L'audit informatique au service du contrôle interne

Compte-rendu de la Rencontre Autour d'un verre du 11 octobre 2010

Conférence de Gina Gullà-Menez
rapportée par Martine Otter

Gina Gullà-Menez, Directeur de l'audit des processus et projets informatiques chez Sanofi-Aventis, est venue témoigner de 5 ans d'expérience d'audit informatique au service du contrôle interne. Elle nous a présenté de façon très concrète les différents aspects de l'audit informatique et du déroulement d'une mission d'audit.

Présentations

Gina Gullà-Menez

Gina Gullà-Menez est adhérente d'ADELI depuis de nombreuses années[1].
De formation ingénieur en informatique, elle a travaillé plusieurs années dans le domaine de la qualité du logiciel, en particulier chez France-Telecom R&D, où elle était en charge du programme d'évaluation des processus. Elle continue aujourd'hui à œuvrer à l'amélioration des processus, depuis 8 ans chez Sanofi, d'abord comme responsable qualité à la Direction du SI Groupe, puis depuis 5 ans à la Direction de l'audit informatique.

Le Groupe Sanofi-Aventis

L'activité du Groupe Sanofi-Aventis couvre historiquement l'ensemble du cycle de vie des produits pharmaceutiques, depuis la recherche, jusqu'à la commercialisation, en passant par la production industrielle et le marketing.

Le Groupe, centré sur le monde de la santé dont il est un des leaders[2], déploie aujourd'hui une stratégie de diversification, via l'acquisition d'entreprises (on citera par exemple l'acquisition d'Oenobiol).
Cette stratégie de diversification se traduit pour le contrôle interne, par une nécessité d'adaptation permanente et de flexibilité, permettant d'identifier les risques dans l'ensemble de la structure.

Le Groupe, présent dans une centaine de pays avec plus de 100 000 collaborateurs, est effectivement fortement décentralisé, ce qui a conduit à mettre en place un contrôle interne s'étendant sur l'ensemble des filiales.
Son objectif est l'assurance de maîtrise des opérations et d'identification des risques. L'indépendance de l'audit interne est de ce fait fortement ancrée dans la culture de Sanofi-Aventis.

[1] *Gina avait organisé en 2002 les Assises ADELI, sur le thème des processus*

[2] *Sanofi-Aventis annonçait pour 2009 un chiffre d'affaires de 29 milliards d'euros et une croissance 6%*

