Deloitte.

Les fondamentaux du contrôle interne

Université d'été
Paris, le 11 septembre 2008

Module: prendre connaissance de l'environnement du contrôle interne

Objectifs

- **Maîtriser les principes et les finalités du contrôle interne**
- **Acquérir la méthode, les outils et les techniques pour optimiser le contrôle interne**

Durée : 1 jour

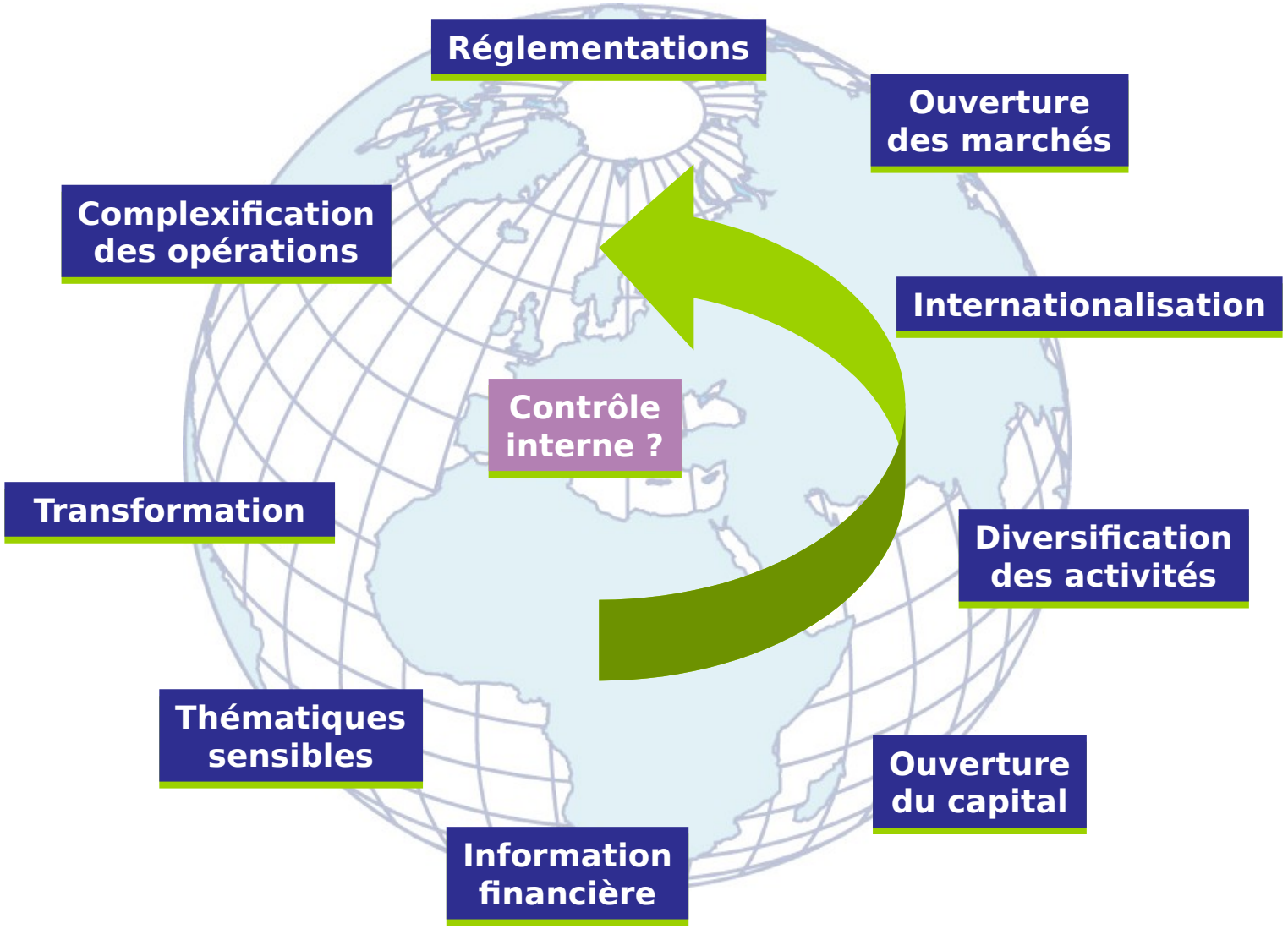
Programme

- **Introduction**
- **Les Risques: définition, la notion de risque, l'évaluation des risques**
- **Le Contrôle Interne: définition, objectifs, maturation**
- **Le Contrôle Interne, une notion en pleine évolution**
- **Le Référentiel du COSO: présentation, référentiels COSO 1 et COSO 2**
- **Les exigences légales en terme de Contrôle Interne**

- **Les outils du Contrôle Interne**
  - **Questionnaire de Contrôle Interne**
  - **Auto-évaluation de Contrôle Interne**
- **Les outils de description**
  - **Diagramme de flux de circulation**
  - **Test de cheminement**
  - **Grille de séparation de fonction et des tâches**
  - **Matrice de contrôle**
- **Les outils techniques / informatiques**

Introduction

Le contrôle interne et les risques sont au centre des enjeux de l'entreprise



Nouveau contexte et nouveaux besoins

Un contexte changeant

- Un environnement en mutation et des enjeux nouveaux:
  - Un cadre réglementaire strict (LSF, Sarbanes Oxley) qui oblige les entreprises à se prononcer formellement sur le degré de fiabilité de leur Contrôle Interne
  - Un business de plus en plus complexe et global
    - Nouveaux schémas organisationnels d'entreprise
    - Risques industriels et environnementaux
    - Ingénierie contractuelle
  - Une pression croissante des marchés financiers en matière d'information financière
    - Raccourcissement des délais de clôture
    - Importance de la publication des résultats
    - Notion de corporate governance
    - Éthique d'entreprise
  - Une évolution rapide des structures et la naissance de nouveaux risques
    - Fusions et acquisitions
    - Valorisation d'entreprises
    - Mise en place de synergies
  - Une responsabilité accrue des dirigeants
    - Pression des actionnaires
    - Risques pénaux

Nouveau contexte et nouveaux besoins

De nouvelles attentes

- Ce nouveau contexte crée de nouvelles attentes:
  - **Direction générale**
    - Degré suffisant de confiance dans la maîtrise du business
    - Mise en perspective des risques en relation avec les objectifs stratégiques
    - Correcte application des instructions
    - Respect des exigences réglementaires et éthiques
    - Missions spéciales d'acquisition
  - **Actionnaires**
    - Identification des risques financiers
    - Pertinence et transparence de l'information financière
  - **Opérationnels**
    - Optimisation des process pour une meilleure maîtrise des risques
    - Mise en place de plans d'actions et de best practices

Un besoin de contrôle et de conseil , d'aide à la décision.

Nouveau contexte et nouveaux besoins

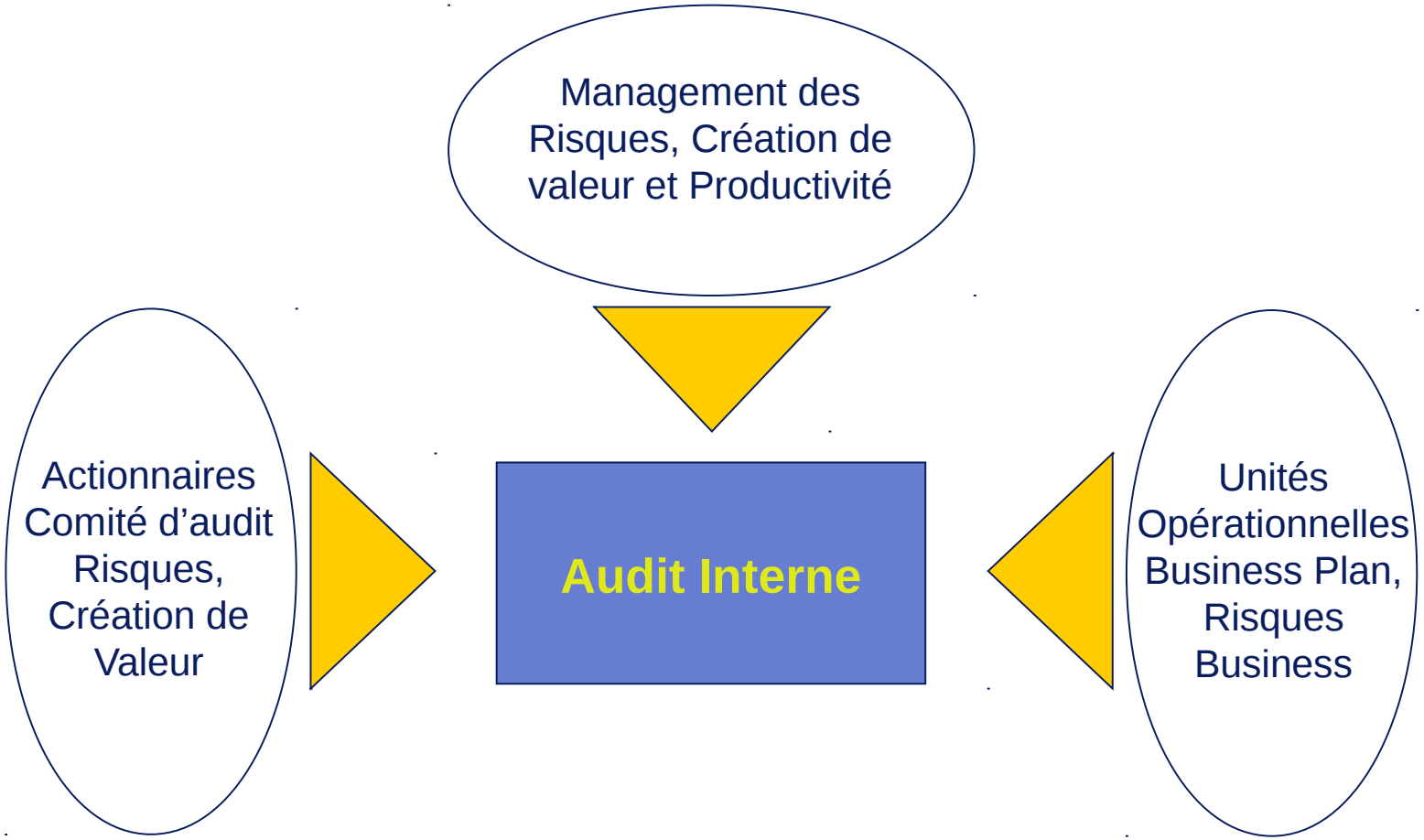
Une double réponse

- Création de services spécifiques: Risk Management
- Prise en charge de ces nouvelles missions par les services d'audit interne:
  - Capitaliser sur ses qualités traditionnelles: méthode, indépendance, flexibilité…
  - Pour assurer de nouvelles missions:

	Approche traditionnelle	**Approche par les risques**
Analyse des risques	Risques comptables	Risques business
Procédure	Transactions routinières et non routinières	Business process
Rapport	Observations et recommandations	Analyse du business et recommandations d'actions
Revue analytique	Ratios financiers	Indicateurs de performance
Observations	Tests de détail	Évaluation

Nouveau contexte et nouveaux besoins

L'audit interne au cœur de l'organisation



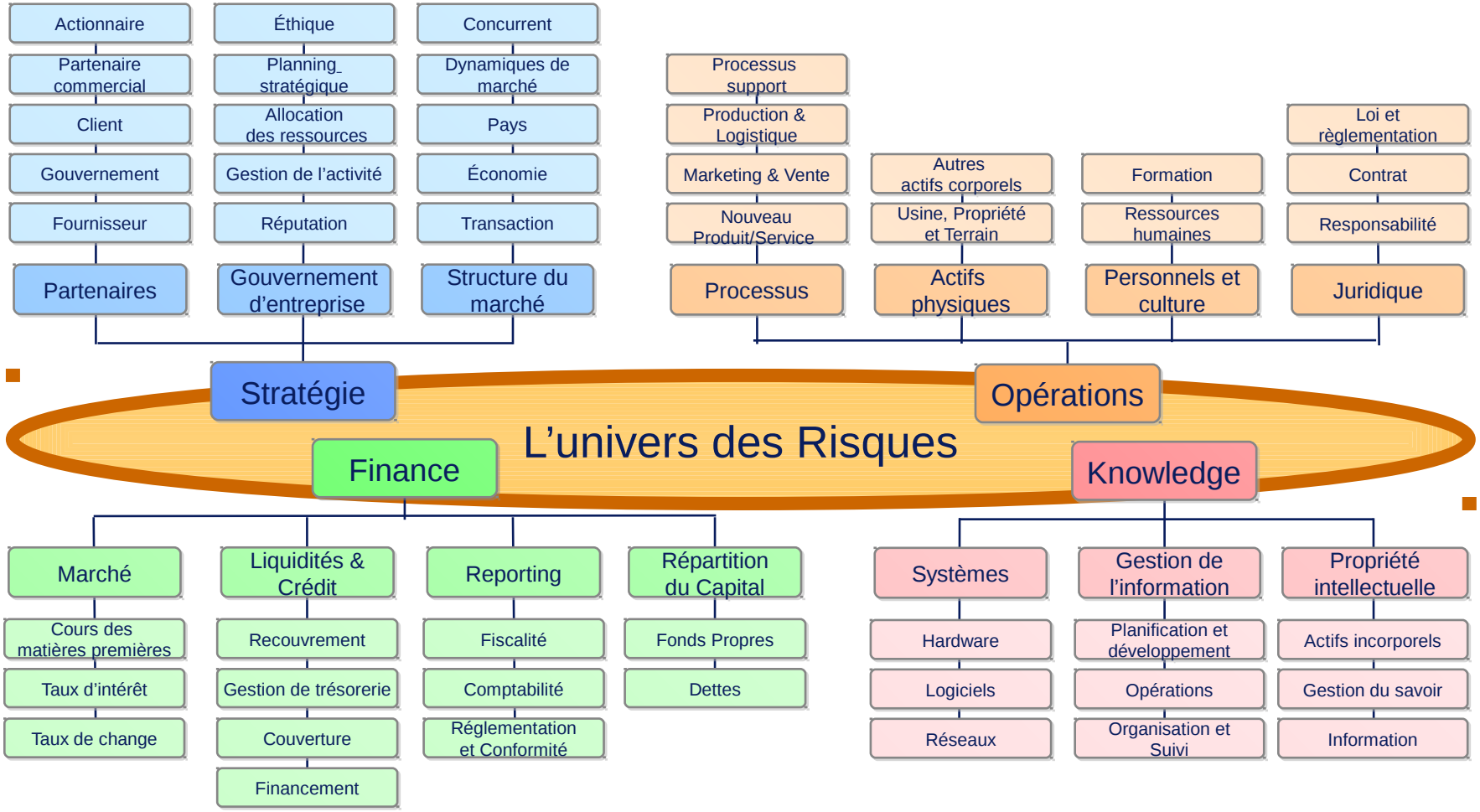
Les Risques

Notion de risque : définition

- Définition généralement admise :
  - «Un risque se définit comme tout événement, action ou inaction de nature :
    - à empêcher une organisation d'atteindre ses objectifs (de façon implicite ou explicite) ou
    - à altérer sa performance» ou
    - Une perte d'opportunités
- Toutefois, chaque organisation accepte une niveau de risque défini en fonction de son activité, de sa sensibilité aux risques, de sa culture mais aussi de ce que peuvent supporter les actionnaires et autres parties prenantes: c'est la notion de risk appetite; dont la responsabilité exclusive incombe au Management.
- Tout système de maîtrise des risques s'inscrit dans le cadre du niveau de risque acceptable.

