2265U08 – Audit Systèmes Informatiques

M. Jérôme BRZEZINSKI

Management Global – Gestion et Informatique

Formation à l'audit informatique
- Synopsis

Organisation des cours d'audit informatique

1/ Introduction – 11 janvier 2007
- La notion de risque
- Les types de risque
- Le management des risques
- Les risques liés aux systèmes d'information
- Impact sur la démarche générale

2/ Revue générale informatique – 18 janvier 2007
- La politique informatique
- L'organisation et les équipes du service informatique
- La configuration matérielle et réseau
- La cartographie applicative
- Les contrôles généraux informatiques
  - La gestion de la sécurité informatique
  - La gestion des changements informatiques
  - Le développement informatique
  - L'exploitation informatique
- Exemples

3/ Revue d'applications informatique – 25 janvier 2007
- Historique et insertion de l'application dans l'architecture globale
- Couverture fonctionnelle & dysfonctionnements
- Schéma des traitements et matrice de contrôle
- Identification des risques
- Approfondissement des risques identifiés
- Analyse des aspects « qualitatifs »

4/ Test informatiques – 1er février 2007
- Avantages des tests informatiques
- Situations amenant à procéder à des test informatiques
- Typologie des tests informatiques
- Démarche dans le cadre d'une mission CAC
- Les facteurs de réussite
- Présentation de l'outil « IDEA »

5/ Audit de la sécurité informatique – 8 février 2007
- Etat des lieux
- Continuité de service
- Confidentialité des informations et risques de fraude
- Risques d'erreur et de dysfonctionnement
- Méthode MARION

6/ Contrôle interne / SOX – 22 février 2007
- Contexte
- Démarche SOX
- Dimension Systèmes d'information
- Cas des processus externalisés

7/ Audit en environnement ERP – 15 février 2007
- Impacts des ERP sur les risques liés au SI
- L'approche spécifique d'audit des ERP
- Exemple de flux SAP
- La fraude et les méthodes de prévention de détection

8/ Examen – 8 mars 2007
- Questionnaire à choix multiple de type CISA

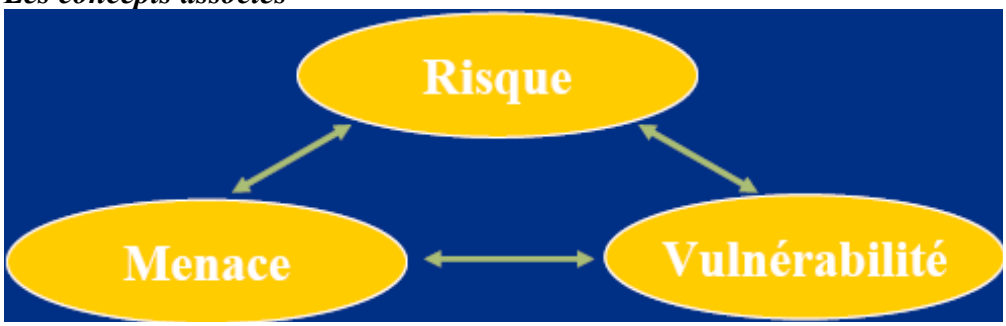
Introduction

Notion de risque

Définition

- Risque
  « Danger, inconvénient plus ou moins probable auquel on est exposé. » (Larousse)
- Les implications directes
  - Risque pour qui ?
    Rq : en fonction de l'activité (ex : industries, banques, etc.) et de la taille (ex : régionale, nationale, internationale) des entreprises, les risques ne sont pas les mêmes.
  - Importance relative / impact ?
  - Probabilité d'occurrence ?

Les concepts associés



- Risque
  - Fonction de la menace et de la vulnérabilité
  - Caractérisé par une probabilité et un impact

Un peu d'histoire

- De la perception de l'avenir…
  - Jusqu'à l'époque de la Renaissance, l'avenir est entre les mains d'une force supérieure, et l'homme agit dans une perspective d'éternité ;
  - La notion de « Progrès » bouleverse le rapport au temps : le présent est dorénavant occupé à construire l'avenir
- …A la perspective du risque
  - La théorie des probabilités date du milieu du XVII^{ème} siècle (Pascal / Fermat) ;

- En cinquante ans, les bases de la probabilité du risque sont posées, entraînant l'émergence des métiers de la finance, de l'assurance, etc. ;
- La dernière pierre est posée au XX^{ème} siècle, avec la mesure du retour sur investissement, ouvrant la voie au « risk management ».

Les types de risque

Multiplicité des risques

- Risque pays
- Risque de taux
- Risque de crédit
- Risque de vol
- Risque d'approvisionnement
- Risque de change
- Risque social
- Risque environnemental
- Risque fiscal
  Rq : fraude fiscale
  Le risque fiscal est sous-estimé en France.
- Risque d'exploitation
- Risque de catastrophe
  Rq : inondation du 1910 à Paris
- Risque stratégique
- Risque d'intrusion

Mode de classification

Par type de menace :

- Risques de marché
  - Risque de taux
  - Risque de change
  - Risque de crédit
  - Risque pays
- Risques stratégiques
  - Risque d'image
  - Risque d'alliance
  - Concurrence
  - investisseurs
- Risques opérationnels
  - Risque d'approvisionnement
  - Risque social
  - Risque de malveillance
  - Risque fiscal
- Risques de catastrophe
  - Catastrophes naturelles
  - Risque juridique catastrophe boursière
  - Risque terroriste

Par moyen de protection :

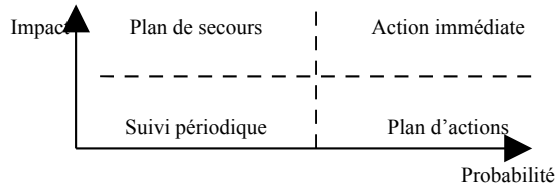
Risque global

- Risque acceptable
  - Risque social
  - Risque fiscal
- Risque couvrable
  - Risque de taux
  - Risque de cours
  - Risque de change
- Risque assurable
  - Risque de vol
  - Risque de catastrophe
  - Risque d'exploitation
- Risque diversifiable
  - Risque d'approvisionnement
  - Risque d'exploitation

La règle du « sur mesure »

- Il n'existe pas de classification universelle des risques, pas plus que de système de gestion prêt à l'emploi
- Chaque entreprise se doit de réaliser sa propre classification, en fonction notamment de :
  - Son secteur d'activité
  - Sa position concurrentielle
  - Son organisation
  - Etc.…

Par propriété pour l'entreprise :



Rq : « plan de secours » est le plan d'organisation et de réaction prévu en cas du risque concerné survenu.

Le management des risques

Démarche générale

- Stratégie
  - Définition et qualification des risques
  - Stratégie d'audit
- Evaluation des vulnérabilités
  - Evaluation de vulnérabilités
  - Plan d'action
- Moyens de protection
  - Mise en œuvre des moyens de protection
  - Plan de communication et de formation
- Actions de suivi

- Mesure de la conformité
- Plan d'audit

Stratégie de risque

Définition et qualification des risques :

- Identifier l'ensemble des risques
  - Inhérents à l'activité et au secteur
  - Propres à l'organisation
  - Etablir une classification (par impact, …)
  - Obtenir la validation de la Direction Générale

Elaboration de la stratégie d'audit :

- concevoir une charte d'audit
- attribuer les responsabilités
- allouer les ressources

Evaluation des risques

Evaluation des vulnérabilités :

- définir les outils et les moyens d'investigation
- évaluer les dispositifs en place
  - détection et prévention
  - protection
  - transfert
- établir la cartographie du risque résiduel

Conception du plan d'actions :

- objectifs claires et mesurables
  Rq : plus il est simple, plus il marcherait mieux.
- responsabilités et moyens identifiés
  Rq : avant tout (càd les moyens de sécurités), la gestion des risques est une mise en place d'une politique de démarches de contrôle.

Mise en œuvre

Mise en œuvre opérationnelle :

- conception et déploiement des solutions
  - mode projet incluant les opérationnels
  - mesure d'efficacité
  - respect des moyens alloués
- intégration dans les processus existant

Communication et formation :

- diffuser les référentiels
  Rq : « comment on mesure et classer les risques ? »
- intégrer la gestion du risque dans les objectifs individuels

Système d'assurance

Mesurer la conformité :

- suivi de la réalisation du plan d'actions
- tableau de bord de la gestion des risques

Etablir le programme d'audit :

- revue périodique des vulnérabilités

- contrôles spécifiques

Pérenniser la démarche :

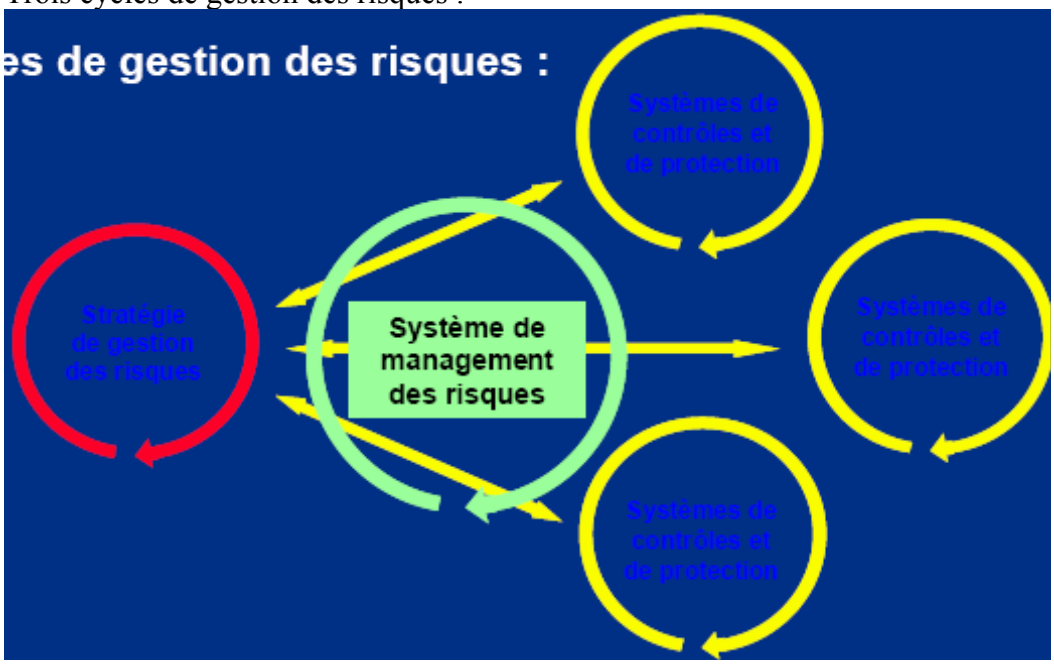
- industrialiser les outils
- maintenir la communication interne

Vers une vision dynamique

Evolution des enjeux et objectifs de l'entreprise :

- amélioration de la performance
- modification des contraintes réglementaires
- apparition de nouveaux concepts :
  - développement durable
    Rq : « social », « environnemental » et « économique »
  - éthique
- recours aux nouvelles technologies
- étendue du champ de certification

Trois cycles de gestion des risques :

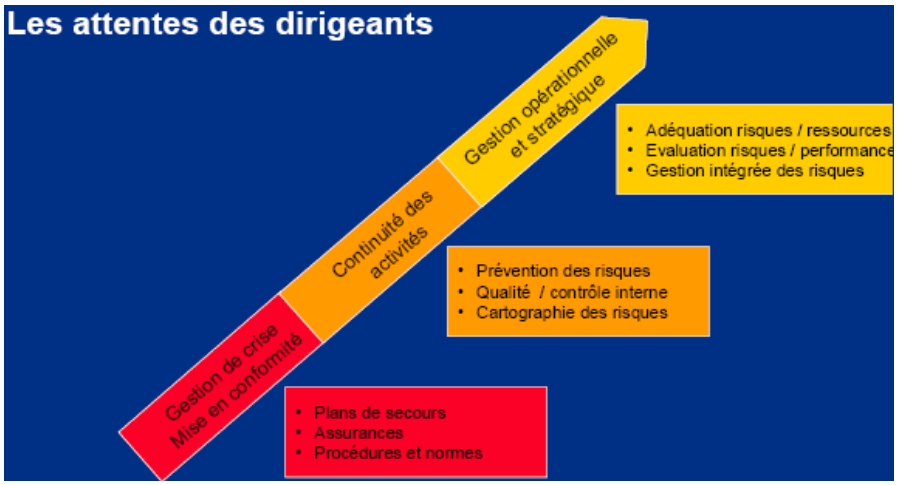


Rq : les systèmes ont une auto-évaluation et remontent les informations à travers le système de management des risques qui fait la synthèse.

La position des organisations

Le « business model » de l'entreprise

- Processus de l'exécutif : stratégie, organisation, pilotage, …
- Processus opérationnels : production, achat, vente, …
- Processus support :
  - Gestion comptable et financière
  - Gestion des ressources humaines
  - Système d'information
  - Fonction juridique



Rq : en fonction de leurs niveaux différents, on communique sur de différents termes.

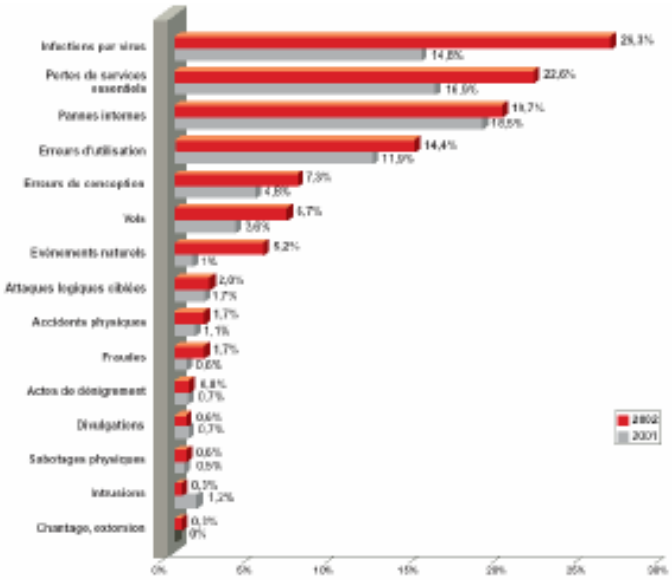
Les structures de gestion des risques
- Niveau 1 : responsabilité implicite
  - va de paire avec la fonction
  - absence de processus de suivi
- Niveau 2 : responsabilité définie
  - délégation formelle
  - intégration à l'organigramme
- Niveau 3 : responsabilité globale
  - Comité ou direction des Risques
  - Risk Manager
- tendances :
  - gestion du risque liée aux contraintes réglementaires (organismes de crédit)
  - notion de gestion intégrée :
    - responsabilité transversale
    - optimisation des polices d'assurance

    Rq : il faut intégrer tout cela dans les pratiques quotidiennes.
  - évolutions des pratiques liées au gouvernement d'entreprise
  - communication externe sur la gestion des risques

Les risques liés au système d'information
Des risques à la hauteur des enjeux
Définition de la notion de systèmes d'information

Le systèmes d'Information : une fonction transversale
- participe à tous les processus de l'entreprise
- reflet de la stratégie

... à hauts risques
- évolution des technologies
- ouverture sur l'extérieur / image
- risques inhérents



- Coût des pertes supérieur à 2 milliards d'€
- Progression forte de la malveillance au cours des dix dernière années

Les types de risques

En utilisant les projets à la mise en conformité des contraintes externes… :

- Fraude
- Malveillance
- Contrôle interne
- Légal
- Continuité

…on cherche de plus une performance meilleure :

- Maîtrise
- Coûts
- Efficacité
- Efficience

Le positionnement de la DSI

- La tendance à la nomination de RSSI mais avec des difficultés de positionnement hiérarchique
- La possibilité du RSSI qui a la capacité d'évoluer vers un poste de RS
- Recours à des expertises externes: schéma directeur, pilotage de projets, sécurité...
  Rq : « schéma directeur » : une déclinaison informatique et business des acteurs opérationnels

Evolution des moyens mis en œuvre

Les tendances observées :

- utilisation de normes et méthodes reconnues (Afnor, Clusif, …) et des best practices
- niveau de formalisation plus élevé
  Rq : la quantité des documentations augmente
- compréhension et traduction des besoins utilisateurs
- niveau de service, performances, satisfaction : évolution vers des relations de type client / fournisseur

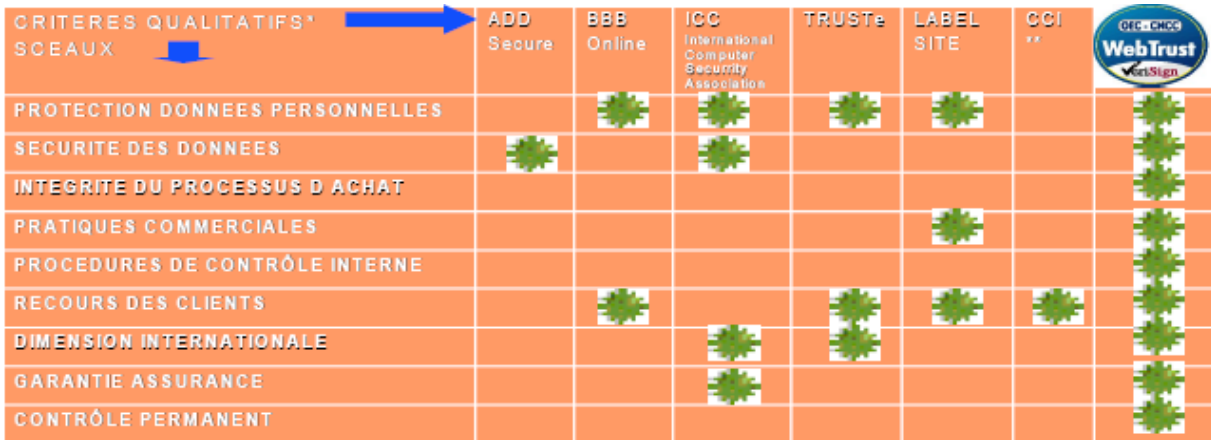
Les méthodes d'investigation

Couverture des risques inhérents :

- Revue Générale Informatique
  - la politique informatique
  - l'organisation et les équipes du service informatique
  - la configuration matérielle et réseau
  - la cartographie applicative
  - la gestion de la sécurité informatique
  - le développement informatique
  - l'exploitation informatique
- Audit sécurité: sécurité physique et logique, continuité d'exploitation

Couverture des risques liés aux processus externes :

- revue d'application
  - application "traditionnelle"
  - Audit des flux versus audit des traitements
- approche ERP
  - audit du paramétrage
- certification de sites de commerce électronique



- tests informatique
  - tests de valeur
  - tests de détection d'anomalies
  - tests de recoupement de bases
  - tests de simulation
  - outils d'audit : WinIdea, ACL, …
- respect des contraintes réglementaires :
  - article 103
  - environnement de contrôle fonction de la réglementation en vigueur

Synthèse

- En matière de gestion de risque, la pratique n'évolue pas au même rythme que la théorie
- La France reste globalement en retard par rapport aux pays anglo-saxons
- Les freins souvent observés :
  - sensibilisation de la DG

- appréciation de l'impact et de la probabilité
- vision dynamique
- lacunes de compétences ad hoc

Impact sur la démarche générale

Conséquence de l'« informatisation » pour l'auditeur

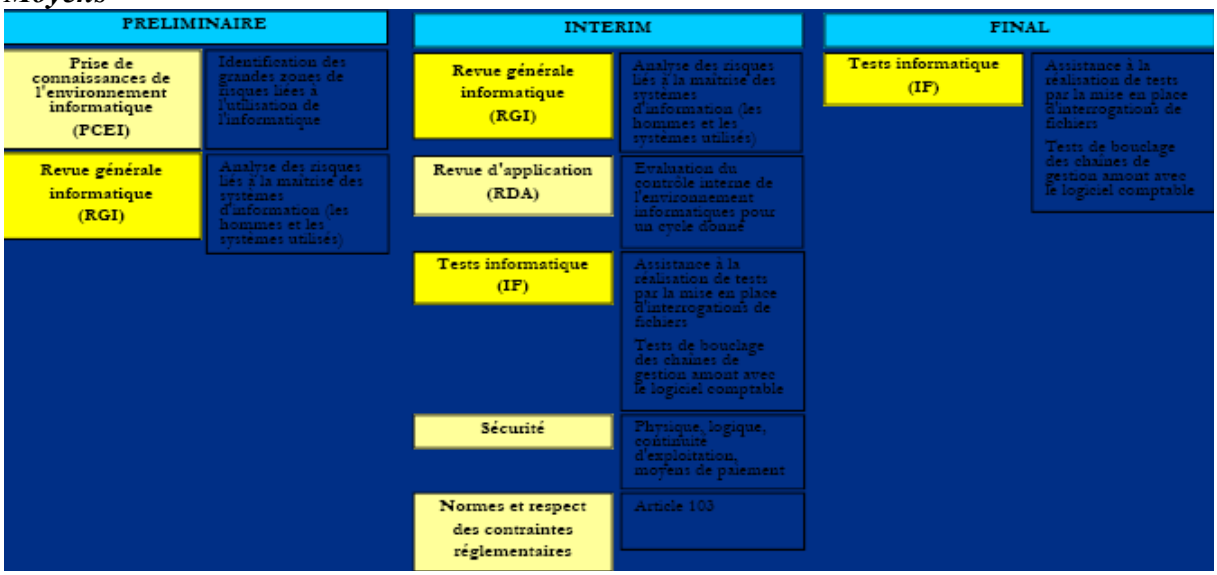
Apparition de nouveaux risques

- Augmentation des volumes
- Dématérialisation de l'information
- Barrière technique
- Automatisation des processus
- Évolution du périmètre du contrôle interne

Objectif

- Intégrer les travaux d'audit informatique dans l'approche de la mission pour participer à l'émission de l'opinion sur les comptes de la société
- Cette étape doit permettre de mesurer les risques liés à la présence de traitements automatisés
- La démarche vise à évaluer en particulier les risques suivants
  - principalement les risques "E", "e", "V" et dans une moindre mesure "A"
    Rq : « E » : exhaustive (« doit-on retraiter toutes les informations ? »)
    « e » : existante (« y a-t-il des informations fictives, ex : RIB des Frs ? »)
    « V » : valorisation
    « A » : appartenance (« l'écriture appartient-elle à l'entreprise ? »)
  - et au delà:
    - pérennité
    - fiabilité
    - sécurité (confidentialité)
    - disponibilité

Moyens



Préliminaire

Prise de connaissances de l'environnement informatique (PCEI)	Identification des grandes zones de risques liées à l'utilisation de l'informatique
Revue générale informatique (RGI)	Analyse des risques liés à la maîtrise des systèmes d'information (les hommes et les systèmes utilisés)

Intérim	
Revue générale informatique (RGI)	Analyse des risques liés à la maîtrise des systèmes d'information (les hommes et les systèmes utilisés)
Revue d'application (RDA)	Evaluation du contrôle interne de l'environnement informatiques pour un cycle donné
Tests informatique (IF)	Assistance à la réalisation de tests par la mise en place d'interrogations de fichiers Tests de bouclage des chaines de gestion amont avec le logiciel comptable
Sécurité	Physique, logique, continuité d'exploitation, moyens de paiement
Normes et respect des contraintes réglementaire	

Missions spécifiques

- La maîtrise des coûts informatiques
- L'audit de la politique informatique
- L'audit des études
- L'audit de l'exploitation
- L'audit sécurité(cf. audit de la sécurité informatique)
- L'audit du respect des contraintes fiscales
- L'audit de réseau
- etc.