Contrôle interne et audit informatique

La place du contrôle interne

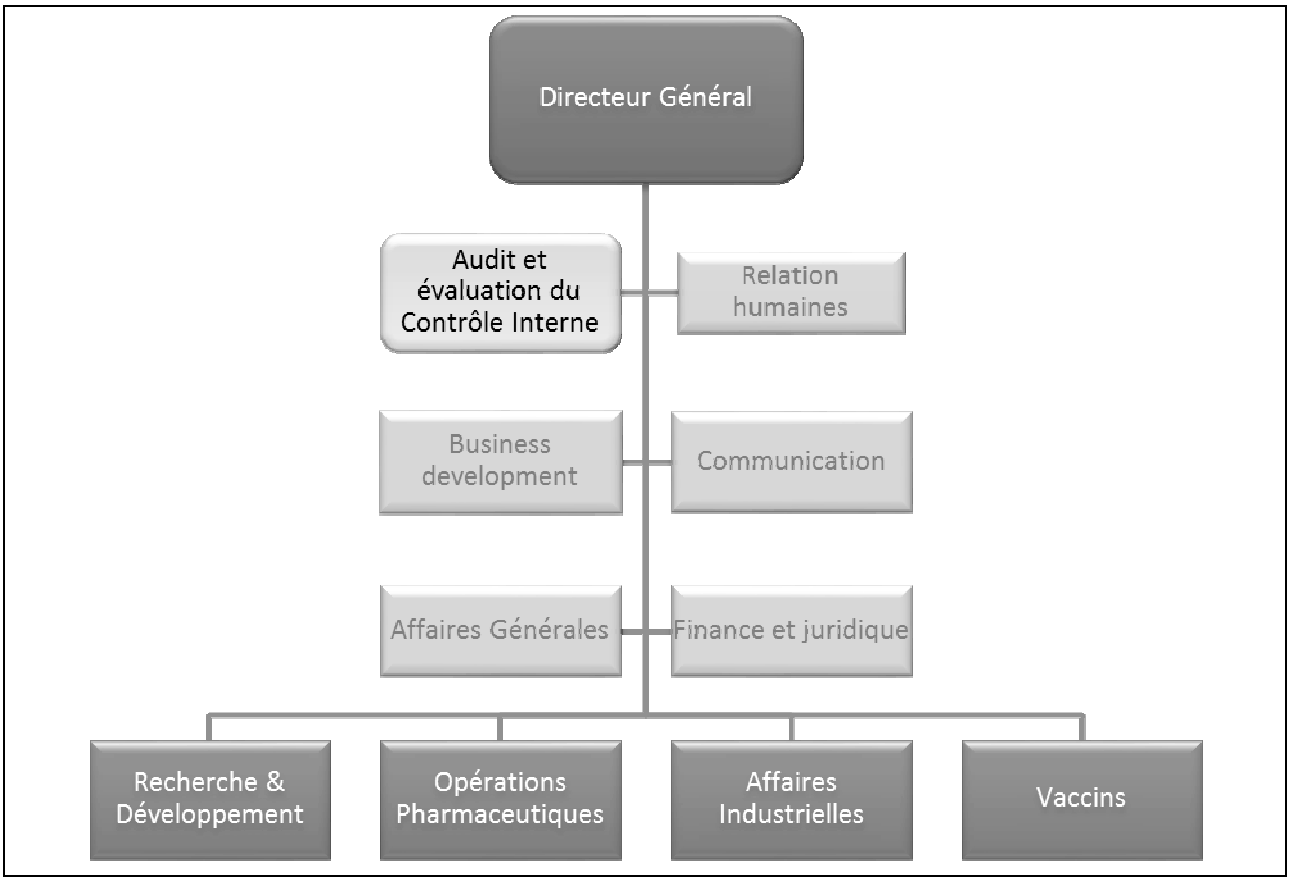

Figure 1 : Sanofi-Aventis - place du contrôle interne

Le contrôle interne est positionné de façon indépendante. Ainsi, à l'origine de sa création, il était rattaché au PDG, et depuis 2 ans, date à laquelle les fonctions de Président et Directeur Général ont été séparées, il rapporte à la Direction générale et à un comité d'audit, créé lors de la fusion Sanofi Aventis.
Il n'a ni autorité, ni responsabilité dans les opérations qu'il contrôle et effectue ses travaux d'audit librement. Il a pour responsabilité de fournir à la Direction Générale, et au conseil d'administration à travers le comité d'audit, « une assurance raisonnable sur le degré de maîtrise des opérations au sein du Groupe et sur l'efficacité du contrôle interne ».
On notera que l'audit interne Sanofi-Aventis a obtenu en 2006 la certification de l'IFACI (Institut Français de l'Audit et du Contrôle Interne) attestant de la conformité de ses prestations aux normes professionnelles internationales.

La place de l'audit informatique dans le contrôle interne

L'audit des systèmes d'information, apparu au cours des années 1970, a pour objet l'évaluation de la mise en conformité des processus et méthodes de l'entreprise avec un ensemble de règles en vigueur en matière fiscale, juridique ou technologique.
En cela, il se distingue de l'audit qualité qui vise l'évaluation de la seule conformité au référentiel ISO 9001.

L'apparition de la loi de sécurité financière (LSF), adoptée par le Parlement français le 17 juillet 2003, ainsi que les nouvelles exigences réglementaires de type Sarbanes-Oxley, ont eu pour effet de généraliser et de systématiser la pratique de ces audits.

