ITIL, dont 341 pour Foundations, 51 pour le niveau 2, 14 pour le bridge V2/V3 et 1 pour le niveau 3. Les activités de développement de la DSI des fonctions support ont, quant à elles, été certifiées CMM niveau 2 en 2010.

**SAS 70**

Pour ce qui relève de SAS 70, c'est en tant que Prestataire de Services, via sa filiale Extelia[4] que le groupe La Poste a pris connaissance de ce standard. Extelia, en effet, s'est impliquée, à la demande de certains clients, dans une démarche SAS 70. Le Groupe a pu se rendre compte à ce titre que les thématiques d'eSCM et de SAS 70 comportaient certains points communs. L'intérêt de SAS 70 pour La Poste, en tant que Client et Fournisseur, s'impose comme une évidence.

**Conclusion**

Le groupe La Poste est en mouvement dans un monde de turbulence. Le développement de l'entreprise, les ambitions qui sont les siennes ne peuvent se réaliser sans un SI performant. Le SI ne peut évoluer sans le concours et le recours à des partenaires externes dans le cadre

[4] EXTELIA est née le 1er novembre 2008, de la reprise par le groupe La Poste des activités BPO du Groupe Experian. Filiale à 100 % du holding Docapost, EXTELIA intervient notamment dans la gestion de back-offices externalisés

d’une relation équilibrée. eSCM, comme tous les référentiels est un outil au service de la performance du SI, un moyen mais non une fin. C’est pourquoi il est important de l’utiliser, de manière pragmatique et non dogmatique en choisissant les bonnes pratiques répondant au mieux à ses besoins. La démarche eSCM permet de préserver l’avenir en aidant à préparer les évolutions du sourcing IT telles que celles induites par l’extension de l’utilisation d’offres de type Cloud Computing ou SaaS. SAS 70 permettra de garantir aux clients de nos filiales que, nos processus étant sous contrôle, nous contribuerons à la performance de leur SI.

**La personne interviewée**

Jean-Pierre AGAZZI, Associé, Commissaire aux Comptes, Responsable Global Accounting Advisory Services

**Deloitte, en quelques mots**

Deloitte fournit des services professionnels dans les domaines de l'audit, de la fiscalité, du consulting et du financial advisory à ses clients des secteurs public ou privé, de toutes tailles et de toutes activités. Fort d'un réseau de cabinets membres dans plus de 150 pays et comptant 170 000 professionnels, Deloitte allie des compétences de niveau international à des expertises locales pointues afin d'accompagner ses clients dans leur développement partout où ils opèrent.

**SAS 70**

En France, Deloitte mobilise un ensemble de compétences diversifiées pour répondre aux enjeux de ses clients, de toutes tailles et de tous secteurs – des grandes entreprises multinationales aux micro-entreprises locales, en passant par les entreprises moyennes. Fort de l'expertise de ses 6 400 collaborateurs et associés, Deloitte en France est un acteur de référence en audit et risk services (incluant la mise en place d'une démarche SAS 70 et l'émission de tels rapports), consulting, financial advisory, juridique & fiscal et expertise comptable, dans le cadre d'une offre pluridisciplinaire et de principes d'action en phase avec les exigences de notre environnement.

La démarche d'audit adoptée pour les clients soumis au Sarbanes-Oxley Act est calquée sur l'AS5 (Audit Standard n°5) édicté par le PCAOB (Public Company Accounting Oversight Board – organisme chargé de superviser les audits de sociétés cotées aux USA).

L'externalisation d'une activité nécessite d'en maîtriser les risques. Les entreprises bénéficiant de services fournis par des tiers, ayant un impact sur la présentation de l'information financière ou sur les activités exercées dans l'environnement du contrôle interne, se doivent de justifier que des contrôles ont été mis en place et fonctionnent de manière adéquate chez leur prestataire.

Aussi, si le prestataire dispose d'un rapport SAS 70 de type 2 (i.e. l'efficacité opérationnelle des contrôles est testée), l'auditeur le prend en considération et évalue sa pertinence et sa qualité avec les spécialistes du cabinet. Par exemple, pour une infogérance de système d'information, l'auditeur financier consulte ses auditeurs informatiques afin de déterminer s'il peut s'appuyer sur le rapport SAS 70. Pour cela, le rapport SAS 70 doit couvrir un périmètre adéquat au regard des activités externalisées par le client, être réalisé sur une période de 6 mois minimum et proche de la date de clôture comptable du client, respecter la démarche type d'un SAS 70 et bien sûr ne pas avoir de qualification c'est-à-dire de déficience significative au niveau de l'opinion émise par l'auditeur SAS 70 et figurant dans la première section du rapport. Enfin, le SAS 70 doit être émis par un cabinet d'audit reconnu sur la place

pour ce genre de rapport et disposant de compétences avérées sur le sujet. Si ces critères ne sont pas remplis, l'auditeur ne peut s'appuyer sur le rapport SAS 70 et devra mener des diligences complémentaires chez le prestataire de services. En effet, l'auditeur doit être confortable avec le rapport SAS 70 car il endosse la responsabilité de l'opinion du rapport dans le cadre de sa certification des comptes de l'entité utilisatrice du rapport.

L'auditeur fait une lecture détaillée de l'opinion et de la liste des déficiences mais recourt à des spécialistes du sujet traité dans le rapport SAS 70 pour apprécier sa suffisance et sa complétude et l'exploiter de façon ad-hoc.

La difficulté éventuelle à laquelle peut être confronté un auditeur financier est le fait de ne pas être spécialiste de l'objet du rapport SAS 70 et donc la nécessité de faire appel à des experts habitués à traiter à la fois ce domaine et la préparation de rapports type SAS 70.

Les limites d'un rapport SAS 70 résident dans le fait que, même si l'auditeur (ou les spécialistes du sujet au sein du cabinet) n'a pas réalisé les travaux chez le prestataire de services, il doit en endosser la responsabilité et n'est pas exonéré de sa responsabilité personnelle sur cette partie de l'audit.

Aussi, pour être confortable sur le sujet, il convient d'impliquer des spécialistes du SAS 70 de bout en bout afin d'avoir la bonne lecture du rapport.

**Conclusion**

Il y a un gain financier lié au fait que le contrôle interne n'est pour partie pas réalisé par les clients eux-mêmes mais déplacé chez leurs prestataires de services. D'autre part, la responsabilité du client et de son Audit Interne est également partiellement déplacée chez le prestataire.

En matière de gestion des risques, le client recevant un rapport SAS 70 dispose d'une vision claire de ses processus, peut-être plus claire que s'ils étaient gérés en interne. D'autre part, l'évaluation du contrôle interne est réalisée par des spécialistes disposant d'une compétence pointue sur le sujet et donc à-même d'apprécier la couverture des risques. En contrepartie, le client ne maîtrise pas le programme de travail appliqué par l'auditeur SAS 70 et perd en visibilité de ce côté-là.

Parmi d'autres bénéfices que l'on pourrait attendre d'une démarche SAS 70, l'amélioration de la gouvernance fait figure de candidat toutefois cela reste un élément difficile à quantifier.