Les acteurs

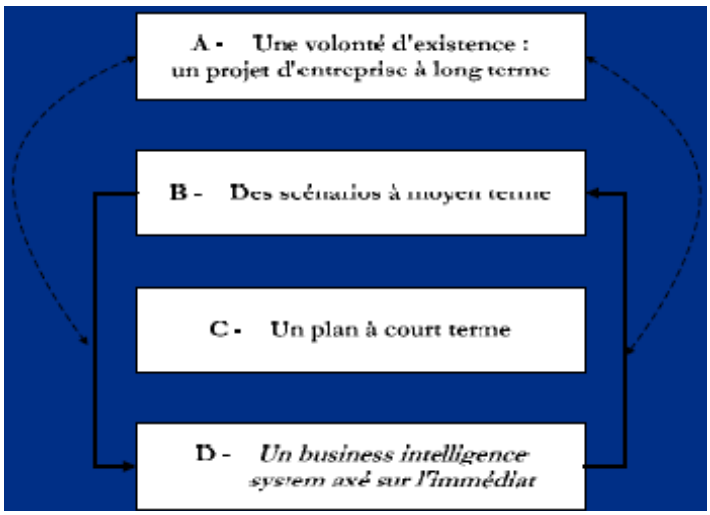
- Tous les «grands»cabinets d'audit et de conseil ont mis en place des démarches d'audit informatique en support à l'audit comptable s'appuyant sur des experts généralistes et des spécialistes
  - CISA (Certified Information System Auditor)
  - CISM (Certified Information Security Manager)
  - …
- Les S.S.I.I. réalisent également des audits informatiques mais dans un cadre moins réglementés
  - expertise technique
  - expertise fonctionnelle

2007-01-18

Formation à l'audit informatique
- Revue générale informatique

La politique informatique

Rappel : le schéma directeur (R. ACKOFF)



Rq :

A. Une volonté d'existence : un projet d'entreprise à long terme
   Rq : c'est un plan stratégique
B. Des scénarios à moyen terme
   Rq : en fonction du projet à long terme, on liste des scénarios à moyen terme qui sont susceptibles de le réaliser.
C. Un plan à court terme
D. Un business intelligence system axé sur l'immédiat

- L'entreprise dispose-t-elle d'une stratégie en matière de système d'information et d'outil informatique ?
- Le plan informatique combine-t-il au mieux les ressources disponibles pour traduire les orientations en programmes d'actions ?
- Principaux problèmes rencontrés
  - Absence de schéma directeur
  - Absence de méthodologie pour la réalisation du schéma directeur
  - Recensement des besoins des utilisateurs sans véritable relation avec les objectifs généraux et informatiques de l'entreprise
  - Chantier étalé dans le temps : difficulté à réaliser les objectifs énoncés dans le schéma directeur
  - Le schéma directeur est souvent une proposition du département informatique sans véritable adhésion de l'entreprise

L'organisation et les équipes du service informatique

Risques liés au positionnement du service informatique

- Indépendance trop importante du service informatique
- Non respect des procédures
- Non prise en compte de la dimension stratégique des systèmes d'information
- Mauvaise utilisation de l'outil informatique
- Cumul de fonctions incompatibles

Organisation du service informatique

- Unicité du savoir de nature à causer des préjudices graves en cas d'indisponibilité des personnes
- Suivi insuffisant des travaux effectués et de la qualité des services rendus
- Turn-over des équipes
  Rq : un fort Turn-over représente un risque de pertes des savoirs dans l'entreprise.
- Absence de suivi transversal des projets
- Formation des équipes
- Séparation des fonctions
- Procédures en place

- Compétence fonctionnelle

La configuration matérielle et réseau

- Appel à des techniques ou à des technologies difficiles à maintenir / faire évoluer
- Cohérence d'ensemble
  Rq : à travers des interfaces supplémentaires (ex : couche web), on arrive à faire marcher plusieurs systèmes différents qui ne se sont pas communiqués avant.
- Concentration des informations sensibles sur des matériels uniques
- Suivi de l'évolution des capacités disponibles
- Répétition intempestive de pannes
- Fournisseur en difficulté financière

Établir l'architecture du système informatique (y compris réseau et équipement bureautique) de façon à :

- identifier les risques éventuels :
  - complexité/hétérogénéité relative du système
  - matériels clés sensibles (réseau, …)
  - interconnexions avec d'autres systèmes (clients, fournisseurs, prestataires, ...)
  - disponibilité
  - incidents répertoriés
- apprécier le degré de modernité
  - machines centrales, postes de travail et réseau

La cartographie applicative

Les objectifs

- Quelles sont les principales applications composant le système d'information ?
- Comment la comptabilité est-elle alimentée ?
- Quelle est la nature et la périodicité des interfaces ?
- Tous les flux sont-ils informatisés ?
- Mieux connaître les liens qui existent entre les domaines, afin de mieux positionner une application dans son contexte global

Etapes à suivre

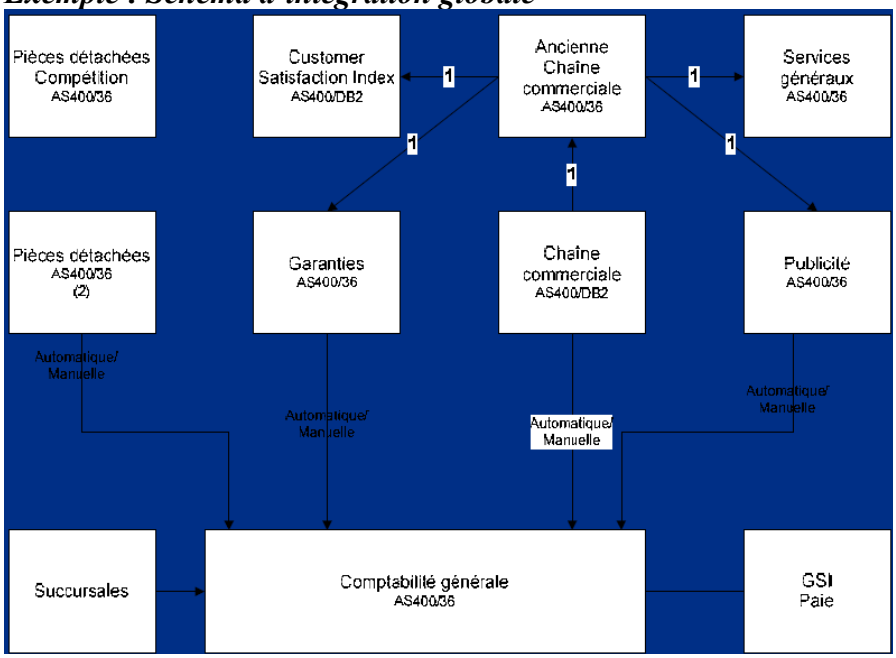
- Recensement des divers domaines d'activité de l'entreprise
- Inventaire des systèmes applicatifs
- Identification des liens entre systèmes applicatifs et description de la nature des interfaces existantes
- Formalisation de l'ensemble des informations recueillies :
  - Tableau récapitulatif
  - Schéma d'intégration global

Identification des risques

- Couverture des besoins de l'entreprise
- Intégration ou interfaçage entre les applications
  Différence : « intégré » & « interfacé »
- Cohérence d'ensemble

- Appel à des progiciels ou à des prestataires de service qui rencontrent des difficultés financières
- Identification des applications sensibles
  - poids financier et stratégique
    Rq : en fonction de leurs impacts financiers et stratégiques.
  - données sensibles (financières, commerciales ou techniques ...)
  - fragilité (développement spécifique, …)

Exemple : Schéma d'intégration globale



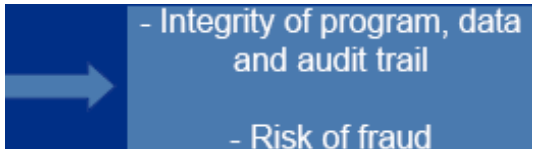
Les chaînes garantie, publicité, CSI et services généraux exploitent des données issues de la nouvelle chaîne commerciale qui transitent via l'ancienne chaîne commerciale. Ces données sont relatives aux fichiers Clients et Produits pour l'essentiel.
La MAJ du fichier des clients dans les applications périphériques est réalisée après chaque modification dans la nouvelle chaîne commerciale. En revanche, la MAJ du fichier des véhicules n'est réalisée qu'une seule fois par semaine. Cette procédure a pour inconvénient de ne pas assurer l'homogénéité des données exploitées à un instant « t ». néanmoins, cette MAJ peut être réalisée selon une périodicité plus courte.

La chine Pièces Détachées exploite ses propres fichiers clients et produits, cel qui ne garantit pas l'homogénéité des données traitées

Les contrôles généraux informatiques

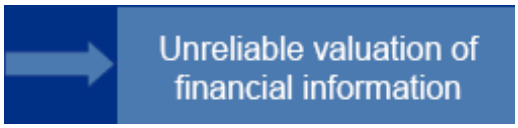
Présentation
Définition des IT General Controls : Ensemble des procédures de contrôles contribuant à assurer un bon fonctionnement continu des systèmes d'information.
Principe des travaux :
- Identification des contrôles en place
- Evaluation du design et de l'efficacité de ces contrôles par la réalisation de tests (entretiens, collecte et revue de documentation…)

1. Access to programs and data
   - 1.A – Implementation of security practices
   - 1.B – Logical and physical access to IT computing resources
   - 1.C – Segregation of duties

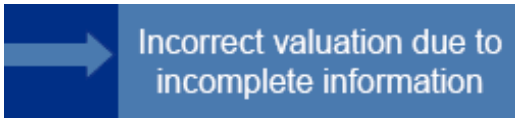


2. Program changes
   - 2.A – Changes have been authorized, documented and tested
   - 2.B – System and application configuration changes
   - 2.C – Migration of changes into production

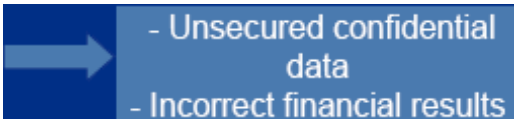
3. Program development
   - 3.A – Authorization, development, and testing of new systems and applications



4. Computer operations
   - 4.A – Implementation backup and recovery procedures
   - 4.B – Problem management procedures
   - 4.C – Accuracy, completeness, and timely processing of systems jobs



5. End-user computing
   - 5.A – IT general controls applied to end-user computing environments
     - Spreadsheets and other user developed programs
     - Common in financial consolidation, reporting and disclosures
     - Document and test in relevant Audit Program



La gestion de la sécurité informatique

Présentation

La sécurité logique

- informations confidentielles ou sensibles
- gestion des droits d'accès
  - différents mécanismes en place
  - modalités de gestion des identifiants et mots de passe
  - procédures d'attribution des droits
  - (les droits d'accès en place font a priori partie de la revue d'application)

La sécurité physique et la continuité d'exploitation

- protection des matériels
- procédures de sauvegarde
- plan de secours
- plan de fonctionnement dégradé

Démarche

Identification des contrôles en place par entretien et revue de documentation

Thème	Contrôles à tester
Accès aux programmes et aux données	

Implementation of security practices	Une politique de sécurité de l'information existe, a été approuvée par le management et communiquée aux utilisateurs.
	Des standards de sécurité ont été mis en place afin d'atteindre les objectifs définis dans la politique de sécurité. Ces standards doivent couvrir les thèmes suivants : - Organigramme de la fonction sécurité - Rôles et responsabilités - Sécurité physique et environnementale - Sécurité des OS - Sécurité des réseaux - Sécurité des applications - Sécurité des bases de données
	Un plan de sécurité IT existe et est en ligne avec le plan stratégique IT.
	Le plan de sécurité IT est mis à jour des changements apportés à l'environnement IT ainsi que des besoins identifiés en terme de sécurité pour les systèmes.
Segregation of duties	Des contrôles existent lors du processus de demande et de création des droits utilisateurs afin de garantir le principe de séparation de fonction.
	Les applications et les systèmes hébergeant les données sont correctement configurés pour autoriser l'accès aux utilisateurs selon leurs besoins (consultation, création, modification ou suppression des données).
Logical and physical access to IT computing resources	Des procédures existent et sont suivies afin de : - garantir l'efficacité des mécanismes d'accès et d'authentification - s'assurer que tous les utilisateurs sont authentifiés par le système garantissant ainsi la validité des transactions passées.
	Un processus de contrôle est en place afin d'effectuer une revue périodique des droits d'accès et de s'assurer de leur correcte attribution.
	Des procédures sont mises en place et suivies pour s'assurer que les comptes utilisateurs sont créés, modifiés, suspendus et fermés en temps et en heure.
	Des contrôles appropriés, incluant les Firewalls, la détection d'intrusion, l'évaluation des vulnérabilités existent et sont utilisés pour se prémunir des accès non-autorisés à partir des connectivités réseaux.
	Des logs tracent les opérations liées à la sécurité des OS, des applications et des bases de données. La revue de ces logs permet d'identifier les violations de sécurité et de les remonter au management.
	S'assurer que l'accès aux salles IT est restreint et que les règles de sécurité sont définies et appliquées. Des procédures d'accès sont en place pour les employés, les contractants et les équipes de maintenance.
	Des moyens de protection physiques permettent de maintenir les systèmes en fonctionnement et d'assurer la disponibilité des données (messages d' alarmes pour l' eau, le feu, les intrusions,

	extincteurs, air conditionné, groupes électrogènes…). Seules les logiciels autorisés sont utilisés par les utilisateurs.
	Des tests périodiques sont effectués pour s'assurer que l'infrastructure matérielle et logicielle est configurée de façon appropriée.
	La direction Informatique a défini des procédures permettant de protéger le système d'information et les équipements informatiques des virus informatiques

La gestion des changements

Démarche

Thème Changement applicatifs	Objectif de contrôle
Changes have been authorized, documented and tested	Les demandes de : - changement des programmes, - maintenance des systèmes (incluant les changements apportés aux OS), - changement des infrastructures, sont standardisées, tracées, approuvées, documentées et respectent les procédures de gestion es changements.
	Les procédures de gestion des changements tiennent compte des changements urgents effectués directement en environnement de production. Comme tous changements, les changements dits urgents sont documentés de la même manière a postériori.
Migration of changes into production	Des contrôles sont en place afin que les migrations des programmes dans l'environnement de production soient limitées aux seules personnes autorisées.
System and application configuration changes	La Direction Informatique garantit que l'implémentation des logiciels et systèmes ne met pas en danger la sécurité des données et des programmes des systèmes.

Le développement informatique

Rappel des phases de la gestion de projet

- Étude d'opportunité et de faisabilité
- conception fonctionnelle (spécifications générales, spécifications détaillées)
- conception technique
- développement (programmation)
- Tests
- Recette
- mise en production
- maintenance

Les principaux risques par phase de développement

Identification des risques par une revue des méthodologies de développement

- Etude d'opportunité et de faisabilité
  - implication de la direction dans l'initialisation du projet
  - étape de validation de la faisabilité technique et économique
- Conception
  - participation des utilisateurs, …
  - découpage du projet en plusieurs étapes
  - intégration de thèmes relatifs à :
    - la sécurité
    - les contrôles programmés
    - la piste d'audit

Les principaux risques par phase de développement

- Réalisation
  - outils utilisés, …
  - bugs rencontrés
    - En moyenne, un "bug" pour cent lignes de code produites
    - Tous les bugs ne peuvent être détectés avant la mise en production
    - Le coût de la correction est évidemment plus élevé lorsque l'application est en service
  - Absence ou non respect des normes de programmation
- Test / Recette
  - Existence de tests unitaires d'intégration et tests de non-régression
  - adéquation de la solution au besoin (recette fonctionnelle)
  - non création d 'un échantillon représentatif
  - non suivi des incidents
- Maintenance
  - perte de connaissance de l'application
    - absence de documentation
    - turn-over
  - versions successives non gérées
  - absence de base de test (ou base non à jour)
  - mise en exploitation non contrôlée

Démarche

Thème Gestion des développements	Objectif de contrôle
Authorization, development, and testing of new systems and applications	L'organisation dispose d'une méthodologie de cycle de vie de développement de système (SDLC) intégrant les besoins de l'organisation en terme de sécurité et d'intégrité des données et traitements
	Les politiques et procédures SDLC considèrent le développement et l'acquisition de nouveaux systèmes ainsi que les évolutions majeures apportées aux systèmes existants.
	La méthodologie de cycle de vie de développement de système (SDLC) assure que les systèmes d'information sont conçus pour inclure les contrôles applicatifs qui garantissent que les traitements sont complets, exacts, autorisés, et valides, et que tous les

	composants (programmes et données) fonctionnent ensemble sans erreur.
	L'organisation dispose d'un processus d'acquisition et de planification en cohérence avec les orientations stratégiques d'ensemble.
	La Direction Informatique garantit que les utilisateurs sont impliqués de manière appropriée dans la conception des applications, la sélection des progiciels, et leurs tests afin de garantir un environnement fiable.
Authorization, development, and testing of new systems and applications	L'organisation acquiert les logiciels et systèmes conformément à ses processus d'acquisition, de développement et de planification.
	L'organisation a défini des politiques et procédures pour la gestion des développements et évolutions applicatifs, revues périodiquement, mises à jour et approuvées par le management.
	L'organisation développe, maintient et utilise ses systèmes et ses applications en accord avec les politiques et procédures qu'elle a définie.
	Des revues de post-implémentation sont effectuées afin de vérifier l'efficacité des contrôles implémentés.
	Il existe une stratégie de test pour tous les changements applicatifs et technologiques significatifs, qui garantissent que les systèmes déployés fonctionnent comme prévu. Les tests sont réalisés à différents niveaux : - tests unitaires, - tests d'intégration, - tests utilisateurs.
	Les tests de chargement et de stress sont réalisés conformément au plan de test et aux standards de tests établis.
	Les interfaces avec les autres systèmes sont testées afin de s'assurer de l'exhaustivité, l'exactitude et l'intégrité des données interfacées.
	La conversion des données est testée (rapprochement entre leur état original et final) afin de s'assurer de l'exhaustivité, l'exactitude et l'intégrité des données converties.

L'exploitation informatique

- Gestion des travaux
- Gestion des moyens
- Procédures de mise en exploitation

Gestion des travaux et des moyens

- Gestion des travaux
  - Planning
  - Documentation
  - Gestion des incidents
  - Contrôle de la production
  - Distribution des restitutions
- Gestion des moyens

- Gestion des matériels
- Plan de secours
- Procédures de sauvegarde
- Gestion

Procédures de mise en exploitation

- Implication de l'exploitation lors du développement de nouvelles applications
  - Evaluation de l'impact sur le planning de traitements
- Procédure d'approbation des transferts de programmes en exploitation
- Séparation bien établie des fonctions avec les études
- Existence de plusieurs environnements ?
  - Environnement de développement
  - Environnement de test
  - Environnement de production

Points d'attention liés à la gestion des travaux

- Existence d'une planification automatique
- Existence d'une procédure formalisée pour les travaux exceptionnels non planifiés?
- Existence de procédures écrites
- Conservation de la maîtrise de l'enchaînement des traitements
- Standardisation du dossier d'exploitation
- Les opérateurs ont-ils accès aux logiciels de production? Aux données de production?
- Peuvent-ils modifier les programmes sources ?
- Rotation des fonctions entre les opérateurs?
- Utilisation de moyens permettant de contrôler la bonne exécution des traitements
- Procédure de suivi des incidents?
- Définition d'un niveau de gravité des incidents?
- Revue périodique des incidents non clos?
- Identification des sorties sensibles?

Points d'attention liés à la gestion des moyens

- Maintenance
- suivi des performances
- suivi de l 'espace disque disponible
- suivi des consommations
- le plan de secours couvre-t-il tous les sites ? Toutes les applications?
- s 'appuie-t-il sur une analyse des risques associés à l 'indisponibilité des différentes applications?
- Tests réguliers du plan de secours?
- Conservation à l 'extérieur du centre informatique des copies de fichiers de données et des programmes de production?
- Contrôle du contenu des sauvegardes avec les fichiers en production?
- Restauration périodique des sauvegardes?
- Refacturation aux utilisateurs

Démarche

Thème	Objectif de contrôle

Exploitation	
Accuracy, completeness, and timely processing of systems jobs	Des contrats de service internes et externes (Service Level Agreement) sont définis et gérés afin de répondre aux besoins des systèmes de reporting financier. Ces contrats définissent les rôles et responsabilités de chacune des parties et explicitent les services fournis et attendus.
	Pour gérer les contrats de service aussi bien internes qu'externes, des indicateurs clés de performance sont définis.
	Un responsable est nommé afin de suivre régulièrement les critères de performance des prestataires.
	La sélection des fournisseurs de services d'outsourcing est réalisée conformément à la politique de l'organisation en matière de gestion des fournisseurs.
	Les fournisseurs pressentis sont correctement qualifiés au travers d'une démonstration de leur capacité à fournir le service demandé et de leur solidité financière.
	Les contrats avec les tiers définissent les risques identifiés, les contrôles et procédures de sécurité mis en place pour les systèmes et réseaux concernés.
	Des procédures existent et sont suivies afin qu'un contrat formel soit défini et convenu pour tous les services tiers avant le début des travaux, y compris la définition des exigences de contrôle interne et l'acceptation des politiques et procédures de l'entreprise
	Des revues régulières des prestataires sont effectuées au travers d'audits (exemple : SAS 70).
	Des politiques et procédures existent pour gérer la distribution et la rétention des données ainsi que pour les rapports.
	Des contrôles de fin de traitement sont réalisés par la DSI afin de vérifier l'exactitude, la complétude et la validité des traitements informatiques.
Problem management procedures	La Direction Informatique a défini et mis en place un système de gestion des problèmes et incidents de telle manière que les incidents liés à l'intégrité des données et aux contrôles d'accès sont enregistrés, analysés, résolus en temps et en heure et remonter au management le cas échéant.
	Le système de gestion des problèmes assure la piste d'audit entre le problème ou l'incident relevé jusqu'à la cause identifiée.
	Un processus de réponse aux incidents de sécurité existe afin de mettre en place les actions correctives dans les meilleurs délais et d'analyser les opérations non-autorisées.
Implementation backup and recovery procedures	Le management protège les informations sensibles - logique et physique -, dans leur stockage et durant leur transmission, contre les accès ou les modifications non-autorisés.
	La période de rétention et les conditions de stockage sont définis pour les documents, les données, les programmes et les messages (entrants/sortants) ainsi que pour les données (clés, certificats) utilisées pour leur encryption et authentification.
	Le management a implémenté une stratégie de backup des données et des programmes.
	Des procédures existent et sont suivies pour tester périodiquement

	l'efficacité du processus de restauration et la qualité des bandes de sauvegarde.
	Les historiques d'événements des systèmes sont conservées assez longtemps pour générer une chronologie et un journal qui permettront de contrôler, examiner et reconstruire le système et le traitement des données.
	Les changements apportées à la structure des données sont autorisés et implémentés en accord avec les spécifications, et en temps et en heure.
	La Direction Informatique a défini des procédures standards pour l'exécution des travaux IT y compris l'ordonnancement, la gestion, la surveillance et la réaction aux incidents de sécurité, la disponibilité et l'intégrité des traitements.