Compte tenu de l'importance du marché américain, le groupe Sanofi-Aventis se trouve soumis à la conformité à la règlementation de la FDA (*Food and Drug Administration : administration américaine des denrées alimentaires et des médicaments, qui a le pouvoir d'autoriser la commercialisation des médicaments sur le territoire des États-Unis*).
Le besoin de visibilité du contrôle interne du groupe, a évolué depuis 5 ans en étendant sa demande de visibilité aux opérations informatiques dont le rôle crucial en matière de maîtrise des risques a été reconnu.

L'équipe d'audit informatique est une équipe composée de 7 personnes.
Elle est organisée en 3 branches :

- sécurité et infrastructure ;
- applications informatiques ;
- processus et projets informatiques.

Elle s'appuie sur des ressources externes, d'équipes d'auditeurs spécialisés dans ces différents domaines, chaque équipe se constituant de façon dynamique en fonction du scope de l'audit.
Le métier d'auditeur interne informatique est fondé sur l'analyse de risque, ce qui est une différence supplémentaire avec l'audit qualité qui s'intéresse d'abord à la satisfaction du client.

L'audit informatique

Les missions d'audit informatique

Elles peuvent porter sur des thèmes de différente nature : sécurité, infrastructure (data center), applications, processus SI, projets, nécessitant le recours à des compétences variées.

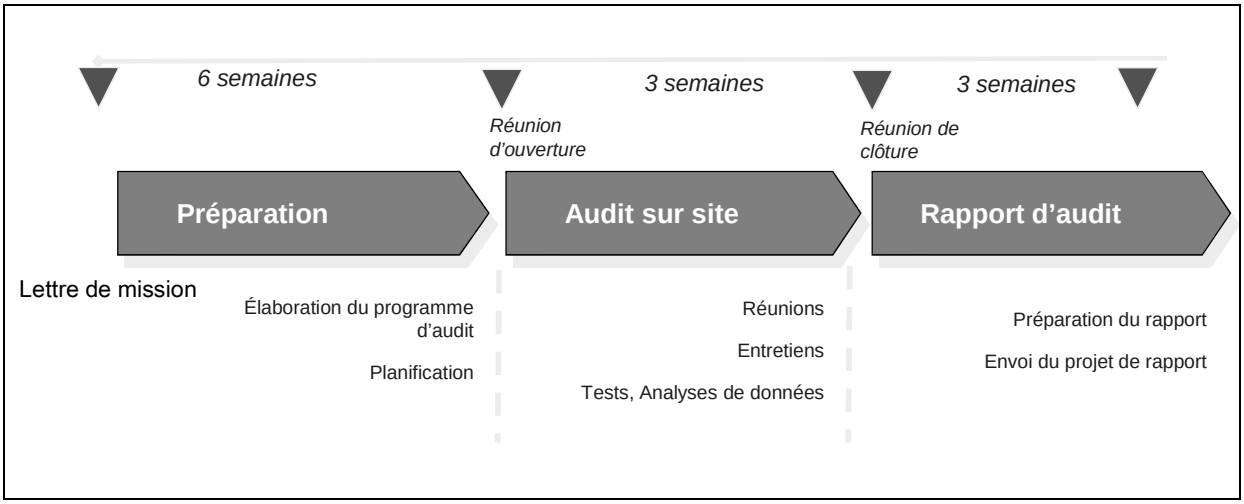

Figure 2 : Réalisation d'une mission d'audit

Ce cycle de mission s'étale sur une durée de plusieurs mois qui ne convient pas aux projets courts. La solution appliquée pour ce type de projet consiste à effectuer un audit de processus dont les recommandations pourront être appliquées sur le développement suivant.

L'analyse de données, au cœur de l'audit informatique

Gina insiste sur l'importance cruciale de l'analyse de données dans l'activité d'audit informatique. Il est en effet essentiel de ne pas baser les conclusions de l'audit sur des échantillons qui seraient fournis par les audités.

