

## ÉDITO

**L**a maîtrise des risques liés à l'informatique est devenue une chose trop sérieuse pour être confiée uniquement aux managers IT. Face à une DSI aux budgets sous pression, de multiples acteurs interviennent dans la gestion des risques. Les responsabilités de chacun doivent être soigneusement orchestrées. Des référentiels aideront, mais il faudra les considérer avec pragmatisme. Nous vous souhaitons de bonnes vacances et nous vous retrouverons fin août pour un numéro sur l'intelligence économique.

## SOMMAIRE

## RETOUR D'EXPÉRIENCES

**La maîtrise des risques IT dépend du dialogue dans l'entreprise**

p. 1 à 6

## GESTION DE CARRIÈRE

**Hervé Gouëzel de BNP Paribas : « le DSI est un chef d'entreprise »**

p. 8 à 9

## INTERNATIONAL

**Incitez votre entreprise à rechercher votre successeur en interne**

p. 15 à 16

## SYSTÈME D'INFORMATION ET MÉTIERS

**DG de Randstad : « Le DSI doit parler fort »**

p. 19 à 20

## HUMEUR

p. 21

## RETOUR D'EXPÉRIENCES

## La maîtrise des risques IT dépend du dialogue dans l'entreprise

*Le risque informatique est un risque d'entreprise. Sa maîtrise passe par un meilleur dialogue entre les acteurs concernés, dont la DSI. L'organisation et certains référentiels apportent des éléments de réponse. En revanche, la réglementation et les certifications ont une influence modérée.*

**Le risque lié aux systèmes d'information est un risque d'entreprise.** Doit-il être maîtrisé directement par la DSI ? Les témoignages montrent que la responsabilité est souvent éclatée entre de multiples intervenants, dont les équipes IT. Comment les rôles de chacun s'organisent-ils ? Il n'existe pas de solution unique en la matière lorsque l'on écoute la Caisse des dépôts et Consignations, le groupe de protection sociale AG2R La Mondiale, le leader du nucléaire Areva ou le spécialiste des services pétroliers Schlumberger.

### *Il est impossible de tout protéger*

« Le risque informatique est avant tout un risque métier découlant de l'utilisation de l'informatique » définit Jean-Louis Bleicher, consultant et ancien responsable du pôle sécurité et continuité d'activité du Groupe Banque Populaire. Et l'informatique est aujourd'hui une ressource aussi indispensable aux activités de l'entreprise que l'électricité. En outre, le risque informatique évolue rapidement sous la pression du Web 2.0 et du Cloud Computing. « Le système d'information s'ouvre tout azimut, on doit accepter l'impossibilité de tout protéger. Il faut se concentrer sur l'essentiel » conseille **Alain Bouillé, RSSI (Responsable de la sécurité des systèmes d'information) de la Caisse des Dépôts et Consignations.** ▶

### 5 DÉCIDEURS IT TÉMOIGNENT

**Alain Bouillé**Caisse des dépôts et  
Consignations**Jean-François Louâpre**

AG2R La Mondiale

**Julien Camus**

Schlumberger

**Sébastien Bombal**

Areva

**Carlos Martin**

Groupe Carrefour



## Identifier ce qu'il faut protéger est un effort de longue haleine

**Alain Bouillé**

Caisse des dépôts

« Identifier l'essentiel est alors un effort de longue haleine. Il faut pour cela entamer un travail de fond, sous la forme de dialogue, notamment avec les métiers et l'audit » précise-t-il.

Ce dialogue est d'autant plus complexe que la liste des acteurs impliqués dans la gestion des risques liés à l'informatique est longue : métiers, direction informatique, direction juridique, audit interne, direction de la sécurité et de la continuité d'activité, direction des risques, direction de la conformité ou encore, direction des assurances, jusqu'au conseil d'administration et à la direction générale.

**Dès lors, comment mettre en place les fondamentaux de la maîtrise des risques ?** Trois leviers d'action existent : l'organisation, les référentiels et la réglementation. Mais aucun d'entre eux n'apporte de solution miracle. Un extrême pragmatisme s'impose en privilégiant les relations humaines plutôt que l'organisation, et les référentiels faits maison plutôt que les normes. On évitera la dictature de la réglementation et on réservera les démarches de certification aux rares situations qui l'imposent.

### Positionner les différents acteurs

Comment est organisée la sécurité IT dans les entreprises ? « Il n'y a pas d'organisation type » répond Jean-Louis Bleicher. Il précise : « Sur les six premiers groupes bancaires français, deux ont un rattachement de la sécurité IT à la direction du risque, deux autres à la DSI, et deux autres à la direction des opérations ou des ressources. » Selon lui, ces trois types d'organisation interne se justifient.

« Toutes ces directions participent à la gestion du risque. L'important est que les missions des acteurs concernés puissent être correctement assurées » rassure-t-il. Car, au-delà de l'organisation, le plus important est de définir des règles de fonctionnement. Ceci dit, il y aura des frictions, car les objectifs sont souvent divergents. La DSI a des budgets sous contrainte alors que la direction du risque et la Sécurité des Systèmes d'Information (la SSI) ont pour mission de réduire les risques, ce qui génère forcément des coûts.

**À la Caisse des Dépôts et Consignations, la SSI est intégrée à la direction des risques.** Elle est donc indépendante de la DSI qui est le pilote des projets transverses et de la direction informatique, organisée pour sa part en GIE. « Un RSSI qui est indépendant de la DSI évite le risque d'être à la fois juge et parti mais il peut tomber dans un autre travers, celui d'être isolé et éloigné des problématiques informatiques » relève Alain Bouillé. Comment résoudre cette difficulté ? « Il lui faut redoubler d'énergie pour être près du DSI et rester présent dans tous les projets. » Et de conclure : « notre organisation fonctionne très bien même si elle n'a pas la prétention d'être considérée comme un modèle. Il faut simplement mettre la SSI là où elle a des chances d'être la plus efficace. »

## 11 BONNES PRATIQUES POUR MAÎTRISER LES RISQUES IT par Jean-Louis Bleicher

- 1 La gouvernance du management des risques doit tenir compte des contraintes de l'entreprise,
- 2 Attribuer des rôles et des responsabilités à tous les acteurs concernés,
- 3 Mettre en place des instances de pilotage et de coordination, avec des structures telles que le comité des risques ou le comité sécurité,
- 4 S'appuyer sur un référentiel reconnu de management des risques et éventuellement des référentiels spécifiques qui devront s'articuler entre eux,
- 5 Analyser les risques d'abord sur les nouveaux projets puis passer à tous les systèmes,
- 6 Mener une démarche active d'anticipation et de veille vis-à-vis des nouvelles menaces, en achetant des études et des services de veille ou en échangeant avec d'autres entreprises,
- 7 Éviter de traiter les risques de façon trop théorique en suivant les normes au pied de la lettre. Au contraire, les traiter de façon opérationnelle, via une politique de sécurité informatique et un plan de continuité d'activité adéquats,
- 8 Traiter les risques en gérant efficacement les vulnérabilités, les incidents et les crises,
- 9 Assurer une surveillance de l'évolution des risques par un suivi des incidents, un contrôle des règles et des indicateurs situés au niveau de la DSI et des métiers afin de mesurer les risques effectifs et vérifier qu'ils restent compatibles avec l'appétence de l'entreprise au risque,
- 10 Sensibiliser et former tous les acteurs impliqués dans la gestion du risque et communiquer de manière exhaustive et cohérente au travers de tableaux de bord,
- 11 Améliorer continuellement, de façon itérative, l'ensemble du dispositif dédié à la gestion des risques.



## Le dialogue de la DSI avec la SSI relève d'un équilibre à trouver

Jean-François Louâpre  
AG2R La Mondiale

**De même à la société de prévoyance AG2R La Mondiale, le RSSI travaille au sein de la direction des risques.** La société emploie 6 800 collaborateurs au service de huit millions de personnes ou ayants droits, pour 13,7 milliards d'euros de cotisations. **Jean-François Louâpre est aujourd'hui responsable sécurité à la direction des risques d'AG2R La Mondiale.** Il était auparavant rattaché à la DSI d'AG2R. C'est à l'occasion du rapprochement de La Mondiale et d'AG2R en 2008 que les organisations ont été remises en cause.

« *Je me suis éloigné de la DSI mais j'ai gardé les mêmes habitudes de collaboration et nous intervenons toujours à un niveau de détails assez poussé* », précise Jean-François Louâpre. Il ajoute : « *La communication entre les différents acteurs relève davantage d'une question de relations humaines et de confiance que d'organisation. C'est un équilibre à trouver, quel que soit le positionnement de la SSI.* »

## Le Risk Management suit les actions

Ce rattachement de la sécurité IT à la gestion des risques se retrouve chez Schlumberger, avec une variante. Ce géant international emploie 83 000 personnes dans le monde pour un chiffre d'affaires de 22,7 milliards de dollars. Le Risk Management porte les processus de réduction des risques, dont l'informatique. Le Risk Management suit les actions à entreprendre, avec des plans détaillés et des certifications. Il est rattaché à la direction générale, qui considère que cette entité est la mieux placée pour gérer l'ensemble des risques principaux de chaque niveau de management : géographique, métiers ou fonctions.

« *La cartographie des risques est orientée concrètement sur les plans d'action. La taille et la diversité géographique et fonctionnelle de Schlumberger représentent un défi. Un suivi rigoureux des mesures de prévention et de protection permet un meilleur contrôle* », précise **Julien Camus, Deputy Risk and Insurance Manager chez Schlumberger** et vice président de la commission en charge des systèmes d'information à l'AMRAE (Association pour le Management des Risques et des Assurances d'Entreprises). Chez Schlumberger, le RSSI est donc rattaché au Risk Management. Il est également rattaché à la DSI. Ce double rattachement s'explique car la DSI est aussi « propriétaire » de ses risques et de ses actions. Mais les arbitrages sont réalisés par le comité exécutif des risques. Cela permet d'éviter les contraintes budgétaires lorsque cela est nécessaire. « *En pratique, la DSI, comme les autres fonctions de Schlumberger, s'appuie en partie sur le Risk Management pour prendre les décisions lorsque cela est nécessaire, que ce soit sur les grands projets ou pour la sélection des options techniques et organisationnelles majeures* », affirme Julien Camus.

Cette organisation où la DSI doit prendre en charge ses propres risques sous l'impulsion du Risk Manager, est également défendue par François Beaume, Risk Manager chez Dalkia, le pôle énergie de Veolia Environnement, et président de la commission SI de l'AMRAE. (Voir *CIO.pdf* numéro 16)

**La dichotomie entre l'évaluation des risques et la mise en place concrète des solutions IT existe aussi chez Areva** (Voir *CIO.pdf* numéro 8). Le leader du nucléaire emploie 50 000 personnes, et est présent dans une centaine de pays. La maîtrise de la sécurité IT a été séparée entre la définition du plan de traitement des risques d'un côté, et sa mise en œuvre opérationnelle de l'autre.