Exemple
Entreprise commerciale sur AS400

Thèmes présentés
1) L'équipe informatique
2) La configuration matérielle
3) La cartographie applicative
4) La politique informatique
5) La gestion de la sécurité informatique
6) Le développement informatique
7) L'exploitation informatique

Equipes
Existant

Function	Age	Formation	Experience	Ancienneté	Langage
DI	54	BTS	37	01/04/95	COBOL
CPI	46	Secondaires	12	23/06/94	GAP/COBOL/ODYSSEE
CP2	35	Niveau BAC	14	02/08/96	COBOL
AP1	41	BAC D	13	14/05/95	GAP/COBOL/ODYSSEE
AP2	31	BAC C BTS	3	28/10/96	COBOL
P1	37	BAC	7	16/11/92	
P2	25	BEP BAC	5	27/07/96	
MOY	38	-BAC	13	3 ans	

Configuration matérielle
Existant
- Un IBM AS 400 B 60
  - équipé de :
    - 96 MO de mémoire centrale et 10,2 GO de disques
    - 108 écrans, 4 PC connectés, 30 imprimantes
  - charge de l'AS400 :
    - fonction de collecte des mesures de performances non utilisée en interne
    - temps de réponse mauvais
    - UC occupé à plus de 85 % dans la journée
    - espace disque occupée à 68 %

- héberge actuellement gestion commerciale, la comptabilité générale, la paye et la trésorerie (étude et production)
- acheté en leasing
- acquisition d'un AS400 E10 envisagé pour supporter la comptabilité

- 64 micros ordinations
  - ratio nombre de licences achetées / nombre d'utilisateurs pouvant être estimé à 50%
  - absence de normes pour les applications bureautiques du type tableur et traitement de texte
    - Excel, Multiplan et Lotus pour les tableurs

Cartographie applicative

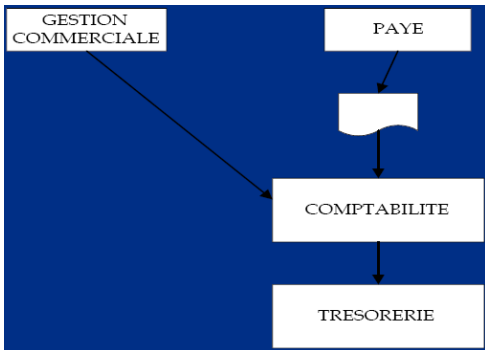
Existant

- Applications significatives

Comptabilité	Logiciel spécifique « maison » (1)
Gestion commerciale	Progiciel ANTALIA de PRISME
Paye	Progiciel PMP 38 de PROLAND
Trésorerie	CONCEPT

(1) Application développée en 1982 sur IBM 36. Les informations à l'origine du développement ne font plus partie de l'entreprise.
La documentation est quasi inexistante même après divers évolutions majeures de l'application (an 2000 et euro)

SIG



Politique informatique

Existant

- L'informatique évolue au fil de l'eau

Sécurité logique

Existant

- accès aux applications
  - les utilisateurs possèdent a priori des identifiants et des mots de passe
  - il existe un mécanisme de sécurité propre à "PRISME"
  - les autres applications n'offrent pas de mécanisme propre de gestion de la confidentialité
- accès au système
  - le niveau de sécurité choisi au sein du système = 20
  - la clef (keylog Switch de l 'AS 400 est sur la position « Normal »)

Sécurité physique
Existant

- Quatre niveaux de sauvegarde sont effectués :
  - tous les soirs :
    - Les neuf bibliothèques de données applicatives, de disque à disque, et sur cartouche
    - une société extérieure récupère les sauvegardes de l'avant-veille et les stocke dans ses locaux trois fois par semaine
  - une fois par semaine :
    - l'ensemble des bibliothèques systèmes (sauvegardées sur bande)
  - après chaque traitement mensuel :
    - les neuf bibliothèques de données statistiques, les cartouches étant conservées sur place
  - à chaque modification :
    - le système d'exploitation
- Back-up
  - contrat de back-up signé en 1989 avec une société extérieure prévoyant la mise à disposition en cas d'incident majeur

Etudes – Développement informatique
Existant

- Rôle des équipes
  - Les quatre développeurs se partagent la maintenance (M) des applications et les nouveaux développements (ND) de la façon suivante :

	Comptabilité	Gestion commerciale	Spécifiques	Paye
LANGAGE	GAP	GAP	ODYSSEE Cobol	
CP1		ND	M + ND	
CP2	M + ND	M + ND	M	
AP1			M + ND	
AP2			ND	
SSII Proland				M

  - Une seule personne (CP2) intervient sur la comptabilité
  - La documentation existante est quasi nulle
  - Certains mécanisme de la gestion commerciale sont inconnus de l'équipe en place en l'absence de documentation et de liens avec le fournisseur

Exploitation informatique
Existant

- Maîtrise des travaux batch
  - les travaux liés à certaines applications sont lancés manuellement
  - les incidents ne sont pas répertoriés
  - il n ’y a pas d ’historique des incidents
  - les travaux sont insuffisamment documentés (fichiers en E/S, traitements effectués, …)
  - des contrôles par totaux sont effectués

- Maîtrise des environnements
  - il n'y a pas d'environnement de test
  - les tests sont effectués sur les données réelles

2007-01-25

Formation à l'audit informatique
- Revue d'application informatique

Historique et insertion de l'application dans l'architecture globale

- Historique de l'application
  - prise de connaissance des interventions précédentes
    Rq : on peut demander à des collègues qui ont des expériences sur le logiciel pour savoir des difficultés qu'on rencontre souvent, etc.
  - gestion du projet
    Rq : « accouchement difficile » ? passage sans difficultés ?
  - développement interne / externe
  - cahier des charges
  - maîtrise de l'existant-notion de "boîte noire"
    Rq : est-ce que le client a suffisamment d'informations pour maitriser le logiciel ?
  - gestion des évolutions
  - …
- Insertion de l'application dans l'architecture globale
  - référence à la RGI
  - établir un schéma d'intégration global

Couverture fonctionnelle

- Liste des fonctionnalités
  Rq : il peut qu'en fonction de l'activité de l'entreprise, elle retient de telles fonctionnalités, mais pas d'autres.
- Schémas des traitements
  Rq : par ce schéma, on essaie de savoir comment initialiser, enregistrer (par qui, comment), traiter (de quelle manière : séquentielle, continue, etc.), valider et contrôler.
- Revue des documentations (utilisation, conception, exploitation)
  Rq : manuel d'utilisateur
  A partir du manuel d'utilisation, il faut intégrer la formation d'utilisation.
- Identification des utilisateurs
  Rq : informaticiens, MOA, contrôleur d'accès, les stagiaires, etc.
- Identification des informaticiens
- ...

Schéma des traitements et matrice de contrôle

La démarche à suivre est la suivante

- découpage de l'application en phases logiques de traitement
- élaboration d'un schéma de flux sur lequel sont présentés :

    - les phases logiques de traitement
    - les principaux fichiers ou tables concernées
- pour chaque phase logique, établissement d'une matrice de contrôle comprenant :
    - les informations reprises du schéma de flux (phase logique de traitement, entrées, fichiers de référence, sorties)
    - la description du traitement effectué
    - la liste des contrôles programmés ou d'exploitation et les objectifs des contrôles
    - la liste des contrôles effectués par les utilisateurs sur la base des restitutions disponibles et les objectifs des contrôles opérés

Identification des risques

Fiabilité des interfaces

- les contrôles effectués
- les procédures de recyclage des rejets (ou anomalies)
- la nature et la fréquence des rejets

Contrôle interne applicatif

- le contrôle interne applicatif ne diffère en rien du contrôle interne manuel
- il se décline de la manière suivante :
    - autorisation :toutes les transactions, font-elles l'objet d'un autorisation en accord avec la politique de délégation (contrôle d'accès et séparation des fonctions)?
    - Exhaustivité : les données entrées dans l'application sont-elles bien disponibles dans les bases de données?
        - Absence de perte de données aux différents niveaux de traitement?
        - Existence de contrôle de flux?
    - exactitude :
        - L'application permet-elle de garantir la non altération des données ?
        - Existe-t-il des contrôles de valorisation (tests en production, requêtes, simulation…)?

Paramétrage

- identification des tables
- procédures et fréquences des mises à jour
- vérification du code (séparation données/traitements)
- personnes concernées
- ...

Pour apprécier si une application est "facile à exploiter", il convient d'étudier :

- les fiches d'incident tenus par l'exploitation informatique et/ou par les utilisateurs
- le dossier d'exploitation de l'application pour apprécier l'existence de points de reprise en cas d'incident
- les procédures utilisateurs pour le recyclage des anomalies
- le planning d'exploitation pour apprécier si une attention particulière est donnée à l'application

Approfondissement des risques identifiés

- Procédures palliatives
  - contrôles par les utilisateurs
  - existence d'une cellule de pilotage et de contrôle des données produites
  - proposer la mise en œuvre de contrôles complémentaires

- Mise en place éventuelle de tests informatiques ciblés
  - identification des risques
  - réalisation d'un cahier des charges
  - mise en place des tests
    Rq : distinguer les anomalies intrinsèques ou les anomalies engendrées par la mauvaise construction ou interprétation des tests.
  - réunion de synthèse

Analyse des aspects « qualitatifs »
- L'adéquation fonctionnelle
- La satisfaction des utilisateurs
- L'évolutivité
- Le bilan économique
- Les performances

L'adéquation fonctionnelle
Étude des points suivants :
- implication des utilisateurs dans les choix et/ou développements informatiques
- cohérence et stabilité de la demande exprimée : collecter les demandes de mise à jour de l'application
- apprécier la fréquence de maintenance corrective sur l'application
- vérifier que les restitutions produites par l'application sont effectivement utilisées
- apprécier si les retraitements ou remaniements manuels d'informations issues de l'application ne pourraient pas être informatisés

Rq : plus l'entreprise est grosse, plus on a des traitements manuels pour remonter les informations, plus on a des incertitudes sur l'exactitude et l'exhaustivité des informations.

La satisfaction des utilisateurs
Par entretien avec les utilisateurs, obtenir les motifs d'insatisfaction éventuels, ils pourront résulter :
- d'un manque de communication entre utilisateurs et informaticiens
- de retard dans les travaux de maintenance évolutive ou corrective
- d'un manque de formation des utilisateurs
- de contraintes techniques

L'évolutivité
La capacité d'une application à évoluer selon les souhaits de l'entreprise se mesure suivant les critères suivants :
- qualité de la programmation
- pertinence des choix techniques
- qualité de la documentation

- pertinence de l'analyse fonctionnelle
- externalisation du paramétrage

Le bilan économique
L'établissement d'un bilan économique nécessite l'étude des points suivants :
- le coût réel d'acquisition ou de développement et de mise en place de l'application / coût prévu au plan informatique
- le coût de l'application développée ou acquise par rapport à des progiciels équivalents du marché
- les gains de productivité
- le coût de fonctionnement
- les coûts de maintenance

Les performances
Les performances d'une application peuvent s'apprécier selon les points de contrôle suivants :
- fréquence de réorganisation des bases de données ou fichiers accédés par l'application
- reporting sur le délai moyen de restitution des réponses attendues et évolution dans le temps
- fréquence et nombre de passages batch sur de gros volumes de fichiers séquentiels
- interactions entre applications

Exemple :
Audit d'une application de comptage et de facturation
Etapes de traitement :
- "contrôle syntaxique" :
  - contrôle de présence des informations nécessaires à la valorisation
- " contrôle logique" :
  - éclatement des événements unitaires selon leur nature
- rapprochement au contrat et valorisation
- prise en compte des produits (services inclus dans le contrat) et des acomptes
- facturation :
  - des consommations
  - des abonnements
  - des PFA (Produits Facturés à l'Acte)
- calcul de la facture
- calcul des lignes de chiffre d'affaires et des écritures de cut-off

Risques étudiés :
- exhaustivité de la remontée ?
  - Existe-t-il des contrôles de l'exhaustivité de la prise en compte de l'ensemble des bandes magnétiques remontant de compteurs ?
  - En l'absence de numérotation des événements unitaires, peut-on s'assurer de l'exhaustivité de la présence de ces derniers ?
- exhaustivité du recyclage ?
  - deux faiblesses recensées :
  - perte de quelques tickets en anomalie de type 'I'
  - non recyclage des anomalies de type 'W'
- exhaustivité du traitement des lots de facturation ?

- Absence de vérification par tests programmés
- exhaustivité de la facturation des contrats ?
  - Absence de vérification par tests programmés
- Unicité du numéro de facture ?
  - non séquentialité des numéros de facture
  - l'unicité du couple contrat-numéro de facture dépend de l'unicité des numéros de contrat

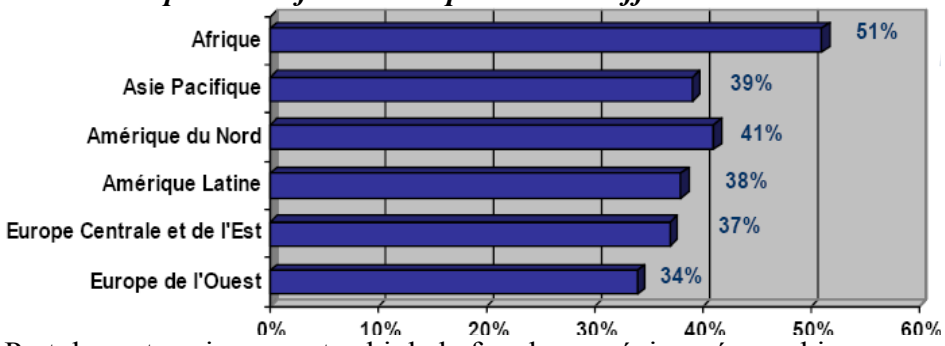
Risques financiers identifiés :

- exhaustivité de la facturation des ventes ?
  - manque de fiabilité des compteurs d'événements unitaires
- comptabilisation des prestations ?
  - existence de contrats ayant un plan tarifaire nul
    Rq : comment traiter les contrats ayant une valeur nulle ?
- valorisation des prestations ?
  - utilisation du coût minimum en cas d'anomalie
- diminution non justifiée du compte client ?
  - émission de 500 KF d'avoirs chaque mois
    Rq : il faut vérifier que soient bien justifiés les avoirs qui sont une source de fraude
  - à valider à partir des tests effectués
- cut-off
  - non respecté en cas de retard dans la remontée des tickets
    Rq : on vérifie le délai entre la date de ticket et la date de facturation.
- provision pour dépréciation des clients mal calculée
  - reste à valider à partir des tests effectués

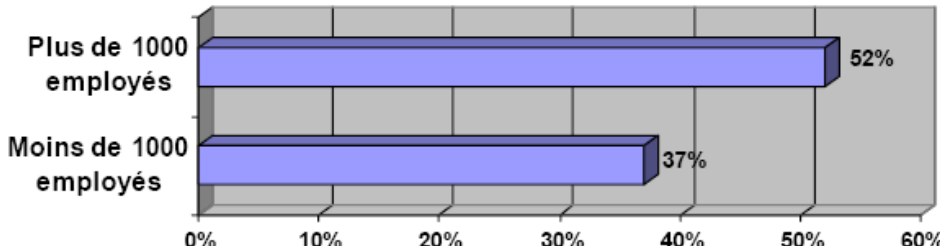
Formation à l'audit informatique
- La fraude : méthodes de prévention et détection

La fraude et les méthodes de prévention et détection

Caractéristiques de la fraude: un phénomène affectant l'ensemble des entreprises 34%

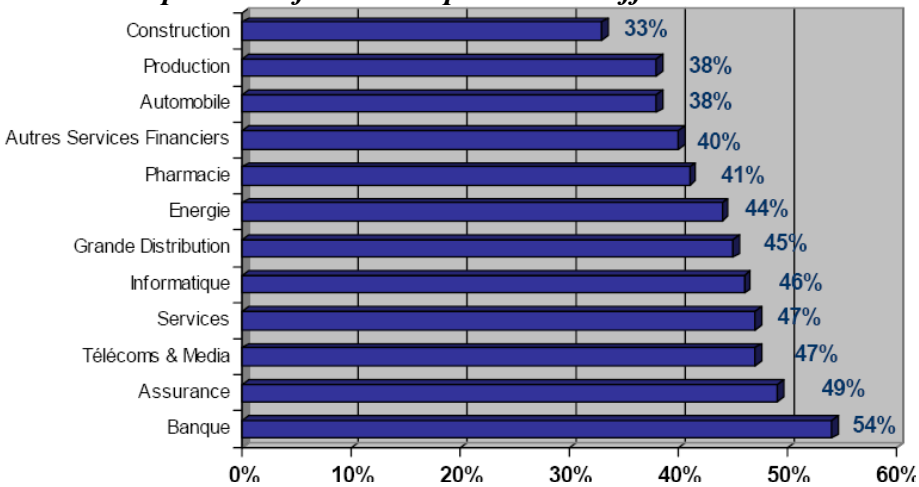


Part des entreprises ayant subi de la fraude par région géographique



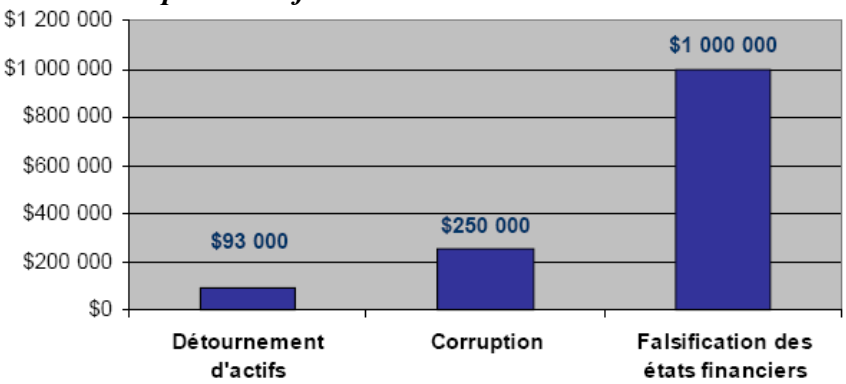
Part des entreprises ayant subi de la fraude par secteur d'activité

Caractéristiques de la fraude: un phénomène affectant l'ensemble des entreprises



Part des entreprises ayant subi de la fraude par secteur d'activité

Caractéristiques de la fraude: un coût élevé

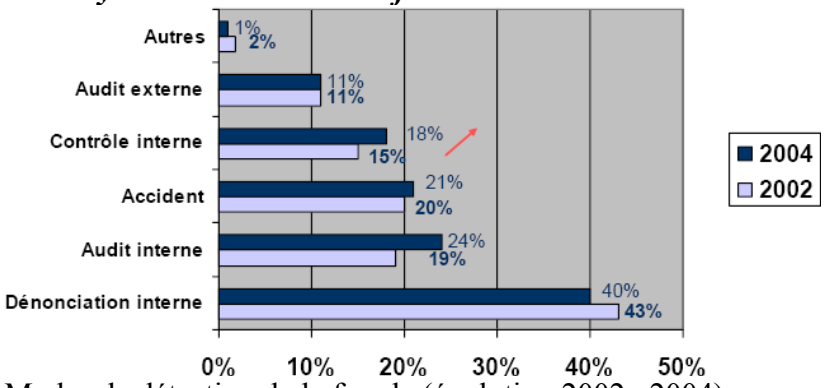


Coût moyen du préjudice par type de fraude en 2003-2004 (aux US)

Caractéristiques de la fraude: un profil type

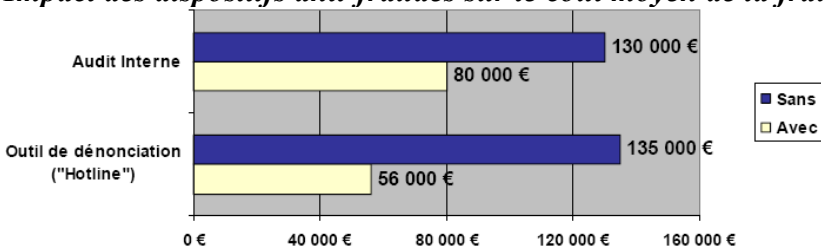
- Un homme (53% des cas)
- Niveau employé (67% des cas)
- Âgé d'une quarantaine d'années
- Sans antécédent juridique (83% des cas)
- Facteurs aggravant l'impact de la fraude :
  - le niveau hiérarchique (de 62k$ pour un employé à 900k$ pour un dirigeant)
  - le salaire élevé
  - l'âge, l'ancienneté
  - le niveau universitaire.

Les moyens de lutte contre la fraude



Modes de détection de la fraude (évolution 2002 –2004)

Impact des dispositifs anti-fraudes sur le coût moyen de la fraude



- **La protection des flux d'informations critiques de l'entreprise** (sécurité des réseaux, tests d'intrusions, cryptographie des message…)
  - **Exemple de fraude** : L'espionnage industriel peut se faire par l'écoute téléphonique mais également par «l'écoute»des communications Internet au sein de la société où vers l'extérieur (mail, échange de fichiers électroniques…). L'accès au réseau d'une entreprise par une personne malveillante peut également aboutir à des situations de chantage et de tentative d'extorsion comme la société Softbank dont la base de données clients avait été copiée en février 2004 par un «hacker»et qui menaçait de publier des informations confidentielles.
  - **Rôle de l'auditeur en SI** : spécialiste en sécurité des réseaux, il peut effectuer des tests d'intrusion sur les réseaux des entreprises afin de tester leur vulnérabilité et d'identifier les éventuelles failles.
- **La protection anti-virus** (sécurité des réseaux, tests d'intrusions, cryptographie des message…)
  - **Exemple de fraude** : Les entreprises sont quotidiennement soumises à des centaines, voire à des milliers d'attaques virales. Ces virus peuvent engendrer des mises en indisponibilité de leurs systèmes d'information, des pertes de données, des destructions matérielles qui peuvent également faire l'objet de chantage par des personnes malveillantes (ex, «I love you»). Les virus peuvent aussi être utilisés par des tiers pour prendre le contrôle du système d'information et ainsi copier, modifier ou supprimer des données sensibles et/ou confidentielles.
  - **Rôle de l'auditeur en SI** : spécialiste dans les procédures de protection des données, il peut par exemple effectuer des tests sur le système de gestion des virus de l'entreprise afin de s'assurer notamment de la mise à jour au moins quotidiennes des signatures de virus sur les PC et la bonne protection des postes nomades.
- **Le contrôle des développements informatiques**

- **Exemple de fraude** : des personnes malveillantes internes ou externes peuvent insérer au sein des applications informatiques de programmes destinés à détourner des fonds. Ainsi, les techniques dites «salamis»consistent à tronquer une somme d'une ou plusieurs décimales sur chaque transaction puis de virer cet argent sur un compte bancaire.
- **Rôle de l'auditeur en SI** : spécialiste dans la gestion des projets de développements information, il peut évaluer la méthodologie de gestion de projet (par exemple «SDLC –System Development Life Cycle»). Il peut également vérifier la séparation des fonctions entre les développeurs et les personnes migrant en environnement de production les programmes, l'existence d'un dispositif automatique de traçage des modifications sur le code informatique en environnement de production («Library Management System»avec le suivi et la documentation des versions du code source…)...