Il est préférable d'aller chercher les informations à la source.
Par exemple, sur un processus de continuité d'activité, l'analyse de la base des incidents permet d'apprécier des éléments tels que les délais de résolution et la qualité du service.
De même pour comprendre comment une application est protégée, une analyse systématique de l'extraction des bases de données permet de vérifier la bonne séparation des tâches, ce qui est souvent complexe sur les ERP !

Quelle méthodologie pour l'audit informatique ?

La mise en place de l'audit informatique chez Sanofi a bénéficié de l'expérience acquise sur l'audit interne. Les principes de la méthodologie d'audit interne ont pu être transposés à l'audit informatique.

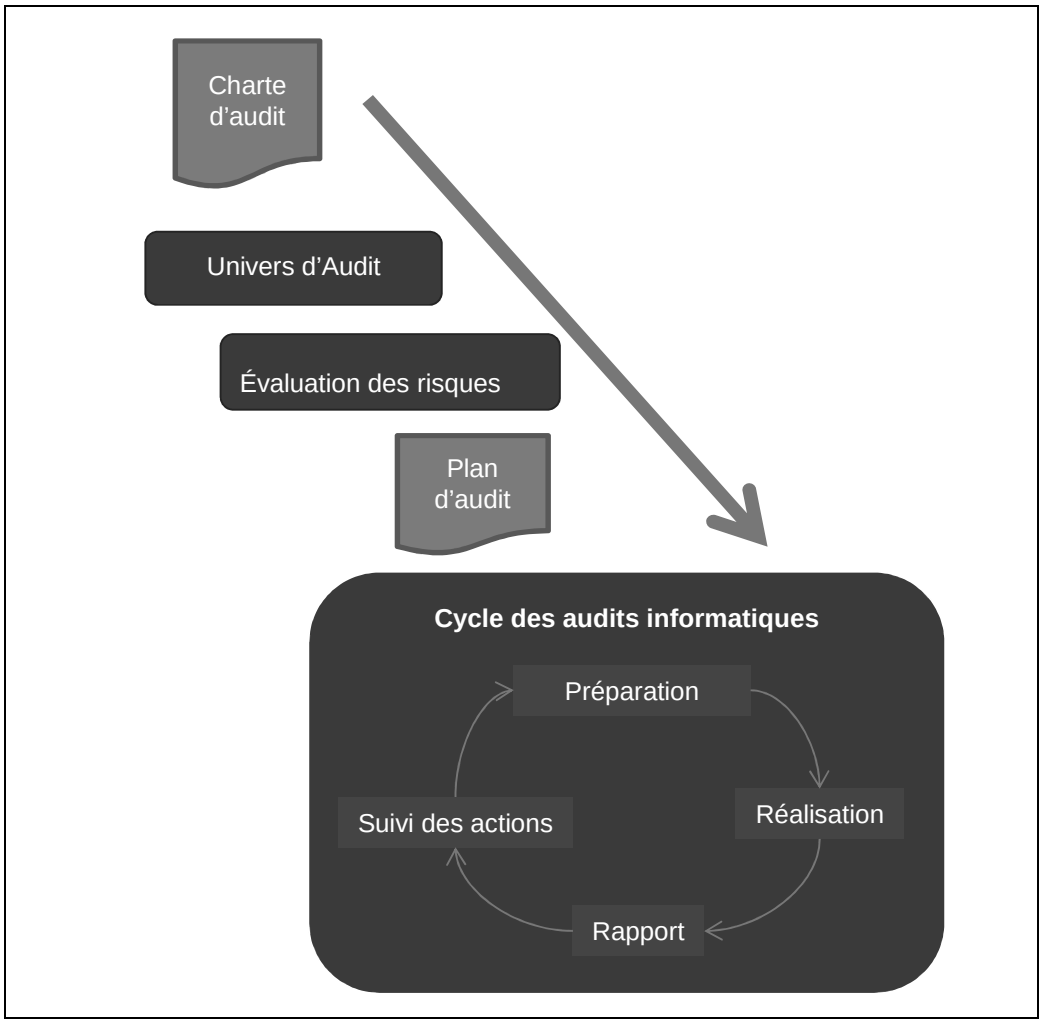

Figure 3 : Le processus d'audit SI

La charte d'audit définit les responsabilités, droits et devoirs des auditeurs et des audités.
L'univers d'audit est précisé : il s'agit de la liste d'objets auditables : centre de calcul, applications critiques, projets.
Le plan d'audit annuel s'appuie sur une analyse de risque partagée avec le contrôle interne et avec les DSI. Il énumère la liste des projets qui pourraient être audités. Il constitue le programme de travail, précisant les objectifs d'audit, c'est-à-dire en pratique l'ensemble des risques dont on veut tester la couverture : par exemple sur un risque de dérapage de projet on va tester l'application de bonnes pratiques de planification et l'utilisation effective d'une méthodologie. Ce programme de travail s'appuie sur des référentiels connus, tels CobiT, CMMI, ITIL.

Préparation de l'audit

Point de départ : une lettre de mission, signée au plus haut niveau, est envoyée au futur audité avec copie à l'ensemble de sa hiérarchie.
L'analyse de risque est préparée dans la mesure du possible par extraction et analyse de données. Dans le meilleur des cas on n'aura plus qu'à valider les observations sur site.
La constitution de l'équipe doit permettre de faire face aux difficultés culturelles qui peuvent survenir dans certaines filiales étrangères : dans certains pays, l'accompagnement par du personnel local apporte la crédibilité nécessaire ; l'équipe française pourra être complétée, si nécessaire, d'auditeurs locaux.