Notion de risque : définition

Un univers complexe



La notion de risque

- Les facteurs d'un risque

  - Probabilité de se réaliser, de se manifester.
  - Type de menace.
  - Nature de l'impact engendré (financier, réputation, etc., immédiat ou différé).
  - Durée de l'impact.
  - Absence ou non de contrôle pour l'identifier.

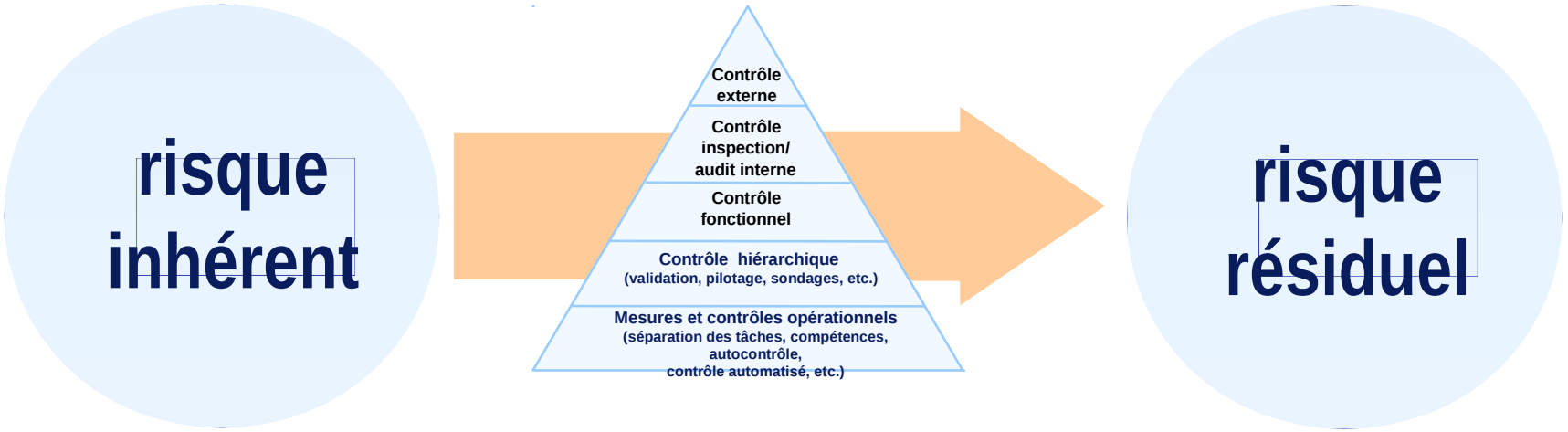
La notion de risque

- Les différentes facettes d'un risque :
  - Le risque est inhérent à l'activité de l'entreprise
  - Il peut être :
    - commun à toutes les fonctions.
    - Spécifique à une fonction déterminée.
  - Le risque est lié au niveau de contrôle interne de l'entreprise.
  - Le risque est lié à la capacité de l'entreprise à l'identifier (risque d'audit/audit risk).

L’évaluation des risques

- Le poids d’un risque peut être corrigé par un dispositif de maîtrise (contrôle interne ou assurances) il convient alors d’évaluer le risque résiduel supporté par l’entreprise.
- Le but est de dresser une cartographie des risques de toutes natures auxquels l’entreprise est confrontée
- La méthodologie qui gouverne l’élaboration d’une cartographie des risques repose sur les étapes clés suivantes:
  - Brainstorming de tous les risques pouvant affecter les différentes fonctions/activités/métiers de l’entreprise
  - Hiérarchisation des risques vis-à-vis de l’atteinte des objectifs lors d’atelier débouchant sur un vote
  - Priorisation des risques majeurs et élaboration de la cartographie de ces risques
  - Traitement des risques via des plans d’actions appropriés
- Il s’agit d’un processus itératif dans la mesure où les risques vivent et évoluent en permanence: la cartographie des risques ne saurait donc être un document figé dans le temps; elle doit être mise à jour régulièrement

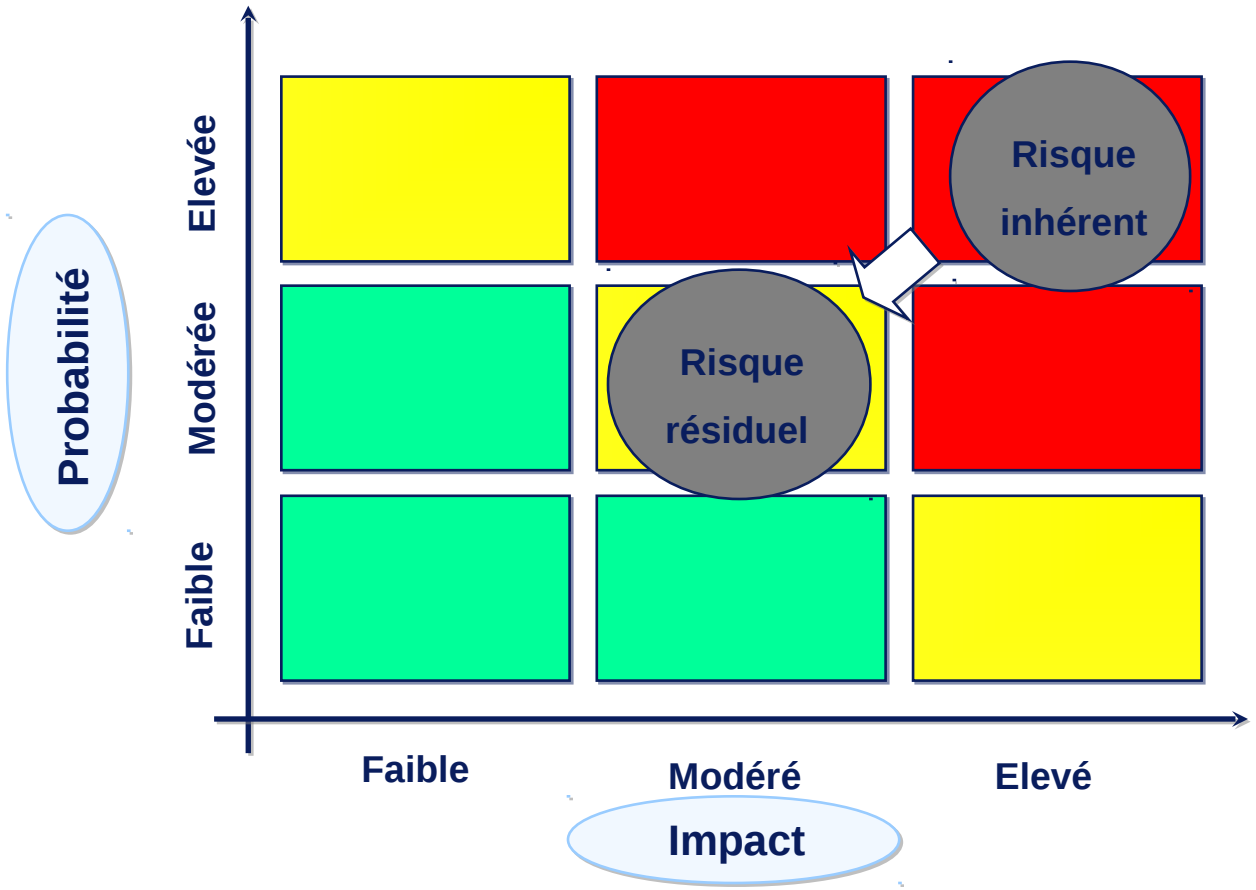
L’évaluation des risques



Prise en compte
du dispositif de maîtrise interne existant

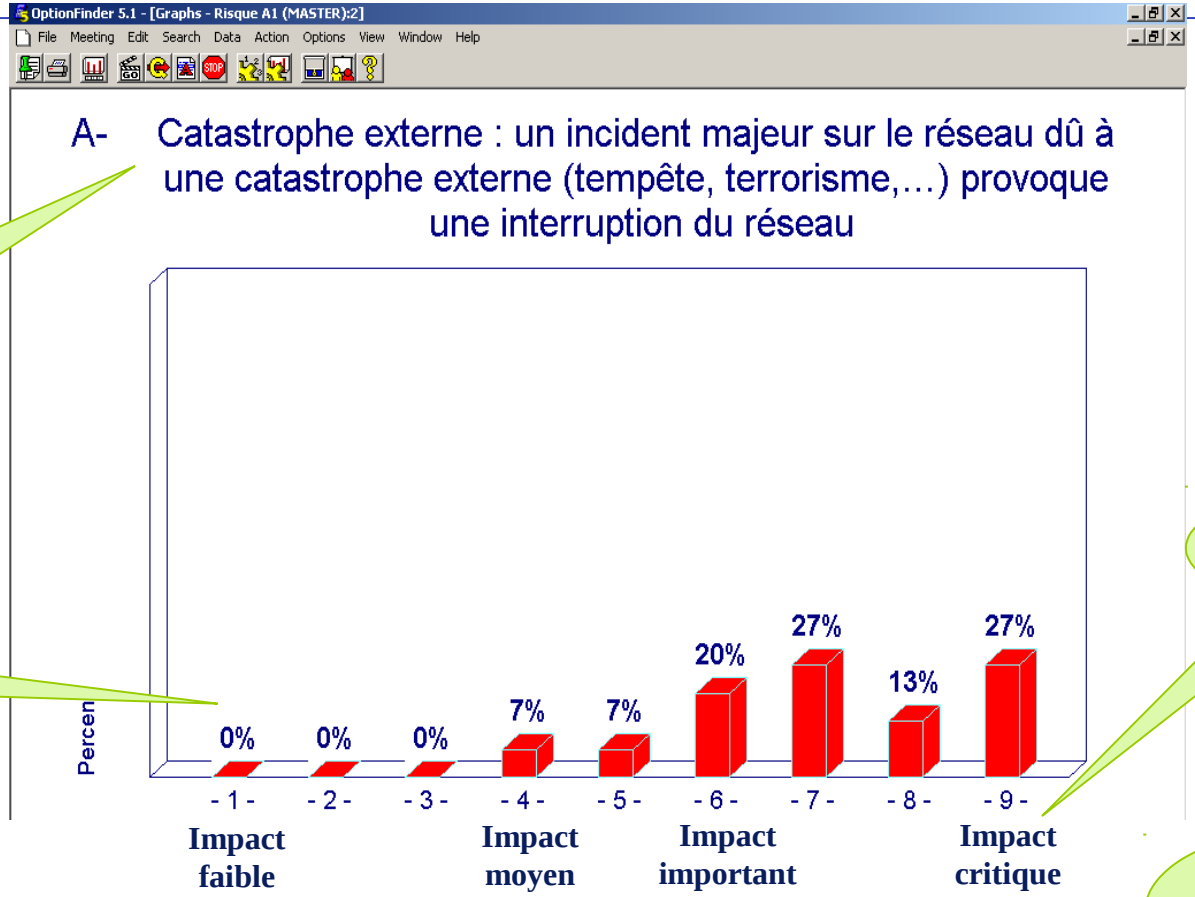
L’évaluation des risques: cartographie des risques

Évaluation du dispositif de contrôle interne



L'évaluation des risques: cartographie des risques;

Votes lors de l'atelier: « Voter est intéressant, Discuter est essentiel »



Risque et définition concernés par le vote

Nombre de votants sur chaque note

Echelle de vote

Critère de vote

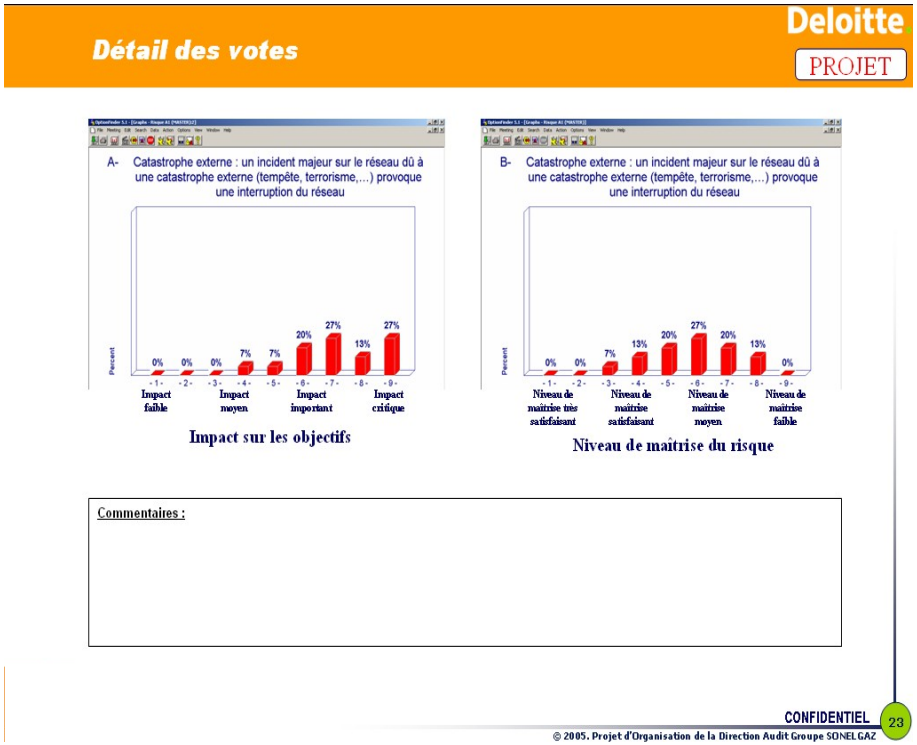
Commentaires :