- **Le contrôle des accès aux données et aux programmes**
  - **Exemple de fraude** : Un individu ayant un profil de «super-utilisateur »sur un ERP, c'est à dire avec des droits d'accès très étendus, contourne les contrôles mis en place et fraude (par exemple, création d'un fournisseur ou d'un client fictif, création d'un paiement injustifié, contre-passation de charges…)
  - **Rôle de l'auditeur en SI** : spécialiste dans la sécurité logique des ERP, il peut effectuer des revues d'habitations informatiques afin d'identifier d'une part les utilisateurs présentant des droits d'accès à des fonctionnalités critiques de manière injustifiée et, d'autre part, les utilisateurs dont les droits d'accès présentent des conflits de séparation de fonctions (cf. section 4.2). Par exemple, un même utilisateur ne doit pas pouvoir créer un fournisseur, une commande d'achat, une réception de stock, une facture et un paiement.
- **L'identification de comportements susceptibles de se rapporter à la fraude**
  - **Exemple de fraude n°1** : La majorité des cas de fraudes liées à la falsification des états financiers concernent la surestimation des comptes clients.
  - **Rôle de l'auditeur en SI** : Identification des factures clients non justifiées par un flux vente classique (commandes et /ou bon de livraison). Ces factures clients créées directement en comptabilité devraient être extrêmement rares et il est donc nécessaire d'établir leur liste afin de les revoir ligne par ligne avec un Responsable approprié
- **L'identification de comportements susceptibles de se rapporter à la fraude**
  - **Exemple de fraude n°2** : Le processus achats présente de nombreux risques puisqu'il engendre la sortie d'argent. La collusion avec un fournisseur est un cas de fraude fréquent dans les sociétés.
  - **Rôle de l'auditeur en SI** : Identification des factures fournisseurs non justifiées par un flux achat classique (commandes achat et /ou bon de réception). Ces factures clients créées directement en comptabilité devraient être liés à des types de dépense clairement identifiés (impôts, cas d'urgence…) et il est donc nécessaire d'établir leur liste afin de les revoir ligne par ligne avec un Responsable approprié.
- **L'identification de comportements susceptibles de se rapporter à la fraude**
  - **Exemple de fraude n°3** : De nombreux comportements suspects des employés sont des indicateurs de fraude potentielle.
  - **Rôle de l'auditeur en SI**
    - Identification des employés ayant accédé au système informatique et ayant créé des documents de gestion et / ou des pièces comptables en dehors des horaires normaux de travail (par exemple, la nuit, les week-end, les jours fériés…).

- Identification des utilisateurs ayant des droits d'accès étendus et ayant créé des factures et/ ou des paiements fournisseurs très ponctuellement (par exemple, moins de 10 en 1 an).
- Identification des utilisateurs ayant créé des pièces tout le long d'un processus à la fois dans les systèmes de gestion et dans les systèmes comptables (exemple de la création du fournisseur, de la commande et du paiement de la facture).

Formation à l'audit informatique - Tests Informatiques

Mme. Ezan

Sommaire

- Pourquoi réaliser des tests informatiques ?
- Avantages des interrogations de fichiers
- Situation amenant à procéder à des interrogations de fichiers
- Typologie des test informatiques
- Démarche de mise en œuvre
- Les facteurs de réussite
- Outils de traitement

Pourquoi réaliser des tests informatiques

Justification fondamentale : la dématérialisation des écritures ou des documents de gestion ne doit pas constituer un obstacle au travail de l'auditeur

Plus pragmatiquement, ***trois avantages essentiels*** :

- Efficacité de l'audit
- Productivité des travaux
- Meilleure compréhension des systèmes

Avantages des interrogations de fichiers

Efficacité de l'audit

Représentativité des échantillons testés

- l'automatisation des tâches permet de ne plus travaille sur un échantillon de la population mais sur sa totalité et d'accroître la pertinence et la productivité des travaux
- les erreurs de contrôle interne, difficile à déceler de par leur caractère exceptionnel, peuvent être découvertes par un examen systématique des données

Validation des calculs complexes

- il est possible d'effectuer des calculs complexes ou des simulations qui apportent une valeur probante de certaines hypothèses sur le résultat comptable

Productivité des travaux

Réutilisation des travaux

- dans le cas de missions récurrentes, les tests informatiques ou autre programmes développés (macros) sont utilisables sur plusieurs exercices moyennant une mise à jour peu coûteuse

« Batterie de tests » standards

- une série de tests développée pour une société ou un site peut être réutilisée pour tout autre client disposant d'un stockage magnétique d'information conçu selon la même structure

Meilleure compréhension des systèmes

- évite l'effet « boîte noire » des systèmes
- plus généralement, l'intervention de « spécialistes de l'informatique » permet d'élargir la perception des métiers de l'intervenant

Situation amenant à procéder à des interrogations de fichiers

- Volume d'informations trop important pour permettre des contrôles manuels significatifs
- Travaux récurrents sur des données stockées dans les fichiers de l'entreprise
- Données en entrée et en sortie d'une chaîne de traitement non approchables aisément
- Contrôle manuel nécessaire sur un échantillon à tirer aléatoirement

Typologie des tests informatiques

Tests de recoupement

Objectifs des tests

- effectuer un recoupement entre deux fichiers
- établir un recoupement entre des états séparés par une rupture du chemin d'audit fonctionnel
- reconstituer des données lorsqu'elles sont issues d'informations très nombreuses

Nature des tests

- réconciliation simple
  - rapprocher le total d'éléments calculés stockés dans un fichier avec le chiffre audité
- réconciliation complexe
  - le résultat des calculs n'a pas été conservé dans un fichier. Il convient donc de procéder au recalcul des opérations, ou de reconstituer les données à une date donnée. Le chiffre ainsi obtenu est rapproché du chiffre audité.

Exemples

- reconstitution du chiffre d'affaires à partir des fichiers quantités facturées, tarifs et conditions particulières
- rapprochement des commandes clients avec les factures émises
- rapprochement des temps imputés sur comptes rendus d'activité et des temps facturés
- réconciliation entre les charges sociales enregistrées en comptabilité et les différentes rubriques enregistrées dans la paie
- cumul des soldes des contrats créditeurs et débiteurs au 31/12/N

Tests de détection d'anomalies

Objectifs et natures des tests

- ***tester l'exhaustivité et la réalité d'un fichier*** : s'assurer que le fichier ne présente ni manque, ni sur-ajout d'informations
  - faire ressortir les trous de séquence ou les doublons dans une numérotation séquentielle

    Rq : « trous de séquence » => il s'agit généralement de la numérotation des factures.
- ***tester l'intégrité d'un fichier (exactitude)*** : s'assurer de la cohérence, dans l'absolu, des données de la base et de la mécanique de certains calculs
  - contrôler l'intégrité de chacune des données d'un fichier, prises individuellement

    - rechercher des incohérences entre deux, ou plusieurs données, soit au sein d'un même fichier, soit dans plusieurs fichiers distincts
- ***tester la conformité d'un fichier (exactitude)*** : s'assurer que les données respectent les règles de calcul ou les principes comptables de la société
    - appliquer les règles de calcul aux données stockées et comparer le résultat obtenu au réel

Exemples

- édition de la liste des factures dont la référence apparaît deux fois (ou plus) dans un fichier, ce qui peut signifier que ces factures ont été enregistrées plusieurs fois
- détection de bulletins de salaries pour lesquels le taux moyen de charges sociales est aberrant
- recherche des clients dont le taux de remise ne correspond pas au niveau de chiffre d'affaires
- recherche de données dont la valeur ne correspond pas à celle que l'on attend :
    - quantité négative en stock
    - date à zéro
    - prix unitaires nuls
    - ventes sans date de sortie
    - prix de vente inférieur au prix de revient
- vérification qu'un prix total dans un fichier est bien égal au prix unitaire multiplié par la quantité, etc.

Extraction de données

Objectifs et natures des tests

- ***sondages statistiques*** : sélection d'un certain nombre de données selon des règles statistiques, afin de procéder à ne extrapolation des anomalies rencontrées
- ***interrogations ciblées*** : faire ressortir certains cas « limites » par rapport à un risque identifié afin de restreindre le champ d'investigation et ainsi augmenter la productivité des travaux
    - une telle approche permet de se concentrer sur les cas les plus intéressants

Extraction de données

Exemples

- extraction de factures payées afin de contrôler le respect des conditions fournisseur
- contrôle d'écarts importants d'un exercice sur l'autre (en quantité ou en valeur) d'articles en stock
- extraction de factures présentant un écart important entre la date de comptabilisation et la date de facturation
- détection de taux de remise accordés supérieurs au seuil défini
- application de la méthode de sondage pour le contrôle de la provision sur créances douteuses
- extraction des relances gelées

Simulations

Objectifs et natures des tests

- recalcul de certaines données
- recalcul de certains éléments avec variation des paramètres de calcul

- évaluation rétroactive d'éléments dont les modalités de calcul étaient erronées, afin de chiffrer l'écart avec le réel
- établissement de données prévisionnelles

Exemples

- calculs d'amortissements selon différentes méthodes (linéaire, dégressif, …), afin d'en étudier l'impact financier sur plusieurs exercices
- reconstituer la valeur d'inventaire d'un stock
- contrôle de la quantité et de la valorisation d'un stock

Démarche de mise en œuvre

Les grandes étapes

- Etude de faisabilité
- Positionnement des données auditées au sein de l'environnement informatique
- Définition des tests à effectuer :
  - Données en entrée
  - Critères de sélection
  - Type de test
  - Restitutions
- Récupération des fichiers
- Réalisation des tests
- Bouclage sur réalisation (ajustement des critères, suppression ou ajouts de tests)

Le lien avec la démarche d'audit

Préliminaire

- planification de la mission et information du client
- étude de faisabilité technique

Intérim

- définition des objectifs et des tests à réaliser
- prise de connaissance des applications et de la structure des fichiers du client
- formalisation de l'engagement du client pour la mise à disposition des données

Final

- développement des programmes
- réalisation des tests et exploitation
- remontée aux auditeurs financiers des anomalies rencontrées lors de l'exploitation pour adaptation des tests futures

Les facteurs de réussite

Les principaux points d'attention

La réussite et la pertinence des tests informatiques dépendent en grande partie de l'attention accordée à la <u>préparation</u> de la mission

- les intervenants étant multiples, la coordination des différents <u>acteurs</u> est essentielle
- aucune des principales <u>étapes</u> qui composent la démarche des interrogations de fichiers, depuis la prise de connaissance du système jusqu'à lexploitation des résultats ne doit être négligée
- le <u>planning</u> des tâches concourant à la mise en œuvre d'interrogations de fichiers respecte les mêmes phases que celui d'une intervention traditionnelle et doit être prévu dans le plan de mission global

La phase de préparation

La phase de préparation doit inclure une étude du système informatique pour éviter notamment des interrogations de fichier inutiles ou n'ayant pas de signification

- elle doit permettre de connaître avec exactitude le contenu des fichiers, notamment la définition des champs
- il faut être attentif à l'origine de données des fichiers : ne pas chercher par exemple à recouper deux fichiers issus de la même base de données
- ne conserver que les tests réellement pertinents
- s'assurer que les fichiers contiennent bien les informations recherchées
- contrôler l'exactitude des fichiers clients en les rapprochant des sources « externes » disponibles

La phase d'exploitation

Première exploitation commune des résultats par les auditeurs informatiques et les auditeurs financiers pour valider les résultats du test avant de les remettre au client

- Les tests mis en œuvre permettent-ils de répondre aux interrogations du CAC ?
  - Les auditeurs financiers et informatiques doivent vérifier a posteriori que le travail des premiers répond à l'attente des seconds
- Les tests mise en œuvre sont-ils utiles ?
  - Préparation de la saison suivante : supprimer certains tests que l'expérience a rendu inutiles, ou au contraire en rajouter d'autres plus pertinents, ou complémentaires
- Les tests sont-ils fiables ?
  - Malgré tout le professionnalisme des auditeurs, il se peut que les résultats des tests informatiques ne soient pas pertinents du fait d'erreurs qui se seraient glissées dans les programmes d'extraction
  - Un audit de l'audit informatique s'impose ; attention aux conclusions trop hâtives…

Outils de traitement

Les outils d'interrogation de fichiers sont trop nombreux pour dresser ici une liste exhaustive. Nous avons retenu les principaux outils commercialisés :

Sur micro-ordinateur :

- IDEA (Interactive Data Extraction and Analysis) : outil développé par l'institut canadien des experts comptables agréés et utilisé par KPMG
- ACL (Audit Command Language) : outil américain développé avec le concours de PWC

Sur gros système IBM :

- Panaudit + : outil basé sur le langage Easytrieve de la société Pansophic
- EDP/Auditor : outil basé sur le langage Cullprit de la société Computer Associates

2007-02-08

Formation à l'audit informatique - Audit de la sécurité

Sommaire

- Rappel du contexte
- Continuité de service
- Confidentialité des informations et risques de fraude
- Risques d'erreur et de dysfonctionnement

- Méthode MARION

Rappel du contexte

Objectif

La sécurité du SI a pour objectif de participer à la continuité de l'activité de l'entreprise (« Business Oriented »)

Pour ce faire, son rôle est de protéger le SI de toute dégradation de service sur 3 axes majeurs :

- Confidentialité
- Intégrité
- Disponibilité

Elle peut parfois être un facteur de qualité supplémentaire, voire participer au développement de l'activité (exigences commerciales)

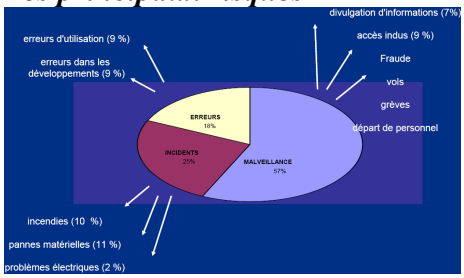
Le coût

Le remboursement des sinistres informatiques coûte chaque année progression constante (+15% par an)

Les pertes réelles des entreprises sont certainement beaucoup plus importantes si on considère :

- les pertes et délits non déclarés
- les pertes de crédibilité

Les principaux risques



Les secteurs d'activité les plus touchés

Part des différents secteurs dans les sinistres déclarés :

Banque Finance Assurances	Industrie	Services	Distribution	Secteur public
43%	22%	15%	14%	5%

Part des différents risques de malveillance pour certains secteurs :

	Banque Finance Assurances	Industrie	Services	Distribution	Secteur public
Fraude	59%	35%	13%	17%	10%
Sabotages	29%	28%	56%	38%	30%

Les protections mises en place par les entreprises

- Ces dépenses des entreprises liées à la sécurité se répartissent de la façon suivante :

Logiciels	Matériels	Etudes				Réseaux
		10%				
65%	10%	Logique	Physique	Audit	Autres	7%
		26%	14%	24%	36%	

- Cela ne représente que 1% des budgets informatiques des entreprises

La sécurité, une préoccupation majeure

- L'informatique est un outil stratégique
- Les Directions Générales sont particulièrement sensibles aux conséquences d'un éventuel sinistre
- Un sinistre important peut remettre en cause la survie de l'entreprise : les risques doivent être évalués

Les principes fondamentaux

Composants	Description
Confidentialité	Protection des données et systèmes sensibles contre toute divulgation non autorisée
Intégrité	Préservation de l'exactitude et de la cohérence des données, des systèmes et des logiciels
Disponibilité	Garantie d'accès aux données et aux systèmes dans des conditions satisfaisantes

Les bonnes pratiques

- Mise en place d'un poste de RSSI
- Définition d'une politique de sécurité
- Plan de sécurité IT (analyse des risques, plan d'action)
- Définition des standards en matières de sécurité
- Mise en place de procédures de sécurité (physique, logique, applications, réseaux…)
- Définition d'une charte de sécurité signée par les collaborateur
- Suivis des incidents de sécurité
- Audit périodique de la sécurité (test d'intrusion…)
- Définition de niveau de service (SLA)

Continuité de service

Les risques

Un serveur tombe en panne
Un fichier important est détruit
Un Boeing 747 s'écrase sur le site
La Seine déborde
Une grève bloque l'accès
Le fournisseur dépose le bilan

Les protections en place

- contre l'incendie
  - Alarmes, gaz Inergen, sprintler, extincteurs, …
- contre les dégâts des eaux
  - Faux plancher, salle informatique à l'étage, pompes, …
- contre les intrusions
  - contrôle d'accès physique par badge, …
- contre les pannes électriques
  - Onduleurs, serveurs redondants, mirroring…

- contre les pannes matérielles
  - stock de rechange, délai d'intervention, de remplacement, …

Les procédures de sauvegarde

Les fichiers nécessaires au fonctionnement de l'entreprise sont-ils sauvegardés régulièrement ?

- données
- sources des programmes
- applications systèmes

Quelle est la fréquence des sauvegardes ?
Les supports de sauvegarde sont-ils lisibles ?
Les lieux de stockage sont-ils sûrs ?

- Coffre ignifugé, stockage hors site

Quelle est l'ampleur de la perte en cas de nécessité de restauration sur un site externe ?

Le site de secours

Existe-t-il un site de back-up ?

- Si oui :
  - De quel type (salle blanche, salle équipée, …) ?
  - Nombre d'adhérents
  - Durée possible d'utilisation ?
  - Les sauvegardes sont-elles sur place ?
  - Peut-on s'y connecter ?
- Si non :
  - Quelle est la solution prévue ?
  - Quel est le délai de renouvellement du matériel ?

Le plan de reprise

Les applications ont-elles été classées selon leur caractère stratégique ?
Les actions à entreprendre ont-elles été formalisées :

- nomination d'un responsable ?
- priorisation des actions à mener ?
- affectation des tâches ?

Le plan de reprise est-il testé régulièrement ?
Le temps de reprise est-il acceptable ?

Les procédures de fonctionnement dégradé

Les procédures de fonctionnement en cas de panne prolongée de l'informatiques ont-elles été définies ?

- Si non :
  - Les protections en place permettent-elles d'affirmer que le risque est faible ?
  - Quel serait l'impact en cas de réalisation du risque ?
- Si oui :
  - Les procédures sont-elles pertinentes ?

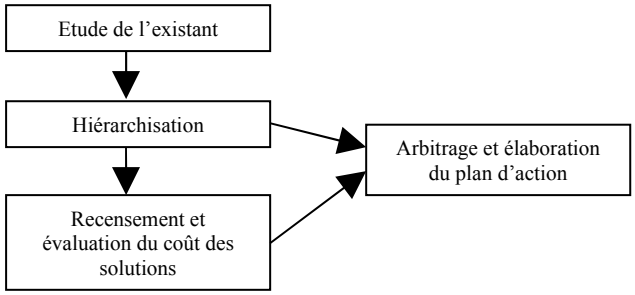
Exemple : une entreprise du secteur de la presse

Objectifs de départ

- Evaluer les risques significatifs d'arrêt de l'informatique de production

- Recenser les solutions permettant de couvrir ces risques en évaluant les investissements nécessaires
- Envisager en priorité les solutions économiques couvrant les risques coûteux
- Etre concret : ne pas viser seulement à se donner bonne conscience

Démarche suivie :



Moyens de protection en place
- un matériel fiabilisé :
  - redondance (2 unités centrales)
  - mirroring (2 copies sur disque)
  - matériels standards
- une salle informatique bien équipée
  - Accès gaz Inergen
  - climatisation
- des sauvegardes régulières et testées

Risques recensés
- Risque de panne du réseau local
  - L'ensemble des communications de l'entreprise sur un seul câble
  - Plan de câblage non à jour
- Risque de « crash » informatique pour une des publications
  - Pas de site de back-up
  - Délai de 5 semaines pour obtenir une nouvelle machine
- Risque de dégât des eaux
  - Circuit d'alimentation d'une photocomposeuse dans la salle machine
- Risque de non parution d'un numéro
  - Epuration des fichiers avant impression réelle chez l'imprimeur
  - Impossibilité de reconstituer l'ensemble de la mise en page

Plusieurs actions à mener hiérarchisées et panifiées
- quelques solutions simples, d'un coût cumulé inférieur à 15k€, courant 50% des risques, à mettre en place dans les trois mois
  - duplication des sauvegardes
  - mise à jour du plan du réseau
  - isolation de la photocomposeuse, …
- quelques solutions, plus lourdes
  - mise en place d'une deuxième nœud du réseau,…

- une solution complexe à mettre en œuvre, d'un coût évalué à plus de 100 k€, portant le taux de couverture à 80%, à mener dans les 2 ans
  - définition d'un plan de secours croisé avec une autre filiale du même groupe (même outils, …)

Autres types d'interventions envisageables
Assistance à la définition du plan de reprise
Assistance à la définition du plan de fonctionnement dégradé
Recherche d'une solution de secours extérieure
Revue des assurances
…

Confidentialité et risque de fraude
Les risques
- La concurrence accède au fichier client
- Un informaticien modifie un paramètre
- Un utilisateur accède au fichier des virements
- Des agents accèdent à des fonctionnalités sensibles
- Un « hackers » se connecte sur la machine centrale
- Un salarié accède à la paye et augmente son salaire
- Le trésorier détourne 1 millions d'Euros
- Un informaticien détourne les arrondis à son profit
- Un visiteur vole les lettres chèques

Les solutions existantes
- Authentification
  - Mots de passe
  - Reconnaissance vocale, biométrique,
  - Identification par carte à puce
- Droits d'accès logiques
- Clés de chiffrement
- Protection du réseau interne :
  - DMZ (isolation des accès Internet)
  - VPN
  - Serveur Proxy (centralise les requêtes Internet, blocage des utilisateurs)
  - Firewall (autorisation des accès, analyse des flux)
  - Routeur filtrants (routage des requêtes et des réponses)
- Contrôles a priori et a posteriori

Les thèmes à étudier
- Recensement des données confidentielles
  - Il s'agit de recenser :
    - Les données dont la divulgation porterait préjudice à l'entreprise
    - Les transactions / fonctionnalités dont l'usage doit être restreint
    - Les zones à risques (virements, lettres-chèques, …)
  - Ce recensement doit avoir été effectué par l'entreprise ou doit être effectué en collaboration avec elle

- Couche système
  - Un utilisateur se connectant doit s'identifier et s'authentifier
  - Déconnection automatique, nombre maximum de tentatives infructueuses
  - Gestion des accès aux objets sous MVS : RACF, Top Secret
  - Gestion des autorisations sous AS/400 : OS400
- Mécanisme interne à l'application
  - Gestion de profils
  - Certains fichiers et transactions sont réservés à des utilisateurs définis
  - Les mots de passe (application, bases de données, OS) :
    - Sont-ils régulièrement modifiés ?
    - Intègrent-ils des critères de complexité suffisants ?