Patrick Clément, IS Security & Management system, est en charge de la première. **Sébastien Bombal, RSSI d'Areva**, est responsable de la seconde. « *Patrick Clément a défini la politique* ►



## La DSI s'appuie en partie sur le Risk Management

Julien Camus  
Schlumberger

## MANAGEMENT DES RISQUES : COMMENT IL FAUT S'Y PRENDRE

Jean-Louis Bleicher est consultant indépendant en management des risques opérationnels. Il dresse un constat pessimiste de la façon dont les risques sont identifiés et traités dans de nombreuses entreprises. Selon lui, le principal écueil réside dans un manque de coordination entre les nombreuses directions concernées. « *Ces acteurs travaillent avec des référentiels plus ou moins bien mis en œuvre et qui sont souvent incohérents entre eux* », explique-t-il. Il en découle de multiples rapports de management des risques qui ne sont pas consolidables. À cela s'ajoute une réglementation de plus en plus contraignante avec de nouvelles lois dont la prise en compte est réalisée par tel ou tel silo. Pour mettre fin à cette cacophonie, Jean-Louis Bleicher propose tout d'abord de mettre en œuvre une gouvernance du management des risques tenant

compte des contextes métiers et stratégiques de l'entreprise, de ses moyens financiers et humains et de sa tolérance au risque. « *En second lieu, il faut attribuer très précisément des rôles et des responsabilités à tous les acteurs concernés* », conseille-t-il. Enfin, il s'agit de mettre en place des instances de pilotage et de coordination, avec des structures ad hoc telles que comité des risques ou comité sécurité. Dans ce contexte, on définira un référentiel groupe ainsi éventuellement que des référentiels spécifiques. Au final, le processus de management des risques sera partagé par tous les intervenants concernés, avec une direction de la gestion des risques qui donnera le cap et s'assurera qu'il est tenu par tous. « *L'ensemble de ces dispositions impose une implication forte de la direction générale* », insiste Jean-Louis Bleicher. ■



## L'auditeur ne regarde pas les choix technologiques mais les mesures mises en place

Sébastien Bombal  
Areva

permettant d'être certifié ISO 27001, 14001 et 9001, et j'ai implémenté les mesures correspondantes », précise le RSSI.

**En aval, les audits vérifient que les risques ont été identifiés et que les plans d'actions ont été menés.** « L'auditeur regarde si nous avons sélectionné, mis en oeuvre ou budgété telle ou telle mesure mais il ne juge pas les choix technologiques ni les produits », ajoute Sébastien Bombal.

### Deux catégories d'entreprises

Plus globalement, le rattachement de la sécurité informatique à la gestion des risques est-il la tendance? Ce n'est pas ce que pense Pascal Antonini, associé chez Ernst & Young, qui effectue des audits d'entreprises dans le cadre de ses missions. Selon lui, tout est question de maturité du contrôle interne et de la culture de l'entreprise. Il avance qu'« il n'y a pas de modèle, l'organisation doit être fonction du contexte. » Ainsi, il sépare les entreprises en deux catégories. « Si la DSI n'est pas encore mûre en matière de sécurité et de contrôle, il est bon d'avoir une entité forte chargée du contrôle interne et de la sécurité. » En revanche, « dans les entreprises les plus matures, tous les acteurs avancent ensemble plutôt que de se surveiller mutuellement. La question du rattachement est alors plutôt une question de contexte et de culture. »

**Dans ce cadre, l'audit interne joue un rôle de garde-fou final.** D'ailleurs, Pascal Antonini considère que même lorsque la SSI est rattachée à la DSI - ce qui reste le cas le plus fréquent - l'audit et la gestion du risque rétablissent le balancier et évitent les dérives. A cela s'ajoute la réglementation. « La direction générale ne peut pas ignorer les différentes réglementations qui concernent le contrôle interne - LSF ou Sarbanes-Oxley », conclut-il.

Etonnamment, Alain Bouillé de la Caisse des dépôts estime que le cadre réglementaire a un impact limité: « Je ne justifierai jamais un projet uniquement parce que la réglementation m'y oblige mais aussi pour une couverture optimum des risques », déclare-t-il. La réglementation peut s'avérer cependant un véritable aiguillon. « Par exemple, lorsqu'un projet de gestion des accès et des identités a du mal à décoller, il peut être pertinent d'utiliser l'argument réglementaire mais il ne faut pas en abuser », illustre-t-il.

### L'audit recherche une cohérence globale

Une fois l'organisation et les solutions de sécurité mises en place, il faut passer l'épreuve du feu: l'audit. « Il faut au préalable définir le périmètre de l'audit. C'est-à-dire quelle est la stratégie mise en oeuvre afin de couvrir le risque identifié? » décrit Pascal Antonini.

**Le champ d'action d'un audit n'est donc pas réduit aux technologies mises en oeuvre ni au paramétrage des outils.** « Au-delà des audits ponctuels centrés sur ces aspects, il va y avoir aussi la recherche d'une cohérence de l'ensemble. Typiquement, on mènera d'abord un premier audit flash avec des questions très générales. Il offrira une première vision, avant ►

## LE GROUPE CARREFOUR DÉPLOIE UN TABLEAU DE BORD DES RISQUES IT À L'ÉCHELLE MONDIALE

Dans la continuité d'une démarche d'évaluation des risques liée notamment à la protection des données et à la continuité d'activité, Carrefour a mis en place un tableau de bord de la sécurité qui a d'abord pris la forme d'un outil Excel et qui sera prochainement disponible sur un site Intranet. Son objectif: identifier les risques et communiquer avec les acteurs concernés pour proposer des solutions appropriées. Ce tableau de bord est composé d'une série d'indicateurs qui sont renseignés par des programmes d'évaluation, d'auto-déclarations ou de vérifications techniques automatisées. Certains indicateurs sont quantifiables (procédures mises en place, logiciels déployés, mesures), tandis que d'autres sont qualitatifs. De plus, ils donnent des évolutions plutôt que des valeurs absolues. Les domaines ciblés: le réseau, les équipements, la continuité d'activité, la protection des données, la gestion des identités... « La présentation et la lisibilité sont communes à toutes les business units de Carrefour », précise Carlos Martin, Head of information systems Security du groupe Carrefour. Les

indicateurs sont identiques pour toutes les filiales et les organisations, afin que chacun puisse les renseigner de la même façon. Leur nature est constante dans le temps, même si les objectifs associés évoluent chaque année. Des vues différentes sont générées selon les destinataires: RSSI local, DSI, métiers ou directeur de filiale. Les RSSI et les DSI auront ainsi des vues plus techniques, tandis que les patrons de filiales auront des vues de plus haut niveau leur permettant de voir comment ils se positionnent par rapport à leurs collègues, en termes de niveau de risque général. Ce tableau de bord est incitatif, le but étant que chaque organisation ait la capacité de fixer ses priorités en matière de gestion de la sécurité en connaissance de cause. Le tableau de bord est mis à jour tous les 2 mois suite à des conférences téléphoniques avec les RSSI locaux. De plus, tous les deux ans, la DSSI vérifie sur place que les indicateurs correspondent à une réalité. Opérationnel depuis 18 mois, cet outil évolue. Par exemple, un niveau de maturité en matière de sécurité est en cours d'expérimentation. ■



## Il faut un triple contrôle par l'IT, la SSI et le dispositif de contrôle interne

**Alain Bouillé**  
Caisse des dépôts

un approfondissement », affirme-t-il. En somme, l'audit est un ensemble de missions qui permettront d'améliorer peu à peu les dispositifs de contrôle en termes d'organisation et de technologie.

**Pour sa part, Alain Bouillé tient à replacer l'audit dans un contexte plus large.** « Le risque informatique est un risque opérationnel comme un autre. Il doit donc répondre aux mêmes règles », explique-t-il en préambule. Le risque IT doit subir un triple contrôle : celui des métiers, de la SSI et par le dispositif de contrôle interne permanent et périodique. Ces contrôles sont complémentaires. « C'est une fusée à trois étages. Lorsqu'un métier déploie un service Web, l'informatique effectue un premier niveau de contrôle sur l'architecture qu'elle déploie et sur la qualité du code de l'application mise en ligne » décrit-il. Le deuxième niveau de contrôle est réalisé par la SSI. « La SSI procède à un test d'intrusion puis enfin l'audit, composante concrète du contrôle permanent, vérifiera périodiquement l'efficacité de ces deux niveaux de contrôle, » illustre Alain Bouillé.

### L'auditeur doit se former ou se faire aider

Ce RSSI constate que le métier d'auditeur est en pleine évolution. « Traditionnellement, l'auditeur travaille à partir de procédures et vérifie si elles sont correctement appliquées. Mais il se trouve confronté à une complexité croissante du système d'information et à l'émergence de nouvelles problématiques comme le Cloud Computing », indique-t-il. Selon lui, l'audit doit évoluer en même temps que la SSI afin de rester pertinent dans le processus de réduction des risques.

**La maturité de l'audit est variable d'un secteur à l'autre et dépend également de la taille de l'entreprise.** « Dans une grande banque internationale par laquelle je suis passé, l'audit était très présent en sécurité des systèmes d'information » se souvient Jean-François Louâpre. « L'audit est moins présent et moins pointu dans une entreprise d'assurance de personnes et de retraites complémentaires comme AG2R La Mondiale. Mais la SSI compense cette faiblesse en générant un contre-pouvoir parce qu'elle est placée en dehors de la DSI » analyse-t-il. Il cite un autre contre-pouvoir efficace : l'audit externe, qu'il s'agisse du commissaire aux comptes ou des organismes de tutelle.

Ceci dit, « les auditeurs informatiques internes n'existent pas toujours » rappelle Jean-Louis Bleicher, « et même lorsqu'ils existent, ils doivent être capables d'aborder tous les sujets, pas seulement la sécurité. » Dès lors, « Ils ne peuvent pas être aussi pointus que le RSSI ou les experts de la DSI. » Ils ont alors la possibilité de faire appel à des auditeurs ou à des consultants externes.

### Normes et référentiels : du pragmatisme

Et sur cette route difficile, ils pourront aussi trouver une aide du côté des nombreux référentiels existants. Les normes et les référentiels apportent une aide précieuse permettant aux différents acteurs de ne rien oublier. Ils représentent aussi un moyen d'homogénéiser le dialogue entre eux. Ces référentiels sont à la fois pléthoriques et pour nombre d'entre eux, récents. « Les auditeurs, les DSI et les RSSI n'ont souvent pas encore eu le temps de tous les étudier », prévient Alain Bleicher. Parmi les référentiels et les méthodologies centrés sur la sécurité, on citera, l'ISO 27002, RiskIT - récemment diffusé par l'ISACA (l'Information Systems Audit and Control Association), il couvre les risques liés aux systèmes d'information -, Mehari (une méthode diffusée en France par le Clusif) et Ebios (de l'ANSSI, ex-DCSSI), plus répandu dans les activités gouvernementales et recommandé pour identifier les besoins en sécurité par rapport à l'analyse de risque. A cela s'ajoute le cortège des normes ISO. « L'ISO 27005 est centré sur l'analyse des risques, et bien adapté si l'on veut plus tard être certifié ISO 27001, qui est un cadre général de certification du système de management de la sécurité », précise Pascal Antonini.

**Face à cette profusion, nombre d'entreprises se montrent à la fois intéressées et circonspectes.** « Les normes et les référentiels constituent une bonne panoplie mais il faut rester pragmatique », affirme Alain Bouillé. Il constate que d'une manière générale, les processus de certification n'ont pas un grand succès en France et que les normes ISO constituent un langage commun intéressant dans le contexte d'une multinationale. Elles s'avèrent aussi utiles dans une institution nationale comme la Caisse des Dépôts. « Les activités du groupe sont très différentes, l'ISO nous permet d'appréhender les problématiques de risque des systèmes d'information de manière cohérente, quelle que soit l'entité », précise-t-il. A la Caisse des dépôts, la SSI dispose d'un référentiel interne qui constitue sa politique de sécurité. « Sans être bâti strictement sur les normes, ce référentiel reprend tout ce qu'elles comportent d'intéressant et est compatible avec l'ISO », déclare Alain Bouillé. ►



## Les DSI, les RSSI et les auditeurs n'ont pas encore eu le temps d'étudier les référentiels récents

**Jean-Louis Bleicher**  
Consultant



## Les référentiels ne sont pas directement déclinables dans notre entreprise

Jean-François Louâpre  
AG2R La Mondiale

**Chez AG2R La Mondiale, Jean-François Louâpre n'est pas non plus engagé dans une démarche de certification.** « Les référentiels ne sont pas directement déclinables dans une entreprise comme la nôtre. Ils nous aident cependant au quotidien et nous donnent des bonnes pratiques », affirme-t-il. AG2R La Mondiale a donc aussi constitué son propre référentiel inspiré des normes. « Cela permet de nous assurer que nous n'avons rien oublié. Mais notre démarche est pragmatique, cela se traduit par un référentiel assez simple, tout en étant relativement détaillé et dont les objectifs demeurent atteignables », précise Jean-François Louâpre.