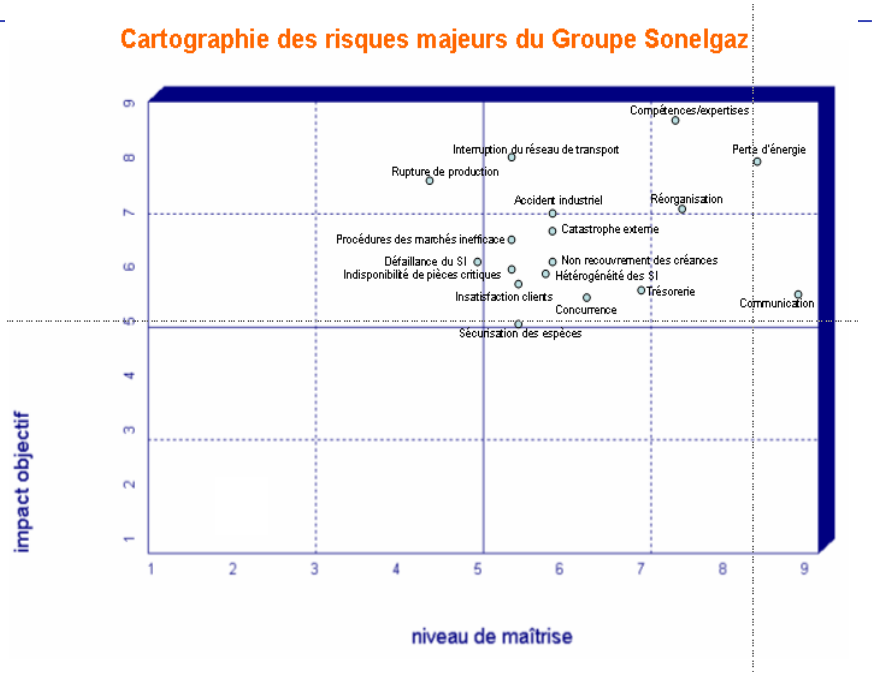
Commentaires et informations collectés au cours de l 'atelier

L'évaluation des risques: cartographie des risques;
Atelier: matrice des risques et synthèse

Exemple dans le secteur de l'énergie

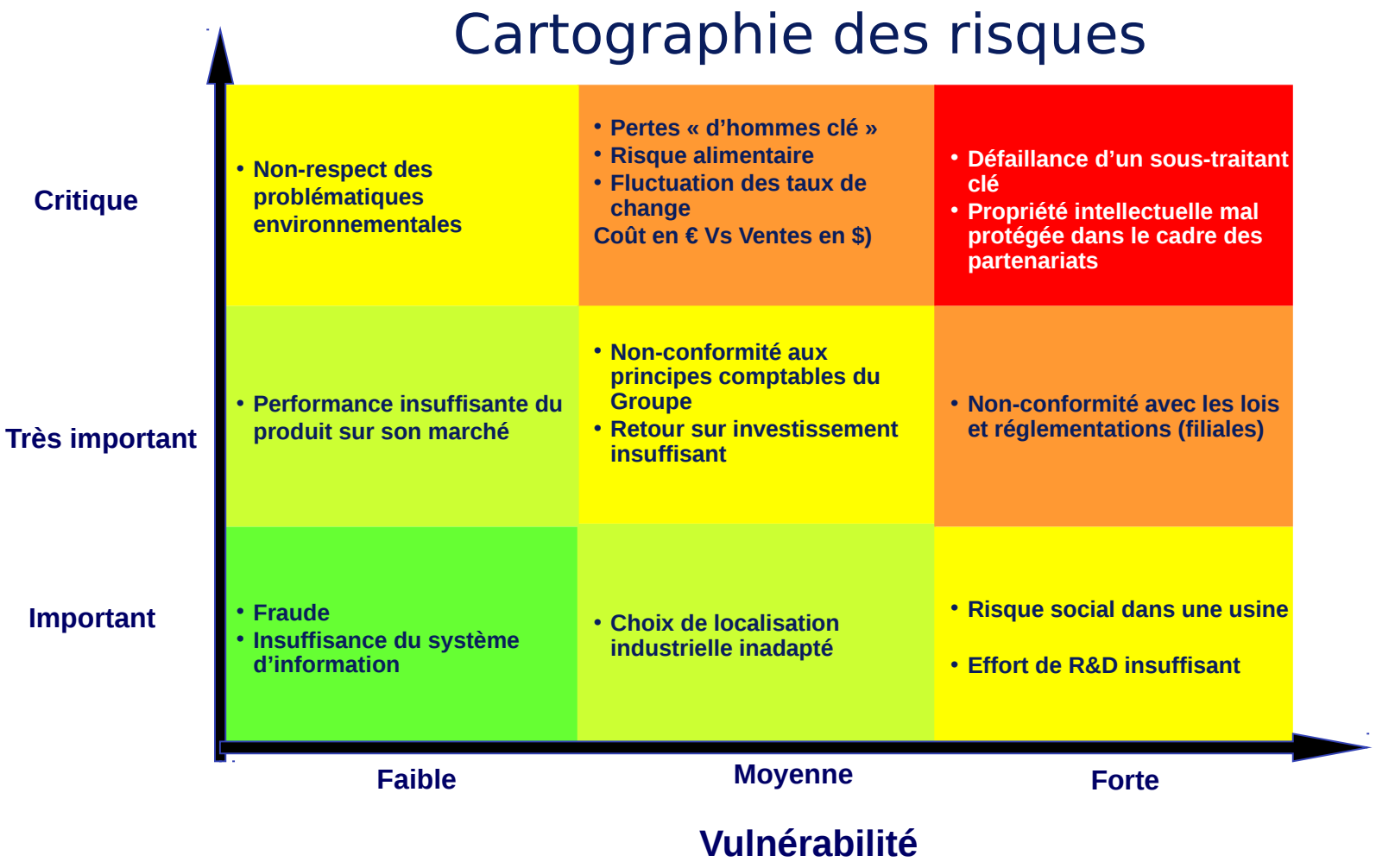
- Cartographie unique, construite et validée par les participants





- Compte rendu détaillé des votes et des commentaires

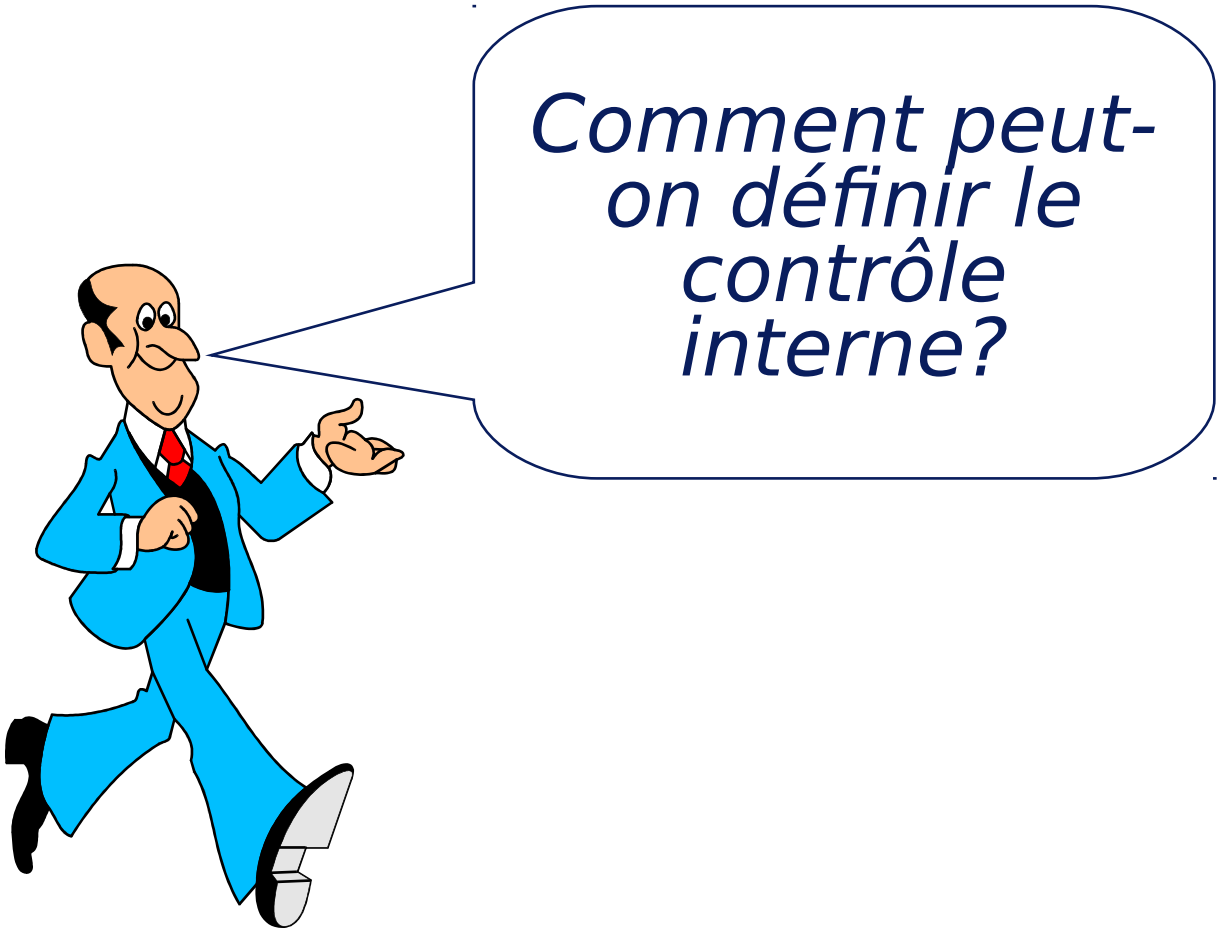
L’évaluation des risques: cartographie des risques;
Exemple: groupe industriel agroalimentaire international



Le traitement des risques

- Après avoir évalué les risques, l'entreprise doit mettre en œuvre les mesures et/ou stratégies qui permettent de les traiter
- Il existe quatre mesures fondamentales de traitement des risques:
  - Accepter le risque (ex: la possibilité qu'un avion s'écrase sur une usine)
  - Réduire le risque (ex: entrepôts sous sprinkler)
  - Transférer le risque (ex: dans le cadre d'un contrat de sous-traitance)
  - Stopper le risque (ex: arrêt d'une gamme de produits)
- Les mesures de traitement sont proportionnées, notamment, à la probabilité que le risque se réalise et à l'impact qu'il engendre. Ainsi, le risque qu'un avion s'écrase sur une usine est généralement accepté sans aucune forme de traitement dans la mesure où bien que l'impact soit extrêmement important (arrêt des activités) sa probabilité de réalisation est extrêmement faible

Le Contrôle Interne



Définition du contrôle interne

- Définition du contrôle interne

  - Le contrôle interne d’une activité est le dispositif de protection contre les risques de toute nature qui pèsent sur une activité
    - Mauvaise ou sous exploitation de ressources
    - Investissements injustifiés
    - Pertes d’opportunités
    - Risques inacceptables
    - …

  - Le contrôle interne est un ensemble de dispositifs mis en œuvre par l'ensemble des personnels de tous niveaux pour maîtriser le fonctionnement de leurs activités

Définition du contrôle interne

Le contrôle interne est un **processus** mis en œuvre par le personnel de tout niveau destiné à fournir une **assurance raisonnable** quant à **la réalisation des objectifs**:

- optimisation des opérations,
- fiabilité des informations financières,
- conformité aux lois et aux réglementations en vigueur

Objectifs du contrôle interne

- Les objectifs du dispositif de contrôle interne d'une entreprise

Opérations	– Assurer l'amélioration des résultats
	  – Optimiser les procédures
	  – Développer l'efficacité économique
	– Promouvoir l'efficacité du fonctionnement de l'entreprise
	  – maximiser l'efficience (rapport qualité/coût)
	  – limiter les coûts et le délai de réponse aux changements de situation

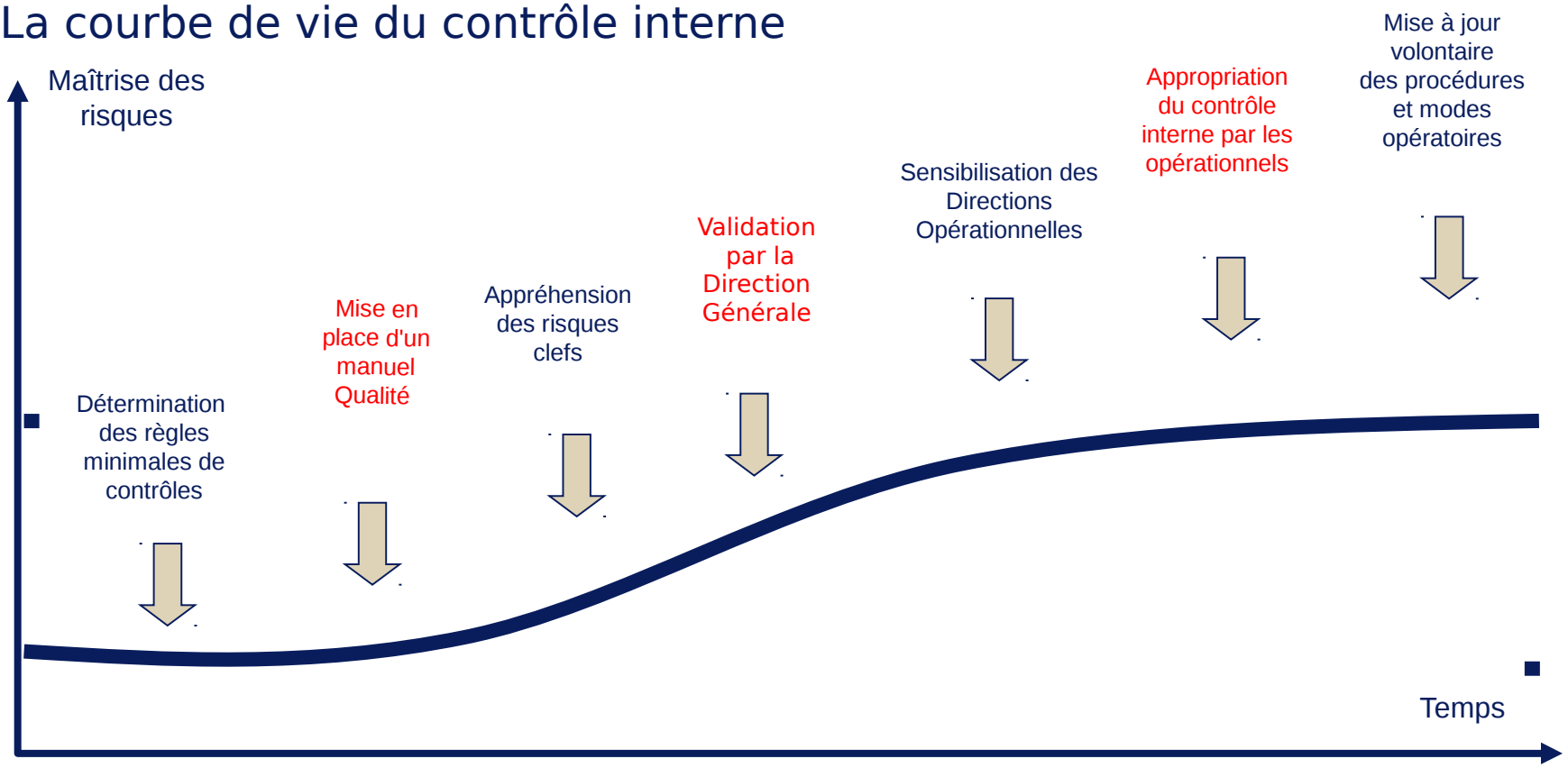
Information financière	– Assurer la protection du patrimoine
	  – éviter la perte des ressources
	  – éviter les catastrophes (incendie, explosion, …)
	– Assurer la qualité et la fiabilité de l'information financière
	  – en interne (performance, budget)
	  – en externe (AMF, analystes, actionnaires, tiers…)