Les thèmes à étudier

- La procédure de demande d'autorisation est-elle formalisée ?
- Les accès et les droits sont-ils accordés par des responsables définis ?
- Les départs de personnels donnent-ils lieu à des suppressions des droits accordés ?
- Des audits des droits accordés sont-ils régulièrement effectués ?
- Les comptes génériques sont-ils limités. Les comptes techniques sont-ils correctement sécurisés ?
- Contrôles a posteriori : trace des accès
  - Revue de l'utilisation des super utilisateurs
  - Revue des tentatives d'accès infructueuses
- Les contrôles d'accès physiques
  - Bâtiment, bureaux, armoires
  - Badges, digicodes
- Les procédures organisationnelles
  - Séparation des fonctions
  - Procédure d'autorisations d'engagement de dépenses (seuil)
- Contrôle de gestion
  - Suivi des volumes versés, recoupements, …
- Analyse des écritures comptables (OD-opérations diverses)
  - Analyse des opérations répondant à certains critères (seuils, montant ronds, écritures passées le week-end…)
- Traces des accès
  - Possibilité de retrouver l'ensemble des manipulations effectuées tel jour, par tel agent, sur tel dossier, …
- Application des patchs de sécurité sur les firewalls et les routeurs
- Sécurisation des mots de passe d'accès au routeur/firewall

Les thèmes à étudier : les accès des informaticiens

Les informaticiens constituent une population à risque

- Ils maîtrisent les traitements autant sous leurs aspects fonctionnels que techniques
- Ils sont capables de cerner s'il y a ou non une possibilité de détection
- Ils sont quelquefois en mesure d'effacer les traces de leurs manipulations

Il est donc nécessaire de :

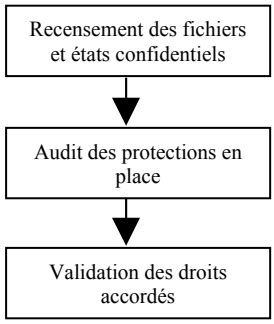
- Leur interdire l'accès direct à l'environnement de production
- Mettre en place une procédure de contrôle des mises en production des programmes

Exemple dans le secteur de la distribution

Objectifs de départ

- Dans le secteur de la distribution, les ristournes accordés par les fournisseurs sont des informations stratégiques et donc très confidentielles
- Les risques de divulgation à l'extérieur sont-ils faibles ?
- Comment améliorer encore la protection ?

Démarche suivie



Moyens de protection en place

- un service dédié à la gestion des ristournes
- des mots de passe
- une procédure d'habilitation étoffée

Risque recensés

- Risque organisationnel
  - Les agents du service ont accès chacun à l'ensemble des informations (pas de séparation des fonctions)
  - Les documents émis sont nombreux et trop largement diffusés
- Risque informatique
  - Au sein du service, les mots de passe sont connus de tous
  - Des sites éloignés auraient la possibilité d'accéder aux informations sensibles
  - Les fichiers sensibles sont accessibles

Risques de dysfonctionnement

Les risques

- Une fonctionnalité récente, mal « testée », génère des erreurs
- Une application ne traite pas bien un cas particulier
- Une erreur de saisie entraîne un approvisionnement dix fois supérieur à ce qui est nécessaire
- Incidents majeurs d'exploitation
- Un virus se propage dans le système
- …

Les solutions existantes

- Méthodes de développement
  - MERISE, AXIAL,…
- Recette
- Contrôles à la saisie

- Détecteur de virus
- Automatisation de l'exploitation
- Assurance qualité
  - MAQ, INCAS-MESSIE

Les thèmes à étudier
- Les « Etudes »
- L' « Exploitation »
- La fiabilité des applications
- Les mécanismes et procédures de détection

?
- L'informatique évolue « au fil de l'eau »
- La société doit évaluer à chaque évolution si les traitements peuvent être entachés de dysfonctionnements de nature à perturber gravement la bonne marche de l'entreprise ?

Risques recensés
- Développement
  - Développement « anarchique » autour du progiciel
    - Acquisition de nouvelles versions impossible
  - Pas de séparation des environnements
    - Mise directe en exploitation
- Exploitation
  - Documentation insuffisante
  - Maîtrise difficile
    - Exemple : les fichiers liés à une filiale vendue à l'extérieur, était toujours traités
  - Suivi peu étoffé, pas de gestionnaire de travaux
    - Pas d'état synthétique

Eclairage : les virus

Différentes terminologies existent :
- « chevaux de Troie » : fonction illicite dans un programme
- « bombes logiques » : déclenchement différé
- « vers » : déplacement en mémoire
- « virus » : multiplication en mémoire

Les « virus » sont dangereux car :
- ils s'auto-reproduisent
- ils peuvent détruire les fichiers sur disque

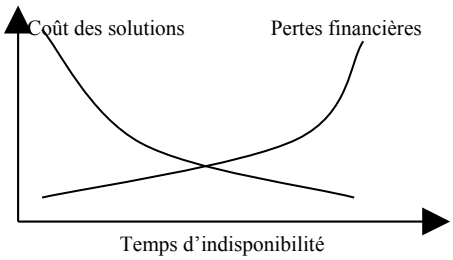
Une dizaine seulement de « virus » est responsables de 99% des infections
- ils sont détectables, car connus

Méthode « MARION »

Les intérêts de la méthode
- Permet de donner un avis sur le niveau de sécurité existant d'une entreprise
- Evalue les risques potentiels
- Ne s'intéresse pas exclusivement à l'informatique
- Mais à l'ensemble des facteurs qui contribuent à la sécurité
- Quantifie les enjeux financiers

- Met l'accent sur la quantification financière des pertes
- Débouche, après arbitrage, sur un plan d'action

L'arbitrage entre les pertes financières prévisibles et les investissements envisagés :



Les principes de la méthode

Questionnaire de 640 questions se rapportant à 27 thèmes

- Chaque réponse est notée de 0 à 4 et est pondérée en fonction de l'importance du thème concerné

Parallèlement les risques sont identifiés

- leur probabilité d'apparition est estimée
- leurs conséquences sont évalués

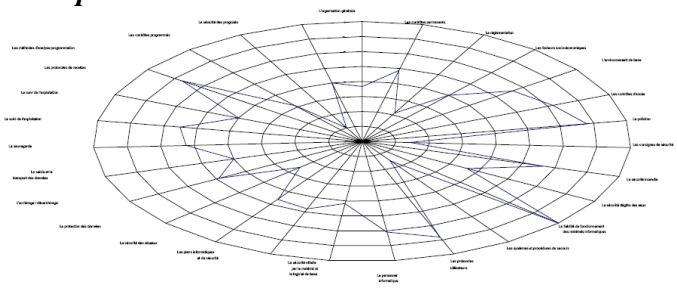
Le rapprochement des points de faiblesse et des risques permet le recensement des solutions envisageables

Ses modalités

L'application « pure et dure » de la méthode est lourde et nécessite une étude de plus de trois mois

Mais il paraît envisageable de mener de « mini-études » MARION, surtout axées sur l'utilisation du questionnaire

Exemple



2007-02-15

Formation à l'audit informatique
- Audit en environnement ERP

Plan :

- Présentation des ERP et introduction à SAP
- Impacts des ERP sur les risques liés au SI
- L'approche spécifique d'audit des ERP

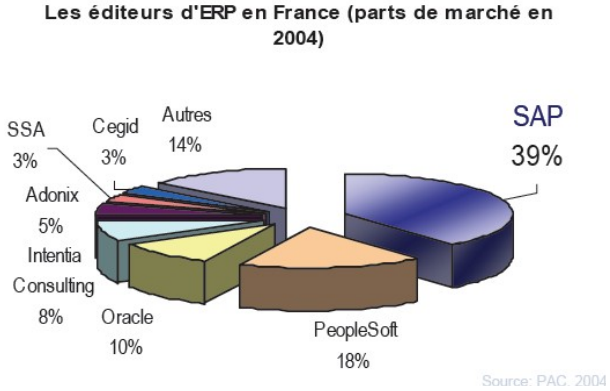
- Exemple des flux SAP

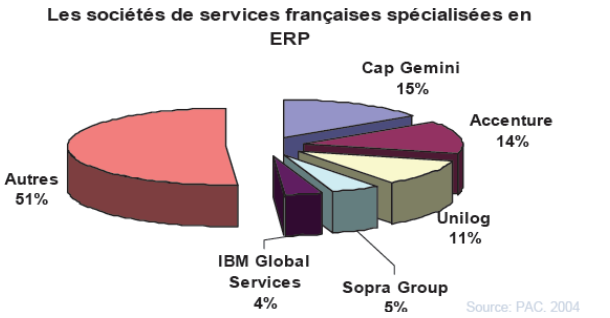
Présentation des ERP et introduction à SAP
Présentation des ERP
Définition
Ensemble de logiciels intégrant les principales fonctions nécessaires à la gestion des flux et des procédures de l'entreprise (comptabilité et finances, logistique, paie et ressources humaines, etc.). Tous ces logiciels accèdent à des ressources communes, en particulier des bases de données (et donc des données de base).

Segments du marché des ERP
Le marché des ERP comporte plusieurs segments primaires par taille de clients, auxquels correspondent des éditeurs différents :
- grands comptes :SAP, Oracle/PeopleSoft
- grosses PME :Microsoft, Lawson, SSA Global, Geac, SAP, Oracle/PeopleSoft,
- petites PME :Microsoft, Epicor, Exacta, Sage, NetSuite, SAP BusinessOne,
- petites entreprises :Sage, Intuit, ACCPAC, NetSuite.

Taille du marché français des ERP en 2004 : 3,4 Milliards d'Euros

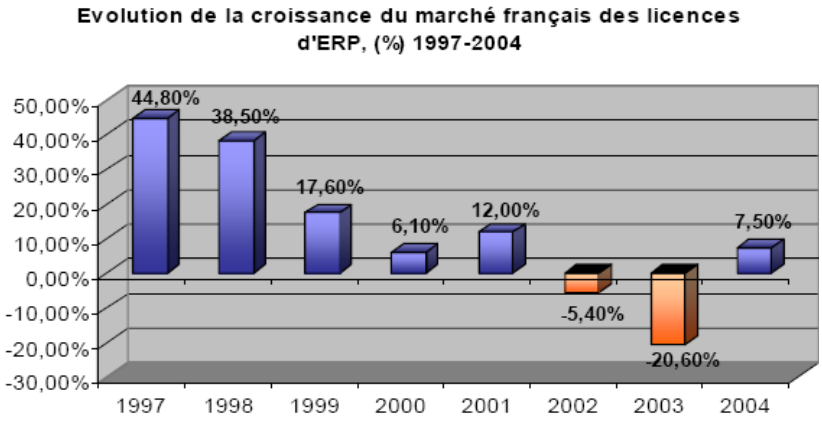
Les principaux acteurs du marché ERP en France :



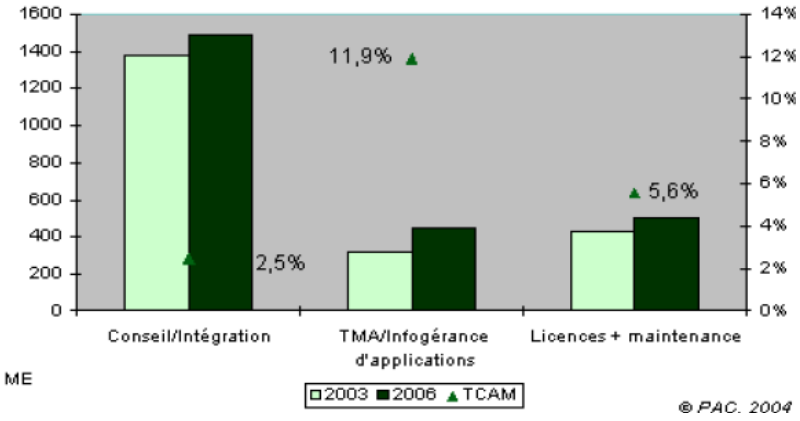


Rq : en décembre 2004, Oracle a racheté PeopleSoft pour 10 milliards de $

Les tendances du marché ERP en France :



(Source : IDC, 2004)



Introduction à SAP

SAP : signification ?

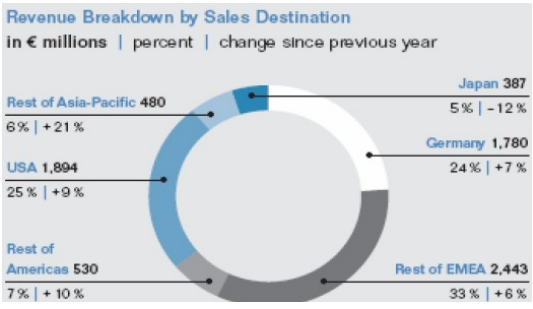
- Système
- Application
- Produit

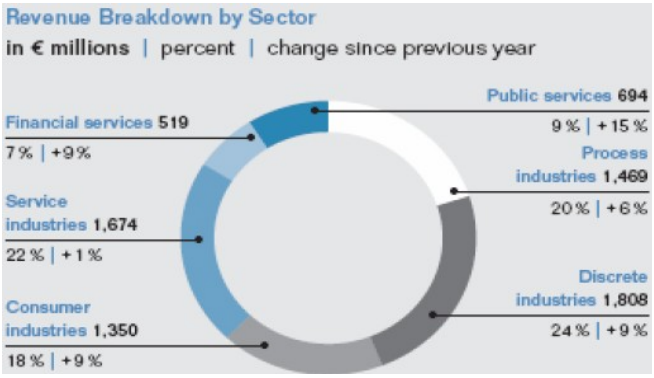
SAP : créé en Allemagne à Walldorf en 1972

SAP : leader mondial des ERP*

- 12 millions d'utilisateurs dans plus de 50 pays
- 91 500 installations
- 1500 partenaires

Les chiffres clés du CA mondial de SAP en 2004





Le produit SAP

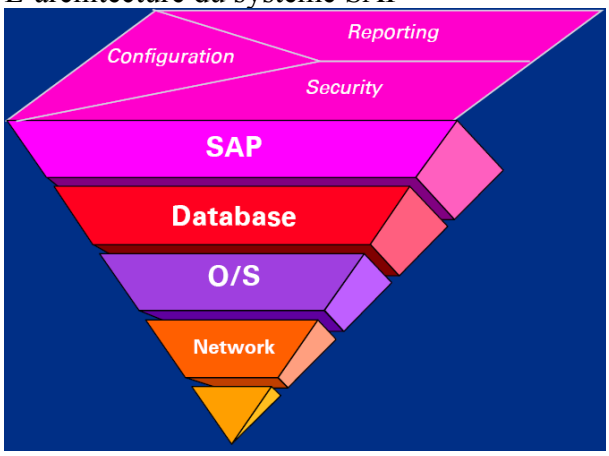
- Original product was SAP R/2 on the mainframe introduced in 1974
- SAP R/3 introduced for smaller platforms using 3-tier architecture in October 1992
- SAP code is written in a proprietary fourth generation (4GL) programming language developed by SAP known as Advanced Business Application Programming or "ABAP/4"
- SAP has bought other software companies to supplement its own, e.g. HR module was not originally SAP's

Les versions SAP

- 2.2h 1970's, 1980's
- 3.0d, 3.0e, 3.0f 1996/1997
- 3.1g, 3.1h, 3,1i1997/1998
- 4.0b1998
- 4.5a,b1999
- 4.6a,b,c2000/2001
- 4.70 (Enterprise)2004

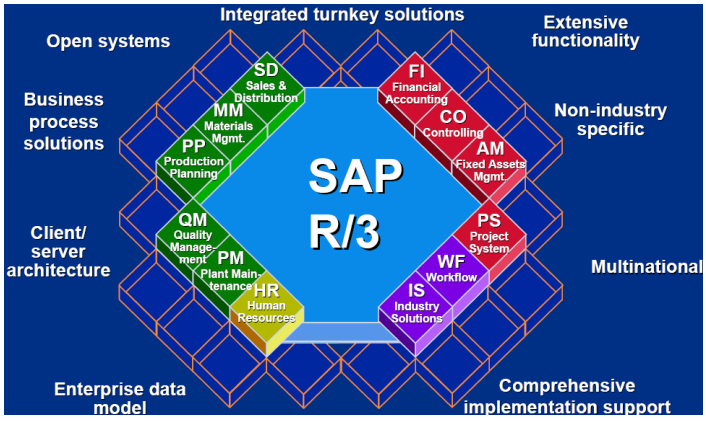
Les versions non maintenues par SAP : jusqu'à la 4.0b => risque pour le client

L'architecture du système SAP



La structure modulaire de SAP

- Les modules SAP
- Le module Finance (FI)
  - General Ledger (FI-GL)
  - Accounts Receivable (FI-AR)
  - Accounts Payable (FI-AP)



    - Tax and Financial Reports
    - Special Purpose Ledger
    - Special Purpose Ledger
    - Legal Consolidations

  Financial Applications…
- Le module Contrôle de Gestion (CO)
    - Cost Center Accounting
    - Profit Center Accounting
    - Product Cost Controlling
    - Profitability Analysis
    - Activity Cost Management
    - Internal Orders

  Financial Applications…
- Le module Gestion des Immobilisation (FI-AA)
    - Depreciation
    - Property Values
    - Insurance Policies
    - Capital Investment Grants

  Financial Applications…
- Le module Gestion des Achats (MM)
    - Procurement
    - Inventory Management
    - Vendor Evaluation
    - Invoice Verification
    - Warehouse Management

  Logistics Applications…
- Le module Gestion de la Production (PP)
    - Sales & Operations Planning
    - Demand Management
    - Material Requirements Planning
    - Production Activity Control
    - Capacity Planning

  Logistics Applications…
- Le module Gestion des Ventes (SD)
    - Quotations
    - Sales Order Management
    - Pricing
    - Delivery
    - Invoicing

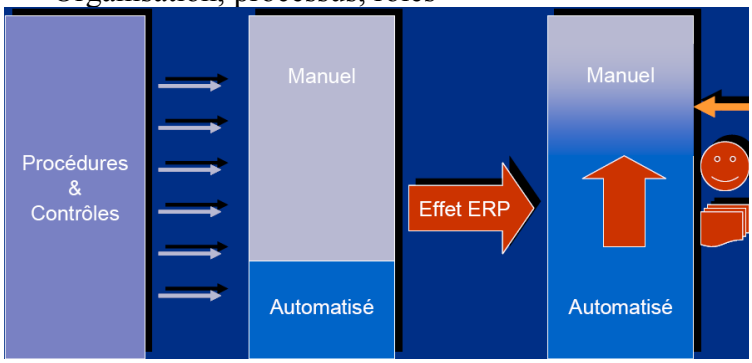
  Logistics Applications…
- Le module Gestion des Ressources Humaines (HR)
    - Personnel Administration
    - Payroll, Benefits
    - Time Management
    - Planning and Development
    - Organisation Management

  Human Resources…

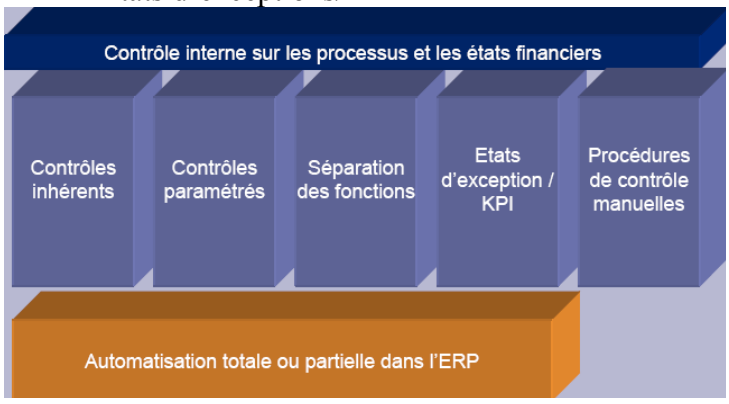
Impacts des ERP sur les risques liés au SI

- Facteurs de risques aggravés en environnement intégré:
  - Traitements basés sur des données fondamentales erronées (tarifs, conditions de paiement…)
  - Partage en temps réel d'informations erronées (niveau de stock, encours des projets d'investissement…)
  - Accès illicite à des informations confidentielles ou à des transactions sensibles
  - Absence de séparation de fonctions
  - Manque de fiabilité des traitements automatisés
  - Utilisation non adéquate du système
  - Contournement des contrôles programmés
  - Effet «boîte noire»

- Organisation, processus, rôles



- Les contrôles se transforment et se déplacent…
- Le découpage en processus est défini par l'ERP
- Les contrôles au sein des programmes sont de plusieurs types :
  - Contrôles inhérents
  - Contrôles paramétrés
  - Séparation des fonctions
  - Etats d'exceptions/KPI



- Il existe souvent un Core Model, décliné (adapté) ensuite localement

L'approche spécifique d'audit des ERP

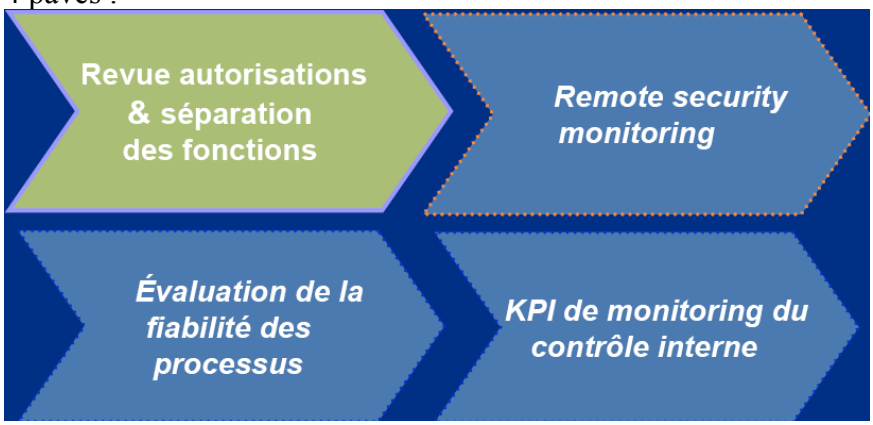
Les missions d'audit en environnement ERP doivent inclure :

- Pour les revues de sécuritélogique :

- Une revue détaillée des autorisations
- Une revue de la correcte mise en oeuvre de la séparation des fonctions

- Pour les revues de processus :
  - Une revue de la correcte implémentation des contrôles totalement automatisés (contrôles paramétrés)
  - Une revue de la correcte appréhension/réalisation par les utilisateurs des contrôles partiellement automatisés (revue d'états d'anomalies)

4 pavés :



Revue autorisations & séparation des fonctions

Objectif : couvrir les risques de diffusion d'informations confidentielles et d'accès à des transactions critiques

L'évaluation des contrôles mis en place pour assurer la sécurisation des actifs et le respect de la confidentialité des informations les plus sensibles au sein de SAP se déroule en 3 étapes :

- analyse de la politique générale de sécurité logique et des procédures sous-jacentes de gestion
- analyse des accès aux fonctionnalités SAP les plus critiques au regard des définitions de poste des utilisateurs concernés
- revue des risques de non séparation des fonctions au sein du système d'information (par exemple, utilisateurs pouvant créer un fournisseur, créer une facture et déclencher le paiement)

Les fondamentaux de la sécurité:

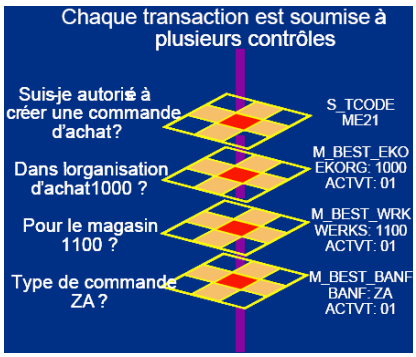
- Plusieurs sociétés
- Plusieurs organisations commerciales, sites de production…
- Plusieurs milliers de transactions en standard
- Plusieurs milliers d'utilisateurs
- Plusieurs environnements