### Identifier le niveau de risque

Depuis le rapprochement entre AG2R et La Mondiale, ce référentiel est mis en œuvre au niveau du groupe, tout en intégrant la démarche de sécurité du système d'information dans la démarche du groupe en matière de gestion des risques opérationnels. « Le référentiel ISO 27000 peut également être utilisé comme référentiel d'audit » ajoute Jean-François Louâpre. Il prévient « Il faut alors veiller à ce que l'audit ne soit pas trop théorique et prenne bien en compte le niveau de risque de l'entreprise par rapport à son activité. »

**Chez Schlumberger, le référentiel interne est aligné sur les référentiels standards, tout en étant plus contraignant que ceux-ci.** Les objectifs fixés en matière de maîtrise des risques IT ont été placés très haut mais ils demeurent toujours atteignables. Le référentiel est transverse à tous les projets et appliqué par tous les métiers et toutes les implantations, quelles que soient les réglementations locales. « La culture de Schlumberger est synthétisée dans le Code d'Ethique de l'entreprise. Elle nous pousse à appliquer les normes les plus contraignantes », résume Julien Camus.

« Chaque société place la barre où elle le souhaite. Si la direction générale a une volonté d'exigence forte en matière de gestion du risque, cette barre sera très haut », commente Jean-Louis Bleicher, tout en considérant qu'il vaut mieux éviter de mettre la barre trop haut en retenant les exigences supérieures de tous les référentiels, sauf si l'on peut en justifier les avantages.

Selon ce consultant, les référentiels sont très utiles mais ils ne sont effectivement pas applicables en l'état. Ils imposent un gros travail de personnalisation selon les enjeux fixés par les dirigeants, selon la culture de l'entreprise et le risque. Jean-Louis Bleicher prône également le pragmatisme vis-à-vis des certifications : « cela ne vaut la peine que s'il existe un bénéfice potentiel. » Dans le cas contraire, la démarche se réduit à une source de coût d'autant plus importante que les normes nécessitent des audits récurrents pour maintenir la certification.

### Tenir compte de la maturité de l'entreprise

Pascal Antonini va dans le même sens : « Il faut être très souple dans l'utilisation des référentiels standards et prendre ce qui convient selon la maturité de l'entreprise et la complexité des problématiques de sécurité. » Si on applique les référentiels à la lettre, ils se révèlent trop lourds et trop complexes. Pour autant, ils apportent un langage commun, une trame de base pour éviter d'oublier des sujets, et donnent un moyen de rationaliser le travail de la DSI. Pascal Antonini considère en outre que les acteurs de la sécurité ne doivent pas se limiter aux référentiels centrés sur celle-ci. « Cobit, Itil ou CMMI renforcent la fiabilité et le niveau de contrôle bien qu'ils ne relèvent pas directement de la sécurité. Quand un auditeur constate que l'on applique des normes, c'est un gage de professionnalisation de nature à permettre de ne rien oublier dans l'ensemble du processus que l'on a mis en place », explique-t-il. De manière générale, un auditeur trouvera une démarche sérieuse à partir du moment où un DSI peut lui fournir un fichier de traces, montrant que des procédures automatisées de contrôle ont été mises en place. On citera par exemple, le fait que les changements de paramétrage sur les serveurs ou sur les applicatifs soient enregistrés. A l'inverse, certains responsables jouent de cette méthode, et délivrent des centaines de pages de listing aux auditeurs afin de les noyer sous un maximum d'informations inutiles. Auquel cas, comme le dit Farid Aractingi, directeur de l'audit interne de Renault, le pire péché d'un DSI est le déguisement de performances. (Voir CIO.pdf numéro 7).

En conclusion, entre les multiples référentiels centrés sur la sécurité et ceux qui concernent de près ou de loin la sécurité, il existe des zones de recouvrements mais cette profusion n'est pas forcément gênante. « Ces référentiels forment des nuages qui se superposent un peu mais ils sont essentiellement complémentaires. On peut par exemple utiliser Cobit et compléter son volet sécurité par les normes ISO 27001 et 27002 », termine ainsi Pascal Antonini. ■

Thierry Lévy-Abégnoli

Pour en savoir plus



Retrouvez en vidéo  
la table ronde  
**Maîtriser les risques**  
du 1<sup>er</sup> juin 2010  
sur **CIO Online**



# Les bonnes pratiques du Sourcing : Industrialiser et optimiser l'externalisation de prestations IT

*En partenariat avec Metrixware et IronMountain, CIO a organisé une manifestation sur la relation fournisseurs et les bonnes pratiques d'achat en matière de services IT. L'externalisation est une solution à regarder pour réduire les coûts et améliorer la qualité de service à condition de savoir choisir et piloter ses prestataires.*

**F**ace à la pression constante sur les budgets, les DSI se doivent d'industrialiser leurs services afin de faire toujours mieux avec moins. Pour atteindre cet objectif, l'externalisation est une voie car elle permet de confier la couverture de besoins banalisés à des spécialistes. Dès lors, comment recourir au bon prestataire avec une demande adaptée à ses besoins et l'assurance que cette demande sera effectivement satisfaite ? Afin de répondre aux interrogations légitimes des DSI autour de cette problématique, CIO, en partenariat avec Metrixware et IronMountain, les a invités à une matinée sur les bonnes pratiques du sourcing, le 10 juin 2010 au centre de conférence Etoile Saint Honoré (Paris). En ouverture, Laurent Bellefin, directeur de la practice gouvernance du cabinet de conseil Solucom, a présenté l'état du marché de l'externalisation. Il a notamment insisté sur la rareté du global sourcing au profit d'une externalisation sélective par domaine.

## Externaliser en contrôlant la qualité

Vincent Ruelland, directeur des opérations de l'éditeur Metrixware, a, quant à lui, précisé que « *les conventions de service encadrent la qualité des processus et l'aspect fonctionnel des systèmes d'information ou de portions de système d'information externalisées mais rarement la qualité des livrables eux-mêmes alors que cela devrait être le cas* ». Or, pour maîtriser et optimiser la qualité d'une application informatique, il convient déjà d'en connaître et d'en mesurer la qualité selon des critères objectifs. Des outils d'analyse de code sont donc essentiels lorsqu'un développement est confié à un prestataire externe.

Pour gérer la qualité, le rôle des référentiels de bonnes pratiques dans une externalisation réussie est certain. C'était le thème abordé dans la première table ronde qui réunissait Claude Durand, vice-président de l'AeSCM (association de promotion du référentiel eSCM), fondateur et trésorier de l'itSMF France, co-auteur de l'ouvrage « ITIL et la gestion des services » chez Dunod, Nathalie Rachline, membre du bureau de l'EOA (European Outsourcing Association) et responsable de la Vie Courante Informatique du groupe Gefco et Didier Lambert, consultant (ancien DSI d'Essilor, ancien président du Cigref).

## Externaliser pour assumer la croissance des volumes

Mais le développement logiciel n'est pas le seul domaine de l'externalisation en informatique. Pour faire face à l'accroissement exponentiel des volumes de données, les entreprises ont de plus en plus recours à des prestataires de stockage et d'archivage. Le stockage concerne des données vivantes auxquelles l'accès doit être rapide, notamment en cas de sinistre dans le cadre d'un PRA. A l'inverse, l'archivage ne retient que des données qui ne sont quasiment jamais accédées au quotidien. Stéphane Benaïs, responsable technique, et Saïd Filali, directeur commercial de Iron Mountain ont montré les avantages de l'externalisation en la matière que ce soit pour absorber la croissance - de 10 % à 30 % par an – des volumes d'information grâce au recours à des capacités virtuellement illimitées ou que ce soit pour bénéficier d'infrastructures industrialisées et mutualisées donc moins coûteuses.

Une deuxième table ronde s'est ensuite penchée sur les nouvelles manières d'externaliser. Elle réunissait Patricia Wolff-Péron, responsable du sourcing dans l'une des entités de BNP Paribas, Jean-Michel Tixier, directeur mondial des infrastructures IT du groupe Michelin, Audrey Louail, directrice de la Web agency Churchill et Jean-Paul Binot, président de la commission Global Sourcing de l'EOA et consultant indépendant. Afin de clôturer la matinée, Christiane Féral-Schuhl, avocate associée du Cabinet Féral-Schuhl & Sainte Marie, a présenté les règles de base pour contractualiser son externalisation en évitant les pièges classiques, en prenant les précautions indispensables et en sachant prévenir ou gérer les litiges. ■

Pour en savoir plus



Retrouvez  
l'événement  
sur CIO Online

## Hervé Gouëzel de BNP Paribas : « le DSI est un chef d'entreprise »

*Un DSI doit rassembler des qualités de manager, d'entrepreneur, d'industriel et de commercial. C'est le point de vue d'Hervé Gouëzel, Head of Integration pour le groupe bancaire BNP Paribas et ancien DSI du groupe durant douze ans.*

**CEO :** *Vous avez une triple compétence en contrôle de gestion, en management et en informatique. Pourquoi ce choix de la pluridisciplinarité ?*

**Hervé Gouëzel :** En fait, je n'aime pas trop la technique. Et dans mes études, je n'aurais pas du commencer par l'Ecole Polytechnique mais plutôt par HEC. C'est pourquoi après avoir obtenu mon diplôme de l'X en 1972, j'ai fait un MBA à HEC. Puis, j'ai débuté ma carrière dans le contrôle de gestion en 1977, à la Seita [NDLR: l'ancienne régie des tabacs], devenue plus tard Altadis. Mais très vite j'ai fait de la stratégie de management, au sein de la Direction des Systèmes d'Information.

**CEO :** *Comment avez-vous débuté votre carrière chez BNP ?*

**Hervé Gouëzel :** En 1988, je suis entré à l'inspection générale du groupe BNP, pour ensuite contribuer aux différentes activités bancaires de l'entreprise via un poste de directeur adjoint au réseau des agences de la région parisienne. C'était le bon côté de la banque, celui qui fait gagner de l'argent. Et surtout, j'avais enfin fui la technique. Mais la direction a souhaité que je regagne l'informatique. J'ai donc replongé. En 1995, après avoir rejoint la direction de l'Organisation en tant que second du Directeur en charge des domaines techniques, j'en ai été nommé directeur par Michel Pebereau, [NDLR: ancien directeur général de BNP auquel a succédé Baudouin Prot] et trois mois plus tard je faisais partie du Comité de Direction Générale de la BNP. Je suis resté durant douze ans au poste de DSI. J'ai eu beaucoup de chance.

