1 –

# Audit informatique – audit des systèmes d'information

Evaluer les risques informatiques, risques des systèmes d'information

## Introduction à l'audit informatique

L'audit informatique, l'audit des systèmes d'information évalue les risques d'un environnement informatique ou d'une application, par exemple, les salaires ou la facturation. Ces missions se font en choisissant avec le client les processus métiers à évaluer, de même que les processus CobiT à évaluer parmi les 34 proposés.

L'audit d'un environnement informatique peut concerner l'évaluation des risques informatiques de la sécurité physique, de la sécurité logique, de la gestion des changements, du plan de secours, etc. Ou bien un ensemble de processus informatiques - ce qui est généralement le cas - pour répondre à une demande précise du client. Par exemple, apprécier la *disponibilité* des informations et des systèmes. Le CobiT permet justement de rechercher quels processus informatiques répondent le plus efficacement à une telle demande. Dans le cas de la *disponibilité :* par exemple la gestion des performances et des capacités et le plan de continuité.

Services offerts:

- Approche générale
- Audit de l'infrastructure informatique
- Audit d'un système - d'une application inforrmatique en cours de réalisation
- Audit d'une application informatique

Approche générale

Un audit informatique, audit des systèmes d'information, se fait selon un schéma en 4 phases :

1. Définition précise du plan de travail, récolte d'information, recherche et schématisation des processus métiers et/ou informatiques à apprécier, définition des rôles et responsabilités, analyse des forces - faiblesses.

2. Analyse des processus importants, définition des risques, évaluation préliminaire des risques, de l'efficacité des contrôles.

3. Tests des contrôles.

4. Tests de matérialité.

Un audit informatique, audit des systèmes d'information ne concerne pas nécessairement la sécurité. En effet, il peut servir à évaluer des aspects stratégiques ou de qualité des systèmes d'information. Par exemple, répondre à la question suivante : Est-ce que les systèmes d'information de l'entreprise répondent efficacement aux besoins des services métiers ? La démarche est très similaire, en choisissant et évaluant les processus informatiques proposés par le CobiT qui répondent le mieux à la demande et aux objectifs du client.

#### Audit de l'infrastructure informatique

Mission
Evaluer les risques des systèmes d'information nécessaires au fonctionnement des applications. Par exemple : Sécurité physique, sécurité logique, sécurité des réseaux, plan de secours.

Livrable
Rapport contenant les faiblesses relevées, leur niveau de risque et les mesures correctives proposées.

#### Audit d'un système - d'une application informatique en cours de réalisation

Mission
Assister l'équipe de projet à évaluer les risques lors des différentes étapes de réalisation d'un système / application informatique, proposer des mesures de réduction et de contrôle des risques importants et vérifier la qualité des processus de gestion des changements et de test du nouveau système / de la nouvelle application.

On distingue les contrôles applicatifs suivants (Guide d'audit des applications informatiques, Chambre fiduciaire suisse, 20.5.2008):

- création et autorisation,
- saisie et enregistrement des données,
- traitement des données,
- sortie des données (output),
- interfaces.

L'objectif des contrôles applicatifs est d'assurer (Auditing application controls, GTAG-08, The IIA, juillet 2007) que:

- toutes les données inputs sont exactes, complètes, autorisées et correctes,
- toutes les données sont traitées comme convenu dans une période acceptable,
- l'enregistrement des données est exact et complet,

- les outputs sont exacts et complets,
- un enregistrement est maintenu pour tracer le traitement des données depuis l'input jusqu'à l'enregistrement et à l'output éventuel.

Livrable
Mesures proposées de réduction et de contrôle des risques importants du nouveau système / application informatique.

**Audit d'une application informatique**

Mission
Apprécier une application informatique en production, par exemple une application de gestion des salaires, une application financière, etc. Très souvent plusieurs domaines font partie d'un audit d'une application, en particulier:

- les données opérationnelles,
- les données de base,
- les paramètres,
- les interfaces entre l'application et d'autres applications,
- la gestion des droits d'accès à l'application.

Bien entendu, tout audit d'une application doit également apprécier la sécurité de l'infrastructure informatique nécessaire au fonctionnement de l'application (cf. ci-dessus).

Livrable
Rapport contenant les faiblesses relevées, leur niveau de risque et les mesures correctives proposées.



**10 conseils pour piloter son audit des systèmes d'information**
***Les enjeux de la mise en œuvre d'un audit sont multiples et répondent à des problématiques de mise en conformité et de prévention des risques.***

Le concept d'audit des systèmes d'information, apparu au cours des années 1970, a pour but d'évaluer la mise en conformité des processus et méthodes de l'entreprise avec un ensemble de règles en vigueur (fiscales, juridiques, technologiques...).