Deloitte accueille favorablement les nouvelles normes ISAE 3402 et SSAE 16 qui vont venir se substituer au SAS 70 à compter du 15 juin 2011. L'évaluation du contrôle interne que devra fournir le prestataire de services va le contraindre à s'engager davantage et constitue donc une garantie supplémentaire pour les clients et les auditeurs utilisateurs des rapports, qui vont donc gagner en confort avec les nouvelles normes.

# Conclusion

eSCM est un ensemble de bonnes pratiques couvrant tous les processus relatifs à l'externalisation de services informatiques. SAS 70 est une norme d'audit du contrôle interne de services externalisés.

Marier les 2, c'est pour les parties prenantes collectionner les gains comme le prouvent les témoignages recueillis auprès des clients La Poste, Pôle Emploi, Sanofi-Aventis ainsi qu'auprès des fournisseurs ADP, Capgemini, HR Access et du cabinet d'audit Deloitte :

Valeur ajoutée importante par des gains de nouveaux clients ;

- Incontournable pour répondre aux appels d'offres ;
- Uniformatisation des pratiques ;
- Economie ;
- Obtention d'engagements de résultats ;
- Renforcement des relations clients / fournisseurs ;
- Permet de préparer les évolutions vers le cloud computing ;
- Maîtrise du contrôle interne ;
- Amélioration de la gouvernance.

Et en plus, ces référentiels évoluent et s'enrichissent. En juin 2011 une norme internationale ISAE 3402 remplacera la norme américaine SAS 70.

En conclusion, vous lecteurs qui avez parcouru ce livre blanc, avez-vous encore le choix de ne pas adopter ces 2 référentiels ?

Merci de nous faire part de vos propres expériences pour enrichir la prochaine version de ce livre blanc : ae-scm@laposte.net

# Annexe A : Aperçu du référentiel eSCM

L'IT Services Qualification Center (ITSqc) de l'Université Carnegie Mellon a conçu deux référentiels de bonnes pratiques à adopter pour permettre, aux clients et aux prestataires de services, l'amélioration continue et la mise en place durable et bénéfique de relations de sourcing :

- eSCM-SP : pour Service Provider ou prestataire **[1]**, **[2]**;
- eSCM-CL : pour Client **[3]**, **[4]**.

Le référentiel eSCM-CL **[5]** aide les clients, en recherche de nouveaux leviers de croissance et de gains de productivité, à piloter efficacement les services informatiques fournis par leurs prestataires. Le référentiel eSCM-SP **[6]** offre aux prestataires un ensemble de bonnes pratiques à adopter pour répondre de manière satisfaisante aux besoins de leurs clients et prospects, ainsi qu'à la bonne gestion de leur organisation en fonction de leurs objectifs organisationnels.

Le modèle eSCM pour les prestataires, eSCM-SP, est composé de 84 pratiques dont chacune a pour caractéristiques :

- Sa durée dans le cycle de vie du sourcing : permanente ou rattachée à une des trois phases spécifiques de sourcing : Démarrage, Fourniture ou Réversibilité. Une 4ème phase spécifique (Analyse) se rapporte uniquement au modèle eSCM-CL pour les clients ;
- Son rattachement à l'un des dix domaines d'aptitude regroupant les fonctions critiques de même nature (voir tableau ci-après) ;
- Sa position sur un des cinq niveaux d'aptitude décrivant la trajectoire d'amélioration à emprunter pour passer d'une fourniture empirique des services à l'excellence du sourcing.

Les cinq niveaux d'aptitude d'eSCM-SP sont définis ci-après :

- **Niveau 1 - Fournir empiriquement le service :** le niveau 1 est le niveau de base. Le prestataire reste au niveau 1 tant qu'il n'a pas appliqué la totalité des pratiques de niveau 2. Les capacités des prestataires de niveau 1 varient largement. Certains peuvent n'avoir aucune pratique implémentée ;
- **Niveau 2 - Satisfaire aux exigences de façon cohérente :** les prestataires ont formalisé des procédures permettant de recueillir les exigences et de fournir les services selon les engagements pris. Ces prestataires sont en mesure de fournir des services pour des exigences clients définies dans des domaines proches de leurs spécialités. Ils peuvent démontrer l'implémentation et l'usage effectif de l'ensemble des pratiques de niveau 2 ;
- **Niveau 3 - Gérer la performance de l'organisation :** les prestataires peuvent fournir des services répondant à des exigences définies, même si le domaine ne fait pas partie de leurs spécialités. Au niveau 3, le prestataire peut gérer sa performance globale, comprendre les attentes du marché et ses évolutions, identifier et gérer les risques transverses à l'organisation et concevoir et déployer des services basés sur des procédures définies. Il partage et utilise la connaissance acquise au cours des prestations, mesure objectivement et récompense la performance de son personnel, surveille et contrôle son infrastructure technique. Ayant mis en place des systèmes

permettant de gérer la relation client, il cherche à améliorer continuellement la qualité des services offerts mais ces améliorations sont généralement opérées de façon réactive. L'ensemble des pratiques de niveau 2 et 3 sont implémentées ;

- **Niveau 4 - Accroître pro activement la valeur :** les prestataires sont en mesure d'innover continuellement pour augmenter la valeur des services qu'ils fournissent à leurs clients. Au niveau 4, le prestataire peut personnaliser son approche et le service proposé à ses clients et prospects, comprendre les enjeux de ses clients et prévoir sa performance sur la base des expériences passées. Il évalue systématiquement et introduit les avancées technologiques. Enfin, il se fixe des objectifs de performance sur la base d'une analyse comparative de sa performance actuelle, la « benchmarkant » aussi bien en interne qu'en externe. Au niveau 4, les prestataires exécutent l'ensemble des 95 pratiques de niveau 2, 3 et 4 ;
- **Niveau 5 - Maintenir l'excellence :** les prestataires ont démontré l'excellence et l'amélioration de leur performance en ayant effectivement mis en œuvre toutes les pratiques des niveaux 2, 3 et 4 lors d'au moins deux « évaluations pour certification » consécutives sur une période d'au moins 2 ans. Il n'y a pas de pratique additionnelle à mettre en œuvre pour atteindre le niveau 5. L'implémentation efficace et continue de toutes les pratiques eSCM-SP dans un environnement en rapide évolution démontre l'aptitude du prestataire à maintenir l'excellence au cours du temps, partout dans son organisation.

La structure du modèle eSCM-SP se présente de la façon suivante :

| Cycle de vie | Domaine d'Aptitude eSCM SP | Niveau d'Aptitude | | | TOTAL |
|---|---|---|---|---|---|
| | | 2 | 3 | 4 | |
| | | Nombre de pratiques | | | |
| Pratiques permanentes | Gestion de la connaissance | 3 | 4 | 1 | 8 |
| | Gestion des ressources humaines | 3 | 7 | 1 | 11 |
| | Gestion de la performance | 3 | 3 | 5 | 11 |
| | Gestion des relations | 3 | 4 | 1 | 8 |
| | Gestion de la technologie | 4 | 1 | 1 | 6 |
| | Gestion des risques | 6 | 1 | | 7 |
| Démarrage | Contractualisation | 9 | 2 | | 11 |
| | Conception et déploiement du service | 6 | 2 | | 8 |
| | Transfert du service (1ère partie) | 2 | | | 2 |
| Fourniture | Fourniture du service | 7 | 1 | | 8 |
| Réversibilité | Transfert du service (2ème partie) | 2 | 1 | 1 | 4 |
| | **TOTAL :** | 48 | 26 | 10 | 84 |

Le modèle eSCM-SP pour les prestataires a deux objectifs majeurs :

- Permettre aux prestataires de se différencier de leurs compétiteurs ;
- Permettre aux clients d'évaluer de façon objective l'aptitude des prestataires à fournir des services de qualité.