Les bénéfices pour le Groupe

La mise en place d'une approche par les risques permet de mieux sensibiliser les directions opérationnelles aux risques.
Une analyse des risques projet existait déjà mais se révélait insuffisante, car elle ne permettait pas la consolidation sur l'ensemble des activités.

Cette analyse des risques est faite dans une perspective métier : la fragilité d'une application informatique entraîne de fait celle du métier qui l'utilise.
La valeur ajoutée par l'analyse de risques est ainsi directement opérationnelle : les recommandations de l'audit interne doivent être réalistes, c'est-à-dire implémentables.

C'est la condition de leur application et de la crédibilité de l'audit interne.

Quelques questions

L'audit de l'architecture des systèmes

La qualité de l'architecture est difficile à auditer ; c'est un sujet fondamental mais il est difficile de trouver les bonnes compétences dans les cabinets pour réaliser ces audits.
Les compétences existent en interne mais il faut faire un choix entre les critères d'indépendance et de compétence.

Le suivi des audits

L'étape de contrôle post-audit est indispensable. La preuve de la mise en œuvre des recommandations est demandée aux services audités ; on ne se déplace pas sur site, on télécharge les informations utiles. Lorsque les éléments de suivi fournis ne sont pas satisfaisants, une mission de suivi peut être déclenchée, voire un nouvel audit.
Le pourcentage de recommandations appliquées est élevé et justifie le niveau de confiance accordé par la direction à l'équipe d'audit interne.▲

gina.gulla-menez@sanofi-aventis.com
martine.otter@adeli.org

Webographie

AFAI (Association Française de l'Audit et du Conseil Informatiques) : www.afai.fr
COSO (Committee of Sponsoring Organizations of the Treadway Commission) : www.coso.org
IFACI (Institut Français de l'Audit et du Contrôle Interne) : www.ifaci.com
ISACA (Information Systems Audit and Control Association) : www.isaca.org
Site dédié à l'audit des systèmes d'information : http://www.theiia.org/itaudit
Audit Net, site dédié au partage de connaissance des auditeurs : www.auditnet.org
Distributeur du logiciel ACL : www.acl.com
CNCC Compagnie Nationale des Commissaires aux Comptes : www.cncc.fr