Conformité	– Respecter la réglementation et les politiques du groupe
	  – lois et règlements : LSF, NRE, Sarbanes Oxley, protection de l'environnement…
	  – politique groupe : investissements, maîtrise des frais impayés, qualité, éthique…

Maturation du contrôle interne

- Le contrôle interne est un processus évolutif : Il doit être remis en cause en permanence pour s'adapter à la vie de l'entreprise

- La courbe de vie du contrôle interne



Le Référentiel du COSO

Présentation du COSO

- Historique
  - En 1985, création autour du Sénateur Treadway (USA) d'une commission réunissant les compétences de professionnels représentant l'IIA, l'AAA, la FEI, l'IMA, l'AICPA, le NYSE, des cabinets d'audit externe et de grandes entreprises américaines. Cette commission est connue sous la dénomination COSO (**Committee of Sponsoring Organizations of the Treadway Commission).**
  - **Vocation** :contribuer aux travaux de la « National Commission on Fraudulent Financial Reporting-Treadway Commission » créée en 1985, une commission qui étudie les facteurs qui pourraient conduire à des états financiers frauduleux, et qui développe des recommandations pour les sociétés anonymes,les auditeurs externes,la SEC et autres régulateurs.

Présentation du COSO

- Site internet

  http://www.coso.org

- Publications
  - Edition en 1992 de l'ensemble des travaux sur le contrôle interne dans un ouvrage : « Internal Control – integrated Framework » traduit en 2000 sous le titre « la nouvelle pratique du contrôle interne »

  - Puis en septembre 2004, édition de l'ouvrage : « Enterprise Risk Management – Integrated Framework » (COSO 2).

Le référentiel COSO 1

- Notions clés

  Le référentiel COSO1 “internal audit-integrated framework” comprend:

  - Une définition du contrôle interne
    - Processus
    - Effectué par des personnes (conseil d’administration, direction, salariés)
    - Apportant une assurance raisonnable
    - Quant à la réalisation des objectifs suivants

      - Efficience et efficacité des opérations
      - Fiabilité des états financiers
      - Respect des lois et des réglementations en vigueur

  - Un référentiel pour évaluer l’efficacité du processus de contrôle interne d’une entreprise:
    - **5 composantes** étroitement liées qui découlent de la manière dont l’activité est gérée

Le référentiel COSO 1

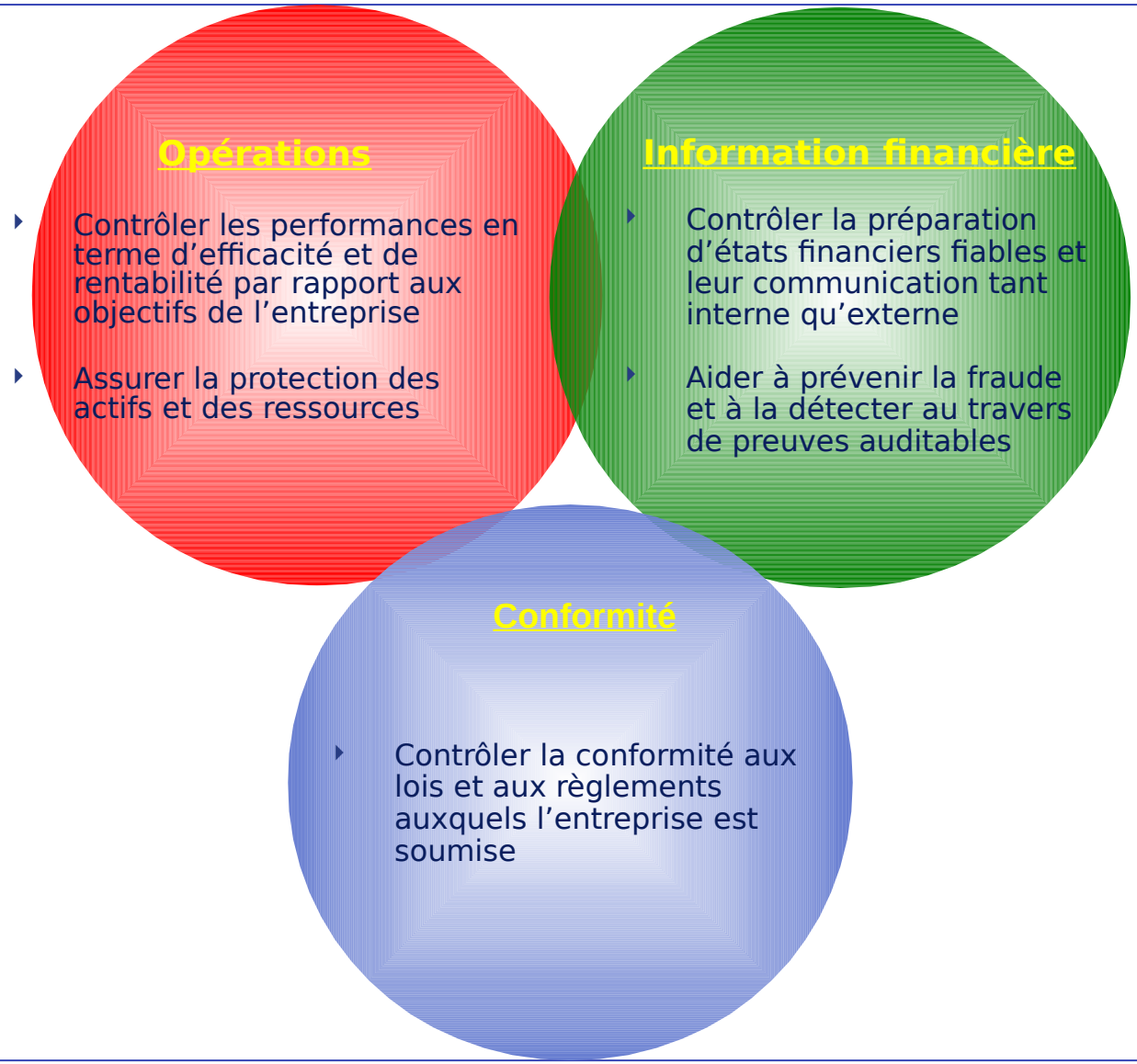
- Notions clés

  - Le contrôle interne fait partie des processus de Direction

  - Le contrôle interne peut aider une entreprise à réaliser ses objectifs en matière de performance et de rentabilité, tout en prévenant la perte des ressources.

  - Toutes les activités de la Direction ne sont pas liées au contrôle interne comme par exemple :
    - Etablir les objectifs de l'entreprise
    - Valider les hypothèses et choix stratégiques
    - Gérer les risques

Le référentiel COSO 1 : 3 Objectifs



Les 5 composantes du COSO 1

- Le COSO1 présente un référentiel intégré qui définit le contrôle interne au travers de 5 composantes liées entre elles :

  - **Environnement de contrôle**
  - **Évaluation du risque**
  - **Activités de contrôles**
  - **Information & Communication**
  - **Pilotage**

Les composantes du COSO 1 (suite)

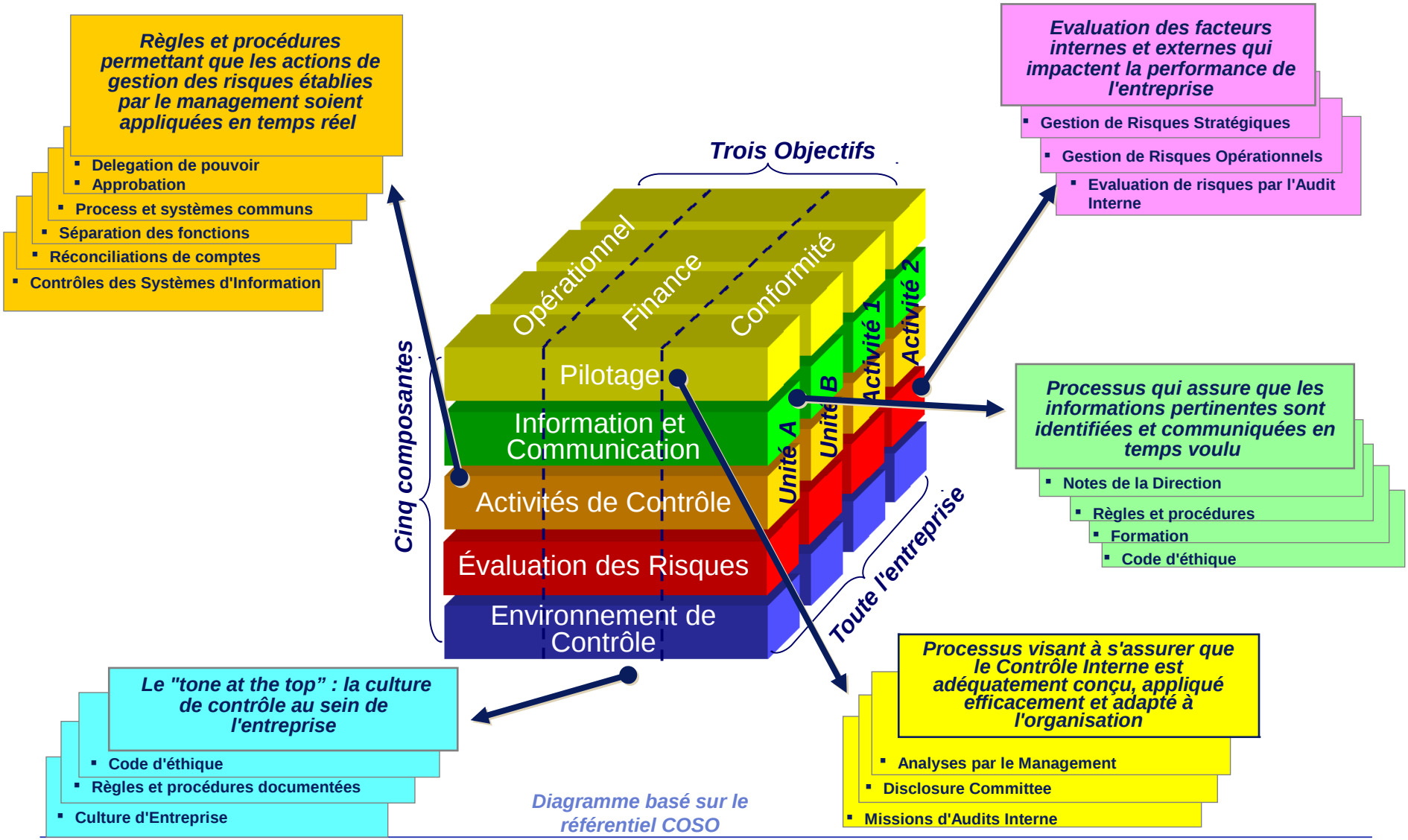


Diagramme basé sur le référentiel COSO

Le référentiel COSO 1: ENTITE versus PROCESSUS

Au niveau de l'entité

Chaque "Entité"

- Environnement de contrôle
- Évaluation des risques
- Activités de contrôle
- Information et Communication
- Contrôle, suivi

Haut en Bas
Bas en Haut

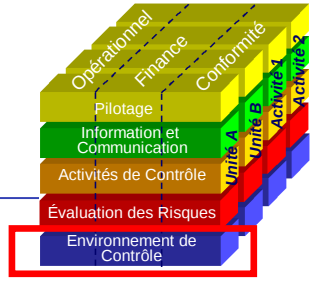
Au niveau des processus

Chaque processus "Significatif", Compte, Transaction ou Communication

- Environnement de contrôle
- Évaluation des risques
- Activités de contrôle
- Information et Communication
- Contrôle, suivi

Le référentiel COSO 1: Environnement de contrôle

(Au niveau de l'entité)

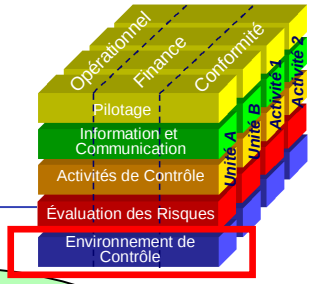


- L'environnement de contrôle détermine le niveau de sensibilisation du personnel au besoin de contrôles. Il constitue le fondement de tous les autres éléments du contrôle interne, en imposant discipline et organisation.

- L'environnement de contrôle se compose de 'soft controls' qui font généralement référence au comportement du Management: style et philosophie de Direction, exemplarité, éthique, valeurs morales, etc.