⇨ Plusieurs millions de combinaisons possibles

⇨ <u>Concept complexe et difficile à maintenir et auditer</u>

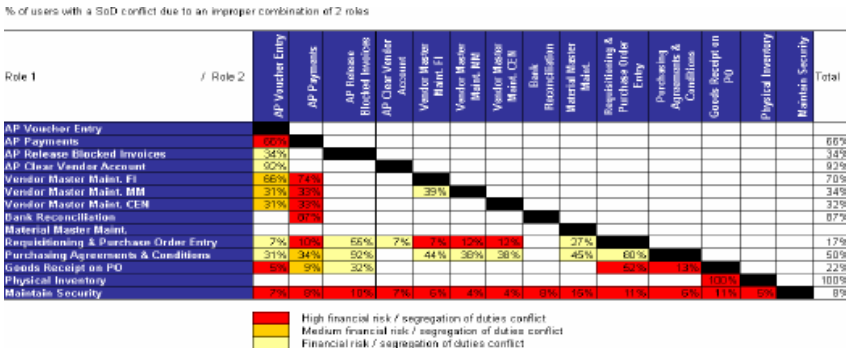
Pour qu'un utilisateur puisse réaliser une opération, il doit avoir accès à l'ensemble des objets requis par la transaction associée :

Ce concept est répété pour plus de 8000 transactions avec environ 600 objets de sécurité contrôlés



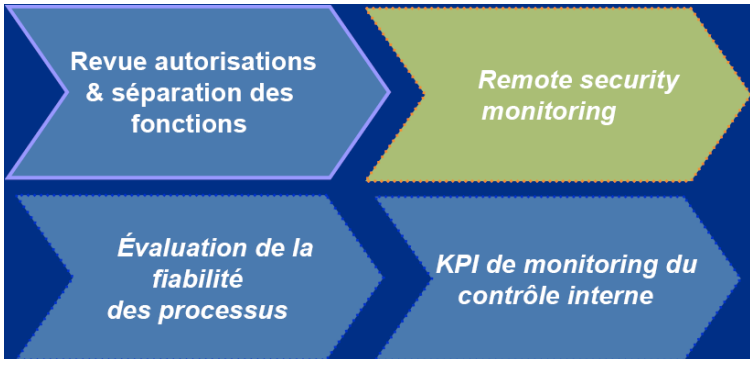
Définition d'un référentiel de séparation des fonctions adapté à l'entité et au système SAP
Réalisation des tests, quel que soit l'outil utilisé, par ou avec l'assistance d'une personne disposant des compétences techniques adéquates

Task Group Description	Group Number	AP Voucher Entry	AP Payments	AP Release Blocked Inv	AP Clear Vendor Account	Vendor Master Maint. FI	Vendor Master Maint. MM	Vendor Master Maint. CEN	Bank Reconciliation	Material Master Maint.	Requisitioning & Purchase Order Entry	Purchasing Agreements & Conditions	Goods Receipt on PO	Physical Inventory	Maintain Security
		PU01	PU02	PU03	PU04	PU05	PU06	PU07	PU08	PU09	PU10	PU11	PU12	PU13	PU14
AP Voucher Entry	PU01		HX	X	X	MX	MX	MX			X	X	HX		HX
AP Payments	PU02	HX				HX	HX	HX	HX		HX	MX	MX		HX
AP Release Blocked Invoices	PU03	X									X	X	X		HX
AP Clear Vendor Account	PU04	X									X				HX
Vendor Master Maint. FI	PU05	MX	HX				X				HX	X			HX
Vendor Master Maint. MM	PU06	MX	HX			X									HX
Vendor Master Maint. CEN	PU07	MX	HX								HX	X			HX
Bank Reconciliation	PU08	MX	HX												HX
Material Master Maint.	PU09										X	X			HX
Requisitioning & Purchase Order	PU10	X	HX	X	X	HX	HX	HX		X		X	HX		HX
Purchasing Agreements &	PU11	X	MX	X		X	X	X		X	X		HX		HX
Goods Receipt on PO	PU12	HX	MX	X							HX	HX		HX	HX
Physical Inventory	PU13												HX		HX
Maintain Security	PU14	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	



Il existe de nombreux outils permettant d'auditer les autorisations et la séparation des fonctions en environnement SAP.
Le module «Audit Information System (AIS)»de SAP
Et des outils du marché:

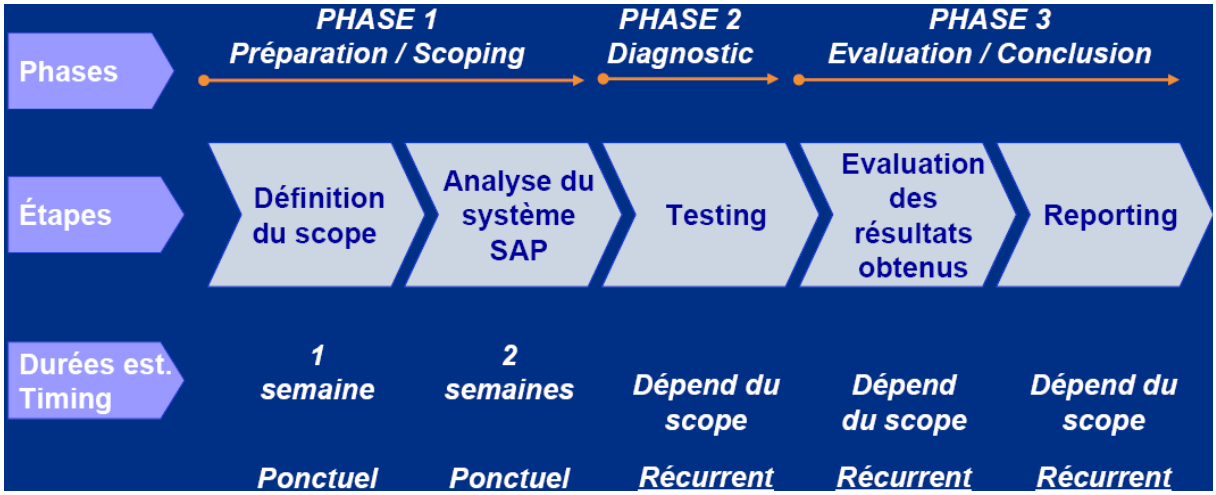
- Virsa: «SAP® Compliance Suite ®»
- CSI : «CSI Authorization Auditor®»
- Bindview: «bv-Control® for SAP®»
- Approva: «BizRights ®»
- …



Remote security monitoring

OBJECTIFS

- Permettre un monitoring continue du niveau de sécurité d'un système SAP grâce à un dispositif de contrôle récurrent
- Satisfaire aux nouvelles obligations en matière de contrôle interne en évaluant les sécurités SAP au niveau Groupe
- Réduire la charge de testing d'un groupe soumis aux obligations Sarbanes-Oxley 404 grâce à la réalisation au niveau Groupe de tests automatisés avec participation limitée des filiales
- Mettre à disposition des «security officers SAP» un moyen de pilotage et de contrôle fiable et simple à utiliser



Définition du scope des revues

- Scoping des entités / sociétés
- Sélection des (sous-)processus critiques à tester
- Définition de la fréquence des revues

Analyse du système SAP

- Identification des transactions utilisées et/ou utilisables (par sous-processus)
- Définition du niveau de détail des tests (transactions ou objets)
- Définition des critères de test par transaction

Testing–suivant une fréquence à définir :

- Extraction des tables de sécurité SAP
- Traitement de ces données à l'aide d'un des outils du marché

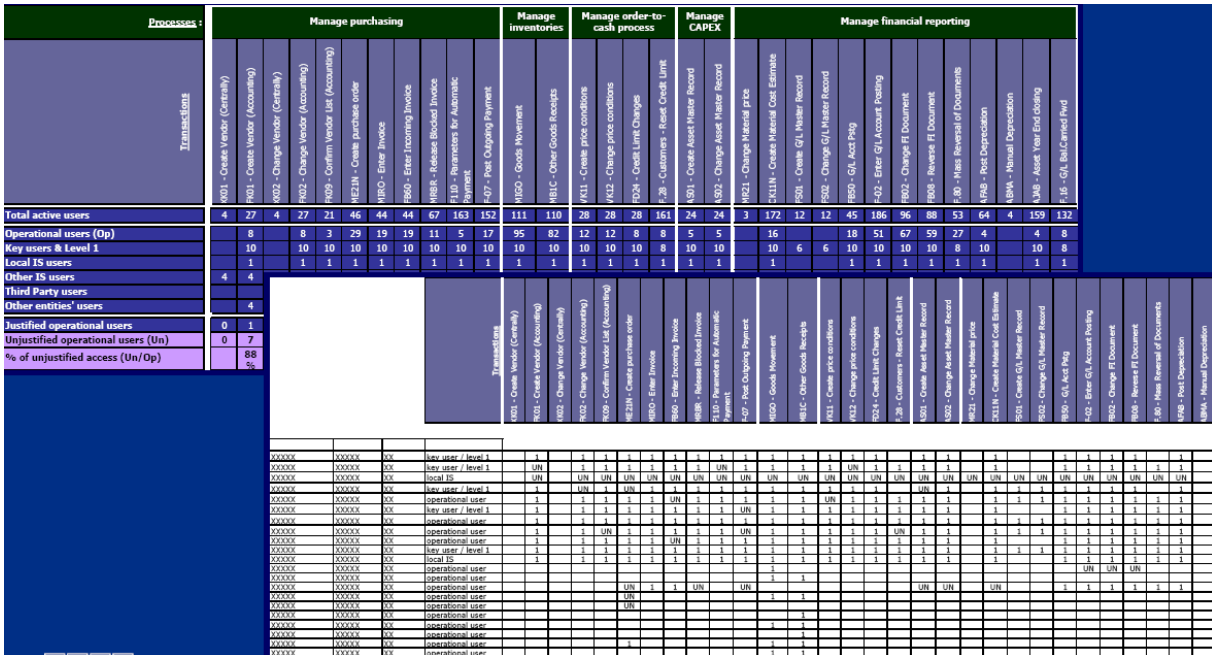
- Création d'un matrice de droits d'accès par entité
- Identification par les security officers de chacune des entités, des accès non justifiés par user

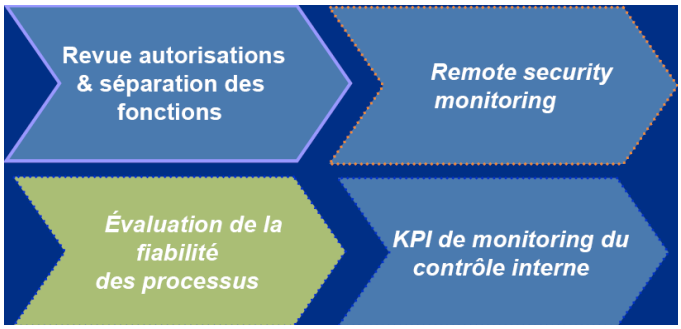
Évaluation des résultats obtenus

- Calcul de KPI sécurité aux niveaux entité et Groupe
- Identification des “Best in class” au sein du Groupe
- Suivi de l’évolution des résultats période après période

Reporting

- Formalisation d’un rapport synthétique par entité
- Reporting graphique pour le Groupe / Comité d’Audit





Evaluation de la fiabilité des processus

OBJECTIFS

- Identifier et tester l’ensemble des contrôles clés d’un processus et notamment ceux automatisé
- Augmenter la pertinence des tests réalisés en s’appuyant sur le système et les contrôles paramétrés
- Augmenter le degré de précision des tests grâce à des populations de test plus larges (exhaustive)
- Gagner en efficacité grâce à l’automatisation des tests

Exemples de contrôles

Global system settings	Les structures organisationnelles (sociétés, controlling area, organisation d'achat, usines, divisions…) ont été définies de manière à refléter l'organisation du Groupe
	Le log des modifications sur les tables sensibles a été activé
Achats	Des champs sensibles ont été définis sur les fiches fournisseurs requérant une validation par une tierce personne pour toute modification
	Le flag « Contrôle des factures en doublons » est actif pour tous les groupes de fournisseurs
	Les tolérances lors du contrôle facture ont été paramétrées de manière à blouer au paiement toute facture au-delà d'un écart de prix de +2%
	Les stratégies de validation paramétrées sur les demandes d'achat et les commandes respectent la délégation de pouvoirs en vigueur
	Les structures d'écran définissant les champs obligatoires à la saisie des demandes d'achat / commandes ont été définis et adaptés pour les différents types de pièce en fonction des diverses typologies / scénarios d'achat

Exemples de contrôles

Achats	Sur une commande, les champs X, Y, Z sont hérités de la demande d'achat et ne sont pas modifiables
	Les tolérances sur les réceptions ont été paramétrées de manière à bloquer toute entrée de marchandise avec un écart de +5% sur la quantité commandée
	Les conditions de paiement ne sont pas modifiables sur la facture fournisseur
	Les factures FI (sans engagement) sont systématiquement bloquées au paiement
	Les avoirs sont paramétrés de telle sorte que la référence à la facture d'origine est obligatoire
Ventes	Le paramétrage requiert qu'une expédition ait été réalisée avant tout émission de facture
	Les fonctionnalités de relance automatique ont été activées dans SAP
	Des limités de crédit ont été paramétrées pour l'ensemble des clients. Le système bloque toute commande au-delà des limites de crédit paramétrées

Exemples de contrôles

Stocks	Le code mouvement 561 permettant de modifier directement la valeur des articles en stock est bloqué.
	Les stocks négatifs ne sont pas autorisés.
Immobilisations	Les modes et les durées d'amortissement ont été paramétrés sur les différents tableaux d'évaluation en fonction des règles Groupe et ne peuvent pas être modifiés sur la fiche immobilisations
Comptabilité	Les comptes alimentés par les comptabilités auxiliaires Clients, Fournisseurs, Immobilisations ont été définis en tant que compte de réconciliation
	Les comptes alimentés par des processus automatisés ont été définis comme tel en vue de bloquer toute imputation manuelle

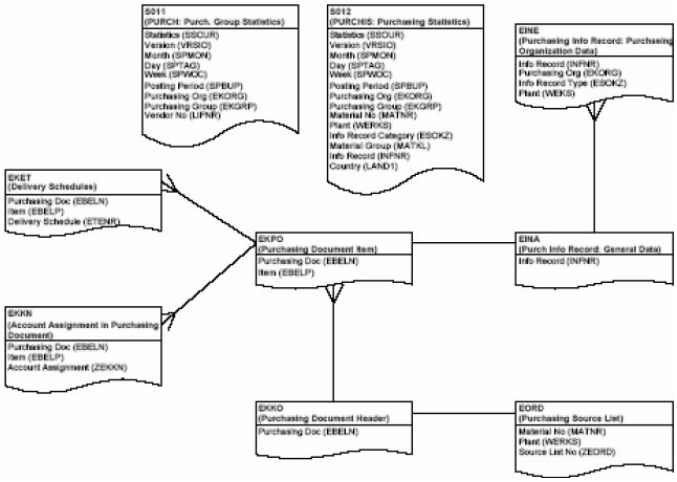
LA DEMARCHE

Les processus étant standardisés, la majorité des contrôles est connue, et le temps nécessaire à leur identification réduit de manière très significative
La phase de préparation de la mission d'audit peut être renforcée par :

- Une analyse du système SAP
- Le lancement d'états d'exceptions
- Des extractions de données et réalisation de requêtes

et ainsi permettre de concentrer le temps d'intervention terrain sur l'analyse de résultats de tests
Nécessité d'intégrer dans l'équipe d'audit des auditeurs spécialisés ERP

Les données étant structurées en tables dans les ERP, de nombreux tests peuvent être réalisés à partir d'extractions de données puis retraitements et requêtes (SQL, Access, IDEA…)
Ex : tables SAP relatives aux commandes d'achats



AUGMENTER LA PERTINENCE DES TESTS
Diminution du nombre de tests réalisés par échantillonnage au profit de tests réalisés sur des bases exhaustives. Exemple :

- l'existence d'une commande pour chaque facture fournisseur peut être vérifiée par échantillonnage et retour aux pièces justificatives…
- …mais aussi àl'aide de requêtes SAP sur une base exhaustive.

La connaissance technique de SAP permet d'évaluer des contrôles critiques programmés au sein de l'ERP. Exemple :

- l'efficacité du «3-way match»(rapprochement commande / réception et facture fournisseur) peut être évaluée suite à une revue du paramétrage SAP (clés de tolérances entre autres) et à l'analyse d'états d'exceptions produits à l'aide de queries (factures pour lesquelles le «3-way match»a été contourné).

GAGNER EN EFFICACITE
L'auditeur a accès de manière «immédiate»aux informations qui lui sont nécessaires
Automatisation des tests auparavant réalisés manuellement :

- Recherche des factures fournisseurs saisies/payées en double
- Validation par un niveau hiérarchique adéquat des engagements de dépenses
- Cohérence entre les délais de paiement indiqués sur les factures clients et les délais de paiement enregistrés dans les «master data»

- Validation de la provision pour factures à recevoir…

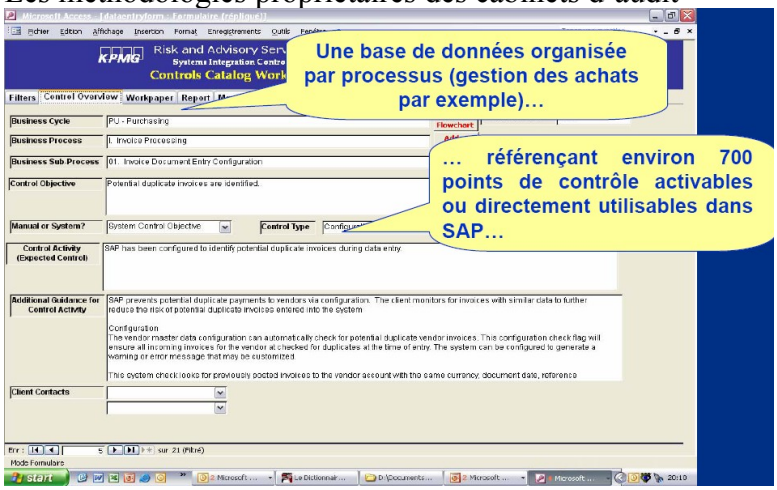
Capitalisation des «outils/requêtes»de tests créés lors d'un premier audit
Mise en place et utilisation d'indicateurs de performance du contrôle interne automatiquement calculés dans SAP (utilisables lors des phases de scoping et/ou de testing)
Les outils pour évaluer la fiabilité des processus

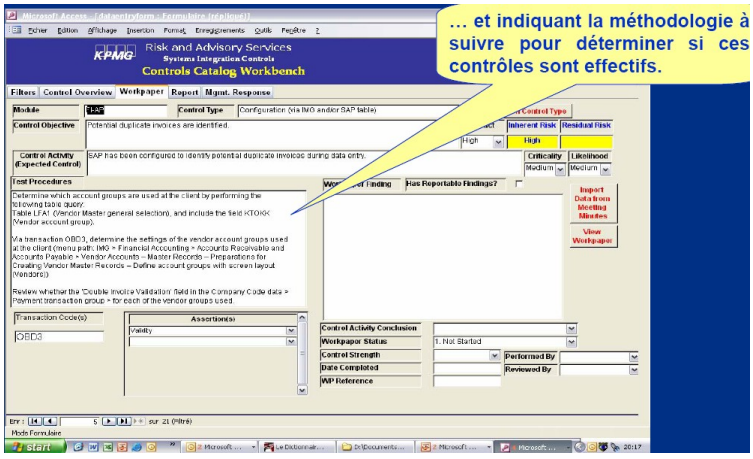
- Le contrôle interne n'étant pas une priorité pour les éditeurs de progiciels ni les intégrateurs, il existe sur le marché peu d'outils référençant l'ensemble des points de contrôles existant dans les ERP (SAP, Oracle Applications, JD Edwards…)
- Les cabinets d'audit, de par leur expérience, ont pour la plupart développés des bases de connaissance en la matière.

Les méthodologies propriétaires des cabinets d'audit

- Les «Controls Catalogs»sont des référentiels de contrôles attendus en environnement ERP basés sur notre connaissance des faiblesses les plus fréquemment constatées, et des fonctionnalités de contrôle proposées en standard par les différents ERP.
- Ces controls catalog sexistent pour les ERP suivants : SAP R/3, Oracle et JD Edwards.

Les méthodologies propriétaires des cabinets d'audit

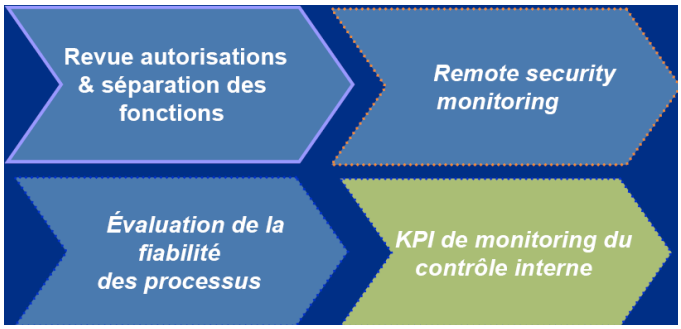




La valeur ajoutée

- Avoir une vision complète et exacte des contrôles au sein des processus
- Permettre une couverture plus large des risques

- Être capable de proposer des recommandations précises grâce àla connaissance technique du système et des possibilités de contrôles qu'il offre
- Identifier des axes d'optimisation du contrôle interne
- Augmenter le niveau d'assurance et renforcer l'image de l'Audit Interne



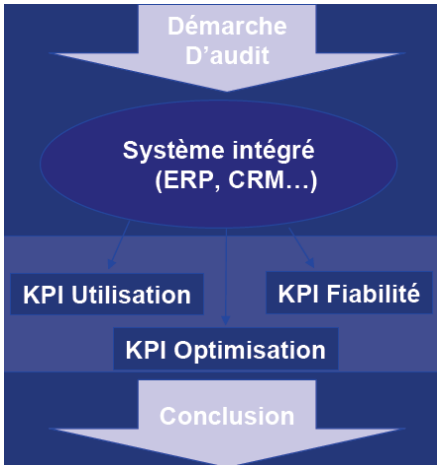
KPI de monitoring du contrôle interne

La démarche KPI
La mise en place et le fonctionnement durable d'un système se caractérise par la recherche :
- D'un niveau d'utilisation optimale
- Tout en disposant d'un niveau de fiabilité satisfaisant

Le niveau d'utilisation peut se mesurer à partir des volumes de transactions:
- Les fonctions implémentées sont-elles utilisées ?

Le niveau de fiabilité peut se mesurer en suivant les erreurs et les rejets :
- Les fonctions sont-elles utilisées correctement ?