**CEO :** *Pourquoi être resté DSI alors que vous préféreriez être du côté des métiers ?*

**Hervé Gouëzel :** On ne m'a pas laissé le choix. On m'a dit « tu restes à la DSI ». Et même si je ne voulais pas faire de la technique, j'avais le profil pour ce type de poste. J'étais suffisamment formé pour que l'on ne me baratine pas. Je savais manager et en même temps je connaissais la technique. Tout au long de ma vie et de ma carrière j'ai traversé toutes les nouvelles technologies. Ce qui m'amène à comprendre vite. Et puis être DSI est valorisant : l'informatique se développe et votre équipe participe activement à la construction de la banque. J'ai appris à travailler avec les informaticiens. Ils ne cherchent pas à se mettre en valeur pourtant ils sont doués. J'ai beaucoup apprécié de pouvoir les aider à changer un peu leur image. Je les ai incités à se vendre.

**CEO :** *Vous êtes en charge de l'intégration du groupe bancaire belge Fortis. Comment cette responsabilité qui n'est pas technique vous a-t-elle été confiée ?*

**Hervé Gouëzel :** Tout a été décidé à l'initiative de l'actuel Directeur Général, Baudouin Prot et de Jean-Laurent Bonnafé, Directeur Général Délégué et CEO de BNP Paribas Fortis. Aujourd'hui je suis une sorte de chef d'orchestre. Ce poste est une suite logique à ma carrière. Tout ce que j'ai fait avant m'a préparé à ce poste. Baudouin Prot et Jean-Laurent Bonnafé m'ont fait confiance. Ils savent que je suis quelqu'un de tenace. J'ai une vision globale de la banque. J'ai contribué à sa construction. Les équipes informatiques sont restées proches de moi. Lorsque j'ai pris mes fonctions de Head of Integration à la tête de

“  
En fait,  
je n'aime  
pas trop  
la technique  
Hervé Gouëzel  
Head of Integration

### LES 7 CONSEILS QU'HERVÉ GOUËZEL DONNERAIT À UN DSI

- 1 Ne pas faire de la technique pour la technique
- 2 Servir les clients externes et internes avec passion
- 3 Obliger les informaticiens à communiquer, à se vendre et à faire du marketing
- 4 Etre membre de la direction générale
- 5 Investir sur les hommes
- 6 Savoir sous-traiter sans perdre le contrôle
- 7 Développer un pôle puissant d'architectes



## Le respect des hommes est majeur

**Hervé Gouëzel**  
Head of Integration

la Mission du Rapprochement de BNP Paribas, BNP Paribas Fortis et BGL BNP Paribas, j'ai d'ailleurs repris deux anciens collaborateurs. Dans une carrière il faut savoir prendre la chance et il m'a fallu à peine dix secondes pour dire oui à Baudouin Prot.

### **CIO**: Quelles bonnes pratiques faut-il appliquer en matière de management ?

**Hervé Gouëzel**: La faiblesse de l'informatique est que le personnel est réparti en silos. Pour manager, il faut donc dialoguer, unir les troupes. L'esprit d'équipe est selon moi un atout majeur. Il faut rassembler les équipes, les motiver. De plus, le respect des hommes est majeur. Dans l'informatique, il y a certes des machines, mais avant tout il y a des hommes. La banque évolue et se distingue par sa marque, par les hommes et par l'IT (*Brand, People, IT*). Et derrière l'IT, se cachent encore des hommes. Il est indispensable d'avoir une culture d'entreprise, de la banque, du service, du client. Plus que tout, il faut accepter le fait que la DSI d'une banque soit devenue une industrie. A ce titre, nous sommes la première banque à avoir des équipes informatiques certifiées ISO 20 000, ISO 9 000 et CMMI 3. Nous sommes véritablement une entreprise industrielle. La DSI est l'usine de la banque.

### **CIO**: Comment mener un bon projet IT ?

**Hervé Gouëzel**: Il faut faire des projets utiles et non des beaux projets. Il ne faut surtout pas faire de l'informatique pour le plaisir car dans ce cas on ne satisfait pas le client. C'est la raison pour laquelle les informaticiens doivent communiquer beaucoup avec leurs clients. Les équipes de la DSI doivent comprendre les besoins des métiers. Nous réalisons des enquêtes qualité sur nos clients internes afin d'améliorer leur satisfaction. Les projets sélectionnés ne doivent pas nécessairement tous avoir un ROI élevé mais ils doivent tous satisfaire les clients. Et, pour bien servir les clients, le personnel doit lui-même être satisfait de son IT. Enfin, les Managers IT doivent être passionnés par les personnes qu'ils servent. C'est le cas pour les Chefs de Projets avec leurs clients mais trop d'équipes de la technique n'en sont pas encore là. Ils doivent montrer leurs réalisations aux utilisateurs et les valoriser. Il faut savoir parler le langage des métiers et les connaître.

### **CIO**: L'informatique est-elle plutôt un levier ou un centre de coûts ?

**Hervé Gouëzel**: L'informatique est importante. C'est la matière première de la banque. L'IT a remplacé les billets et la monnaie. Sans informatique, les banquiers ne peuvent plus exercer leur rôle. Chaque jour, des millions d'emails sont échangés et des millions de transactions sont effectuées. Nous ne pouvons pas considérer l'IT uniquement comme un centre de coûts. Il faut aussi regarder les « *best practices* » des autres. Ce n'est pas à la DSI de décider si oui ou non un projet informatique sera développé. Cette tâche revient aux directions métiers qui doivent assurer le financement dudit projet. Dans le cas du rapprochement entre BNP Paribas et Fortis, nous avons au total 1 173 projets ! Le plan prévoit un bouclage pour la fin de l'année 2011. Des dizaines de pays sont concernés par le rapprochement. C'est un projet énorme, partout et pour tous les métiers. Il dégagera 900 millions d'euros de synergies par an.

### **CIO**: Quelles sont selon vous les qualités que doit avoir un DSI ?

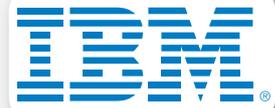
**Hervé Gouëzel**: Il faut comprendre la technique et avoir de bonnes bases en informatique et être un manager, un entrepreneur, un industriel et un commercial. Le DSI est un véritable chef d'entreprise. Je pense qu'il est tout de même nécessaire d'avoir au préalable fait un peu de technique avant d'avoir la casquette de DSI. Il faut savoir rester modeste. Il faut être capable de faire régner un équilibre au sein de l'équipe. Il faut de l'ordre. Il faut bien connaître les projets, le ROI qui en découle, leurs coûts initiaux et induits. Le plus compliqué est de consacrer assez d'argent à la fois à l'entretien et aux projets nouveaux. Avant de soumettre un projet à un Métier, un DSI doit se tourner vers l'architecte, lui demander son avis et prévoir plusieurs alternatives. Enfin, sur un plan général, il faut faire les bons choix et avoir recours à l'outsourcing et à l'offshoring de façon raisonnable, pour optimiser les coûts sans perdre le contrôle. ■

Par Johanna Godet

## BNP PARIBAS, UNE SUCCESS STORY À LA FRANÇAISE

Il y a tout juste dix ans, le groupe bancaire français BNP, employant alors 77 000 personnes, se lançait dans le plus grand rapprochement bancaire jamais réalisé en France avec la banque Paribas, et devenait BNP Paribas. Le groupe était alors sous la houlette de Michel Pébereau. En 2003, Baudouin Prot en prend la tête. Il poursuit la politique d'expansion entamée par son prédécesseur. Ainsi, en 2006, BNP Paribas rachète BNL, alors la sixième banque italienne,

puis prend le contrôle de Fortis Banque à hauteur de 75 % et de BGL au Luxembourg à 66 % en 2009. Toutes ces acquisitions ont mené le groupe dans le top 10 des banques mondiales et en première position en Europe en termes de dépôts. La banque dispose de plus de 9 000 agences au niveau mondial et affiche un produit net bancaire de 40 milliards d'euros. Le groupe est présent dans 80 pays, et emploie 200 000 collaborateurs. ■



# Adapter sa stratégie de Sourcing IT à la transformation de son entreprise

*Les DSI sont confrontés à un double défi. Ils doivent accompagner la transformation de leur entreprise tout en maîtrisant leurs coûts. Dans ce cadre, l'optimisation des stratégies de sourcing IT constitue un levier d'action essentiel. Face à la diversité des options disponibles, quel scénario retenir ? C'est à cette question stratégique qu'a répondu l'événement organisé le 3 juin dernier par CIO en partenariat avec IBM.*

**L'**externalisation de tout ou partie de son système d'information est un levier d'action majeur pour une entreprise, que celle-ci cherche à optimiser son informatique ou qu'elle soit engagée dans une transformation de son modèle économique. Quelle stratégie de Sourcing IT sera alors la plus adaptée à son organisation ? C'est ce thème stratégique qui a été illustré lors de la conférence organisée par CIO en partenariat avec IBM, le 3 juin à l'hôtel Raphaël (Paris) et qui a réuni trente décideurs IT de grandes entreprises.

## Les témoignages de cinq DSI

Cet événement a été l'occasion de partager l'expérience de cinq DSI de grandes entreprises qui ont mis en œuvre des projets d'outsourcing avec IBM. Bertrand Eteneau, DSI de l'équipementier automobile Faurecia, Alexandre Boulgakoff, DSI du groupe de services financiers Lasser, Hervé Thoumyre, DSI du groupe Carrefour, deuxième distributeur mondial, Hans Schenck, DSI de La Lyonnaise des eaux qui dessert douze millions de Français en eau potable et Pierre-Yves Argoud, Head of Infrastructure and Production de BNP Paribas Investment Partners, un établissement financier qui gère 542 milliards d'euros d'actifs ont présenté leur vision du Sourcing IT.

En ouverture de la conférence, une enquête réalisée auprès d'entreprises françaises par le cabinet de conseil Solucom et l'association Ae-SCM a montré à quel point l'externalisation IT est désormais banalisée. Le multi-sourcing demeure le mode privilégié, tant pour l'applicatif que pour les infrastructures. Les objectifs sont alors la réduction des coûts et le gain en souplesse. Une entreprise sur deux désire toutefois une meilleure qualité de service et une forte minorité d'entre elles critique le manque de pro-activité de ses prestataires. Le constat global est que si un processus de pilotage et de recette est mis en place pendant la phase de démarrage, c'est moins souvent le cas pour les phases récurrentes et de réversibilité. On relève également que les ressources humaines sont le parent pauvre de la gestion du changement.

## Des attentes parfois contradictoires

Un autre sondage réalisé exclusivement auprès des responsables IT invités de l'événement a mis en lumière des attentes parfois contradictoires. Ainsi, les deux premiers moteurs de l'externalisation sont la volonté de réduire les coûts et dans le même temps l'amélioration de la qualité de service. Autre sujet d'étonnement, les apports technologiques du prestataire n'apparaissent pas prioritaires. Sinon, on retrouve le fait que l'infogérance sélective a la préférence des entreprises, même si quatre d'entre elles présentes lors de l'événement recourent à l'infogérance globale. Autre enseignement, les nouveaux projets concernent tout autant les applications que les infrastructures. Enfin, si l'assistance technique et l'infogérance forfaitaire sont largement répandues, les entreprises piochent dans divers modèles de *Delivery*, avec par ordre décroissant : les centres de services partagés (60 %), la régie sur site (50 %), le nearshore (40 %) ou l'offshore (30 %). L'importance d'une gouvernance adaptée est alors soulignée par tous les sondés.