Le référentiel COSO 1: Environnement de contrôle

Exemple de critères à prendre en compte



Conseil d'administration et Comité d'audit

Compétences

Structure organisationelle

Environnement de contrôle

Attribution des responsabilités et délégations de pouvoirs

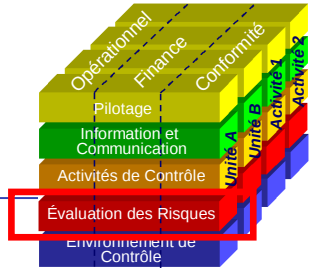
La politique et les pratiques des RH

Philosophie de la Direction

Intégrité et Valeurs éthiques

Le référentiel COSO 1: Evaluation des risques

(Au niveau de l'entité et des processus)

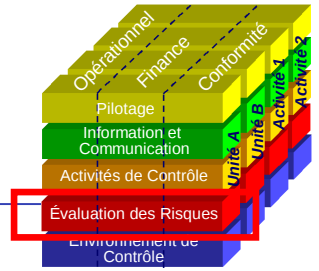


- Le risque est un évènement ou une circonstance qui peut affecter négativement la capacité de l'entreprise à atteindre ses objectifs.

- L'évaluation des risques requiert l'évaluation des facteurs externes et internes à l'entreprise, leurs impacts sur l'exploitation, le reporting financier et la conformité aux lois en vigueur.

Le référentiel COSO 1: Evaluation des risques

(Au niveau de l'entité et des processus)

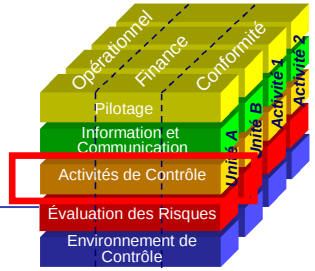


- L'évaluation des risques commence par l'identification des risques associés aux objectifs définis à chaque niveau de l'entreprise
  - Au niveau de l'entreprise
    - Pierre angulaire d'un contrôle effectif, les objectifs de l'entreprise permettent de savoir ce que l'entreprise doit accomplir
    - Les objectifs doivent être cohérents avec le budget, la stratégie, et les plans de développement ("business plans")
  - Au niveau des activités
    - S'aligner avec les objectifs de l'entreprise avec la différence qu'ils se rapportent directement à des objectifs avec des cibles et des délais spécifiques
    - Fournir des informations et conseils sur les priorités de la Direction

Le référentiel COSO 1: Activités de contrôle

- Les activités de contrôles sont des règles et des procédures qui permettent de s’assurer que les mesures identifiées comme nécessaire pour maîtriser les risques sont appliquées correctement et à temps.

Le référentiel COSO 1: Activités de contrôle



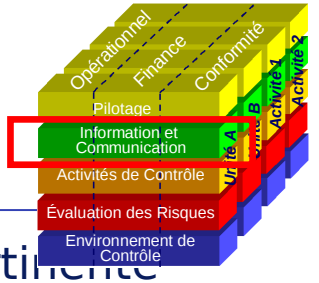
- Les activités de contrôle doivent être intégrées aux opérations / processus habituels et sont destinées à assurer l'exécution des directives émises par le management en vue de maîtriser les risques. Se concentrer sur *la prévention, la détection et la correction*.

Le référentiel COSO 1: Activités de contrôle

- Types d'activités de contrôles:
  - Approbation, autorisation, et vérifications (par exemple : délégation de pouvoirs)
  - Réconciliations
  - Revue des indicateurs de performance
  - Sécurité des biens (par exemple : contrôle d'accès)
  - Séparation des tâches (par exemple surveillance - autorisation - enregistrement)
  - Contrôle des systèmes d'informations
    - Contrôles généraux informatiques (sécurité, développement des applications,..)
    - Contrôle des applications

Le référentiel COSO 1: Information...

(Au niveau de l'entité et des processus)



- Inclut l'identification, l'obtention et la diffusion d'information pertinente (interne ou externe) selon le bon moyen de communication, au bon moment, aux bonnes personnes, afin que ces dernières puissent réagir et assurer leurs responsabilités

- Systèmes d'information
  - Infrastructure
  - Logiciels
  - Personnels
  - Processus – manuels ou automatiques
  - Données

- La qualité de l'information s'évalue selon les critères suivants:
  - Opportunité / Contenu
  - A temps / En retard
  - A jour
  - Exactitude
  - Accessibilité

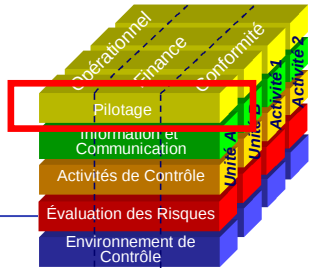
…Et communication

(Au niveau de l'entité et des processus)

- Une bonne compréhension des rôles et responsabilités de chacun
- Les salariés comprennent comment leur travail est lié à celui des autres
- Moyens de signaler des exceptions à la hiérarchie
- Peut être sous la forme de:
  - Manuels de procédures
  - Manuels de comptabilité et de reporting financier
  - Memoranda
  - Électroniquement, oralement (réunions, compte-rendu) et par des actions des Dirigeants
- Faciliter la communication top-down et bottom-up
- Communiquer avec les tiers

Le référentiel COSO 1: Pilotage

(Au niveau de l'entité et des processus)



- L'objectif de cette phase de contrôle est de déterminer si la conception du contrôle interne est adéquate, si le contrôle interne est appliqué, efficace et peut s'adapter aux circonstances.

- Les performances du contrôle interne doivent être contrôlées de manière continue aux travers des opérations à caractère de pilotage, et doivent aussi faire l'objet d'évaluations sous forme de missions d'audit interne

- Le périmètre des activités à contrôler et la fréquence des contrôles dépendent de l'importance relative des risques sous-jacents et des contrôles qui permettent de réduire ces risques.

Atouts d’un contrôle interne fort

- Les atouts d'un contrôle interne fort :
  - Risques identifiés et maîtrisés
  - Confiance accrue des investisseurs
  - Conformité avec la loi et les réglementations
  - Réduction du risque de perte
  - Harmonisation / homogénéisation des procédures
  - Décisions managériales optimisées, prises sur la base d'une information de qualité constamment mise à jour
  - Visibilité accrue sur les zones d'inefficacité opérationnelle
  - Minimisation des "opérations pompiers"
- Les risques d'un contrôle interne défaillant :
  - Risque de fraude accru
  - États financiers faux
  - Impact négatif sur l’image de l’entreprise écornée
  - Impact négatif sur la valeur actionnariale
  - Sanctions des régulateurs
  - Procès, actions judiciaires
  - Pertes d'actifs
  - Décisions managériales hasardeuses

Le référentiel « Enterprise Risk Management-integrated framework (COSO 2)»

- Le COSO est un référentiel de contrôle interne défini par le Committee Of Sponsoring Organizations of the Treadway Commission. Le référentiel initial appelé COSO 1 a évolué depuis 2002 vers un second corpus dénommé COSO 2.
- Face aux scandales récents, les entreprises ont renforcé leur organisation et communication sur les éléments suivants:
  - La gestion des risques
  - Le gouvernement d'entreprise
  - Le contrôle
  - L'assurance

COSO 2: Définition du référentiel

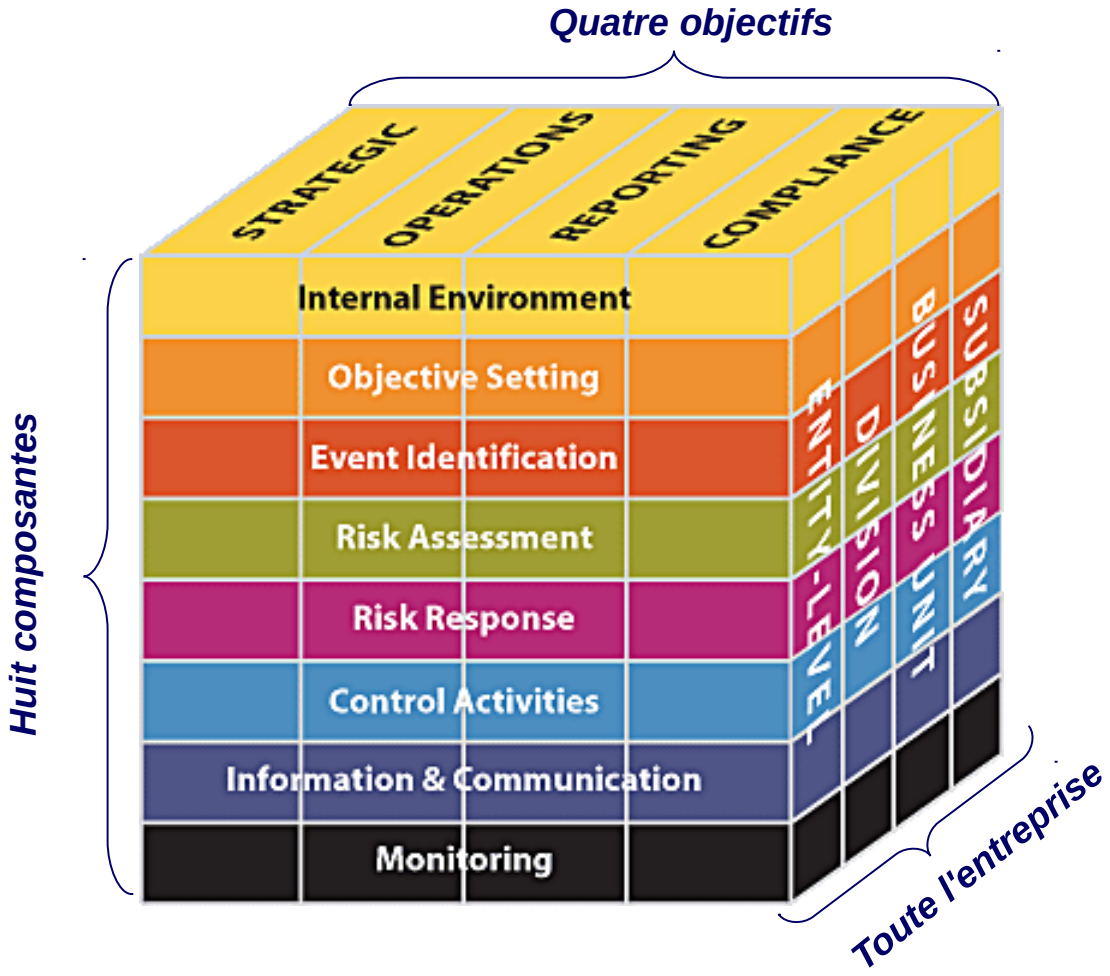
- Principes sous-jacents:
  - **Tous les types de risques doivent être identifiés, évalués et contrôlés**
  - **Une vision par portefeuilles de risques étroitement liés entre eux doit être privilégiée:**
    - Examiner les liens qui existent entre les risques au sein des différentes structures de l'entreprise
    - La vision sous forme de portefeuille se fait à 2 niveaux : l'entité elle même et les Business Unit

COSO 2: Définition du référentiel

- Définition de l'ERM :
  - Un processus
  - Effectué par le Conseil d'administration, la Direction et l'ensemble des salariés
  - Appliqué dans le cadre d'une stratégie prédéfinie
  - Appliqué dans toute l'entreprise (entité, divisions, filiales, BU)
  - Conçu pour identifier d'éventuels évènements qui pourraient affecter l'entreprise
  - Gère les risques afin qu'ils restent dans la limite des risques que l'entreprise est encline à supporter (notion de « risk appetite » et « risk tolerance »)
  - Procure une assurance raisonnable quant à la réalisation des objectifs de l'entreprise

Maîtriser, et non éliminer, la prise de risque qui doit rester une source de croissance et de réussite pour l'entreprise

La matrice COSO2



Le référentiel COSO2

- Les 4 objectifs d'une entreprise :
  - **Stratégique**
    - Objectifs stratégiques « high-level » qui corroborent la vision et la mission de l'entreprise
  - **Opérations**
    - Efficacité et efficience des ressources utilisées
  - **Reporting**
    - Fiabilité des processus de reporting au sens large du terme, pour tout type d'information (financière / non financière; interne / externe)
  - **Conformité**
    - Aux textes et lois en vigueur

Le référentiel COSO 2: Les 8 composantes du COSO2

- 8 composantes étroitement liées, permettant la réalisation des objectifs :
  - **Environnement interne**
  - **Définition des objectifs**
  - **Identification des évènements potentiels**
  - **Evaluation des risques**
  - **Réponses aux risques**
  - **Activités de contrôles**
  - **Information et communication**
  - **Pilotage**

Le référentiel COSO 2: Environnement interne

- **La pierre angulaire des autres composantes car il influence**
  - La mise en place de la stratégie et des objectifs
  - L'organisation des activités opérationnelles (et donc la manière d'identifier et d'évaluer les risques)
  - La conception et le fonctionnement des activités de contrôles
  - La circulation de l'information et la mise en place des systèmes d'information

- **La philosophie de l'entreprise concernant la gestion des risques**
  - Intégrité et éthique
  - Compétences (connaissance et aptitudes nécessaires à l'accomplissement des tâches)
  - Conseil d'administration et Comité d'audit
  - Philosophie et style de management des dirigeants
  - Structure de l'entreprise
  - Délégation de pouvoirs et domaines de responsabilité
  - Politique en matière de ressources humaines
  - Les différences et leurs conséquences

- **La culture de l'entreprise en terme de risque**

Le référentiel COSO 2: Définition des objectifs

- Étape préalable à l'identification et l'analyse des risques: Définition des objectifs stratégiques par rapport à la mission ou vision de l'entreprise afin de définir la stratégie de l'entreprise pour atteindre ces objectifs.

- Identification des « objectifs secondaires » qui découlent des objectifs stratégiques, et qui permettent de fixer les objectifs au niveau des entités ou business units.

- Atteinte des objectifs: Capacité de l'entreprise pour atteindre ses objectifs par rapport aux facteurs externes.

Le référentiel COSO 2: Définition des objectifs

- Attitude de prise de risques (risk appetite): Définition du niveau de risque acceptable pour la direction et conseil d'administration afin d'atteindre les objectifs de l'entreprise.

- Attitude de tolérance des risques (risk tolerance): Définition du niveau acceptable de déviation par rapport aux objectifs prédéfinis.

- Objectifs sélectionnés: Mise en place d'un processus alignant les objectifs stratégiques de l'entreprise et ses missions afin d'assurer leur cohérence avec le risk appetite.