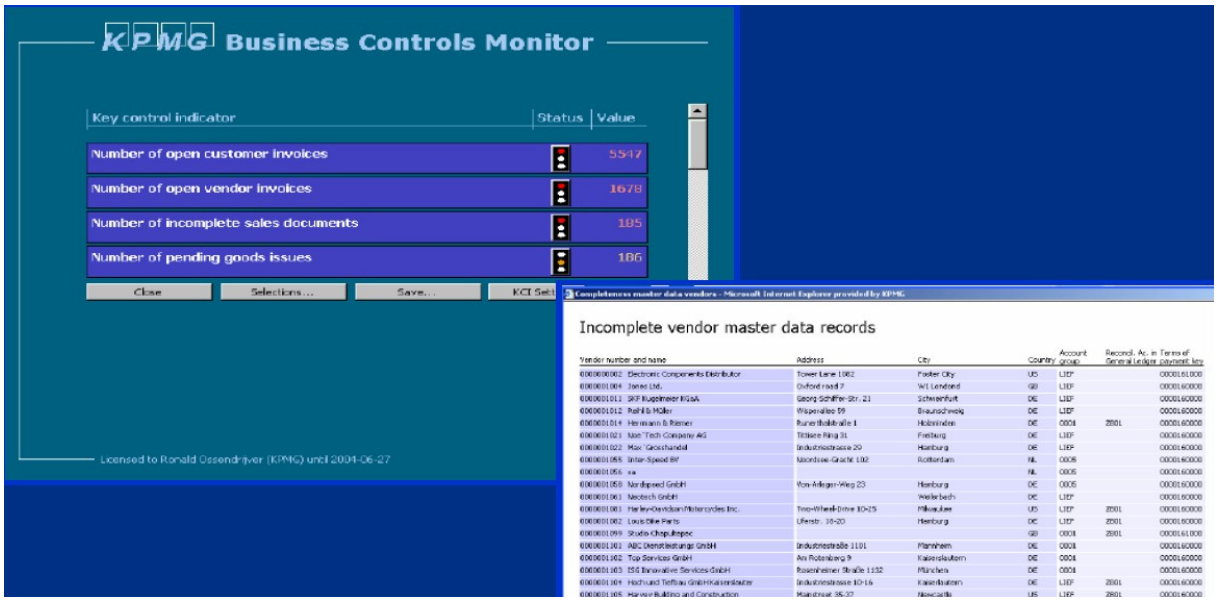
Démarche de mise en œuvre
- Définition des objectifs (utilisation du système, fiabilité des processus, optimisation…)
- Élaboration et tests des KPI en liaison avec le ROI attendu
- Validation des KPI sur un Pilote
- Élaboration d'un Tableau de bord KPI



Les outils
Il existe de nombreux outils de type «contenant» permettant un monitoring à l'aide de KPIs à développer / renseigner mais peu avec du contenu
Les outils du marché:
Virsa Confident Compliance™
- KPMG Business Controls Monitor™…Ces KPIs peuvent aussi faire l'objet de développements spécifiques (mais nécessite des compétences techniques très poussées) :
- Le module AIS de SAP regroupe un certain nombre d'états d'exception pouvant servir de base à l'élaboration de tels KPIs
- Lorsqu'il est implémenté le module BW offre des possibilités de reporting

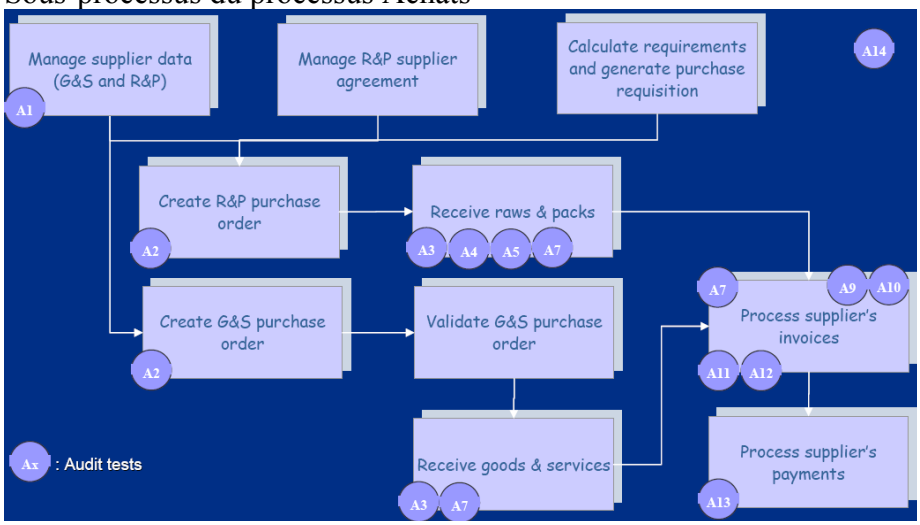
Multiples

Exemple d'automatisation des KPI



Exemples de flux SAP

Sous-processus du processus Achats



Procédures de tests

A1	Risque	Des paiements sont effectués à des fournisseurs non autorisés selon les règles de société		
	Objectif de contrôle	L'utilisation du code fournisseur générique (#999) est limitée aux achats ponctuels (<2 occurrences) et non significatifs (<1000€)	Données nécessaires	• Factures d'achat
	Procédures de tests	• Extraire la table SAP des factures fournisseurs depuis le 1/1/N • Filtrer sur le code fournisseur #999 afin de n'obtenir que les factures relatives au code fournisseur générique • Grouper les factures par nom fournisseur en nombre total et en valeur		

		totale (COUNT & SUM) • Obtenir des explications de la part du Responsable Achats pour 10 fournisseurs sélectionnées aléatoirement pour lesquels le nombre total et/ou le montant total des factures excède les limites autorisées.		
A2	Risque	Les prix utilisés dans les commandes achats sont ceux négociés avec les fournisseurs formellement approuvés dans les contrats		
	Objectif de contrôle	Les prix dans les commandes d'achats sont automatiquement copiés des contrats saisis dans SAP qui correspondent aux contrats papiers signés avec les fournisseurs	Données nécessaires	• Paramétrage SAP • Contrats fournisseurs SAPA
	Procédures de tests	• S'assurer que le système SAP est paramétré de façon à copier automatiquement les prix dans les commandes d'achats à parti des contrats et que ces prix ne peuvent être modifiés manuellement • Extraire la table SAP des contrats fournisseurs valides au cours de l'année testée • Sélectionner aléatoirement 10 contrats d'achats à partir de la liste des contrats SAP et obtenir du Responsable des Achats des copies des contrats papiers correspondants • Réconcilier les 10 contrats SAP avec les contrats papiers et vérifier que les prix sont bien identiques. Si des écarts sont constatés, obtenir des explications du Responsable des Achats		
A5	Risque	Les commandes d'achats ne sont pas livrées par les fournisseurs dans des délais acceptables		
	Objectif de contrôle	Les commandes d'achats en retard de réception sont revues et investiguées hebdomadairement	Données nécessaires	• Commandes d'achats fournisseurs • Entrées de stocks enregistrées
	Procédures de tests	• Extraire les tables SAP contenant les commandes d'achats fournisseurs et les entrées de stocks enregistrées sur la période testée • Faire une jointure entre les 2 tables précédemment extraites et identifier toutes les commandes sans réception et pour lesquelles la date de réception prévisionnelle est dépassée depuis plus d'une semaine • Sélectionner aléatoirement 10 commandes non réceptionnées en retard depuis plus d'une semaine et obtenir des explications du Responsable des Achats		

Etude de cas : Procédures de tests à préparer

A9	Risque	Les factures fournisseurs sont saisies dans le système en double et payées 2 fois au fournisseur		
	Objectif de contrôle	Les factures saisies avec le même fournisseur, la même date de facture, le même numéro de facture fournisseur et le même montant sont identifiées et revues mensuellement	Données nécessaires	?

	Procédures de tests	?		
A10	Risque	Les factures fournisseurs sont saisies avec des quantités supérieures aux quantités de stock effectivement reçues ou avec des prix différents des mentionnés dans les commandes		
	Objectif de contrôle	• les quantités facturées ne peuvent être différentes de plus de 5% des quantités reçues • les prix ne peuvent différer des prix des commandes (tolérance 0%)	Données nécessaires	?
	Procédures de tests	?		
A11	Risque	Les factures fournisseurs sont payées pour des matières premières jamais envoyées par le fournisseur		
	Objectif de contrôle	Les factures fournisseurs ne faisant pas référence à une commande et à une réception de stock font l'objet d'investigations	Données nécessaires	?
	Procédures de tests	?		

2007-02-22

Formation à l'audit informatique
- Contrôle interne, Exigences réglementaires, Dimension SI

Introduction
Objectifs :
- Rappeler le contexte global de renforcement des exigences réglementaires portant sur le contrôle interne
- Définir la notion de contrôle interne
  - Présenter le référentiel utilisé pour l'évaluer
  - Exposer la démarche globale de mise en œuvre
- Définir la manière dont la dimension «système d'information»doit être prise en compte
- Préciser les attentes dans le cas de processus externalisés

Pourquoi une nouvelle réglementation ?
L'origine : diverses affaires
- Remise en cause de la confiance générale des marchés financiers : risque majeur pour les US !
- Mise en évidence de défaillances concernant :
  - La gouvernance de ces entreprises
  - La fiabilité et la sincérité des informations financières publiées,

- L'indépendance des auditeurs.

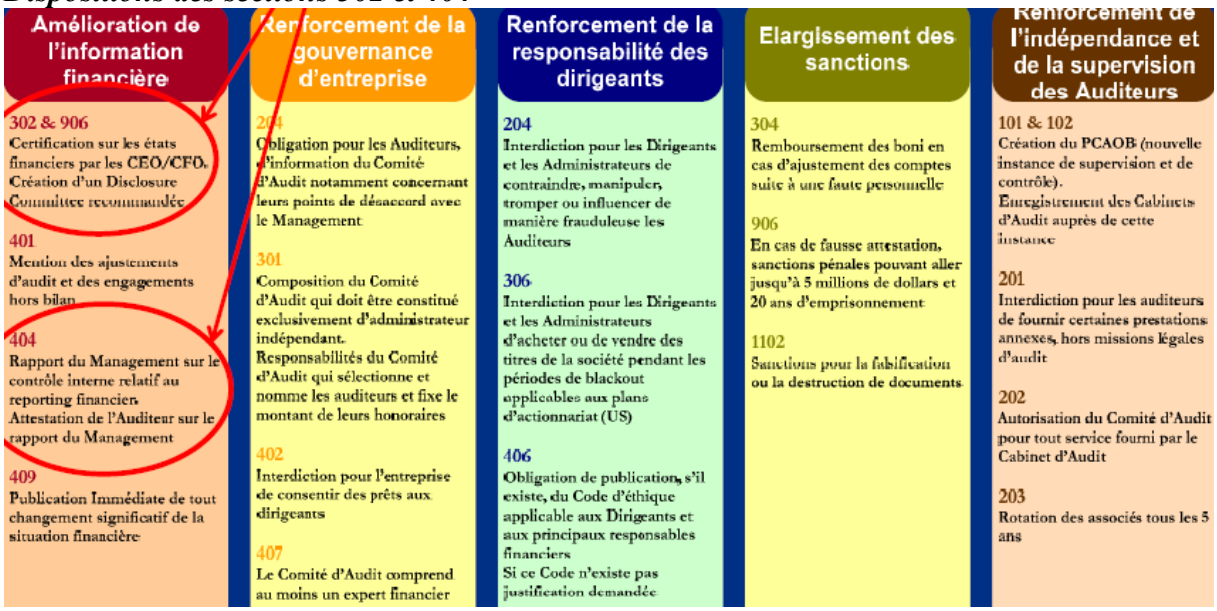
Réponse du législateur US : loi Sarbanes-Oxley (SOX)

- Trois axes d'amélioration
  - Engagement personnel fort des dirigeants
  - Qualité du système de contrôle interne
  - Renforcement de l'indépendance des auditeurs
- Un organisme dédié: PCAOB

Présentation de la loi Sarbanes-Oxley

Les différentes sections de la loi

Dispositions des sections 302 et 404



Section 302

Certification sous la forme d'une attestation des procédures et des contrôles relatifs àla publication de l'information financière (l'ensemble des documents faisant l'objet d'une publication)

Ex : le document de base

Section 404
Rapport de la Direction sur sa propre évaluation de l'efficacité du dispositif de contrôle interne du reporting financier
Rapport des auditeurs externes (CAC) sur :
- L'évaluation faite par la Direction
- Leur propre évaluation de l'efficacité du dispositif
- Leur opinion sur les états financiers

Conséquences de la loi
La loi Sarbanes-Oxley demande plus qu'un "sentiment" sur le contrôle interne

Ce que les sociétés doivent démontrer :
- L'existence de contrôles documentés (décrit, prouvé) pour toutes les activités / entités majeures
- L'existence d'une démarche pour évaluer, la mise en œuvre et l'efficacité des contrôles (conception, fonctionnement)
- L'existence d'un processus pour mettre à jour le dispositif de contrôle et la documentation associée

Audit des états financiers et audit de contrôle interne
Deux natures d'opinions:
- Audit des états financiers = une opinion émise par les CAC sur les comptes
- Audit du contrôle interne = une opinion émise par l'auditeur externe sur:
  - L'efficacité du contrôle interne et du reporting financier
  - L'évaluation réalisée par la Direction

Quelques spécificités de la mission sur le contrôle interne :
- Mission réalisée conjointement avec la mission d'audit des états financiers
- Recours encadré aux travaux réalisés par la société, encouragé par le PCAOB (Public Company Accounting Oversignt Board)

Relations entre les deux opinions
- Les deux conclusions sont liées
  Ex : Un ajustement dans les états financiers post-clôture peut avoir une incidence sur l'opinion des auditeurs externes sur la qualité du processus de clôture.

Comparaison LSF / SOX
Des objectifs communs…

	Loi de Sécurité Financière	Sarbanes-Oxley Act
Réglementation	Française Loi adoptée par l'Assemblée Nationale en juillet 2003	Américaine Loi votée par le Congrès et ratifiée par le Président Bush en juillet 2002
Champ d'application	Les sociétés SA cotées	Les sociétés cotées ou émettant des titres cotés aux Etats-Unis

Pour une approche différente…

	Loi de Sécurité Financière	Sarbanes-Oxley Act
Émetteur du rapport	Président du Conseil d'Administration	DG et DF
Nature du rapport	Descriptif	Descriptif et Evaluatif
Date d'application	Exercices ouverts à compter du1er janvier 2003	Pour les sociétés soumises au reporting accéléré : exercices clos au 15 juin 2004 et après Exercices clos au 15 juillet 2006 et après pour les autres (Foreign Private Issuer)

	Loi de Sécurité Financière	Sarbanes-Oxley Act
Définition et périmètre du contrôle interne	- Non défini implicitement, champ complet du contrôle interne - Champs d'application: S.A.	- Défini et limité au contrôle interne relatif à l'information financière et aux procédures de communication des informations aux marchés. - Champs d'application: Groupe
Référentiel de contrôle interne	Pas d'utilisation obligatoire d'un référentiel mais référentiel de l'AMF recommandé (publication du 31 octobre 2006) (recommandé)	Utilisation obligatoire d'un référentiel reconnu (COSO cité comme exemple par la SEC) (obligation)
Obligation de documentation et de tests des contrôles	Non explicite	Explicite

Le contrôle interne et Sarbanes-Oxley

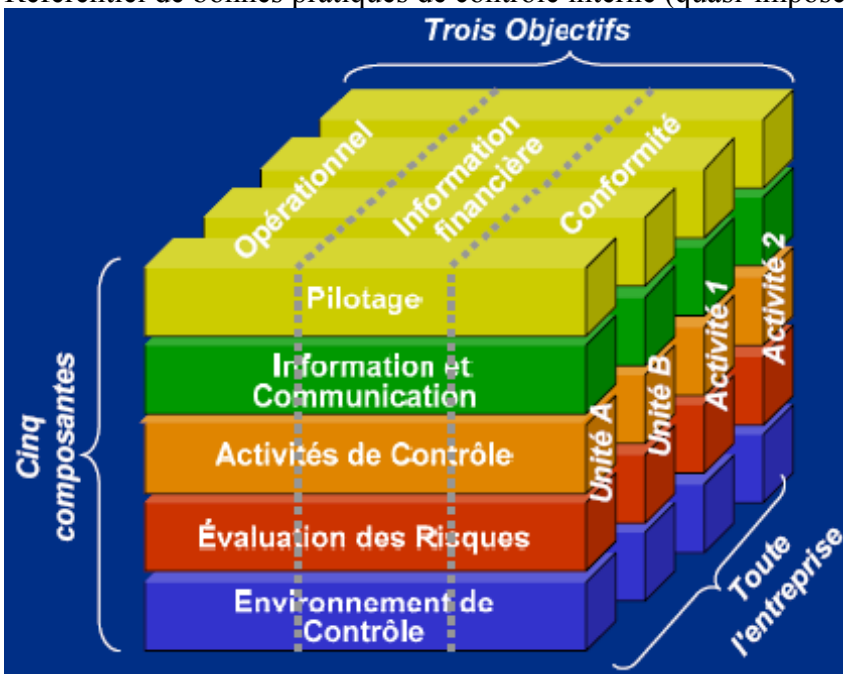
Définition du contrôle interne au sens du COSO

Processus mis en oeuvre par **la Direction Générale, la hiérarchie et le personnel** d'une entreprise, et destiné à fournir une **assurance raisonnable** quant à la **réalisation d'objectifs** entrant dans les catégories suivantes :
- réalisation et optimisation des opérations,
- fiabilité des informations financières,
- conformité aux lois et aux réglementations en vigueur.

- Attention : ne pas avoir une approche limitée de la notion de «contrôle»
- Au sens anglo-saxon, la notion d'«internal control»recouvre aussi bien
  - la notion de contrôle proprement dite, au sens français : vérification, rapprochement, …
  - la notion de «maîtrise»: d'un risque, d'un processus,…
- SOX ne considère que l'objectif «Fiabilité de l'information financière», la LSF française recouvre les trois objectifs

Le référentiel COSO

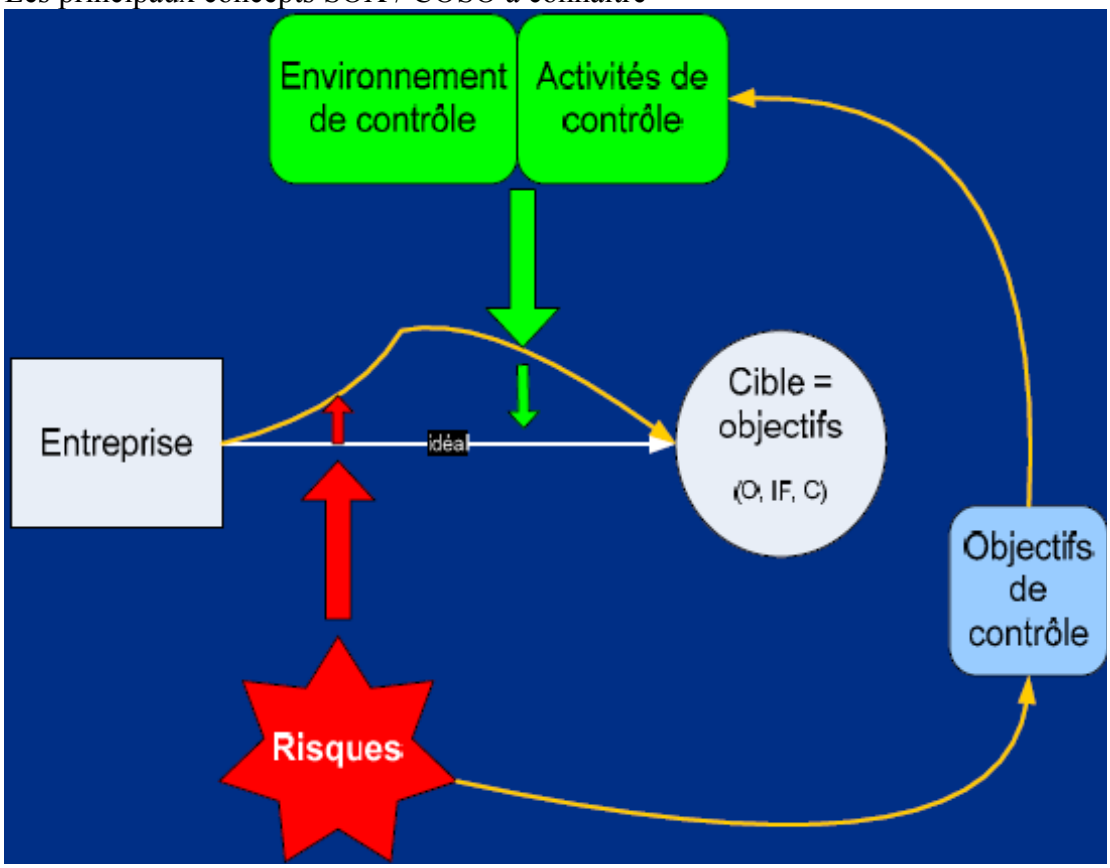
Référentiel de bonnes pratiques de contrôle interne (quasi-imposé par SOX)



- Pilotage : le contrôle interne est correctement le contrôle interne est correctement conçu, appliqué efficacement et adapté efficacement à l'organisation
- Information et communication : identification et communication en temps voulu des informations communication en temps voulu des informations pertinentes

- Activités de contrôle : mise en mise en œuvre des orientations du management ; assurance que les orientations du management ; assurance que les mesures nécessaires sont prises en vue de maîtriser les risques susceptibles d'affecter la réalisation des objectifs
- Évaluation des risques : maîtrise de l'exposition de l'exposition de l'entreprise de l'entreprise à des événements favorables
- Environnement de contrôle : Environnement de contrôle : détermine le niveau de sensibilisation du personnel aux besoins de sensibilisation du personnel aux besoins de contrôle

Les principaux concepts SOX / COSO à connaître



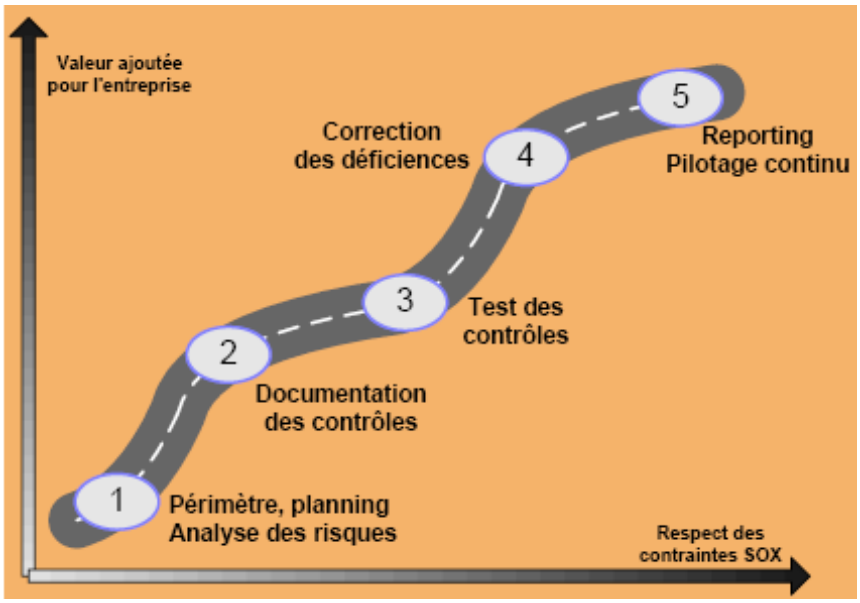
- Risques : ce qui pourrait empêcher ce qui pourrait empêcher l'entreprise d''atteindre ses objectifs
- Objectifs de contrôle : le niveau que l''entreprise se propose d'atteindre concernant la maîtrise de ces risques
- Activités de contrôle : tâche réalisée par l'entreprise, qui permet entreprise d'atteindre l'objectif de contrôle, et objectif de contrôle, et donc concourt à la maîtrise des risques
- Environnement de contrôle : notion plus diffuse, regroupant les politiques/principes qui participe néanmoins à l'atteinte des objectifs de contrôle

La démarche Sarbanes-Oxley

Selon SOX, le management de l'entreprise doit :

- formaliser l'acceptation de son rôle quant à la pertinence et au bon fonctionnement du système de contrôle interne,
- documenter les différents composants de ce système,
- s'interroger sur la bonne conception des contrôles, et tester leur efficacité,

- identifier les déficiences de contrôle, en évaluer l'impact, et y remédier.