Lorsque l'entreprise décide - ou est contrainte - de réaliser un audit, elle est alors amenée à se poser des questions sur la façon de le mener à bien et d'appréhender avec le plus d'objectivité possible les résultats des investigations opérées. Les conseils suivants - non exhaustifs - permettent de s'y préparer.

**1) Bien délimiter le champs d'investigation et les enjeux de l'audit**
L'audit des systèmes d'information (SI) couvre des domaines aussi différents que ceux liés aux processus, à la sécurité du système d'information, à la gestion des droits d'accès ou aux applicatifs métiers (audit de codes...).

L'une des principales problématiques auxquelles les entreprises sont confrontées lors de la mise en place d'une procédure d'audit est "de savoir si les enjeux stratégiques de la direction générale sont correctement déclinés à l'échelle du SI, conformément à la gouvernance d'entreprise", note Dominique Moisand, PDG du Cabinet ASK Conseil et vice-président de l'AFAI (Association Française de l'Audit et du conseil Informatique).

"La typologie d'audits est vaste et se répartit entre deux catégories que sont la fonction informatique d'une part et les applications avec les processus métier auxquelles elles participent d'autre part", fait savoir de son côté Serge Yablonsky, président d'honneur de l'AFAI, et directeur du cabinet d'audit Moore Stephens SYC.

Et le président d'honneur de poursuivre : "l'audit de la fonction informatique basé en général sur le référentiel CobiT peut couvrir l'audit de la stratégie, de la tactique, de l'opérationnel et de management de la fonction, tandis que l'audit des applications avec les processus métier couvrira, par exemple dans le cas de la gestion commerciale, la validation des données, la fiabilité et la réactivité des traitements ou encore la conformité réglementaire"

Mener un audit global sur autant de domaines variés et différents les uns des autres ne devrait sans doute pas être privilégié, et il conviendra de cibler un processus ou un domaine applicatif précis pour tendre vers un maximum de pertinence et d'efficacité.

**2) Se préparer à la procédure d'audit**
La démarche d'audit sera motivée par la volonté de l'entreprise ou de la direction des Systèmes d'information (DSI) à veiller à la bonne mise en conformité de ses processus d'une part, mais aussi à mieux identifier ses points de vulnérabilité d'autre part. Un préalable à l'audit de sécurité serait par exemple de déclencher régulièrement des simulations d'attaques logiques et d'analyser les temps de réaction de la découverte à la clôture de l'incident, de suivi des procédures déjà en place...

**"Les audits peuvent être planifiés ou bien établis dans l'urgence"**
**(Dominique Moisand - ASK Conseil)**

Il peut être nécessaire que l'entreprise soit d'abord consciente de ses propres lacunes et de savoir pourquoi elle est susceptible de repenser et de remettre à plat tout ou partie des procédures existantes. La procédure d'audit permet à la fois de valider une

hypothèse de vulnérabilité ou bien de découvrir une menace éventuelle à laquelle l'entreprise ne s'était pas préparée.

Par ailleurs, deux catégories d'audit peuvent être identifiées : les audits planifiés et ceux qui sont réalisés dans l'urgence ou "à chaud". "Les audits commandités dans l'urgence seront réalisés lorsqu'un projet ne se déroule pas comme prévu, ou lorsque l'entreprise se retrouve en situation de pré-contentieux avec un fournisseur", indique Dominique Moisand.

**3) Séparer le commanditaire de l'entité en charge de l'audit**
L'audit doit théoriquement être mené par des intervenants indépendants de la DSI, mandatés cependant par la direction générale, afin de bénéficier d'un recul suffisant par rapport à l'entité de l'organisation qui est l'objet de l'audit. Cependant, des audits seront commandités spécifiquement par la DSI lorsque les enjeux seront typiquement liés à ses processus internes (suivi de la production, suivi de la qualité de service...).

Les audits mis en œuvre dans le cadre des contrôles des accès, à la conformité avec les réglementations Sarbanes-Oxley (SOX) ou Loi de Sécurité Financière (LSF), dépassent toutefois les préoccupations de la DSI, et requièrent nécessairement l'implication de la direction générale.

**4) Se doter d'une direction de l'audit interne, oui, mais...**
A priori, seules les grandes organisations sont potentiellement en mesure de dédier et mobiliser des ressources internes adéquates visant à mettre en place - et de façon la plus transparente possible - une cellule dédiée à l'audit. Même si cela ne va pas sans poser certaines interrogations.

"L'établissement d'une structure d'audit interne ne peut pas être viable économiquement en étant seulement rattachée à la DSI. Elle doit nécessairement être rattachée à un haut niveau décisionnel et ne pas uniquement concerner la DSI, mais d'autres fonctions de l'entreprise", prévient Dominique Moisand.