Le modèle eSCM-SP guide les prestataires dans l'amélioration de leurs activités de fourniture de services. Il constitue également un standard à utiliser pour évaluer ces activités dans un objectif de certification. Ils pourront dès lors faire valoir leur niveau de certification eSCM-SP sur la base de leur « Profil d'Aptitude au Sourcing », en particulier lors des phases de négociation avec leurs clients potentiels.

## Annexe B : Aperçu du standard SAS 70 et de la norme ISAE 3402

**SAS 70, une réponse au besoin de maîtrise du contrôle interne autour des activités externalisées**

Avec le renforcement des besoins en contrôle interne, les demandes de rapport SAS 70 ont refait leur apparition ces dernières années. Face à ces nouvelles demandes, les sociétés s'interrogent souvent sur la nature des travaux induits et sur les bénéfices qu'elles peuvent en tirer (tant du côté « audité » que du côté « destinataire du rapport »). Avec l'externalisation des activités confiées par les entreprises à des tiers, tant en termes de Systèmes d'Information que de processus opérationnels, la question de l'assurance autour de la maîtrise des risques, et du contrôle interne relatif à ces activités externalisées, s'est posée aux entreprises clientes et à leurs auditeurs (ou encore aux régulateurs).

Ainsi, l'ordre des experts comptables américains (AICPA) a élaboré, en 1992, une norme d'audit (« SAS 70 ») encadrant l'organisation et la nature des travaux requis pour qu'un auditeur soit en mesure d'émettre une opinion, en respect des normes de travail caractérisant sa profession, permettant ainsi une approche homogène et acceptée par l'ensemble des intervenants.

La norme SAS 70, du fait de son approche structurée et homogène, s'est progressivement imposée en dehors du cadre américain et permet de **[7]** :

- Répondre aux attentes des régulateurs, des auditeurs externes et aux besoins propres de l'entreprise fournissant le service ;
- Réduire le nombre d'audits au travers de la production d'un rapport unique, reconnu et utilisable par l'ensemble des acteurs ;
- Fournir aux clients une visibilité sur les risques de leurs activités externalisées, reconnue et utilisée par leurs propres auditeurs externes ;
- Gagner la reconnaissance, par l'ensemble des acteurs de la norme « SAS 70 » qui a été reprise par l' « International Federation of Accountants » (IFAC) au travers de la norme ISA 3402.

Le succès de la norme SAS 70 s'explique par une approche à la fois :

- Flexible : le périmètre est défini conjointement par l'entreprise fournissant le service et ses clients ;
- Structurée : une fois le périmètre défini, la revue du dispositif de contrôle interne et l'émission de l'opinion du tiers externe réalisant la revue sont strictement encadrées;
- Rigoureuse : la démarche se fonde sur un standard d'audit.

La principale force d'un SAS 70 réside dans l'assurance qu'apporte une approche homogène et optimisée et un unique rapport destiné à l'ensemble des acteurs, et notamment :

- Les régulateurs qui y trouvent une réponse à leurs recommandations en matière de gestion des risques ;
- Le management, l'audit interne ou même le Comité d'Audit de l'entité fournissant le service qui obtiennent une vision de la maîtrise de leurs risques et peuvent la communiquer au marché et à leurs auditeurs externes ;

- Les clients qui complètent ainsi la vision de leur dispositif de contrôle et peuvent communiquer une opinion indépendante et reconnue à leurs auditeurs externes.

Ainsi, guide reconnu vers les meilleures pratiques du secteur d'activité, le SAS 70 permet :

- La mise en conformité et l'évaluation du dispositif de contrôle interne par rapport aux meilleures pratiques d'organisation des contrôles au sein d'un métier;
- L'évaluation sur base annuelle de l'efficacité des contrôles en place, en insistant de manière circonstanciée sur la nécessité de structurer et documenter le contrôle interne, et de retenir les bonnes pratiques :
- Mesure dans le temps de son amélioration ou de sa détérioration ;
- Précision de la taille des échantillons en fonction de la fréquence des contrôles.

En produisant un rapport unique, reconnu et utilisable par l'ensemble des acteurs, cette démarche évite la multiplicité des audits. Ainsi, la moindre sollicitation des équipes opérationnelles et du management, du fait de la réduction du nombre des audits qui pourraient être demandés par les clients, permet de gagner du temps et de répondre plus facilement et rapidement aux besoins des clients ou de leurs auditeurs.

Enfin, dernier avantage et non des moindres, le SAS 70 est un outil marketing et un avantage concurrentiel permettant de :

- Promouvoir la qualité du contrôle et de la sécurité de l'environnement du prestataire;
- Promouvoir l'efficacité de l'environnement d'exploitation et de son adéquation par rapport aux besoins des clients.

**Le standard SAS 70 en pratique**

Le standard SAS 70 définit deux types de rapport :

- Type I : opinion sur la conception des contrôles et leur mise en place effective (existence) ;
- Type II : opinion sur la conception des contrôles, leur mise en place effective ET sur l'efficacité opérationnelle de ces contrôles (sur une période de six mois minimum).

Un rapport SAS 70 (type I comme type II) est remis à l'établissement revu qui le diffuse lui-même aux clients à qui il souhaite le transmettre. Le rapport est donc public, à diffusion contrôlée par l'établissement. Le rapport est utilisé par les auditeurs des clients de l'établissement (« the users ») afin de définir les travaux d'audit à mener auprès de l'établissement (« the services »).

Un rapport SAS 70 « type I » contient généralement :

- Des informations sur l'établissement qui subit la revue et sur les processus entrant dans le périmètre de la revue ;
- Une description du dispositif de contrôle interne de cet établissement ;
- Une liste d'objectifs de contrôle et d'activités de contrôle, choisis par l'établissement, relatifs au périmètre de la revue ;

- L'opinion de l'auditeur sur l'existence des contrôles et leur capacité à donner une assurance raisonnable que les objectifs de contrôle sont atteints à une date donnée ;
- Des informations supplémentaires que l'établissement souhaite mentionner (par exemple au sujet de son Plan de Continuité d'Activité).

Un rapport SAS 70 « type II » contient généralement les mêmes éléments qu'un rapport « type I », avec en plus l'opinion de l'auditeur sur la capacité des contrôles à donner une assurance raisonnable que les objectifs de contrôle ont été atteints sur une période de revue d'au moins six mois (généralement un an).

Selon le type, les travaux diffèrent :

- Type I : travaux sur une image («snapshot») des contrôles à une date donnée, l'auditeur donne une opinion sur leur conception («design») et leur existence ;
- Type II : travaux sur les contrôles durant une période de six mois minimum, l'auditeur donne une opinion sur leur conception («design»), leur existence et leur fonctionnement correct tout au long de la période.

Une revue type II se fait sur une période de temps minimale de six mois – ce qui ne signifie pas qu'elle doive être refaite tous les six mois. Une pratique courante est de mener une revue type II annuelle sur une période de six à douze mois (selon la disponibilité de la documentation).