Analyse des risques
- Utiliser les référentiels pour balayer les différents types de risque
- Ensuite, les opérationnels sont les mieux placés pour les préciser

Documentation des contrôles : importance de la formalisation
- des procédures de contrôle : « dire ce qu'on fait »
- des preuves de contrôle : prouver que l'« on fait bien ce que l'on dit »
- Seul moyen de démontrer à un tiers que tous les risques sont couverts !

Tests : deux natures complémentaires
- De conception : le contrôle répond-il bien au risque ?
- D'efficacité: le contrôle est-il bien appliqué ?
- Résultat : la « maturité »de chaque activité de contrôle est évaluée

Déficiences et faiblesses
- Il est normal qu'il y en ait lors de la première application : le contraire serait même inquiétant…

Activités de contrôle: documentation
- Lien avec les processus opérationnels et les risques
  - Quels processus / transaction concernés ? Liens amont / aval ?
  - Quels risques couverts ?
- Détail de l'activité de contrôle
  - Description
  - Nature du contrôle : automatique / manuel
    - Si automatique : quelle application (-> voir le PV de recette) ?
  - Détectif ou préventif
  - Action effectuée : rapprochement ligne à ligne, vérification du visa,…
  - Sources d'information utilisées : états papiers, SI,…
  - Fréquence
  - Acteur / Superviseur

- Action menée en cas d'anomalie identifiée
- Preuve du contrôle
- Procédures applicables
- Qualification «COSO»: objectif (IF, O, C) et assertions de contrôle interne

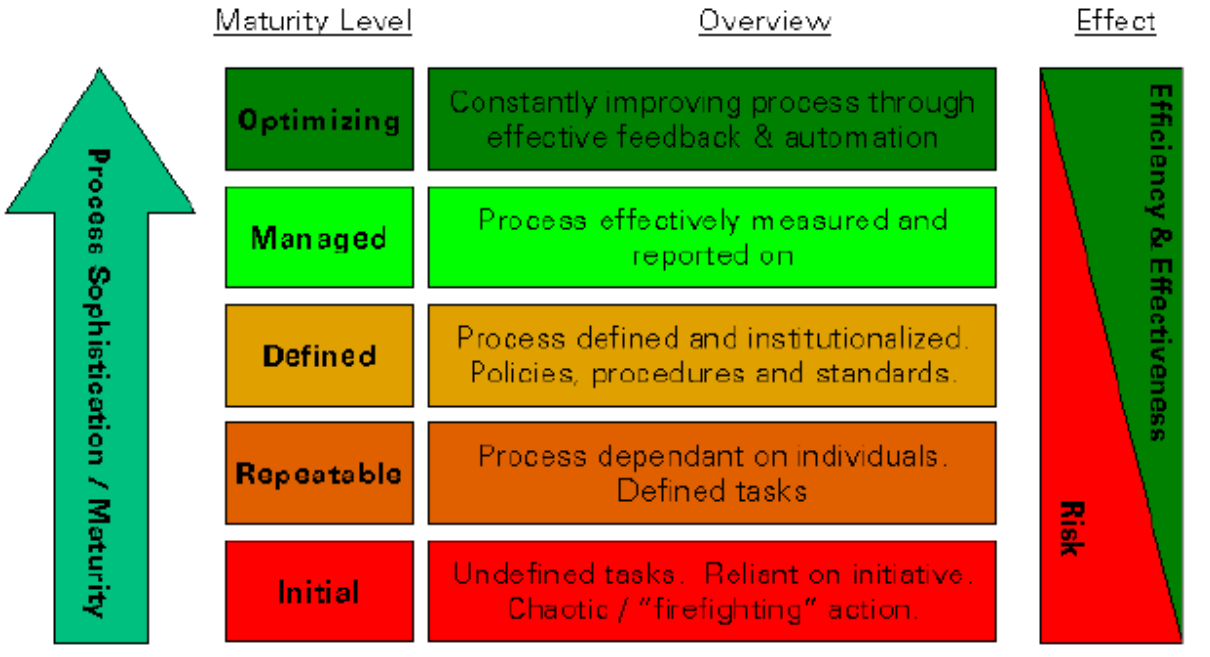
Activités de contrôle: quelques exemples

Exemples issus d'une société d'infogérance :

- Validation par un expert de l'architecture proposée au client par l'avant-vente
- Phase de VABF / VSR (Vérification d'Aptitude au Bon Fonctionnement/ Vérification de Service Régulier)
- Autorisation des mises en production
- Étude d'impact des évolutions de l'infrastructure
- Supervision du niveau de service
- Pilotage des relations avec les prestataires
- Sauvegarde des données
- Suivi des configurations
- Analyse à froid des incidents
- Autorisation client pour les modifications de données
- Maintenance préventive
- Contrôle des opérations d'exploitation

La démarche Sarbanes-Oxley

Evaluation du niveau de maturité



Cible: niveau3 ("defined") pour toutes les activités de contrôle "clés"

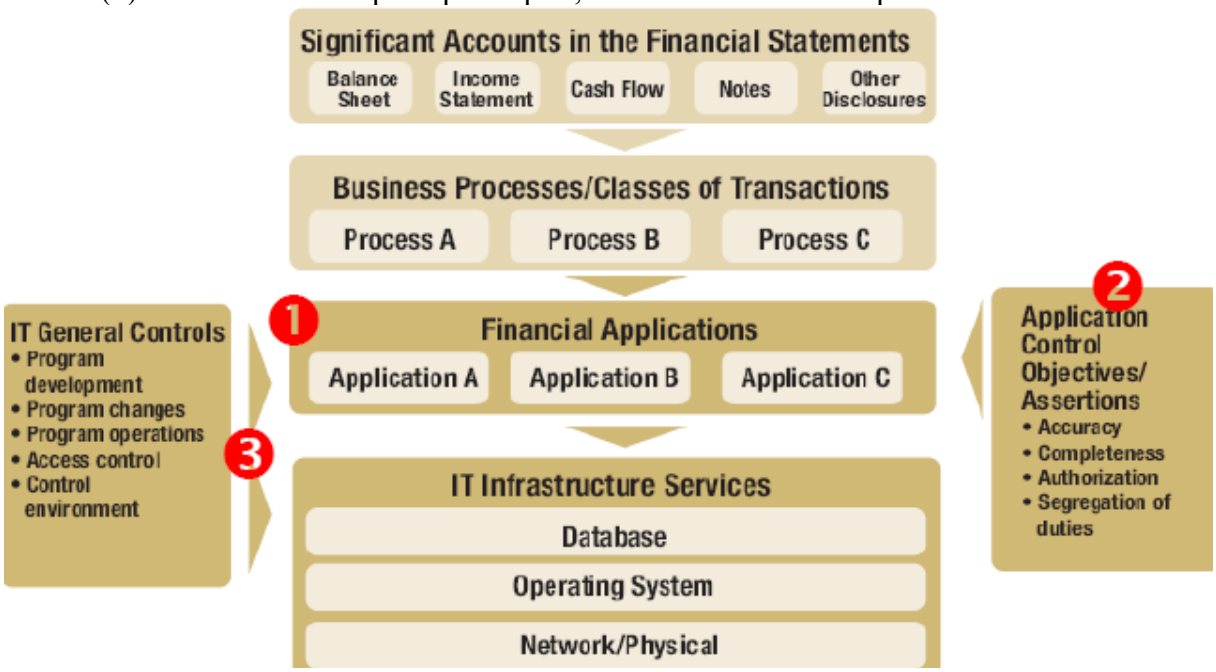
La dimension "système d'information"

Rôle particulier du Système d'Information

(1) Support des processus de l'entreprise (notamment Gestion / Finance)

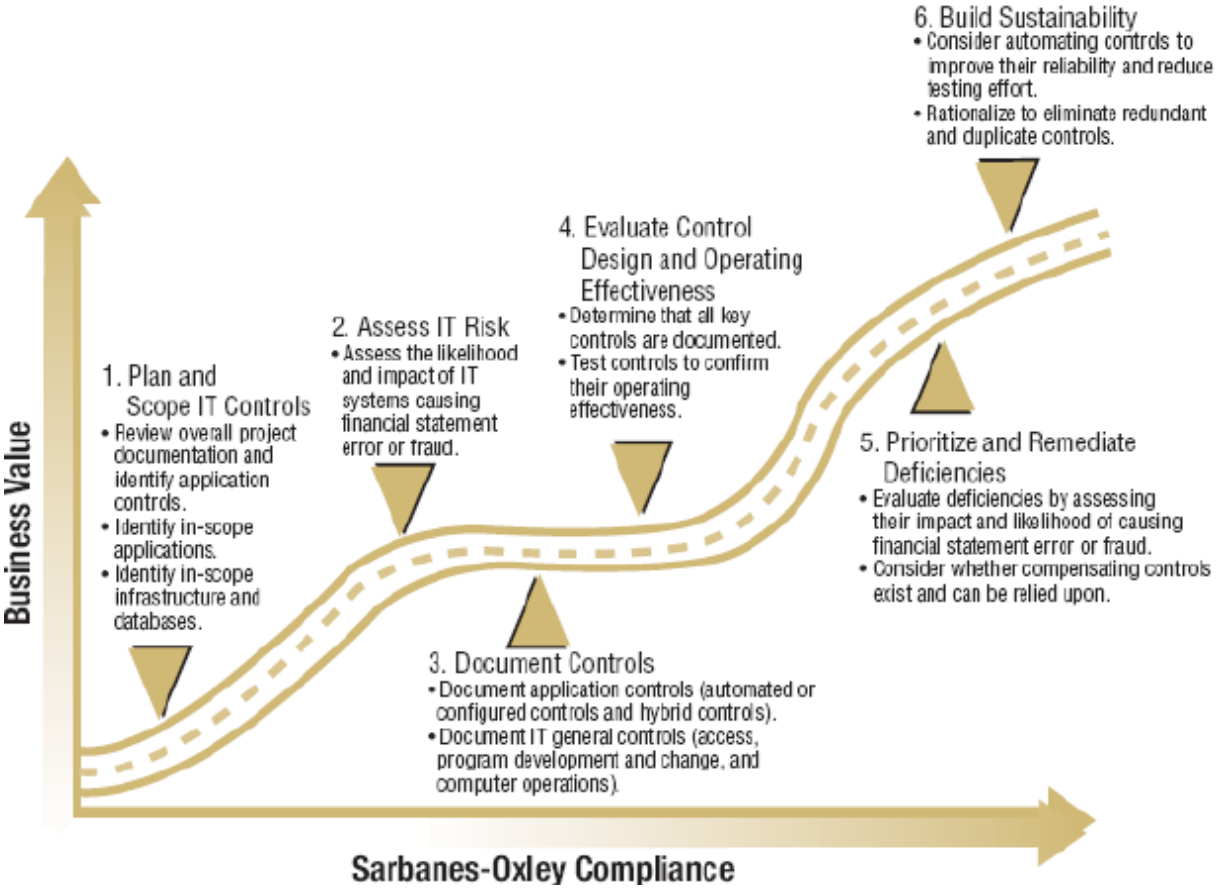
(2) "Acteur" du système de contrôle sur ces processus, via les contrôles automatiques

(3) Source de risques spécifiques, nécessitant la mise en place de contrôles ad hoc



La dimension "système d'information"

La démarche Sarbanes-Oxley appliquée au SI :



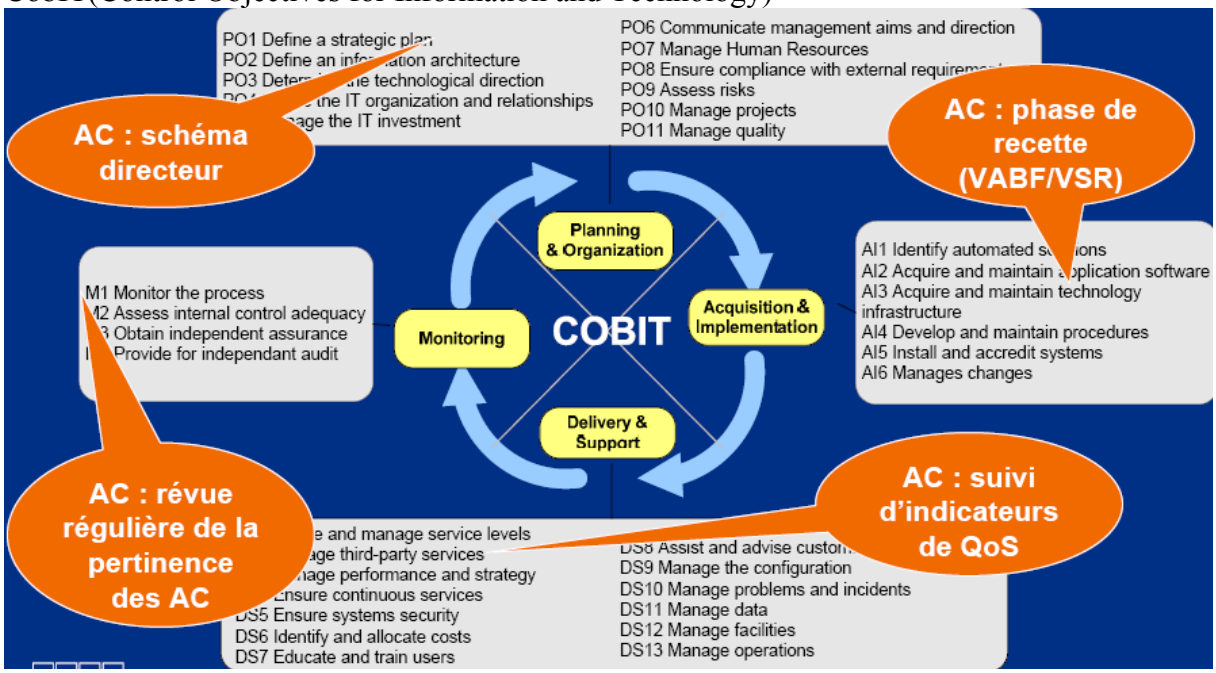
Attentes du PCAOB / IT General Controls

- Gestion de projet/ développement des applications
- Gestion de l'évolution des applications
- Accès aux programmes et aux données
- Exploitation informatique
- Utilisation d'outils bureautiques ("end-user computing")

Problème: ces attentes sont assez peu précises…

- Nécessité d'utiliser un référentiel spécifique, dédié aux activités IT
- Deux principaux référentiels: CobIT et ITIL
- Intérêt:
  - Les référentiels rappellent, en les structurant, les bonnes pratiques IT
  - Leur large diffusion permet de faciliter la communication avec les tiers

CobIT(Control Objectives for Information and Technology)



Liens entre le COSO et le CoBIT

Entity Level	Activity Level	CoaIT IT Processes	COSO Component: Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize (IT Environment)							
●		Define IT strategic planning.		●		●	●
		Define the information architecture.					
		Determine technological direction.					
●		Define the IT processes, organization and relationships.	●			●	●
		Manage the IT investment.					
●		Communicate management aims and direction.	●			●	
●		Manage IT human resources.	●			●	
●		Manage quality.	●		●	●	●
●		Assess and manage IT risks.		●			
		Manage projects.					
Acquire and Implement (Program Development and Program Change)							
		Identify automated solutions.					
	●	Acquire and maintain application software.			●		
	●	Acquire and maintain technology infrastructure.			●		
	●	Enable operation and use.			●	●	
		Procure IT resources.					
	●	Manage changes.		●	●		●
	●	Install and accredit solutions and changes.			●		

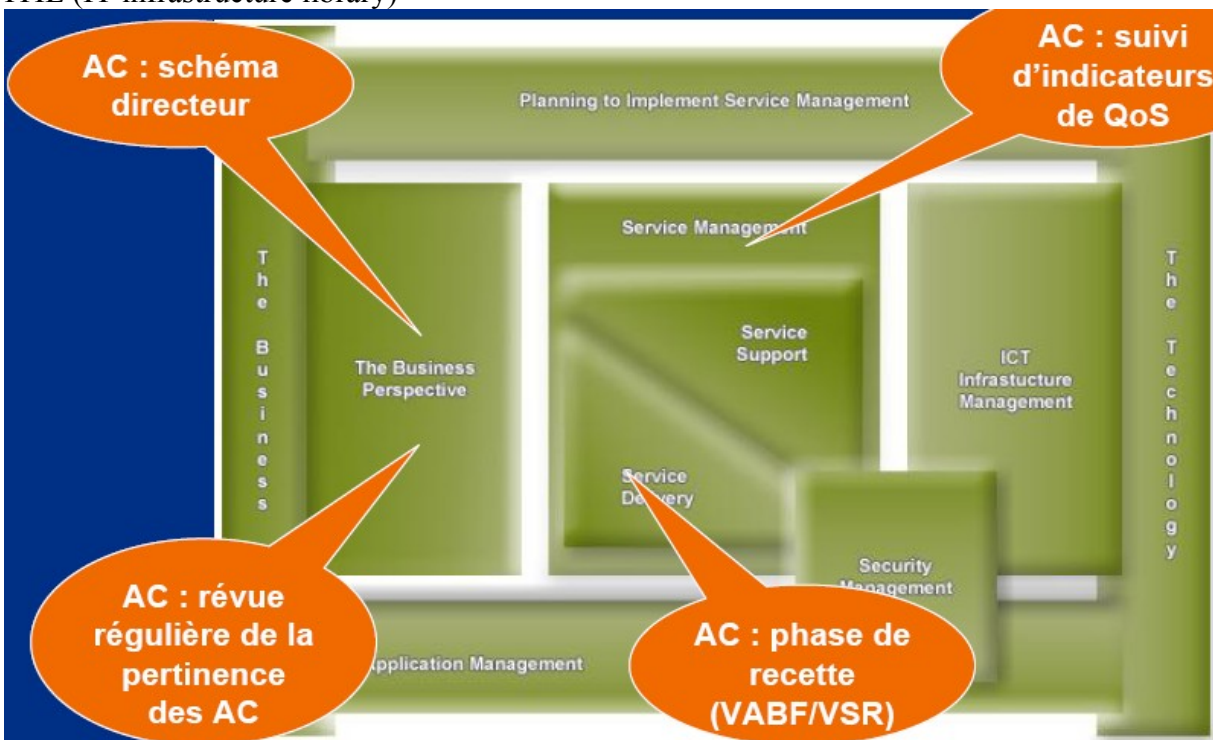
Entity Level	Activity Level	CoaIT IT Processes	COSO Component: Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Deliver and Support (Computer Operations and Access to Programs and Data)							
	●	Define and manage service levels.	●		●	●	●
	●	Manage third-party services.	●	●	●		●
		Manage performance and capacity.					
		Ensure continuous service.					
	●	Ensure systems security.			●	●	●
		Identify and allocate costs.					
●		Educate and train users.	●			●	
	●	Manage service desk and incidents.			●	●	●
	●	Manage the configuration.			●	●	
	●	Manage problems.			●	●	●
	●	Manage data.			●	●	
	●	Manage the physical environment.			●	●	
	●	Manage operations.			●	●	
Monitor and Evaluate (IT Environment)							
●		Monitor and evaluate IT performance.			●	●	●
●		Monitor and evaluate internal control.	●				●
●		Ensure regulatory compliance.			●	●	●
●		Provide IT governance.	●				●

Liens entre les ITGC SOX et le CoBIT

Figure 1—Mapping to PCAOB and CobiT

IT Control Objectives for Sarbanes-Oxley	CobiT	PCAOB IT General Controls			
	Mapping to CobiT 4.0 Processes	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire and maintain application software.	AI2	●	●	●	●
2. Acquire and maintain technology infrastructure.	AI3	●	●	●	
3. Enable operations.	AI4	●	●	●	●
4. Install and accredit solutions and changes.	AI7	●	●	●	●
5. Manage changes.	AI6		●		●
6. Define and manage service levels.	DS1	●	●	●	●
7. Manage third-party services.	DS2	●	●	●	●
8. Ensure systems security.	DS5			●	●
9. Manage the configuration.	DS9			●	●
10. Manage problems and incidents.	DS8, DS10			●	
11. Manage data.	DS11			●	●
12. Manage the physical environment and operations.	DS12, DS13			●	●

ITIL (IT infrastructure library)



Cas des processus externalisés
L'externalisation d'un processus ne modifie pas la responsabilité de l'entreprise en ce qui concerne son contrôle interne

- Lorsque ce processus a un impact sur la fiabilité de son information financière, l'entreprise cliente doit s'engager sur la fiabilité du contrôle interne de son prestataire
- Exemple : externalisation de la paie, des prises de commande, ou de l'hébergement et l'exploitation d'applications

Plusieurs options possibles

- Audit contractuel du prestataire, par le client lui-même ou par un auditeur externe mandaté spécifiquement
  - Problème : risque de multiplication des audits sur un même sujet pour le prestataire…
- Élaboration d'un document engageant le prestataire et un auditeur tiers, certifiant de la qualité du contrôle interne
  - Permet de répondre à toutes les demandes en un seul audit
  - Rapport SAS70 (norme développée par les comptables US)

Contenu type d'un rapport SAS70

- Rapport de l'auditeur (standard)
- Activité du prestataire
- Environnement de contrôle du prestataire
- Objectifs de contrôle et activités de contrôle associées
- Tests réalisés par l'auditeur et résultats (type II seulement)
- «User considerations»
  - Permet au prestataire de préciser ce que son client devrait mettre en œuvre comme activité de contrôle pour assurer que leurs interactions sont bien «sous contrôle»
- Deux types de rapport sont définis
  - Le type II est requis par SOX : incluant une phase de test, il permet de se prononcer sur l'efficacité des contrôles mis en œuvre

Et les évolutions attendues
Internal control embedded in the System Development life cycle : rôle of CIO

Automated and preventive

- Real time IT application including on-line control ???
- ???

Et Demain?
Des outils pour répondre à l'intégration du contrôle interne dans les processus

Pilotage du contrôle interne	Suivi des anomalies	Gestion des tests (formalisation, récurrence, reporting)	Description des activiés de contrôle	?	?

- Moins d'évaluation directe de l'efficacité du contrôle interne et plus de « reassurance » de la confiance dans le système de pilotage du contrôle interne ?
- Un « focus » amplifié sur les « entity level controls » et l'optimisation triangulaire?

- Un sujet nouveau de dialogue avec les acteurs de la gouvernance : le pilotage optimisé du contrôle interne?

En résumé

Quels impacts sur l'identification des risques et des contrôles

- Focus sur l'identification des risques financiers liés à l'information financière
- Renforcement des liens entre les processus et les activités de contrôle
- Affirmation de la criticité des contrôles automatisés au sein des processus et des exigences qui en découlent

Comment évaluer le dispositif de contrôle interne

- Une modélisation du dispositif de contrôle interne via le COSO et plus généralement des référentiels Cobit, ITIL…
- Une maturité relative des offres de logiciel sur les interactions entre les processus et le pilotage des contrôles

Les apports sur l'efficacité du contrôle interne

- Vers un renforcement des contrôles permanents et des évolutions prévisibles sur le contenu ???

Quelques liens pour aller plus loin

Le document de référence IT & SOX

- «IT control objectives for Sarbanes-Oxley v2»/ www.itgi.org
- Sur le même site : introduction au COBIT

Le COSO : www.coso.org

Les références officielles pour SOX

- Le site du PCAOB, avec les standards applicables www.pcaobus.org

Réponses aux principales questions concernant SAS70 www.sas70.com