Le référentiel COSO 2: Identification des évènements potentiels

- Évènements : Un évènement est un incident interne ou externe, positif ou négatif affectant l'implémentation des stratégies ou l'atteinte des objectifs de l'entreprise.
- Facteurs externes (économie, environnement naturel, politique et social, technologie) et internes (infrastructure, personnel, processus, technologie).
- Techniques d'identification des évènements: Différentes méthodes et outils peuvent être utilisés selon les différentes entreprises.
- Interdépendance des évènements: Les événements sont interactifs.
- Catégories des évènements: La définition des catégories permet au management de vérifier si les évènements sont identifiés d'une manière complète.
- Distinction entre risques et opportunités: Un évènement peut avoir un impact négatif, positif ou les deux sur l'activité de l'entreprise.

Le référentiel COSO 2: Evaluation des risques

- Contexte : Les contextes peuvent varier selon les métiers, les profils, la taille, la complexité et l'environnement réglementaire de l'entreprise
- Risques inhérents et risques résiduels : Le risque résiduel est celui qui subsiste après la mise en place de l'activité de contrôle diminuant l'impact ou la probabilité de survenance du risque inhérent
- Evaluation de l'impact et de la probabilité : Un risque peut être évalué en terme d'impact et de probabilité
- Techniques d'évaluation : Combinaison des méthodes qualitatives et quantitatives
- Relation entre les évènements : Les évènements liés l'un à l'autre doivent être évalués groupés. Sinon, ils doivent être évalués individuellement.

Le référentiel COSO 2: Réponses aux risques

- Identifier les plans d'actions possibles:
  - Éviter les risques
  - Réduire les risques
  - Partager les risques
  - Accepter les risques

- Évaluation des différents plans d'actions:
  - Évaluer l'effet sur l'impact et la probabilité
  - Évaluer coûts / profils

- Sélectionner les plans d'action sur la base de l'évaluation du portefeuille global de risques et de l'évaluation des différents plans d'actions possibles.

Le référentiel COSO 2: Activités de contrôles

- Mise en place du plan d'action
- Définition des activités de contrôle correspondant au plan d'action
- Identification des types d'activité de contrôle : préventif/détectif, manuel/informatique, etc…
- Etablissement des règles et procédures
- Contrôles spécifiques des différentes entités
- Contrôles informatisés :
  - Contrôles généraux informatiques
  - Contrôle d'application

Le référentiel COSO 2: Information et communication

- Information: L'information est nécessaire à tous les niveaux de l'entreprise pour identifier, évaluer et répondre aux risques
  - Information interne/externe
  - Information financière/non financière

- Communication: La communication se repose sur le système d'information
  - Communication interne
  - Communication externe

Le référentiel COSO 2: Pilotage

- Pilotage en permanence au travers des activités au quotidien:
  - Des activités routinières permettent à l'entreprise de piloter l'efficacité du risk management en permanence
- Revue indépendante:
  - Des revues indépendantes régulières concentrées sur l'efficacité du risk management sont aussi nécessaires
- Reporting des défaillances:
  - Quelles sources d'informations ?
  - Quoi ?
  - Qui ?
  - Quelles sont les informations nécessaires pour la prise de décision à un niveau précis du management ?

Liens avec le COSO1

- Le COSO 1 propose un cadre de référence pour la gestion du contrôle interne.
- Le COSO 2 propose un cadre de référence pour la gestion des risques de l'entreprise (Enterprise Risk Management Framework).
  - *Il apparaît que **le COSO 2 inclut les composantes du COSO 1** et le complète sur le concept de gestion des risques. Le COSO 2 est basé sur une vision orientée risques de l'entreprise.*

- Une **nouvelle notion, le « Risk Appetite »**
  - La composante « Environnement Interne » s'enrichit d'une nouvelle notion : celle de Risk Appetite : c'est-à-dire la prise de risque acceptée par l'entreprise dans le but d'accroître sa valeur. Ce « Risk Appetite » permet ensuite de déterminer le niveau de la tolérance de risque aux différents niveaux de l'organisation. Cette notion est nécessaire et précède la définition de la stratégie de l'entreprise.

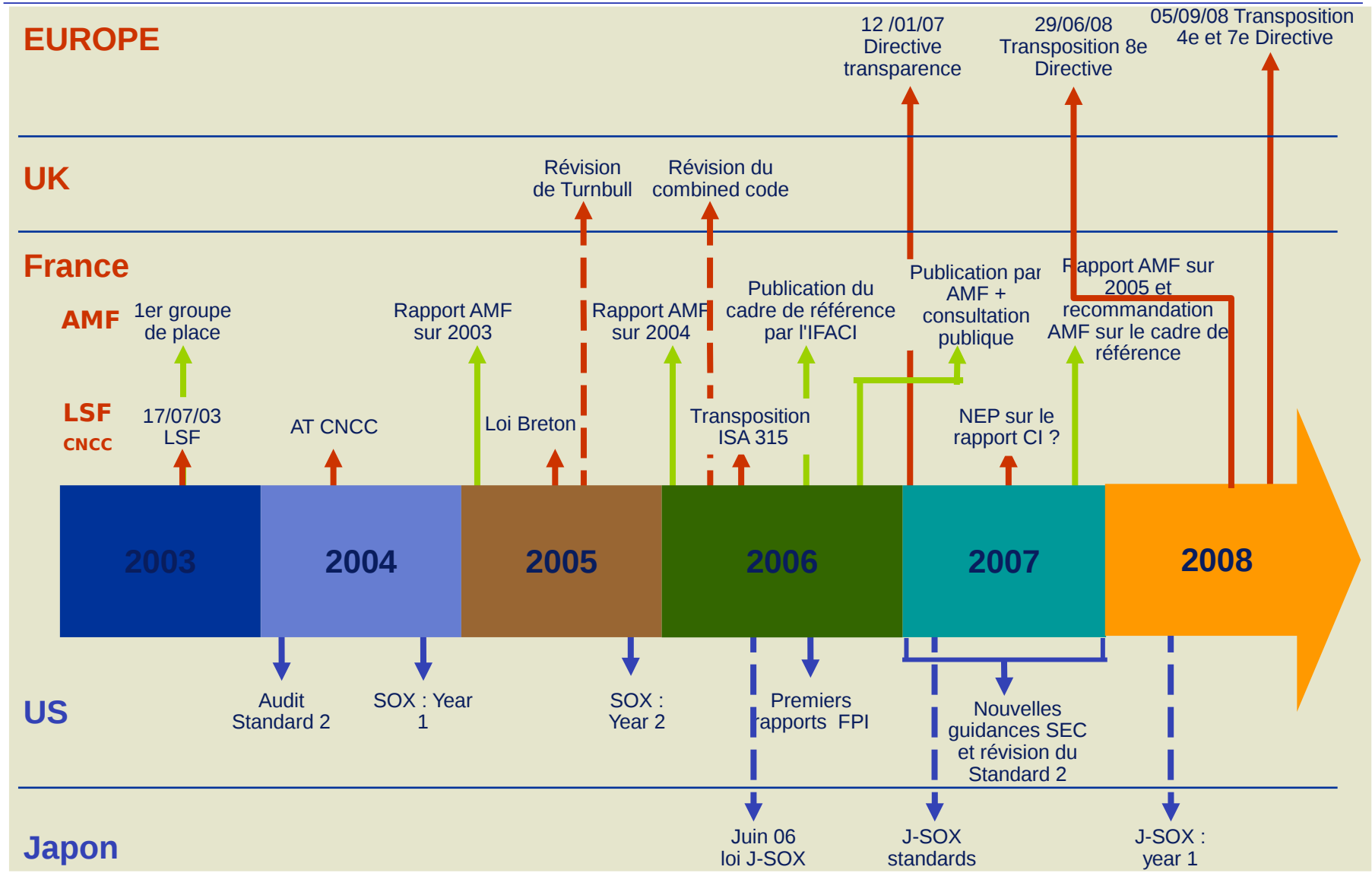
- Apport d'un **nouvel objectif : « stratégique ».**
  - la mise en œuvre de COSO 2 nécessite d'avoir une vision des objectifs stratégiques de l'entreprise en plus des « related » objectifs.

Liens avec le COSO1

- **Composante de risques**
  - Par rapport à COSO 1, les différents éléments de cette composante sont plus détaillés et fixent un cadre plus précis :
    - pour l'identification des événements potentiels (tendances, événements passés)
    - pour l'évaluation des risques (risque inhérent, risque résiduel) ,
    - pour les réponses aux risques (catégorisation des types de réponses).
- **Information et Communication**
  - Nécessité de considérer que les informations sont issues des événements passés, permettant :
    - une comparaison des performances de l'organisation (passées, et potentielles futures) et l'identification des évolutions et tendances de l'activité de l'organisation,
    - l'aide à la détection des potentiels événements futurs qui affectent le profil de risques actuel de l'organisation.
  - COSO 2 insiste sur le concept de présentation de l'information pour communiquer, i.e. l'information doit être communiquée sous une forme adaptée en fonction de l'interlocuteur destinataire.
- **Rôles et responsabilités**
  - Le COSO 2 souligne l'importance de la prise de responsabilité dans une entreprise et détaille ce qu'elle recouvre pour chacun des acteurs.
    - Un nouveau rôle apparaît: le « Risk officer »,
    - Le rôle du Comité de Direction est plus étendu que dans le COSO 1

Les exigences légales

Le contexte réglementaire
L'environnement international



Sarbanes Oxley vs. Loi de la Sécurité Financière

- Réglementations sur le contrôle interne

  > Série de scandales pour certaines entreprises américaines ou européennes

  - Affaire Enron
  - Affaire Worldcom
  - Vivendi

  > Nécessité de protéger les intérêts des investisseurs et des employés des entreprises concernées

  > Réponse à la crise de confiance des investisseurs

  - Stabilité et fiabilité du marché des capitaux américains pour SOA
  - Réponse française pour LSF

- Adoption des textes

SOA (Sarbanes-Oxley Act)	LSF (Loi de Sécurité Financière)
Congrès américain	Parlement Français
30 juillet 2002	17 juillet 2003

Présentation succincte

	Loi Sarbanes-Oxley (404)	Loi de Sécurité Financière
TEXTE	Le management doit établir un rapport sur le contrôle interne relatif au reporting financier contenant : - une affirmation de responsabilité sur l'établissement et le maintien d'un dispositif adéquat - une évaluation de l'efficacité de ce dispositif	Le Président du Conseil d'Administration rend compte, dans un rapport[…] des procédures de contrôle interne mises en place par la société […] (art.117)
Responsabilité	Management (CEO/CFO)	Président du CA/CS
Périmètre	Contrôle interne relatif au reporting financier	Ensemble du Contrôle interne
Nature de l'affirmation	Évaluer l'efficacité	Rendre compte
Référentiel	Exigé PCAOB recommande l'utilisation du COSO	Non mentionné par la loi Recommandation de l'AMF d'un cadre de référence à partir du 1er janvier 2007

Présentation succincte

	Loi Sarbanes-Oxley (404)	Loi de Sécurité Financière
METHODES		
Sociétés	Sociétés cotées aux USA	Initialement l'ensemble des SA Uniquement APE depuis 2006
Périmètre	Consolidé	Social + consolidé
Délais	Exercice clos après le 15/6/2004 (15/7/2006 pour les foreign registrants)	Exercices ouverts à compter du 1/1/2003
SANCTIONS	Le management (CEO, CFO) est responsable du contrôle interne - Sanctions pour fausse certification non intentionnelle : jusqu'à 1 millions de dollars et 10 ans d'emprisonnement - Sanctions pour fausse certification intentionnelle : jusqu'à 5 millions de dollars et 20 ans d'emprisonnement	La responsabilité est portée par le Président du Conseil d' Administration - Pas de sanction prévue à ce jour mais possibilité d'une publication rectificative - Sanction dans le cadre de la diffusion de fausses informations : 2 ans d'emprisonnement, 1,5 M€ d'amende, sanctions administratives
CAC	Opinion sur l'efficacité du contrôle interne	Rapport sur les informations portées dans le rapport du président

Le cadre de référence sur le dispositif de contrôle interne présenté par l'AMF

- **Les objectifs :**
  - Les pratiques des entreprises en matière de contrôle interne, telles qu'observées depuis 2003, témoignent d'une grande diversité en matière de contrôle interne

    ⇒ Rechercher une transcription pratique du concept de contrôle interne sous la forme d'un cadre de référence

    ⇒ Présenter un cadre de référence de contrôle interne global (qui reste applicable dans un environnement en mutation et permet à chaque société de le mettre en œuvre quelque soit ses spécificités particulières)

Le cadre de référence sur le dispositif de contrôle interne présenté par l'AMF

- **Le cadre de référence comprend :**
  - Les principes généraux de contrôle interne
  - Un guide d'application sur 14 processus concourant à l'élaboration de l'information comptable et financière
  - 2 questionnaires de portée générale
    - Relatif au contrôle interne comptable et financier
    - Sur l'analyse et la maîtrise des risques
- Le cadre de référence n'a pas vocation à être imposé aux sociétés ni à se substituer aux règlementations spécifiques en vigueur dans certains secteurs d'activités
- C'est un outil que les sociétés peuvent utiliser pour superviser ou développer leur dispositif de contrôle interne, si elle font appel public à l'épargne.