Une revue type II doit donc intervenir, en toute sécurité, au moins six mois après la date où la revue type I a été menée. Les types de tests effectués pour un type II se décomposent comme suit :

- Vérifier par entretien («inquiry») ;
- Observer le contrôle («observation») ;
- Vérifier sur pièces («inspection») : test sur un échantillon – c'est le test le plus répandu ;
- Rejouer le contrôle («reperformance»).

Différents niveaux d'anomalies pouvant être rencontrés au cours de la revue :

- Si l'existence, le design, ou l'efficacité (type II) du contrôle concerné ne sont pas compromis : pas de mention dans le rapport ;
- Si l'existence, le design, ou l'efficacité (type II) du contrôle concerné sont incorrects mais que l'objectif de contrôle est toujours atteint avec une assurance raisonnable : mention dans le corps du rapport, pas de mention dans l'opinion au début du rapport ;
- Si les auditeurs ne disposent pas de l'assurance raisonnable qu'un objectif de contrôle est atteint, ou si un contrôle revu n'existe pas : mention de l'objectif ou du contrôle dans l'opinion au début du rapport.

**ISAE 3402, une nouvelle norme applicable à partir 15 juin 2011 et capitalisant sur les forces de SAS 70 et renforçant le rôle du management du prestataire**

L'International Auditing and Assurance Standards Board (IAASB) a publié en décembre 2009 une nouvelle norme visant à établir un standard commun (et moins typé US) pour l'audit des activités externalisées : l'International Standard on Assurance Engagements 3402 (ISAE 3402).

La norme ISAE 3402, applicable en France dès juin 2011, ne vise pas à changer la façon dont le rapport sur les contrôles effectués est élaboré. Au contraire, il a été préparé pour répondre à la demande d'une norme internationalement reconnue et s'intégrant dans le cadre actuel de normes d'assurance. La nouvelle norme comprend toutefois de nouvelles exigences et des changements au regard des exigences antérieures de SAS 70.

Les principales similitudes entre le standard SAS 70 et la norme ISAE 3402 se déclinent comme suit :

- Le périmètre est axé sur les contrôles qui sont susceptibles d'être pertinents pour le contrôle interne des entités utilisatrices (contrôles portants sur la maîtrise de l'information financière) ;
- Des rapports Type I ou Type II peuvent être émis par l'auditeur. Les rapports peuvent inclure (méthode « inclusive ») ou exclure (méthode « carve-out ») les services fournis par des sociétés tierces ;
- La description des contrôles de la société de services dans le cadre SAS 70 seront généralement une base pour la description du système dans le cadre de l'ISAE 3402 ;
- Le rapport est limité à une utilisation par le management de la société de services, les clients de ladite société et les commissaires aux comptes de leurs clients.

Les principales différences entre le standard SAS 70 et la norme ISAE 3402 se déclinent comme suit :

- Le management de la société de services est tenu de fournir une affirmation écrite décrivant les responsabilités de la société au regard des systèmes et des contrôles liés ;
- Les sociétés tierces sont tenues de fournir une affirmation semblable quand elles sont incluses dans le périmètre du rapport (méthode « inclusive ») ;
- Dans un rapport Type II, l'auditeur émet une opinion sur la pertinence de la conception des contrôles liés aux objectifs de contrôle sur l'intégralité de la période ;
- L'auditeur est tenu de communiquer explicitement sur l'utilisation dans le cadre de son rapport de travaux de l'audit interne (ou d'autres fonctions indépendantes de la société de services réalisant des tests).

En conclusion, la mise en œuvre de la norme ISAE 3402 va permettre de donner une impulsion nouvelle à la maîtrise du contrôle interne autour des activités externalisées en capitalisant sur les bonnes pratiques issues de l'expérience d'années d'utilisation du standard SAS 70 tout en renforçant la responsabilité du management du prestataire, rejoignant en cela le mouvement observé ces dernières années dans les différentes législations nationales et internationales autour des attendus en termes de pilotage du contrôle interne.

## Annexe C : Vue d'ensemble et complémentarité eSCM et SAS 70

Le tableau ci-après donne une vue d'ensemble de la norme SAS 70 et du référentiel eSCM-SP :

| | eSCM-SP v2 | SAS 70 |
|---|---|---|
| **Publics** | Prestataires de services informatiques. | Organisations de services. |
| **Objectif** | Améliorer l'aptitude de sourcing IT du prestataire pour répondre aux besoins des clients et prospects. | Donner une assurance aux clients et à leurs auditeurs sur le contrôle interne autour de leurs activités externalisées. |
| **Dimension** | 84 pratiques réparties dans 10 domaines d'aptitude. | Définition du périmètre, de l'environnement de contrôle, des contrôles de risque et des outils de pilotage.<br>Objectifs de contrôle, contrôles clés et diligences mises en œuvre pour en évaluer soit le design, soit l'efficacité opérationnelle.<br>Informations complémentaires fournies par le prestataire de services (par exemple, communication autour du Plan de Continuité de l'Activité). |
| **Structure** | Pratiques définies par le niveau de maturité :<br>• Niveau 1 : fournir empiriquement le service ;<br>• Niveau 2 : satisfaire aux exigences de façon cohérente ;<br>• Niveau 3 : gérer la performance de l'organisation ;<br>• Niveau 4 : accroître pro activement la valeur ;<br>• Niveau 5 : maintenir l'excellence. | Deux types de rapport :<br>Type 1 :<br>• Opinion de l'auditeur sur la conception des contrôles supportant les objectifs de contrôle ;<br>• Informations générales sur l'audité;<br>• Liste des objectifs de contrôle choisis par l'audité ;<br>• Description des objectifs et activités de contrôle ;<br>• Informations complémentaires.<br>Type 2, idem que le type 1 avec en plus :<br>Opinion de l'auditeur sur l'efficacité opérationnelle des objectifs de contrôle et contrôles associés (sur une période d'au moins six mois). |

| | eSCM-SP v2 | SAS 70 |
|---|---|---|
| **Couverture** | Les trois phases du cycle de vie du sourcing de services :<br>• Démarrage ;<br>• Fourniture ;<br>• Réversibilité. | Le fournisseur choisit les objectifs de contrôle qui sont au périmètre. |

Il s'avère que le rapport SAS 70 peut ne pas renseigner sur l'efficacité des contrôles vraiment critiques à l'assurance raisonnable des activités d'externalisation (ou d'outsourcing). Cette limite de la norme SAS 70 réside dans l'absence de directive quant au choix des objectifs de contrôle à prendre en considération. En quelque sorte, l'apport du référentiel eSCM peut contribuer à une version améliorée du rapport SAS 70 à sa forme actuelle sur le sourcing IT. Le déploiement des pratiques eSCM-SP soutient l'atteinte des objectifs de contrôle en matière de sourcing IT [8].

L'ISACA propose un référentiel de pratiques professionnelles en matière de contrôles et d'audit IT et notamment de sourcing : ITAF 3630.6 [9].

Nous présentons ci-après les objectifs de contrôle à considérer dans le périmètre de l'évaluation selon la norme SAS 70 ainsi que les pratiques eSCM-SP associées [10].