Isabelle Duvernoy, Directeur Infogérance d'IBM France et Jérémie Caullet, Directeur Application Management Services d'IBM France ont ensuite partagé la vision et l'expérience d'IBM en matière de stratégie de sourcing IT. Les résultats de l'étude IBM Global CEO Study 2010 mettent en exergue pour les dirigeants l'importance de différencier leur entreprise dans un monde



L'organisation globale d'IBM est un atout pour la flexibilité des entreprises

**Jérémie Caullet**  
Directeur Application Management Services d'IBM France

Pour en savoir plus



Retrouvez les vidéos de l'événement sur CIO TV

complexe. Les DSI doivent donc définir une stratégie de Sourcing adaptée et adaptable à la transformation de leur entreprise, tout en optimisant leurs infrastructures et leurs applications. « *L'organisation globale d'IBM est un atout pour la recherche de flexibilité des entreprises* » a déclaré Jérémie Caullet. Le modèle de Global Delivery d'IBM vise à apporter une dimension industrielle de l'externalisation. « *Contrairement, à une idée reçue, il est aussi adapté aux petites entreprises* » a-t-il mentionné. Il s'agit alors d'une démarche progressive qui doit être assurée en étant accompagné.

Jérémie Caullet a poursuivi : « *Les stratégies de Sourcing doivent aider à réduire les coûts, à gagner en flexibilité et à libérer des ressources pour investir dans de nouveaux projets ou de nouveaux modèles économiques.* » Des synergies importantes sont alors possibles lorsque l'on retient un même prestataire pour l'outsourcing d'infrastructures et d'applications. « *On peut citer des baisses de coûts de 30 % sur trois ans sur la partie applicative. Avoir un seul interlocuteur permet d'éviter le traditionnel ping-pong entre les infrastructures et les applications* » a souligné le directeur Application Management Services d'IBM France. Les bénéfices viennent également de l'association d'équipes d'experts métiers et techniques afin d'être proche des demandes du business.

### **Etre en permanence à l'écoute**

Isabelle Duvernoy a déclaré que le marché de l'infogérance a atteint une certaine maturité. « *Il nous faut donc en permanence être à l'écoute des besoins métiers de nos clients, vérifier que la qualité de service est celle attendue, et voir si le périmètre couvert nécessite d'être étendu.* » Le défi le plus complexe concerne les grands projets de transformation. « *Il faut alors travailler avec toutes les fonctions de l'entreprise - achats, finances, IT - et répondre à des engagements de résultats, travailler les transitions, la gouvernance, la qualité de delivery* » a résumé Isabelle Duvernoy, indiquant que le contrat doit être dynamisé tout au long de sa vie afin d'apporter de manière régulière les innovations attendues.

### **Une externalisation variable dans le temps**

La table ronde qui a ensuite réuni cinq DSI a mis en exergue les bonnes pratiques et leurs objectifs en matière d'externalisation. On a pu constater que les entreprises non seulement sont adeptes d'une externalisation sélective, pour l'applicatif, le réseau ou l'infrastructure mais qu'en outre, l'externalisation s'avère à géométrie variable dans le temps. Ainsi un domaine externalisé à une période, peut être « ré-insourcé », et inversement selon les priorités et les contraintes du moment.

« *Au niveau mondial, la politique de Sourcing de Carrefour repose sur le renforcement des relations avec cinq grands partenaires, dont IBM. Car on peut prendre des risques à avoir des relations trop fragmentées* » a relaté Hervé Thoumyre. Il entend progressivement standardiser ses ►



**Le défi le plus complexe concerne les grands projets de transformation**

**Isabelle Duvernoy**  
Directeur Infogérance  
d'IBM France

## **LE PILOTAGE DE L'OFFSHORE EST MIEUX MAÎTRISÉ**

Ces dernières années, l'usage de l'offshore ou du nearshore a été de mieux en mieux maîtrisé par les DSI. « *En matière d'offshore, nous avons tout essayé, y compris les grands échecs en Inde pour ne pas avoir compris que la culture est différente et que la manière de délivrer est différente* » se souvient ainsi Alexandre Boulgakoff, DSI du groupe Laser. Il ajoute : « *la deuxième approche que l'on a eu est de faire confiance à un partenaire, en l'occurrence à IBM, qui pilote les ressources en offshore et qui comprend cette dynamique industrielle et la met en place pour atteindre les résultats.* » Il a ainsi migré d'un offshore en Roumanie vers un centre de services au Vietnam, managé par IBM. Laser y fait réaliser une grande partie de ses nouveaux développements. « *Notre objectif est d'avoir un bon mélange entre les tâches à faible valeur ajoutée réalisées en offshore, tout en maintenant tout le reste en proximité* » a-t-il rappelé. Sans oublier, qu'il faut prendre en compte l'externalisation hors Europe de données personnelles qui est soigneusement encadré.

Bertrand Eteneau, pour sa part, a opté pour la création d'une filiale en Tunisie avec IBM, il y a dix huit mois. Ce centre de compétences SAP est chargé de la maintenance applicative et des nouveaux développements autour de cet ERP. Le centre est co-géré avec IBM et assure aussi du pilotage de serveurs pour l'Europe et l'Asie. Il emploie soixante dix personnes et devrait évoluer vers une centaine à la fin de cette année, mêlant les équipes IBM en mode régie et des équipes de Faurecia. « *Ce mode de contractualisation plus souple est plus rapide à mettre en place qu'une co-entreprise qui répond à d'autres enjeux* » a-t-il estimé. Pierre-Yves Argoud a recours quant à lui à un centre de services partagés d'IBM situé en Roumanie. « *Cette externalisation a débuté en 2006. Elle a atteint désormais sa maturité. Pour nous, c'est une extension des équipes internes.* » Il est d'abord passé par une phase d'industrialisation des équipes de développement internes via CMMI avant de recourir à des ressources externes en offshore d'une trentaine de personnes. ■

services afin de pouvoir les *benchmarker* tant d'un point de vue financier que des performances. « *Cela nous aidera à prendre des décisions d'outsourcing ou à ré-insourcer, selon les priorités de l'entreprise et celles sur lesquelles on doit se concentrer* » a-t-il résumé. De plus, le DSI a valorisé le principe du dual sourcing, c'est-à-dire, le fait d'avoir deux partenaires sur chaque grand domaine stratégique, afin de maintenir un bon niveau d'émulation, favoriser l'innovation et réduire les risques.

Le déclencheur de l'externalisation d'infrastructures auprès d'IBM aura été un programme de transformation des applications qui allait avoir des conséquences au niveau des compétences, conduisant à des baisses d'activité sur certains domaines technologiques et inversement à des manques technologiques dans d'autres domaines. « *C'était une problématique de gestion des ressources humaines. Nous n'étions pas en mesure de répondre à ce challenge malgré notre taille* » a constaté Hervé Thoumyre. De plus, cela n'était pas le cœur d'activité du distributeur. L'autre bénéfice attendu était « *de se donner les moyens d'avoir de la variabilité pour piloter nos coûts, au travers d'un catalogue de services* » a précisé le DSI.

### **Assurer les fondamentaux de la DSI**

Hervé Thoumyre a mis le focus sur le lien entre l'outsourcing et les fondamentaux de la DSI : « *Notre stratégie de sourcing, la manière dont on la fait évoluer, est liée au fait qu'il y a des fondamentaux qu'il faut que l'on assure.* » Ceux-ci sont multiples et se retrouvent au sein de nombreuses DSI. Ils concernent d'abord la simplification des systèmes, la robustesse des architectures et des services rendus ainsi que l'évolution des compétences, parce que la DSI ne peut pas positionner des compétences partout, et donc elle doit faire des choix. De même, il y a les fondamentaux en termes de modèles financiers, avec une recherche permanente de « *variabilisation* » des coûts, que ce soit pour accompagner l'accélération d'un business, ou bien la décroissance d'un autre. « *Enfin, il y a des fondamentaux en termes de gouvernance, pour être sûr que l'on maîtrise les risques, et que l'on agit avec un niveau de fiabilité dans nos prévisions et dans notre capacité à délivrer les projets et les services qui fait que l'on est crédible au quotidien* » a-t-il terminé.

Bertrand Eteneau de Faurecia a également détaillé sa manière d'appréhender le sourcing. « *Notre sourcing a changé. Le sourcing d'il y a trois ans était plus opportuniste. Maintenant quand on fait du co-management avec IBM pour créer une équipe IT en Tunisie, c'est quelque chose que l'on construit sur la durée avec un vrai projet industriel des deux côtés* ». Faurecia a également fait des choix de ré-insourcing ou d'outsourcing sur l'infrastructure en fonction des opportunités, des coûts, des salaires recherchés, ou de la capacité que l'entreprise avait à un moment à gérer ou pas un certain nombre de technologies. « *Pour des raisons de coût notamment, on a ré-insourcé une partie de nos infrastructures* » a relevé Bertrand Eteneau, pointant qu'« *Il faut aller chercher les ressources adaptées là où elles sont à un moment donné.* »

### **Il faut être bon soi-même**

Quant à Alexandre Boulgakoff de Laser Cofinoga, il a adopté le modèle de Global Delivery de Big Blue, délivré dans le centre de Montpellier afin de bénéficier pour une partie de sa production des capacités d'industrialisation du prestataire. Il a souligné qu'« *Avoir un bon outsourcer, cela suppose essentiellement d'être bon soi-même. Nous sommes depuis 1999 en recherche permanente d'amélioration de notre outsourcing, et de nos compétences internes.* »

Pierre-Yves Argoud de BNP Paribas Investment Partners, pour sa part, a expliqué que « *le but était de nous transformer, en passant par l'industrialisation de la DSI* ». Il cherchait à monter une structure industrielle qui lui permette de supporter l'évolution de son business, dans une entreprise en forte croissance. « *J'attends un facteur d'innovation au travers du contrat, et il est présent tous les jours. J'ai donc les deux points positifs* » s'est-il félicité.

### **Posséder la capacité à piloter**

Hans Schenck, de la Lyonnaise des eaux, a indiqué qu'il est en train de réaliser un refresh technologique avec IBM. Après une phase d'outsourcing global, l'entreprise a ré-internalisé un certain nombre d'activités considérées comme stratégiques, en particulier le pilotage du fonctionnel de l'IT. Et côté Sourcing, elle applique une approche plus sélective. « *Nous avons recréé notre capacité à piloter l'architecture globale et la stratégie informatique tout en gardant les avantages d'un outsourcing global, en confiant des domaines entiers à IBM, y compris l'infrastructure et l'applicatif* » a précisé le DSI.



**Le déclencheur a été la gestion des ressources humaines**

**Hervé Thoumyre**  
DSI du groupe Carrefour



**Je voulais une structure industrielle qui supporte l'évolution du business**

**Pierre-Yves Argoud**  
BNP Paribas Investment Partners

De fait, le pilotage de l'externalisation est devenu crucial. Il nécessite une réorganisation des équipes de la DSI et de leurs compétences. « *La maîtrise que l'on avait auparavant, on la maintient mais d'une manière un petit peu différente* » a expliqué Alexandre Boulgakoff. Afin de ne pas perdre le contrôle de son informatique, il convient de prendre en charge un certain nombre de fonctions telles que l'architecture, la maîtrise du contrat, et la maîtrise du contenu du contrat, c'est-à-dire ce que l'on paie et pourquoi, et la maîtrise des livrables. « *Pour externaliser, il faut maîtriser. Il ne faut pas conserver des techniciens sur des technologies particulières. En revanche, il faut des personnes capables de discuter avec l'infogérant pour le pousser à s'améliorer* » a-t-il affirmé.