Cadre de référence de l’AMF

- Recommandations de l’AMF

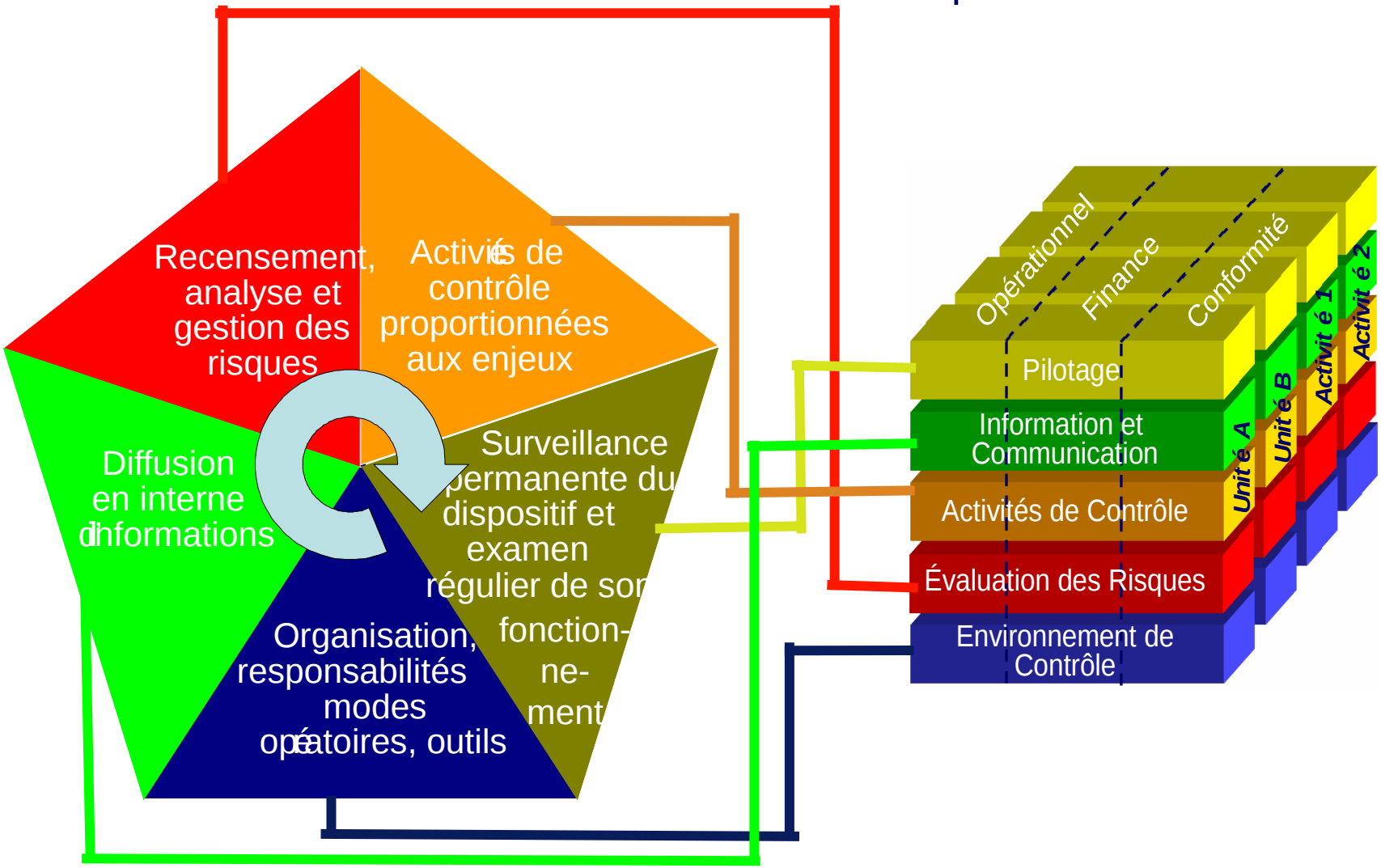
  - « l'AMF **recommande** l'utilisation du cadre de référence et du guide d'application »

  - « Le cadre de référence complété par le guide **n’a certes pas vocation à être imposé aux sociétés**, notamment soumises à un référentiel applicable de par une autre réglementation, ni à se substituer aux réglementations spécifiques en vigueur dans certains secteurs d’activité, notamment le secteur bancaire et celui des assurances. »

  - « Les sociétés sont invitées, toutefois, à préciser, dans le rapport du président, si elles se sont appuyées sur ce cadre de référence, complété du guide d’application, pour la rédaction du rapport. **En cas d’application partielle du cadre de référence ou du guide, les sociétés devront clairement identifier les domaines ou processus clés de contrôle interne qu’elles ont appliqués**, compte tenu de la nature de leurs activités, de leur taille et de leur mode d'organisation. Les sociétés mettront l’accent sur les éléments et informations susceptibles d’avoir un impact significatif sur le patrimoine ou les résultats de la société. »

Principes et concepts du Cadre de référence de l'AMF

Un cadre de référence compatible avec le COSO



Principes et concepts du Cadre de référence de l'AMF
Guide d'application

- 14 Principes et points clés d'analyse permettant d'identifier les principaux risques pouvant affecter les processus concourant à l'élaboration de l'information comptable et financière
  - **Investissements / Désinvestissements / Recherche et Développement**
    - Exemple: « Concernant les frais de développement, une vérification est faite à la date de clôture afin de confirmer que les conditions ayant conduit à leur activation sont toujours remplies. »
  - **Immobilisations incorporelles, corporelles et goodwill**
    - Exemple: « Lorsque la méthode de la juste valeur est appliquée, les évaluations sont réalisées par des spécialistes ou à partir de données de marchés et sont revues périodiquement. »
  - **Immobilisations financières**
    - Exemple: « Les produits se rattachant aux immobilisations financières sont évalués à chaque clôture. »
  - **Achats / Fournisseurs et assimilés**
    - Exemple: « Il existe un suivi et un rapprochement entre les bons de commande, les bons de réception et les factures (quantité, prix, conditions de paiement). Les anomalies éventuelles font l'objet d'une analyse et d'un suivi. »
  - **Coûts de revient/Stocks et encours/Contrats à long terme ou de construction**
    - Exemple: « les marges font l'objet d'un suivi régulier, en vue de permettre un correct suivi de la dépréciation des stocks. »

Principes et concepts du Cadre de référence de l'AMF
Guide d'application

- 14 Principes et points clés d'analyse permettant d'identifier les principaux risques pouvant affecter les processus concourant à l'élaboration de l'information comptable et financière
  - **Produits des activités ordinaires / Clients et assimilés**
    - Exemple: « les fonctions de facturation et de recouvrement sont effectivement séparées. »
  - **Trésorerie / Financement et instruments financiers**
    - Exmple: « Il existe une procédure visant à identifier les instruments financiers complexes afin qu'ils soient approuvés préalablement (selon les règles édictées par la société) et qu'un traitement conforme aux normes en vigueur (IAS 39 par exemple) leur soit appliqué. »
  - **Avantages accordés au personnel**
    - Exemple : « Il existe une séparation des fonctions de calcul, d'enregistrement, de contrôle, de paiement et de transmission des feuilles de paie. »
  - **Impôts, taxes et assimilés**
    - Exemple: « Il existe un processus de veille relatif aux obligations découlant des lois, réglementations et instructions fiscales. »
  - **Opérations sur le capital**
    - Exemple: « Il existe une procédure de suivi des stock-options (documentation des dates d'attribution, suivi des options attribuées ou devenues obsolètes…). »

Principes et concepts du Cadre de référence de l'AMF
Guide d'application

- 14 Principes et points clés d'analyse permettant d'identifier les principaux risques pouvant affecter les processus concourant à l'élaboration de l'information comptable et financière
  - **Provisions et engagements**
    - Exemple: « Il existe un processus visant à ce que la société donne en annexe de ses comptes une information sur ses engagements conformément aux principes comptables applicables. »
  - **Consolidation**
    - Exemple: « Les pourcentages d'intérêt et la situation de contrôle des filiales, participations et entités contrôlées sont analysés au regard de la situation de contrôle afin de vérifier l'adéquation de la méthode de consolidation appliquée à chacune. »
  - **Information de gestion nécessaires à l'élaboration des informations comptables et financières publiées**
    - Exemple: « Il existe un rapprochement entre les données publiées et les informations internes. »
  - **Gestion de l'information financière externe**
    - Exemple: « Il existe un processus de veille sur les obligations en matière d'information financière. »

8e Directive Européenne
Réglementation et évolution à venir

- La 8ème Directive Européenne sur le contrôle légal des comptes du 17 mai 2006 s'applique aux sociétés cotées

  - Obligation d'un Comité d'Audit (exceptée dans certains cas pour les entités d'intérêt public - Article 41)
  - Responsabilité du Comité d'Audit

    *« (…) Chaque entité d'intérêt public doit être dotée d'un **comité d'audit** ».*

    « (…) le comité d'audit est notamment chargé des missions suivantes:

    a) suivi du processus d'élaboration de l'information financière;

    *b) suivi de **l'efficacité des systèmes de contrôle interne**, d'audit interne, le cas échéant, et de gestion des risques de la société (…) »*

- La 8ème Directive Européenne doit être transposée en droit français avant le 29 juin 2008

  - Obligation pour les CAC de communiquer les déficiences significatives relevées lors de l'évaluation du Contrôle Interne au regard du processus de l'information financière.
  - *« Le contrôleur légal des comptes ou le **cabinet d'audit fait rapport au comité d'audit sur les aspects essentiels touchant au contrôle, en particulier les faiblesses significatives du contrôle interne** au regard du processus d'information financière. »*

Se tenir informé

Comment se tenir informé ?

- Site Internet Deloitte

  > **www.deloitte.fr**

  > **www.deloitteaudit.com** **(sur le site US, accès aux méthodologies Deloitte sur plusieurs sujets, dont SOA et la Fraud (Fraud Center)**

- Sites Internet dédiés à l'Audit Interne et au Contrôle Interne:

  > **www.ifaci.com** **(Institut de l'Audit Interne)**

  > **www.theiia.org** **(The Institut of Internal Auditors)**

  > **www.eciia.org** **(European Confederation of Institutes of Internal Auditing)**

  > **www.auditnet.org**

  > **www.coso.org** **(site officiel du COSO)**

  > **http://www.sec.gov/index.htm** **(site officiel de l'US Securities and Exchange Commission)**

  > **http://ue.eu.int/Newsroom** **(site officiel du conseil de l'Union Européenne)**

  > **http://europa.eu.int/eur-lex/lex** **(site officiel des droits de l'Union Européenne)**

Bibliographie

- « Théorie et pratique de l'audit Interne » de Jacques Renard, Editions d'organisation
- « Le management des risques de l'entreprise », Editions d'organisation
- « La pratique du contrôle interne » Coso Report, Editions d'organisation
- « Normes professionnelles de l'audit interne », IIA

Les Outils de Contrôle Interne

Les outils au service de l'auditeur

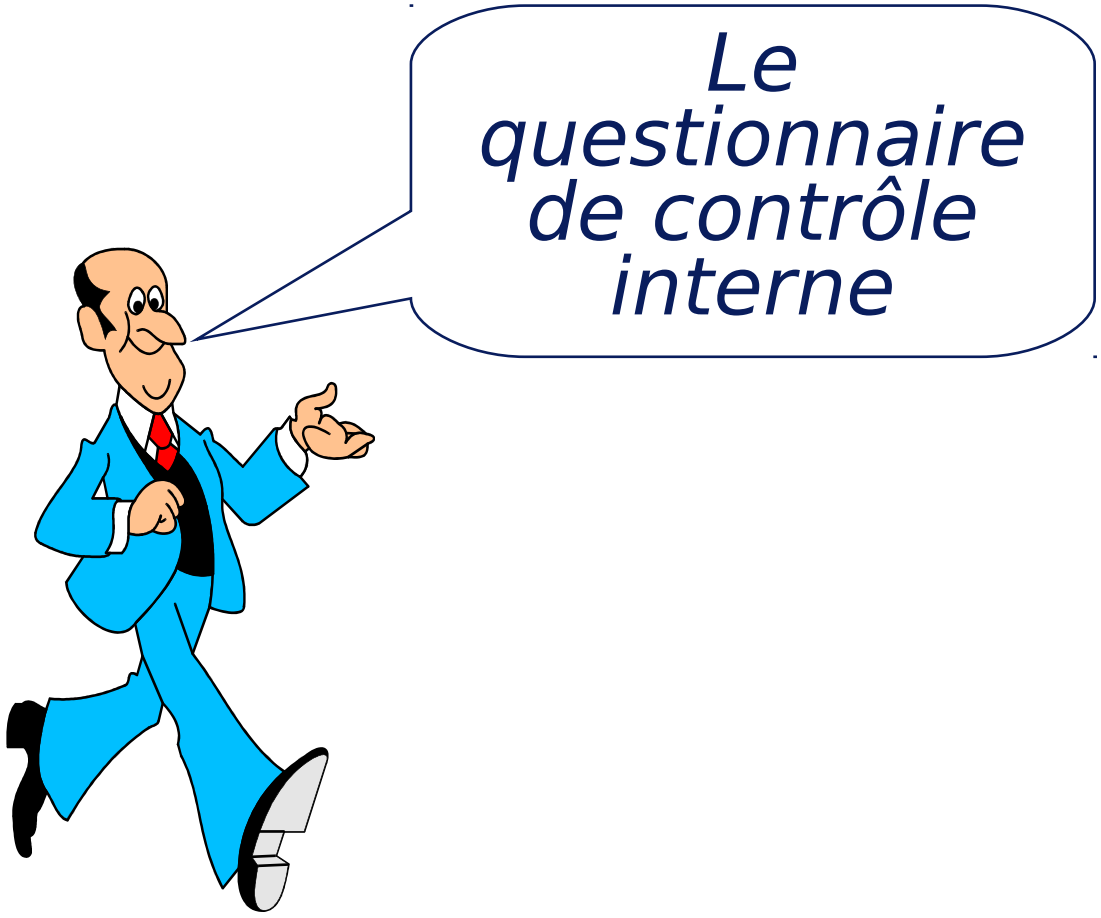
- La réponse à la question essentielle : comment collecter l'information ?
  - Les interviews
  - Les questionnaires d'auto-contrôle
  - Les tests de cheminement (pistes d’audit)
  - Les sondages et tests sur les contrôles
  - Les tableaux de bord
  - Les requêtes informatiques spécifiques

Les outils au service de l'auditeur

- Les critères de classement des outils
  - Les outils d’interrogation
    - Sondages statistiques
    - Interviews
    - ACL
    - Vérifications et rapprochements …
  - Les outils de description
    - Observation physique
    - Narration
    - Organigrammes fonctionnels
    - Diagrammes de flux
    - Grille d’analyse de tâches….

Objectifs

- 3 caractéristiques importantes
  - Il faut choisir le bon outil, celui qui est adapté au contexte ou aux travaux à mener
  - Les outils ne sont pas spécifiques à l'audit interne mais sont communs à de nombreuses fonctions : informaticien, consultant, médecin…
  - On peut combiner plusieurs outils pour un même objectif final de validation



Qu’est-ce qu’un questionnaire de contrôle interne?