Cette représentation s'inspire des travaux réalisés par le CIGREF et l'IFACI sur le thème du contrôle interne du système d'information des organisations [11].

| Objectif de contrôle | Domaine eSCM-SP | Ce que les pratiques d'eSCM-SP développent… |
|---|---|---|
| | Pratiques Permanentes | |
| PO4 - Définir les processus, l'organisation et les relations de travail | Gestion des connaissances | Les pratiques concernées traitent du système de gestion de la connaissance au sens large, y compris les outils, les modes de communication, les allocations de ressources et les responsabilités. Elles permettent de vérifier l'institutionnalisation des pratiques, les ressources dédiées, l'implication des parties prenantes, le maintien et l'amélioration des processus, la communication, le niveau de compétence, les responsabilités et les rôles définis. |
| PO7 - Gérer les ressources humaines de l'informatique | Gestion des ressources humaines | Les pratiques concernées traitent de l'interaction entre l'opérationnel et les ressources humaines. Elles permettent de vérifier les rôles, les délégations, les responsabilités, l'assignation du personnel, le plan d'évolution du personnel, le plan de formation, le plan de développement du personnel, le sourcing des compétences ponctuelles, l'encouragement de l'innovation, le suivi des objectifs individuels annuels, le plan de développement des carrières, le plan d'avantages, le traitement des différences culturelles. |

| Objectif de contrôle | Domaine eSCM-SP | Ce que les pratiques d'eSCM-SP développent… |
|---|---|---|
| PO9 - Évaluer et gérer les risques | Gestion des risques | Les pratiques concernées traitent des risques et menaces pour le fournisseur et ses engagements, ainsi que pour le métier du client. Elles permettent de vérifier : le plan des risques potentiels et des réponses, le plan de reprise d'activité, les procédures de continuité de service, les priorités de traitement, la maitrise des couts, le traitement de la sécurité des données, les accès physiques, la confidentialité et la traçabilité, la propriété intellectuelle, la connaissance des risques liés au métier du client, l'implication des parties prenantes et l'institutionnalisation des réponses. |
| AI2 - Acquérir des applications et en assurer la maintenance | Gestion de la technologie | Les pratiques concernées traitent du mode de gestion des technologies embarquées dans les services proposés. Elles permettent de vérifier la maitrise des actifs, les outils nécessaires et leur utilisation, l'existence des inventaires et leur mise à jour, les procédures de suivi des changements, le suivi des licences, la gestion du stock, la gestion du cycle de vie des technologies. La gestion de la technologie se réalise en intégrant les systèmes tout en prévoyant la séparation Client/Fournisseur lors de la réversibilité. |
| AI5 - Acquérir des ressources informatiques | Gestion de la technologie | Les pratiques concernées traitent de l'approvisionnement des actifs. Elles permettent de vérifier le traitement des demandes d'approvisionnement, l'identification des alternatives, la sélection des fournisseurs potentiels, la gestion des dépendances avec les fournisseurs, le suivi des non-conformités en rapport avec la technologie, le mode de gestion des actifs en relation avec les clients, la mutualisation et l'optimisation des systèmes. |
| DS4 - Assurer un service continu | Gestion des risques | Les pratiques concernées traitent des risques et menaces pour le fournisseur et ses engagements ainsi que pour le métier du client. Elles permettent de vérifier : la gestion des priorités entre les engagements, le plan de continuité, les tests du plan de continuité, les ressources concernées. |
| DS2 - Gérer les services tiers | Gestion des relations | Les pratiques concernées traitent de l'interaction entre un fournisseur et ses sous-traitants. Elles permettent de vérifier les procédures de sélection des sous-traitants, l'existence et l'application des critères de sélection, le mode de décision, la documentation des relations, les rôles, les critères de performance, les outils de suivi, l'existence de procédures de dispute, l'enregistrement de la qualité et des performances délivrées. |
| DS5 - Assurer la sécurité des systèmes | Gestion des risques | Les pratiques concernées traitent de la sécurité d'accès au système d'information. Elles permettent de vérifier les règles d'accès aux plateformes et applications, la gestion des mots de passe, les politiques et moyens d'accès physiques, les exigences physiques et logiques, la liste des actifs à protéger, les risques en fonction des actifs, les approbations dans les procédures d'allocation des mots de passe, la maitrise des accès utilisateurs en fonction de leur métier, la gestion des arrivées et des départs. |
| DS9 - la configuration | Gestion de la technologie | Les pratiques concernées traitent de la gestion des configurations. Elles permettent de vérifier l'identification des composants à |

| Objectif de contrôle | Domaine eSCM-SP | Ce que les pratiques d'eSCM-SP développent… |
|---|---|---|
| | | suivre, le maintien des outils à jour avec les configurations, l'évolution des configurations en fonction des changements, l'optimisation de la technologie par la contrôle des performances. |
| DS11 - Gérer les données | Gestion des risques | Les pratiques concernées traitent de la gestion des données du Client. Elles permettent de vérifier l'identification des données personnelles, les règles légales auxquelles se conformer, les procédures en interaction avec le Client pour les exigences métier, les priorités d'action en cas de risques concernant les données, le plan de risques entre les engagements, la traçabilité d'accès aux données, les règles de confidentialité, les droits d'accès, les outils sécurité en place, la propriété des données. |
| SE1 - Surveiller et évaluer la performance des SI | Gestion de la performance | Les pratiques concernées traitent de la performance de l'engagement par rapport aux attentes du métier et de l'organisation du client. Elles permettent de vérifier l'identification et le suivi des objectifs de performance, la communication, la collecte des données, les revues périodiques des performances, le processus de vérification des performances, le suivi des défauts de performance et les plans d'actions associés, les plans d'amélioration, l'atteinte du dossier métier (business case) d'origine, les bases de référence d'analyse des écarts, les benchmarks et les plans d'innovation. |
| DS12 - Gérer l'environnement physique | Gestion des ressources humaines | Les pratiques concernées traitent de l'environnement de travail nécessaire aux individus pour qu'ils travaillent dans de bonnes conditions. Elles permettent de vérifier l'identification de l'environnement de travail nécessaire, le maintien des locaux, la gestion des disputes et des conflits, le plan des locaux en fonction des fluctuations de l'organisation et de ses engagements. |
| | Phase de Démarrage | |
| PO4 - Définir les processus, l'organisation et les relations de travail | Conception et Déploiement du Service | Les pratiques concernées traitent de la mise en place des services liés à l'engagement pour le bénéfice du client. Elles permettent de vérifier l'anticipation de l'organisation, les processus opérationnels, la planification, les rôles et responsabilités, l'implémentation des outils pour supporter la relation. |
| DS1 - Définir et gérer les niveaux de services | Contractualisation | Les pratiques concernées permettent de réaliser un contrat. Elles permettent de vérifier la contractualiser des niveaux de service en fonction du catalogue de service retenu, la mise en place des procédures de modification de périmètre, la formalisation des avenants, la mise en place d'un suivi qualité impactant (ou non) les prix, l'analyse concurrentielle pour maintenir ses offres au niveau du marché. |
| | Phase de Fourniture | |
| PO8 - Gérer la qualité | Fourniture du Service | Les pratiques concernées se concentrent sur la qualité des services. Elles permettent de vérifier la cohérence des plans de livraison en rapport avec les attentes initiales du client, la bonne tenue des niveaux de service, le suivi des factures en regard du budget prévu, le suivi des pénalités, les apports en innovation, la gestion des relations. |