### Un contrat bon et précis

« *Il faut effectivement pousser le partenaire à s'améliorer en permanence sinon il ne le fera pas* » a confirmé Bertrand Eteneau. Il faut aussi un pilotage juridique du contrat, des unités d'œuvre et de la technique. « *S'il n'y a pas de pilotage du contrat, il y aura insatisfaction des deux côtés. Lors des renouvellements ou des ruptures, cela ne se passera pas comme on aurait pu le souhaiter* » a-t-il relevé. Ceci dit, le contrat initial doit être bon et précis, puis piloté en permanence. Bertrand Eteneau a plaidé pour la possibilité permanente de faire de la réversibilité. « *Car une stratégie de sourcing, c'est une dynamique. C'est de l'out, c'est de l'in, c'est du ré-insourcing, ou du co-management, mais si à un moment je ne maîtrise pas la possibilité de faire du ré-insourcing je suis en position de faiblesse pour ma négociation. On peut aussi faire du ré-insourcing selon nos priorités afin de faire une allocation optimale de nos ressources.* »

### Créer une équipe de gouvernance

Alexandre Boulgakoff a ajouté : « *c'est à la DSI de piloter le volume et le prix des unités d'œuvre de facturation* ». Le DSI a insisté sur la nécessité de créer une équipe de gouvernance de contrat, avec des juristes, des managers, des spécialistes des risques, qui s'appuient sur le savoir-faire technique de la DSI qui est le prescripteur des services. « *C'est cette cellule qui doit passer les conditions à l'infogérant selon que l'on soit en croissance ou en décroissance* » a-t-il avancé.

Le DSI du groupe Laser a plaidé pour la proximité avec l'infogérant. C'est-à-dire des gens que l'on peut toucher et qui ne se motivent pas uniquement lorsqu'il y a des ennuis. « *Ce sont des* ►

“  
Une stratégie  
de Sourcing,  
c'est une  
dynamique

Bertrand Eteneau  
DSI de Faurecia

“  
Il faut  
discuter avec  
l'infogérant  
pour le  
pousser à  
s'améliorer

Alexandre Boulgakoff  
DSI du groupe Laser

## LE RAPPORT QUALITÉ/PRIX MIS EN AVANT

Au final, quelle réduction des coûts peut-on atteindre via l'externalisation ? Étonnamment, les DSI de la table ronde ne placent pas l'importance des économies réalisées en tête de liste comme déclencheur de l'externalisation. « *Si on peut arriver à réduire les coûts, c'est bien, mais il faut faire attention à ne pas gagner à court terme pour payer cher ensuite car on s'est placé dans un modèle extrêmement rigide* » a averti Hervé Thoumyre, DSI du groupe Carrefour. Il estime que le vrai gain est la variabilité sur des services que l'on est arrivé à standardiser et que les vraies économies sont obtenues par la simplification, par la standardisation et par l'industrialisation. « *Le vrai enjeu dans nos coûts c'est de faire en sorte que nos investissements dégagent la valeur attendue* » a-t-il souligné. Il entend être extrêmement sélectif dans ses investissements, car derrière il peut réduire les coûts récurrents qui en résultent. Quant à Alexandre Boulgakoff, DSI de Laser Confinoga, il veut prendre les infogérants au mot. « *Les outsourceurs déclarent qu'ils savent optimiser les coûts en tant qu'industriels, j'attends qu'ils tiennent leurs promesses* » a-t-il affirmé. Il pointe une deuxième source de gain : la DSI elle-même. « *Nous maîtrisons des patrimoines applicatifs et des machines, et nous avons la possibilité de discontinuer des applications, de manière à payer moins en maintenance, à consommer moins en CPU, etc* » a-t-il illustré. Et le troisième axe, c'est la possibilité de jouer sur les volumes d'unités d'œuvre

consommés afin de concrétiser la promesse d'une baisse des coûts en cas de baisse de volume. « *Il est important de maîtriser ce volume. Il faut trouver un moyen de minimiser le récurrent, et l'outsourcing c'est la promesse de la minimisation du récurrent.* » Hans Schenck, DSI de La Lyonnaise des eaux, pense pour sa part que le coût est un enjeu permanent, mais que l'essentiel « *c'est la maîtrise du rapport qualité prix de l'informatique* ». Il a souligné qu'il faut toujours s'assurer que l'on a le bon partenaire pour le bon type de mission. « *Regrouper un certain nombre de prestations peut être très avantageux, mais pour un service spécifique, on peut avoir intérêt à retenir un autre prestataire mieux placé d'un point de vue rapport qualité/prix* ». Même opinion pour Bertrand Eteneau, DSI de Faurecia : « *Le service doit avoir un coût acceptable par les métiers sur toute la planète compte tenu de ses contraintes locales. Nous allons donc regarder le meilleur rapport qualité prix, ceci que le service soit délivré en interne, en outsourcing ou en co-management.* » Enfin, Pierre-Yves Argoud, Head of Infrastructure and Production de BNP Paribas Investment Partners, aura conclu par « *Ce qui m'intéresse c'est l'optimisation du rapport qualité prix. Je peux aller dans un pays trois fois moins cher que la Roumanie, sauf que la DSI ne fonctionne plus. Il faut quelque chose qui soit industriel et qui marche. Le coût pour le coût, à un moment donné cela dysfonctionne.* » ■

gens qui gèrent la relation pour nous, en face, qui existent, c'est aussi de la crédibilité » a-t-il résumé. Face à l'évolution de l'informatique sur les 30 dernières années, on sait que cela va changer encore. « On a besoin d'être en veille par rapport à cela, on a besoin que nos partenaires nous aident, d'où l'intérêt aussi quelque part d'un multi-sourcing » a-t-il ajouté.

On retrouve une illustration de l'importance du pilotage du contrat avec la DSI de La Lyonnaise des eaux. Elle a créé une minuscule filiale de trois personnes en charge de la gestion du contrat « Au début, c'était un financier qui gérait le contrat. Ce n'était pas satisfaisant. Idem avec un technicien. Aujourd'hui, nous avons réuni trois personnes : un acheteur, un juriste et un financier, qui s'appuient sur la DSI pour les aspects techniques. Nous avons repris ainsi la maîtrise, l'équilibre est aujourd'hui plus satisfaisant » s'est réjoui Hans Schenck. Il a ajouté : « On ne peut pas avoir toutes les compétences en interne. Une DSI pousse pour l'alignement sur les besoins métiers. Les contrats invitent plus à pousser l'innovation, à l'amélioration commune de la performance du système d'information. Il faut piloter ses contrats avec une rigueur militaire ».

### **Des clauses d'amélioration continue**

Ceci dit, le contrat va bouger, dans la durée. « Par exemple dans les contrats d'infogérance d'il y a dix ans, on ne voyait jamais apparaître la notion d'amélioration continue. On voyait apparaître la notion d'amélioration des coûts mais pas celle d'amélioration continue » a rappelé Alexandre Boulgakoff. Cette amélioration passe par l'amélioration du parc, la virtualisation, l'impact sur les coûts, l'apport de nouvelles technologies, etc. C'est une nouveauté, qui suppose une gouvernance qui ne soit pas liée aveuglément au contrat, mais qui s'inspire plutôt des pratiques induites par le contrat. « Nous devons comprendre en permanence quelles sont les évolutions dans ce type de métier et apprendre à maîtriser leur implémentation avec nos partenaires » a affirmé Alexandre Boulgakoff.

Enfin, comment l'outsourcing a-t-il aidé plus précisément à accompagner la transformation de l'entreprise ? Bertrand Eteneau répond « Il y a 4 ans, nous avons plus de 150 systèmes d'information. Faurecia a grossi par acquisitions. On devait capitaliser sur les équipes que l'on avait et s'industrialiser rapidement. » La DSI a donc fait appel à un certain nombre de prestataires soit pour le développement de Core Model, soit pour des gestions de nouvelles infrastructures. Faurecia est passé en quatre ans d'infrastructures en local sur chaque site à des infrastructures mondialisées où l'on délivre les mêmes services partout dans le monde dans 33 pays. « C'est une transformation extrêmement rapide. Nous n'avions pas toutes les compétences, ni les capacités pour avoir toutes ces compétences rapidement pour le faire » a rappelé le DSI.

### **La transformation est le maître mot**

Alexandre Boulgakoff a tracé quant à lui les grands projets de sa DSI liés à la transformation. « Nous sommes en transformation permanente » a-t-il confirmé. Il s'emploie à organiser cette transformation au travers de quatre grands programmes qu'il pilote. Le premier est un programme d'alignement sur la stratégie métier, qui débouche sur des refontes. Le deuxième est un programme d'industrialisation des métiers de l'informatique. Le troisième programme est intitulé « ré-engineering et optimisation des coûts des systèmes d'information ». Il s'agit de délivrer le bon prix pour le bon service et la bonne valeur. Dans ce cadre, le pilotage est plutôt réalisé via des indicateurs d'entreprise et par le management des Assets de l'informatique. Et le dernier programme, mené dans le cadre du contrat avec IBM, concerne la gouvernance et l'amélioration continue. Il s'agit alors de l'amélioration des aspects catalogue de services, et de la compréhension des modèles de facturation. « On impose une certaine forme de transparence tout en restant dans nos métiers » a indiqué Alexandre Boulgakoff. Sur ce type de transformation, la DSI de Laser gère une vingtaine de chantiers.

Enfin, on citera La Lyonnaise des eaux, dont le modèle économique va être profondément transformé durant les années qui viennent, notamment au travers des compteurs intelligents, autrement dit le « smart metering » qui change complètement le système d'information de l'entreprise. « Nous voilà obligés de changer rapidement car notre métier de distribution d'eau devient un métier de service, ce qui n'était pas le cas habituellement » a présenté Hans Schenck.

« Il faut donc continuer de professionnaliser la DSI et d'optimiser la stratégie de Sourcing avec le bon choix à chaque fois » a-t-il conclu, résumant ainsi la nécessité générale pour un patron de l'IT de toujours se remettre en question. ■



**Les contrats invitent à l'amélioration commune de la performance**

**Hans Schenck**  
DSI de La Lyonnaise des eaux

Pour en savoir plus



Contact IBM France  
**Isabelle Waché**

isabelle\_wache@fr.ibm.com

## Incitez votre entreprise à rechercher votre successeur en interne

*En tant que DSI, prévoir sa succession est stratégique. Notre confrère CIO américain a interviewé d'anciens DSI sur leur expérience. Ils recommandent de rechercher en interne les profils susceptibles d'être intéressés par le poste et de les former pour assurer leur succession.*

**L**orsque je demande à un DSI comment il envisage sa succession, j'obtiens trois réponses. La moitié me répond « *je forme actuellement deux personnes, mais ils ont encore des progrès à faire* ». Environ un tiers déclare « *j'ai quelqu'un qui pourrait être DSI demain* ». Le reste du temps j'entends « *pas avant longtemps* ». Bien que la plupart des DSI aient un successeur en tête, je parierais que moins de dix pour cent des DSI actuels des grandes entreprises soient issus d'une promotion interne. D'où le paradoxe : vous formez des successeurs, pourtant le patron de l'entreprise va, la plupart du temps, aller chercher son nouveau DSI à l'extérieur. Ce paradoxe a une explication évidente. Le directeur général n'est pas satisfait de son informatique et les successeurs internes potentiels du DSI sont dès lors coupables des mêmes travers par association. Mais d'autres défis, plus facilement gérables, sont également à prendre en compte dans le paradoxe de la planification de sa succession. Des DSI et leurs successeurs m'ont donné leurs solutions pragmatiques.

### *Le dilemme du silo*

Les dirigeants IT ont tendance à être issus d'un silo, soit du domaine des applications soit de celui de l'infrastructure, alors que le rôle du DSI requiert de l'expérience dans ces deux domaines.