**5) Recourir à des référentiels solides**

**Une fois la décision prise de réaliser l'audit, il convient de s'appuyer sur un référentiel reconnu**

Une fois la décision prise de réaliser ou de confier l'exécution de l'audit à un cabinet externe spécialisé, il conviendra de s'appuyer sur un référentiel reconnu et bénéficiant de surcroît d'une forte légitimité. Ainsi, parmi la multitude de référentiels servant de base à la réalisation des audits : ISO, CobiT (*Control Objectives for Business and related Technology*) dans le cadre de processus transverses, CMMI (*Capability Maturity Model Integration*), dans celui du pilotage de projet, ITIL (*Information Technology Infrastructure Library*), pour les services...

"L'audit permet de mesurer un écart entre un référentiel donné et la réalité observée et prendra également en considération les bonnes pratiques métier en vigueur dans l'entreprise", précise Dominique Moisand.

**6) S'entendre sur le référentiel choisi**
L'ensemble des parties prenantes concernées par les enjeux de l'audit doivent avoir une vision sur le référentiel qui aura été choisi. Cette première étape de mise en conformité assurera la clarté de la démarche d'audit qui sera ainsi appréhendée dans le temps.

Partager un référentiel commun consiste également à transmettre et communiquer aux parties prenantes les avancées de la démarche d'audit au fur et à mesure de son évolution.

**7) Préparer les pièces indispensables à l'audit et en faciliter l'accès**
Pièce maîtresse de l'audit des systèmes d'information : le cahier des charges, qui a pour vocation à contractualiser les besoins d'une entité envers un tiers, prestataire de service ou agissant comme tel au sein de l'organisation. Parmi les autres documents nécessaires à la réalisation de l'audit, on trouve le plan qualité, les tableaux de bord et indicateurs de performance, la gestion des problèmes récurrents...

Une fois ces pièces collectées, la structure en charge de l'audit pourra demander à accéder à d'autres types de documents qui concerneront par exemple le suivi des incidents et les procédures de résolutions de problèmes (dans le cadre de l'audit de sécurité et des tests intrusifs) ou bien aux éléments de construction de l'édifice comptable (audit financier).

**8) Confier son audit à une équipe pluridisciplinaire et indépendante**

**Le dispositif d'audit repose avant tout sur les ressources humaines mobilisées**

Le dispositif d'audit repose avant tout sur les ressources humaines mobilisées dont le nombre variera par essence en fonction de la taille de l'entité, des processus ou applications audités. Plusieurs compétences seront nécessairement représentées au sein d'une cellule d'audit qui s'articuleront autour d'un chef de mission.

Disposant de fortes capacités relationnelles, le poste pourra être tenu par un ex-directeur des systèmes d'information disposant par ailleurs de connaissances techniques mais surtout de gestion et de management. Il sera épaulé d'auditeurs opérationnels, dotés : "de capacités d'analyse, d'une propension à mener des investigations, à décortiquer des documents aussi bien comptables, techniques que procédurales", fait savoir Dominique Moisand (ASK Conseil).

Enfin, des experts dans un domaine spécifique (code, sécurisation des réseaux...) pourront éventuellement intervenir ponctuellement, avec pour inévitable effet de faire grimper la facture de la prestation d'audit qui pourra atteindre les 2 600 euros par jour.

**9) Choisir la fréquence et le temps de déroulement de l'audit**
Les audits pourront être réalisés à des intervalles ne devant, *a priori*, pas excéder les deux ans, alors que le temps de réalisation de l'audit en lui-même ne devrait pas excéder un mois, selon Dominique Moisand.

Ce laps de temps -de la mise en place du premier comité de pilotage au rendu des conclusions d'audit-, semble être un maximum afin de limiter les effets anxiogènes de la mise en œuvre d'un audit sur les collaborateurs. Et sans compter sur l'amputation du capital temps des acteurs amenés à collaborer à cette démarche.

Quelques étapes clés peuvent par ailleurs être identifiées : "les principales étapes d'un audit seront notamment de fixer les objectifs, comprendre et cartographier le SI, d'en identifier les forces et les faiblesses, et d'émettre les recommandations pour en rédire les faiblesses et optimiser les forces", indique Serge Yablonsky.

Et le président de préciser : "une revue de contrôle des accès peut nécessiter deux jours pour les procédures, cinq à dix jours pour vérifier leur application effectuer et contrôler les profils,

voire un collaborateur à temps plein dans le cas de la mise en œuvre de tests d'intrusion".

**10) Ne pas sous-estimer les limites d'un audit**

En tant que prestation à forte valeur ajoutée, directions informatiques et générales attendent beaucoup de la publication des résultats d'un audit. Malgré tout, les risques de ne pas identifier l'ensemble des faiblesses et menaces d'un processus ou d'un applicatif ne sont pas nuls.

Parmi les contraintes et les limites potentielles : un temps imparti à l'audit restreint ou une appréciation biaisée du contexte fonctionnel et métier de l'organisation étudiée. Enfin, un léger réajustement technique ou organisationnel exercé a posteriori sur le SI peut remettre en cause tout ou partie des résultats d'un audit.