| Objectif de contrôle | Domaine eSCM-SP | Ce que les pratiques d'eSCM-SP développent… |
|---|---|---|
| AI6 - Gérer les changements | Fourniture du Service | Les pratiques concernées traitent des changements des services délivrés. Elles permettent de vérifier les procédures de changement, le suivi des demandes de changements, l'analyse des risques à la mise en place, la valorisation des changements, l'impact sur les services en place, l'obtention des approbations, la modification des contrats par des avenants. |
| DS1 - Définir et gérer les niveaux de services | Fourniture du Service | Les pratiques concernées traitent des niveaux de service. Elles permettent de vérifier les procédures de suivi des coûts, le suivi du budget, l'utilisation des bons outils, la vérification des niveaux de service, la collecte et l'analyse des données, l'identification des variations, la mise en place des actions correctrices. |
| DS10 - Gérer les problèmes | Fourniture du Service | Les pratiques concernées traitent des incidents et problèmes au sens ITIL, mais aussi des anomalies dans la relation. Elles permettent de vérifier l'identification, le classement et l'analyse des problèmes connus, la documentation et l'outillage de suivi des problèmes et des plans d'actions, la prévention des problèmes, la mise en place d'un plan d'actions préventives, l'audit des budgets de l'engagement, et les procédures de traitement des désaccords (disputes). |
| DS13 - Gérer l'exploitation | Fourniture du Service | Les pratiques concernées traitent de la fourniture des services. La fourniture est très liée au type de service délivré, aussi eSCM traite les fondamentaux. Ces pratiques permettent de vérifie la livraison des services définis dans les plans (BPO, Tierce Maintenance Applicative, Infogérance, Exploitation, Centre de Services), la gestion des mises en production, le suivi des indisponibilités, les ressources et compétences adéquates, les outils permettant le support des processus incidents/problèmes/changements/mise en production/exploitation. |
| | Phase de Réversibilité | |
| DS4 - Assurer un service continu | Réversibilité | Les pratiques concernées traitent du transfert d'un (des) service(s), soit du client vers le fournisseur, soir du fournisseur vers le client. Elles permettent de vérifier l'existence du plan de réversibilité, le plan de continuité des services couvrant la période de transfert des services, l'identification des compétences clés, le transfert des ressources humaines, le transfert des actifs liés au service, l'identification et le transfert de la connaissance et des savoir-faire. |

## Annexe D : Exemple de lettre d'opinion d'un rapport SAS 70

### Rapport Type 1

Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's controls that may be relevant to a user organization's internal controls as it relates to an audit of financial statements (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and (3) such controls had been placed in operation as of December 31, 2010. The control objectives were specified by the management of XYZ Service Organization. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion in the operating effectiveness of any aspects of YYZ Service Organization's controls, individually or in the aggregate.

In our opinion, the attached description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's controls that had been placed in operation as of December 31, 2010. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

The description of controls at XYZ Service Organization is as of December 31, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls as the Service Organization is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.
This report is intended solely for use by management of XYZ Service Organization, its customers, and the independent auditors of its customers.

### Rapport Type 2

We have examined the accompanying description of controls related to the processing of investment transactions, including …. of XYZ Service Organization. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's controls that may be relevant to a user organization's internal controls as it relates to an audit of financial statements (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied

with satisfactorily, and (3) such controls had been placed in operation as of June 30, 2010. The control objectives were specified by the management of XYZ Service Organization. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's controls that had placed in operation as of June 30, 2010. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section X, to obtain evidence about their effectiveness in meeting the control objectives, described in Section X, during the period from January 1, 200710 to June 30, 2010. The specific controls and the nature, timing, extent, and results of the tests are listed in Section X. This information has been provided to user organizations of XYZ Service Organization and to their auditors to be taken into consideration, along with information about the internal control of user organizations, when making assessments of control risk for user organizations. In our opinion the control that were tested as described in Section X were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section X were achieved during the period from January 1, 2010 to June 30, 2010.

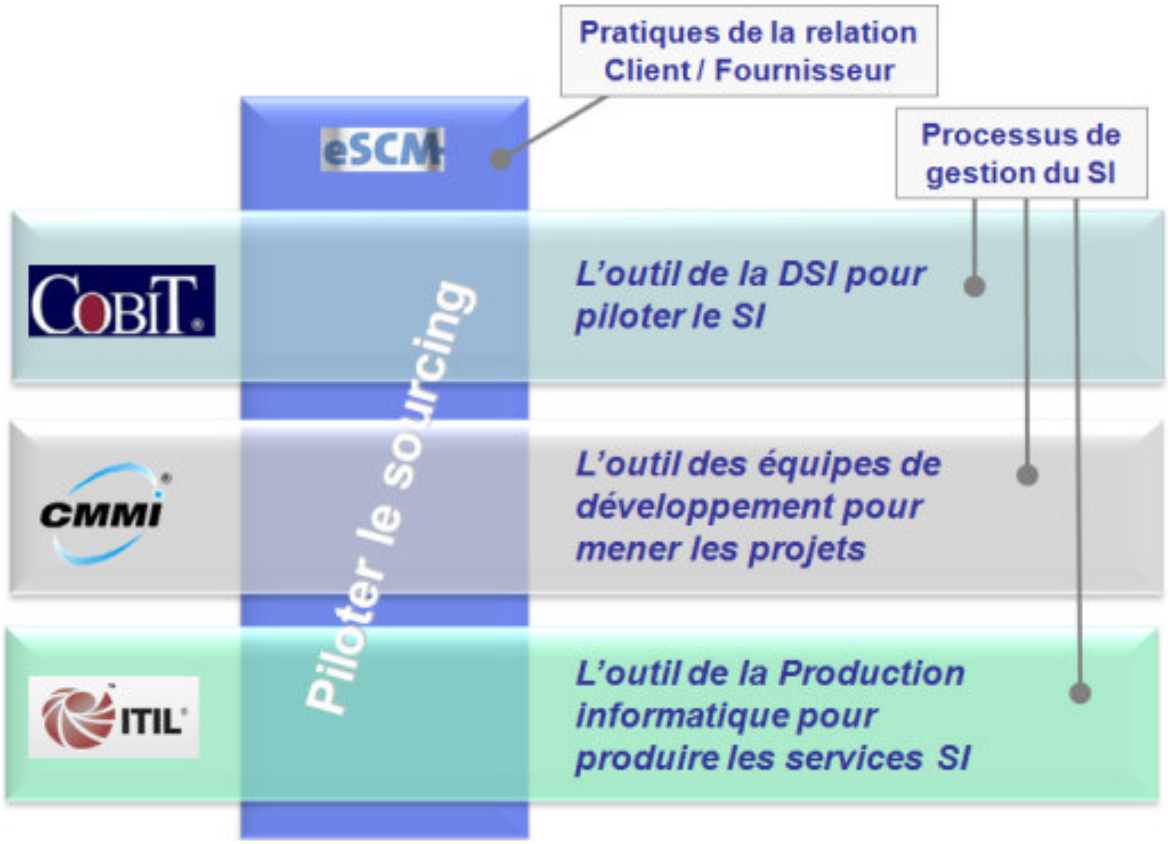
The relative effectiveness and significance of specific controls at XYZ Service Organization and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls at XYZ Service Organization is as of June 30, 2007 and the information about tests of the operating effectiveness of specific controls covers the period from January 1, 2010 to June 30, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specific controls at the Services Organization is subject to inherent limitations, and, accordingly, errors or irregularities may occur and not be detected. Furthermore, the projection of any conclusions, based on our finding, to future periods is subject to the risk may alter the validity of such conclusions.