Quelle est la solution ? Donnez tout l'IT à votre successeur. En 1999, Bruce Goodman a rejoint en tant que DSI, la société Humana, un prestataire de services de santé (qui a réalisé 30 milliards de dollars de chiffre d'affaires en 2009). Trois ans après son arrivée, il est également devenu responsable des opérations. En tant que CIO et responsable des opérations, Bruce Goodman a travaillé avec la direction générale afin de confier les opérations IT et les services techniques au directeur technique, Brian LeClaire, son successeur désigné. Dans le même temps, Brian LeClaire conservait ses responsabilités en matière d'ingénierie des applications. Bruce Goodman explique son attitude : « *il y a des années, j'avais du laisser passer la chance d'une promotion parce que je n'avais pas de successeur* ». Il ajoute : « *si vous voulez avancer et aller plus loin que le poste de DSI, vous devez embaucher des personnes qui ont le potentiel pour faire votre travail et ensuite vous devez leur donner autant de responsabilités IT que vous le pouvez* ».

Autre solution possible : recruter des collaborateurs directs au profil équilibré. Lorsque Rick Davidson était DSI chez Manpower, il disposait de postes de managers dans ses entités infrastructures et applications. Mais il n'a pas recruté des personnes ayant une solide expérience verticale et spécialisée dans l'une ou l'autre de ces disciplines, au contraire de ce que font beaucoup de DSI. A la place, Rick Davidson, désormais directeur chez AlixPartners, a gardé un œil sur la possibilité de faire venir des successeurs potentiels et a donc engagé des responsables ayant une large expérience dans les opérations de services partagés ou côté métiers.

### *Le dilemme de l'exposition*

Trop souvent, lorsque le DSI sortant recommande un successeur, le comité exécutif connaît peu le candidat interne.

Quelle est la solution ? Placer vos successeurs en face des métiers. Rick Davidson de Manpower a donné la responsabilité du programme de transformation du front office à Denis Edwards, qui lui a succédé chez Manpower en 2009. Denis Edwards s'exclame à ce titre : « *c'était le programme le plus important et le plus complexe de toute l'histoire de la société.* » Etant donné l'impact du programme, l'ensemble du comité exécutif s'est investi. Rick Davidson plutôt que d'agir comme étant lui-même le visage du dirigeant sur ce programme, a donné à Denis Edwards le rôle éminemment visible qui consiste à délivrer au comité de pilotage les mises à jour et les présentations. ▶

## Le dilemme du désir

Tous les subordonnés directs ne veulent pas piloter l'informatique. Il est donc crucial que les DSI soient au courant des plans de carrière de leurs collaborateurs. Ainsi, ils savent qu'ils soutiennent un candidat qui veut vraiment le poste.

Quelle est la solution ? Avoir cette conversation. Brian LeClaire de la société Humana précise : « *il y a quelques années, Bruce Goodman m'a donné l'opportunité d'expliquer quel poste je voulais atteindre dans l'entreprise.* » Il ajoute : « *Je lui ai répondu que je voulais acquérir une expérience dans la gestion des opérations, donc Bruce Goodman et ses collaborateurs m'ont donné des responsabilités dans ce domaine, en plus de l'IT.* » Brian LeClaire conseille aux subordonnés directs des DSI : « *si votre DSI n'aborde pas cette discussion avec vous, alors c'est à vous de l'initier.* »

Et si vous, en tant que DSI, avez de la crédibilité auprès du comité exécutif, vous avez le pouvoir de choisir votre successeur. Plutôt que d'attendre jusqu'au moment où vous êtes en train de préparer votre départ, prenez le temps maintenant de donner à vos meilleurs collaborateurs la possibilité de tester le job. ■

Par Martha Heller, de CIO Executive Council

Pour en savoir plus



Retrouvez  
La version  
originale  
sur [CIO.com](http://CIO.com)

# FORUM AGILITE DU SYSTEME D'INFORMATION

## La compétitivité de l'entreprise portée par la réactivité de l'IT

Jeudi 7 octobre 2010 de 8 h 30 à 16 h 00 - Automobile Club de France - Paris 8e

Après une phase d'intense pression sur les budgets due à la crise économique, les entreprises doivent être prêtes pour un changement de perspective replaçant l'esprit entrepreneurial et l'innovation au premier plan, selon l'institut Gartner.

Au-delà des questions de rationalisation et de réduction des coûts qui demeurent d'actualité, la DSI doit apporter des réponses encore plus rapides et pertinentes aux métiers, vis-à-vis desquels elle se positionne en tant que partenaire Business afin de permettre à l'entreprise de créer de la richesse.

Les rédactions de CIO, LeMondelInformatique.fr et Reseaux-telecoms.net vous proposent de participer à cette journée\* conférences et débats autour des gains attendus de l'agilité du système d'information, avec des experts et des décideurs IT impliqués dans l'exploitation, l'évolution et la fourniture de services aux utilisateurs.

### Principaux thèmes abordés durant la conférence :

- Les services de Cloud Computing,
- L'Architecture d'Entreprise, l'urbanisation du système d'information, les SOA,
- La maîtrise de la qualité de service,
- La collaboration entre les métiers et les équipes IT,
- La réduction de la complexité du SI,
- La réduction des délais de développement et de déploiement,
- Le mariage des démarches par silos et transverse

\* Conférence gratuite réservée aux DSI, Directeurs IT, Directions générales, Directions métiers, responsables des infrastructures et responsables sécurité des entreprises utilisatrices.

**INSCRIVEZ-VOUS**

## CONFÉRENCE STRATÉGIQUE

CONFÉRENCE ORGANISÉE LE 20 MAI 2010 PAR CIO

# La maîtrise des risques IT réclame une gouvernance adaptée et la gestion de la complexité

*Maîtriser les risques liés à l'IT est crucial pour les entreprises. Les meilleures pratiques en la matière ont été débattues lors d'une conférence organisée par CIO et Le Monde Informatique le 1<sup>er</sup> juin 2010 en partenariat avec IBM, Websense, Symantec et RSA Security.*

**D**ésormais, dans de nombreuses entreprises, la gestion du risque IT s'inscrit dans une démarche globale de gestion des risques. Dans ce cadre, comment réussir la mise en place concrète d'une politique de sécurité ? C'est ce thème stratégique qui a été débattu lors de la conférence CIO organisée le 1<sup>er</sup> juin à l'Automobile Club de France et qui a réuni cent décideurs IT en entreprise.

De multiples intervenants, internes ou externes, sont mobilisés dans la gestion des risques qu'il s'agisse des Risk Managers, des DSI, des RSSI, des auditeurs ou des managers métiers. Tous ces responsables doivent dialoguer efficacement entre eux et mettre en place une gouvernance ad hoc. Une démarche qui est d'autant plus indispensable que les contraintes réglementaires ne cessent de s'étoffer.

En ouverture de l'événement, Jean-Louis Bleicher, consultant, administrateur de l'AFAI (Association Française de l'Audit et du Conseil Informatique) et ancien directeur de la sécurité du groupe Banque Populaire, a mis en évidence les spécificités du risque IT : « *Les menaces IT se distinguent par leur caractère dynamique et croissent en même temps que la complexité technologique.* » Il a conseillé de mettre en œuvre des instances de pilotage des différents acteurs dont les responsabilités auront été attribuées. « Il faut une gouvernance prenant en compte le contexte de chaque métier » a-t-il souligné.

## Bâtir le dialogue entre les acteurs de la gestion du risque

Cette maîtrise du risque devient d'autant plus complexe que les entreprises font appel à des services de Cloud computing. « *Où sont les serveurs et les données ? Qui gère les sauvegardes ? Comment est assurée la sécurité au quotidien ? Autant de questions auxquelles les réponses, encore floues, posent problème aux Risk managers et aux auditeurs* » a relevé Loïc Guézo, directeur technique IBM Security Solutions chez IBM France, tout en défendant l'idée d'une sécurité embarquée dans les offres de Cloud. Une table ronde a ensuite abordé la question de la répartition des rôles entre les multiples intervenants impliqués dans la gestion du risque, du RSSI à l'audit – interne ou externe - en passant par la DSI ou le Risk Manager avec les témoignages d'AG2R-La Mondiale, de la Caisse des dépôts, d'Ernst and Young et de Schlumberger.

Toujours dans la foulée de l'émergence du Cloud computing et du Web 2.0, ainsi que face au développement de nouvelles réglementations, Frédéric Braut, directeur de Websense France, a pointé la criticité de la fuite d'informations. Une problématique à laquelle s'attaque une nouvelle génération de produits de DLP (Data Loss Prevention) qui réduisent l'effort de classification des données et bénéficient d'un reporting destiné aux non informaticiens. « *Leur mise en œuvre doit démarrer sur un périmètre limité à un département et à un type de données* » a conseillé Frédéric Braut, ajoutant que « *Le projet doit être mené dans le cadre d'une méthodologie consistant à confier aux métiers la définition des données critiques, sous l'égide du RSSI* ».

## Vers une industrialisation de la gouvernance

La gouvernance demeure une question clé. Patrice Payen, responsable Solutions Compliance et DLP chez Symantec, a présenté comment la gestion des risques et de la conformité doit évoluer vers cette gouvernance. « *Souvent réalisée à vue et de façon empirique, la gouvernance peut être industrialisée grâce à l'automatisation du contrôle des protections mises en place. Cela concerne aussi bien le* ►

contrôle de la configuration des comptes des utilisateurs que les processus de révision des règles des firewalls. »

Face à cette question de l'automatisation de la gouvernance et de la mise en conformité, Philippe Fauchay, responsable commercial chez RSA propose « d'automatiser l'ensemble des activités qui sont encore manuelles. Il s'agit par exemple de la gestion des dérogations aux politiques de sécurité pour ce qui est du département sécurité. Il faut également rassembler les informations dans un référentiel unique afin de construire des indicateurs synthétisés dans des tableaux de bord. Ces derniers doivent être adaptés à chaque profil utilisateur qu'il soit sécurité, informatique, métier, ou dirigeant de l'entreprise. » Un domaine que RSA a investi au travers du récent rachat d'Archer Technologies. Pour clore la conférence, les responsables sécurité de cinq grandes entreprises ont montré comment vendre des projets structurants de réduction des risques aux métiers et les réussir. On a ainsi pu écouter les bonnes pratiques mises en œuvre chez Areva, la Caisse des dépôts et Consignations, Carrefour, Eiffage Construction ou EADS. ■

Pour en savoir plus



Retrouvez  
l'évènement  
sur CIO Online

# CONFERENCE DECISIONNEL

## Améliorer la qualité des données au service des métiers

Mardi 21 septembre 2010 de 8 h 30 à 14 h 00 - Pavillon Dauphine - Paris 16<sup>e</sup>

Les outils décisionnels sont le moteur des décisions prises dans l'entreprise en fonction des informations disponibles. « *Savoir pour prévoir, afin de pouvoir* » disait le philosophe Auguste Comte. Le décisionnel est la clé de voûte de la performance pour tous les métiers. L'optimisation de ces outils est aujourd'hui vitale. De nombreux bouleversements ont marqué le marché de l'offre récemment. Et côté utilisateurs, l'heure est à la rationalisation d'une situation trop souvent anarchique ainsi qu'à l'amélioration de la qualité tant des données que des processus mis en œuvre.

Les rédactions de CIO et LeMondelInformatique.fr vous invitent\* le 21 septembre prochain à débattre avec des experts et des utilisateurs, des gains concrets des projets décisionnels récents, des difficultés de mise en œuvre et comment les contourner.