This report is intended solely for use by the management of XYZ Service Organization, its customers, and the independent auditors of its customers.

## Annexe E : COBIT, ITIL, CMMi

On peut représenter l'édifice des référentiels de contrôles et de bonnes pratiques en matière de systèmes d'information, de la manière suivante :

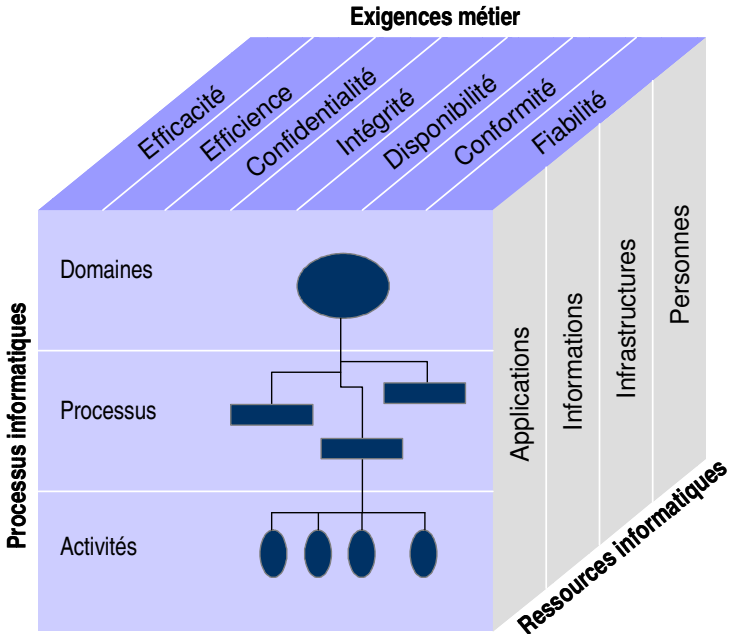



### CobiT

CobiT (Control Objectives for Information and related Technology – Objectifs de contrôle de l'Information et des Technologies Associées) est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information.

Publié en 1996 par l'ISACA, Cobit est un cadre de référence international conçu à partir des meilleures pratiques mondiales en termes d'audit et de maîtrise des SI. Il aide les dirigeants à comprendre et à gérer les risques relatifs à l'informatique en les inscrivants dans un cadre de gouvernance. CobiT constitue un référentiel complet de processus permettant de décrire l'ensemble des activités d'une DSI.

CobiT propose aussi un référentiel permettant de mettre sous contrôle l'ensemble des opérations liées à l'informatique. Il permet en fonction des besoins d'adresser les problématiques de la DSI selon les processus, les ressources et les exigences métier.




Les processus : le modèle décompose l'ensemble des activités d'une DSI en 34 processus regroupés en 4 domaines. Chacun des processus propose des activités clefs et des objectifs de contrôle.

Les ressources ventilées en 4 groupes :
Information : données dans leur sens le plus large (internes et externes, structurées ou non, graphiques, sons,…) ;
Applications : ensemble des procédures manuelles et programmées ;
Infrastructure : matériel, système d'exploitation, systèmes de gestion de base de données, réseau, multimédia, environnement (ressources qui hébergent les systèmes informatique et qui leur servent de support) ;
Personnels : compétence, efficacité,…

Les besoins de l'entreprise :

| | |
|---|---|
| Impératifs de Qualité | Efficacité |
| Impératifs de Sécurité | Confidentialité<br>Intégrité<br>Disponibilité |
| Impératifs économique et fiduciaire | Efficience<br>Fiabilité<br>Conformité |

## CMMi

CMMi (Capability Maturity Model + Integration) est un modèle de référence proposant aussi un ensemble structuré de bonnes pratiques, destiné à appréhender, évaluer et améliorer les activités des entreprises d'ingénierie informatique.

CMMi, comme eSCM, a été développé par l'université Carnegie Mellon. Initialement pour appréhender et mesurer la qualité des services rendus par les fournisseurs de logiciels informatiques du Département de la Défense US (DoD), il est maintenant largement employé par les entreprises d'ingénierie informatique, les Directeurs des Systèmes Informatiques et les industriels pour évaluer et améliorer leurs propres développements de produit. Comme son nom l'indique, le modèle CMMi est basé sur une échelle de maturité à 5 niveaux.

## ITIL

ITIL (Information Technology Infrastructure Library pour "Bibliothèque pour l'infrastructure des technologies de l'information") est un ensemble d'ouvrages recensant les « bonnes pratiques » ("best practices") pour la gestion des services informatiques. Dans sa dernière version (V3), ITIL met donc l'accent sur la maîtrise du cycle de vie des services.

Ces bonnes pratiques traitent principalement des activités de production des services, principalement dans un contexte interne à l'entreprise.

# Glossaire

| | |
|---|---|
| **Aptitude** (eSCM) | L'aptitude au sourcing de l'organisation du client se traduit par une gestion efficace de ses activités de sourcing et des relations avec ses prestataires. |
| **Audit interne** | L'audit interne est une activité de contrôle réalisée par un département dédié et indépendant au sein de l'entreprise visant à certifier la régularité de la gestion de l'entreprise relativement au suivi de ses politiques, de ses procédures et du cadre légal dans lequel évolue l'entreprise. |
| **Benchmark** (eSCM) | Standard de référence utilisé pour faire une comparaison. Mesurer ou comparer les performances d'une entité à un standard de référence. |
| **Business case** | Proposition structurée d'une fonction métier ou activité destinée aux décideurs. Comprend une analyse de la performance des processus métier, les besoins associés ou problèmes, solutions alternatives, hypothèses, contraintes, et une analyse des coûts/bénéfices ajustée aux risques. |
| **Centre de Services Partagé** | Centre de services, dédié à une activité spécifique, et rendant possible la mutualisation avec d'autres organisations. |
| **Certification** (eSCM) | La certification d'une organisation, dans le modèle eSCM, est le fruit d'une évaluation du niveau d'aptitude eSCM de l'organisation. Des certifications d'individus sont possibles indépendamment de la démarche de certification d'une organisation. |
| **Client** | Entité ou personne morale à laquelle un prestataire fournit des services de sourcing. |
| **Composant de processus** | Guide ou document de directives ou recommandations (procédures, processus, politiques, …) ou éléments nécessaires (référentiels, formations, outils) à l'implémentation de cette documentation. |
| **Contrôle** (SAS 70) | Toute activité mise en œuvre par l'entreprise visant à participer à la maîtrise de ses risques et à sécuriser l'atteinte de ses objectifs. |
| **Cycle de vie du sourcing** (eSCM) | Un des quatre attributs temporels, permettant le classement d'une pratique eSCM-SP dans une des phases du cycle de vie de la relation client/fournisseur (permanent, démarrage, fourniture, réversibilité). Les pratiques permanentes sont les seules à faire l'objet d'exécution tout au long du cycle de vie de sourcing. |
| **Directive** | Des exigences de l'organisation portant sur la mise en œuvre de pratiques de manière obligatoire. |
| **Domaine d'Aptitude** (eSCM) | Un des onze regroupements des pratiques eSCM-SP qui représentent des domaines clés pour la gestion du sourcing. |
| **eSourcing** (eSCM) | Type de sourcing qui s'appuie sur les technologies de l'information dans la production et la fourniture du service rendu à l'organisation du client. |
| **Externalisation** (eSCM) | Stratégie de sourcing pour laquelle la gestion et l'administration d'une activité de l'organisation est déléguée à un prestataire. |
| **Externalisation de processus métier (BPO)** | Prise en charge d'un processus métier du client par un prestataire externe qui en détient la propriété, l'administre, et le gère, sur la base de métriques de performance mesurables. |