### Principaux thèmes abordés durant la conférence :

- Améliorer la qualité des données
- Mettre en place une plateforme MDM ou fédérer les sources d'information
- Quelle infrastructure IT pour une stratégie décisionnelle efficace ?
- Les applications qui doivent aller vers le temps réel
- Traiter les gros volumes de données issues du Web
- Les apports des solutions en mode SaaS et du Cloud Computing
- Traiter les données issues du web 2.0 et des réseaux sociaux

Une conférence gratuite réservée aux DSI, Directeurs informatiques, Responsables informatiques, Responsables décisionnels, Responsables métiers et Chefs de projet

**INSCRIVEZ-VOUS**

## DG de Randstad : « Le DSI doit parler fort »

*Le DSI doit parler fort et donner son opinion. Il doit savoir challenger les patrons métiers dans leur job et traduire les enjeux technologiques en enjeux business. C'est l'opinion de Jacques Culioli, directeur général de Randstad, en charge des finances et de l'IT.*

**CIO** : qu'attendez-vous d'un DSI ?

**Jacques Culioli** : Notre DSI doit nous annoncer quelles sont les options, les coûts, ce qui est réalisable ou pas selon les choix qui s'offrent à nous. Par exemple, nous utilisons l'outil eFront pour notre gestion de la relation client et une plateforme de développement .Net. Or, nous sommes en train de nous demander si nous n'allons pas redescendre vers .Net pour redévelopper notre outil. Ce que j'attends du DSI dans ce cadre c'est qu'il puisse expliquer en termes d'évolution de notre système d'information quel sera l'impact de nos choix technologiques sur notre gestion des dossiers, sur l'usage de notre moteur de recherche, etc.

**CIO** : quelle doit être la personnalité d'un DSI ?

**Jacques Culioli** : La qualité première d'un DSI c'est de parler fort, et de donner son opinion, sa vue. En comité de direction, sa personnalité doit lui permettre de s'imposer. Il doit arriver à être crédible, si la RH parle du système de rémunération. Il doit être capable d'intervenir sur le sujet. Ce n'est pas un passe-plat. Il doit proposer des alternatives sur les options. J'attends d'un DSI qu'il puisse challenger un patron des métiers, en lui disant « *Qu'est-ce que tu vas faire demain sur l'iPhone en termes de business de recrutement et d'affectation des intérimaires ? Qu'est-ce que tu vas faire avec ces nouvelles technologies qui émergent car voilà les idées que j'ai. Car je sais construire une voiture alors je ne suis pas forcément le meilleur pilote, mais la voiture est faite, je peux peut-être te guider sur la meilleure manière de l'utiliser ou de la changer dans le futur !* »

**CIO** : dès lors, le DSI doit-il être un technicien ou être passé par les métiers ?

**Jacques Culioli** : Dans dix ans, cela pourrait être quelqu'un des métiers. Mais il faut de l'appétence pour l'IT, et comprendre les enjeux, comment marche un projet. Le DSI doit éclairer la direction générale sur les enjeux business des technologies. Ceci dit, si je devais trouver un remplaçant à notre DSI actuel, et que je n'ai que deux ans devant moi, je n'irai pas chercher une personne des métiers pour la placer en adjoint du DSI actuel. Je prendrais quelqu'un qui comprend les technologies et qui est capable d'appréhender toutes les innovations pour parler aux opérationnels le langage des opérationnels en ayant compris le sens, la portée et les enjeux de ces questions technologiques.

**CIO** : le DSI doit-il être un ensemble ?

**Jacques Culioli** : je vois mal un DSI tout seul qui pilote des prestataires ! Le DSI doit présenter une maîtrise généraliste des problèmes techniques. Il doit présenter une maîtrise organisationnelle de ce qui doit être interne à l'entreprise, et externe à l'entreprise. Il doit comprendre finement les besoins métiers, et arriver potentiellement à être dans le business. En France, la DSI de Randstad c'est une centaine de personnes en interne et vingt personnes issues de prestataires. Nous avons un millier d'agences de trois à quatre personnes. Dans notre groupe, les systèmes d'information sont clé à la fois pour améliorer la productivité de nos agences mais aussi de se différencier auprès de nos clients. L'informatique est vraiment centrale dans la stratégie de l'entreprise.

**CIO** : pensez-vous qu'il y aura encore un DSI dans 10 ans ?

**Jacques Culioli** : Il y aura toujours un DSI dans 10 ans, parce que les problèmes des systèmes d'information sont de plus en plus importants dans les entreprises, et que les technologies se complexifient. Ceci dit, que le DSI fasse encore ce qu'il fait aujourd'hui : non ! Le DSI doit se positionner comme un *Business Partner*. On ira même plus loin, et le DSI deviendra le créateur de valeur ajoutée de l'entreprise qui est elle-même technologique. Le DSI devra expliciter pour le *business* les enjeux technologiques dont on voit qu'ils évoluent très rapidement. De la même façon que le directeur financier ne parle pas de schéma comptable lors des comités de direction, mais de l'impact des normes

comptables sur les résultats ou le bilan de l'entreprise, le DSI doit être capable de transformer des questions d'enjeux technologiques en questions *business* qu'un comité de direction puisse apprécier et trancher.

**CIO**: *quel type d'initiatives business un DSI peut-il prendre ?*

**Jacques Culioli**: plus précisément, dans le cas de Randstad France, notre DSI devient leader sur des lignes de produits issus de la DSI. Ainsi, notre DSI doit bâtir une plateforme d'auto évaluation commune pour nos métiers. Par extension, cette plateforme sert à nos clients pour des tests d'autoévaluation. Ce n'est pas notre directeur marketing qui peut développer cette ligne de produits. Notre DSI doit bâtir un Business Plan pour cela. Il ira également évangéliser les 900 agences avec l'offre fournie sous la forme d'une plateforme Saas.

**CIO**: *avez-vous un autre exemple ?*

**Jacques Culioli**: Une autre ligne de produit est un portail de gestion des candidatures par internet pour les PME, baptisée « *Free Job Posting* ». Dans ce cadre, nous mettons gratuitement en ligne le profil d'un candidat recherché pour une PME. Cette offre est portée par nos commerciaux. Les réponses seront transmises également gratuitement à la PME. Si le poste n'est pas rempli au bout de 15 jours, nous recontactons la PME pour lui proposer alors une mission. Nous pouvions mettre en place un chef de projet marketing sur ce type d'offres, mais celle-ci est trop technologique, le DSI s'impose plus naturellement. L'offre reste toutefois portée par le marketing. Le DSI fait partie de l'équipe de Leadership. Le DSI est ainsi au cœur du business. Cela l'intéresse. Ces offres technologiques pour nous sont l'occasion de nous différencier de la concurrence, car nous ne sommes pas propriétaires de nos intérimaires. Et c'est un plus pour nos clients, cela peut servir à ouvrir des portes. Dans ce cadre, le salaire du DSI comporte une part de 30 % variable. Parmi les objectifs, la réussite commerciale de l'offre de la plateforme d'autoévaluation vient impacter son salaire. L'intéressement comprend le fait que le produit fonctionne et les objectifs commerciaux associés à cette plateforme soient atteints. ■

Pour en savoir plus



Retrouver  
l'interview vidéo de  
**Jacques Culioli**  
sur [CIO-online.com](http://CIO-online.com)

Par Jean Pierre Blettner

## RANDSTAD EN FRANCE

Le Groupe Randstad est un groupe mondial de services en ressources humaines. Il est le deuxième groupe mondial après sa fusion avec Vedior. En France, Randstad est présent depuis cinquante ans et intervient dans tous les secteurs d'activité pour du recrutement, du travail temporaire, de l'approche

directe, du conseil, de la formation et du reclassement. En 2008, le chiffre d'affaires pour la France a été de 3,9 milliards d'euros. Le groupe anime 1000 agences de 3 à 4 personnes sur tout l'hexagone. Randstad emploie 5 000 collaborateurs et délègue environ 400 000 intérimaires par an. ■

# De Décideur IT à Business Partner : la DSI atout concurrentiel

Mardi 19 octobre 2010 de 8 h 30 à 14 h 00 - Hôtel Prince de Galles - Paris 8e

Dans les grandes organisations où le système d'information possède un rôle central, les managers IT doivent jongler entre l'émiettement des entités et des besoins, la pression sur les coûts, et les délais.

Quelle organisation faut-il mettre en place et quels sont les moyens d'action afin de tenir la feuille de route fixée entre les métiers et la direction générale? Comment la DSI passe-t-elle alors du statut de prestataire - dont on peut changer à volonté - à celui de partenaire dans la création de valeur et d'avantage compétitif afin de transformer l'entreprise? Au-delà des traditionnelles questions d'excellence opérationnelle qui demeurent d'actualité, la DSI doit apporter des réponses en profondeur et aider à construire le futur à l'heure où l'entreprise s'attaque à des modèles économiques inédits et veut gagner en efficacité.

Les rédactions de CIO et du MondeInformatique vous invitent à participer à la conférence "De décideurs IT à Business partners" pour débattre avec des experts, des utilisateurs et des leaders technologiques.

\* Conférence gratuite réservée aux DSI, Directeurs IT, Directions générales, Directions métiers, responsables des infrastructures et responsables sécurité des entreprises utilisatrices.

**INSCRIVEZ-VOUS**

SENSIBILISER LES UTILISATEURS À LA SÉCURITÉ



CIO EVENEMENTS 2010

Inscrivez-vous dès à présent aux conférences 2010 sur [cio-online.com](http://cio-online.com)

Mardi 21 septembre 2010

**MATINÉE DÉCISIONNEL**

Le décisionnel est l'arme d'amélioration de la performance indispensable à l'entreprise. Le besoin est transverse : suivi des ventes comme la gestion des ressources humaines, de la relation client ou même de la production.

Judi 7 octobre 2010

**JOURNÉE AGILITÉ DU SYSTÈME D'INFORMATION (FORUM SOA)**

L'agilité est un facteur clé de la réussite d l'entreprise. Le système d'information doit aider à accélérer la mise sur le marché d'offres concurrentielles. Délivrer les bons applicatifs au bon moment nécessite des architectures rapidement reconfigurables du type SOA-BPM, des méthodes de développement agile, des logiciels en mode SaaS et le recours au Cloud.

Mardi 19 octobre 2010

**MATINÉE "DE DÉCIDEUR IT À BUSINESS PARTNER"**

Dans les grandes organisations où le système d'information possède un rôle central, les managers IT doivent jongler entre l'émiettement des entités et des besoins, la pression sur les coûts et les délais. Quelle répartition des rôles adopter et quels sont les moyens d'action afin que la DSI passe du statut de prestataire à celui d'acteur de la création de valeur métier?

Mardi 23 novembre 2010

**MATINÉE INNOVATIONS 2 011**

Qu'il s'agisse d'innovation managériale ou technologique, les décideurs IT sont en première ligne dans les entreprises.

SOMMAIRE N° 22 - AOÛT 2010

GUIDE SOLUTIONS: **Le DSI et l'intelligence économique**

GESTION DE CARRIÈRE: **Mener de grands projets IT publics sans être ni énarque ni polytechnicien**

DONNEURS D'ORDRE: **le trésorier compte sur le DSI**

**Une publication de :**

IT NEWS INFO - 6-8, rue Jean-Jaures 92800 Puteaux • Tél. : 0141976145

**Directeur de la rédaction :** Jean-Pierre Blettner • [jpblettner@it-news-info.com](mailto:jpblettner@it-news-info.com)

**Chef des informations :** Bertrand Lemaire • [blemaire@it-news-info.com](mailto:blemaire@it-news-info.com)

A participé à ce numéro : Johanna Godet

**Principaux associés :** Adthink Media et International Data Group Inc.

**Président :** Bertrand Gros

**Directeur de publication :** Marc Lavigne Delville

**Directeur général :** Jean Royné

**Président du groupe Adthink Media :** Sylvain Morel

**Réalisation :** Rémy Beaudégel

SEPIA Studio - 6 rue Jules Simon 92100 Boulogne

CIO est édité par IT NEWS INFO, SAS au capital de 3 000 000 €

**Durée de la société :**

jusqu'au 7 septembre/2106

**Siret :** 500 034 574 00029 RCS Nanterre