| | |
|---|---|
| **Guide** | Ensemble structuré de directives, manuels ou recommandations fondés sur les meilleures pratiques de sourcing. |
| **ITSqc** (eSCM) | Société Américaine (ITSqc LLC), essaimage de l'Université de Carnegie Mellon (notamment le Centre de Qualification des Services de Technologie de l'Information), qui exploite les droits des modèles eSCM-CL et eSCM-SP et qui prend en charge leurs évolutions. |
| **Meilleure pratique** | Une façon de procéder, d'usage et approuvée, permettant d'améliorer de manière significative la capacité à atteindre des objectifs. |
| **Niveau d'aptitude** (eSCM) | Un des cinq niveaux d'aptitude du modèle eSCM-SP qui décrit la trajectoire d'amélioration pour le prestataire. |
| **Objectif de contrôle** (SAS 70) | Ensemble cohérent de contrôle visant à couvrir un risque. |
| **Objectif métier** | Un objectif, par forcément formalisé et valorisé, de l'entreprise destiné à fixer une orientation ou un cap. |
| **Partie prenante** | Groupe d'individus concerné par, et dans une certaine mesure garant de, la fourniture de services ou produits attendus et le maintien durable des résultats prévus. |
| **Pratique** | Un ensemble d'activités dont l'exécution par l'organisation du client est recommandée afin d'obtenir une relation de sourcing plus efficace. |
| **Pratiques permanentes** (eSCM) | Pratiques eSCM effectuées tout le long du cycle de vie du sourcing. |
| **Prestataire ou fournisseur de service** | Une entité qui fournit, au client, des services qui s'appuient sur les technologies de l'information. Le prestataire est considéré comme faisant l'objet d'un management distinct de l'organisation du client. |
| **Processus métier** | Ensemble de tâches ou d'activités entreprises par l'organisation du client dans l'atteinte d'un but précis (vente ou fourniture de service, distribution de produits, facturation, comptabilité). Les processus métier d'une organisation sont généralement interdépendants. |
| **Réversibilité** (eSCM) | Phase du cycle de vie concernant la fin du sourcing, avant de mettre fin au contrat. Cette phase permet le transfert des activités confiées au prestataire vers l'organisation du client ou un tiers désigné. |
| **SAS 70** | Standards d'évaluation du contrôle interne d'un fournisseur de services dont le rapport constitue une opinion indépendante en général émise par un cabinet d'audit comptable. |
| **Service** | Prestation immatérielle et mesurable, délivrée part un prestataire à un client. |
| **Sourcing** | Approvisionnement (client), ou fourniture de services à une organisation cliente, par une entité prestataire interne, externe ou une combinaison des deux. |
| **SSAE 16** | Le "Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization" est une norme américaine émise en avril 2010 dans sa version définitive, visant à remplacer le SAS 70. C'est le pendant américain de la norme internationale ISAE 3402. |
| **Valeur métier** | Mesure relative des performances et des bénéfices pour les parties prenantes. |

# Références et bibliographie


[1] HYDER Elaine B., HESTON Keith M., PAULK Mark C., The eSCM-SP v2.01: Model Overview. IT Services Qualification Center, Carnegie Mellon University.

[2] HYDER Elaine B., HESTON Keith M., PAULK Mark C., The eSCM-SP v2.01: Practice Details. IT Services Qualification Center, Carnegie Mellon University.

[3] HEFLEY William E., LOESCHE Ethel A., The eSCM-CL v1.1: Model Overview. IT Services Qualification Center, Carnegie Mellon University.

[4] HEFLEY William E., LOESCHE Ethel A., The eSCM-CL v1.1: Practice Details. IT Services Qualification Center, Carnegie Mellon University.

[5] eSCM-CL, le modèle d'aptitude à l'eSourcing pour les clients : Le Guide. AE-SCM publications, ISBN 978-2-9532421-0-2.

[6] eSCM-SP, le modèle d'aptitude à l'eSourcing pour les prestataires : Le Guide. AE-SCM publications, ISBN 978-2-9532421-1-9.

[7] Service Organizations: Applying SAS No. 70, as Amended – AICPA Audit Guide

[8] eSCM et Sourcing IT. Le Référentiel de la relation client-fournisseur. Georges Epinette, Benoît Leboucher, Pierre-Dominique Martin, ISBN 978-2-10-052882-0.

[9] ITAF : A Professional Practices Framework for IT Assurance , 2008 – ISACA & ITGI, ISBN 978-1-60420-036-2

[10] Comparing the eSCM-SP v2 and COBIT. IT Services Qualification Center, Carnegie Mellon University.

[11] Le contrôle interne du système d'information des organisations. CIGREF - IFACI. ISBN 978-2-915042-02-3

## Webographie

| | |
|---|---|
| Ae-SCM | Association francophone pour la promotion des bonnes pratiques de sourcing eSCM.<br>http://www.ae-scm.fr/ |
| AFAI | Association française de l'audit et du conseil informatiques et chapitre français de l'ISACA.<br>http://www.afai.fr/ |
| AICPA | American Institute of Certified Public Accountants : ordre des experts comptables à l'origine de la norme SAS 70.<br>www.aicpa.org |
| IAASB | International Auditing and Assurance Standard Board<br>http://www.iaasb.org |
| IFAC | Organisation mondiale de la profession comptable dont le site propose une base documentaire des normes et standards.<br>http://fr.ifac.org/ |
| ISACA | Information Systems Audit and Control Association (ISACA): association pour la promotion, le développement et l'usage de connaissances et de référentiels de bonnes pratiques en matière d'audit, de contrôle et de gouvernance de systèmes d'information.<br>http://www.isaca.org/ |
| ITSqc | ITSqc LLC est la société Américaine en charge de délivrer les certifications eSCM, individuelles ou d'organisation.<br>http://www.itsqc.org/ |
| ISAE 3402 | Site dédié à l'ISAE3402<br>http://www.isae3402.com |
| ITGI | IT Governance Institute : organisme de recherche dont la mission principale consiste à améliorer la gouvernance des systèmes d'information afin de soutenir les missions et les objectifs des entreprises.<br>http://www.itgi.org/ |
| SAS 70 | Site dédié à la norme SAS 70 et à l'assurance des organisations de services.<br>http://sas70.com/ |

Association (loi de 1901) pour la promotion des bonnes pratiques de sourcing

25, rue du Maréchal Foch
78000 Versailles
France
www.ae-scm.com

contact : ae-scm@laposte.net

Association Française de l'Audit et du Conseil Informatiques

164 bis, avenue Charles de Gaulle
92200 Neuilly-sur-Seine
France
www.afai.fr