- Le questionnaire de contrôle interne est une grille d’analyse qui a pour but de permettre à l’auditeur d’apprécier le niveau et de porter un diagnostic sur le dispositif de contrôle interne de la fonction (ou entité) auditée

  - Il comprend un ensemble de questions qui n’admettent, pour l’essentiel, que les réponses « oui » ou « non » qui servent à recenser les moyens en place pour atteindre les objectifs du contrôle interne

  - Le questionnaire est élaboré de manière telle que les réponses négatives désignent les faiblesses du dispositif de contrôle interne alors que les réponses positives désignent en théorie les points forts

  - L’auditeur devra ensuite évaluer l’impact des « non » sans oublier de vérifier la réalité des « oui »

Quand faut-il recourir au questionnaire de contrôle interne?

- Au cours des entretiens ou après les entretiens:
  - Dans le premier cas, le questionnaire de contrôle interne est un outil d'interview et d'analyse (reformulé par des questions ouvertes): les réponses sont données par les audités
  - Dans le second cas, le questionnaire de contrôle interne est seulement un outil d'analyse: les entretiens et analyses de procédures réalisés préalablement permettent à l'auditeur de répondre lui-même au questionnaire de contrôle interne
- Pendant la phase d'étude:
  - C'est alors un moyen pour effectuer une analyse des risques

Comment ? L’élaboration en 3 étapes du questionnaire de contrôle interne - Étape 1

- Décomposer l’activité à étudier en stades d’exploitation élémentaires retraçant tout le processus depuis la réalisation du fait économique jusqu’à son enregistrement comptable
  - Par exemple pour les achats auprès d’un fournisseur, il faut:
    - Déterminer et approuver les besoins
    - Sélectionner et contracter avec le fournisseur
    - Réceptionner la prestation ou le produit acheté
    - Enregistrer l’achat en comptabilité
    - Vérifier la dépense et autoriser son règlement
    - Effectuer le paiement

Comment? L’élaboration en 3 étapes du questionnaire de contrôle interne - Étape 2

- Pour chaque stade d’exploitation élémentaire, il faut définir des objectifs spécifiques en cohérence avec les objectifs généraux du contrôle interne
  - Exemple d’objectifs spécifiques au stade « réception des achats »
    - Toutes les réceptions correspondent à une prestation qui a été effectivement réalisée (critère rempli: existence)
    - Toutes les prestations demandées et réalisées ont été réceptionnées (critère rempli: exhaustivité)
    - Les réceptions sont effectuées dès que les prestations sont réalisées (critère rempli: allocation)
    - Les quantités et qualités réceptionnées correspondent aux quantités et qualités fournies et aux quantités et qualités demandées (critère rempli: correcte évaluation)

Comment? L’élaboration en 3 étapes du questionnaire de contrôle interne - Étape 3

- Déterminer les modalités de fonctionnement nécessaires à la fonction auditée pour atteindre ces objectifs et formuler des questions pour découvrir si ces moyens sont en place ou s’il s’agit de lacunes

  - Par exemple, pour atteindre les objectifs énumérés lors de l’étape 2, on estime nécessaire que:

    - Les réceptions soient prises en charge par des personnes indépendantes du service achat et du service comptabilité
    - Que ces personnes aient les informations nécessaires aux réceptions
    - Les modalités de comptabilisation des réceptions aient été définies
    - Lors des livraisons, les quantités et qualités sont vérifiées
    - Les écarts doivent être notées et validées de manière contradictoire

Attention!

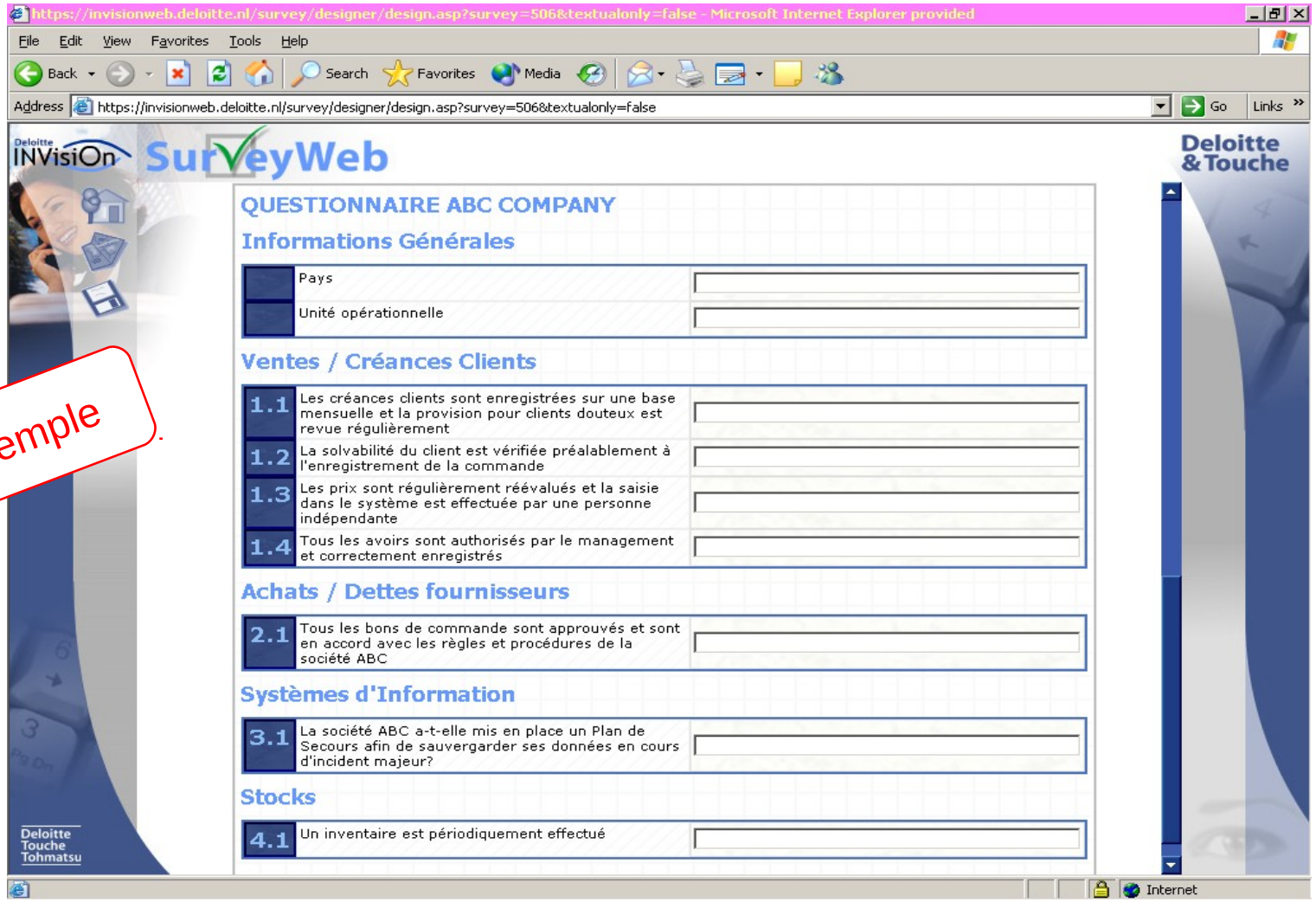
- La technique la plus classique consiste à utiliser des questionnaires de contrôle interne préexistants provenant de la littérature ou de missions précédentes auquel cas on utilisera le terme de questionnaire type:
  - En utilisant des questionnaires type, garder à l'esprit que certaines questions peuvent ne pas être adaptées au cas audité

- Avant d'être utilisés les questionnaires de contrôle interne doivent être approuvés par le chef de mission qui assure sa fonction de responsable en:
  - Éliminant les questions sans objet
  - Vérifiant que toutes les questions utiles ont bien été posées et qu'elles sont adaptées…

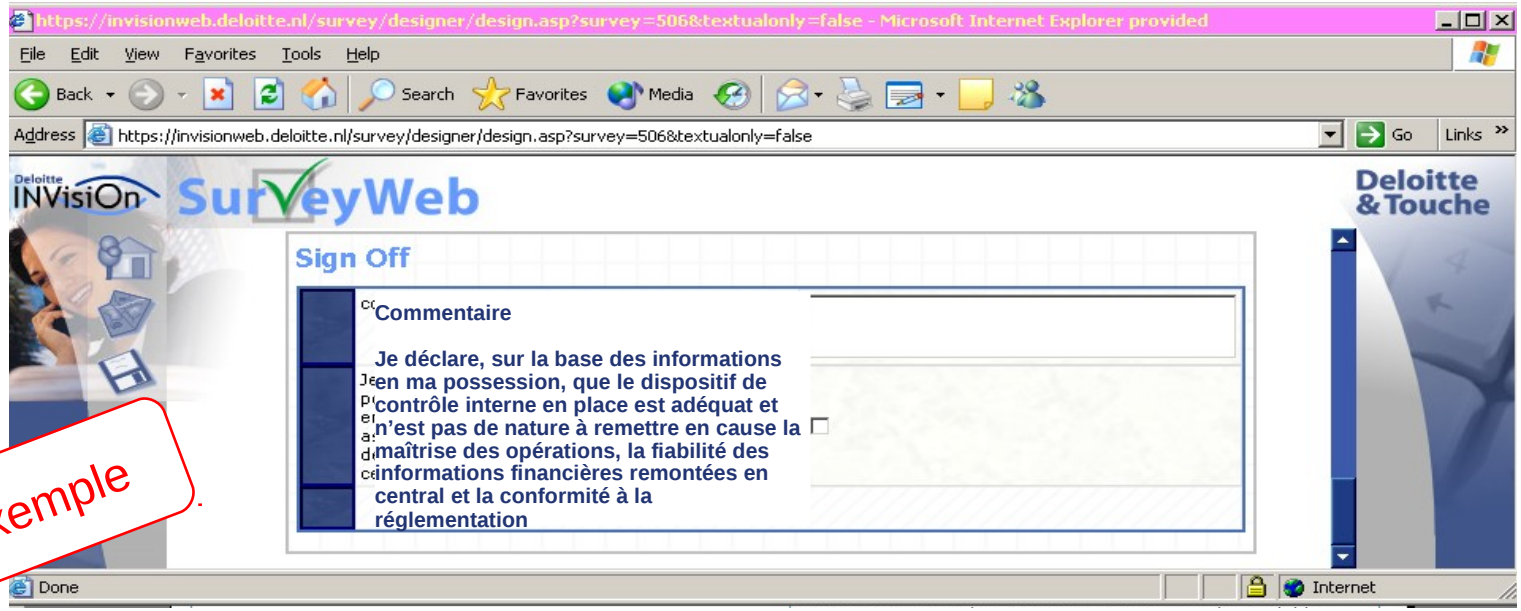
Exemples de questions types

- Le contrôle des commandes est-il satisfaisant?
  - Les commandes sont-elles centralisées en un seul service?
  - Tout achat est-il précédé d'une commande écrite?
  - L'approbation des commandes apparaît-elle sur tous les exemplaires?
  - Existe-il des achats qui sont dispensés de suivre le circuit normal?
  - Le service achats est-il indépendant des autres services?

Exemple de questionnaire de contrôle interne



Exemple de questionnaire de contrôle interne



Exemple

Les auto-évaluations de contrôle interne (ou CSA : Control Self Assessment)

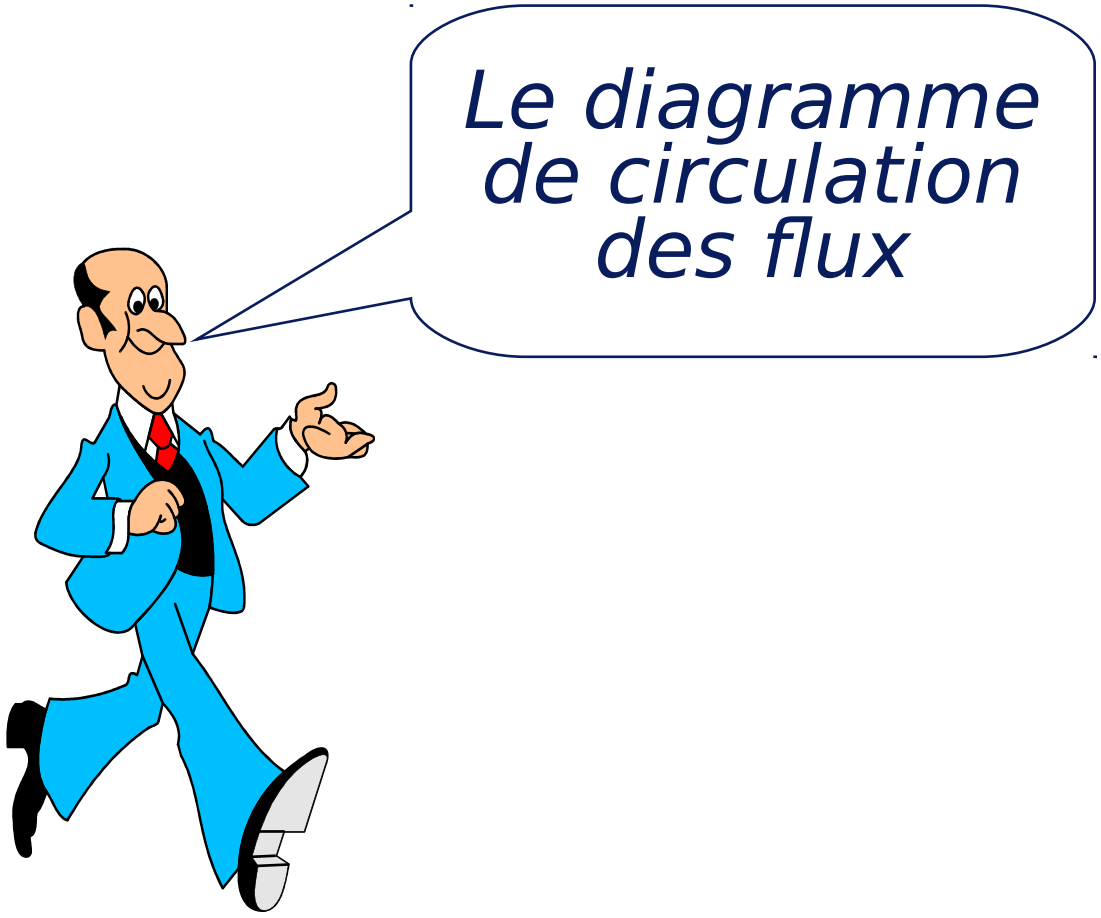
- Les autoévaluations de contrôle se font sous forme de questionnaires, s'adressant à un responsable qui doit répondre aux questions portant sur les contrôles clés de leurs activités.

- Grâce aux techniques d'auto contrôle, une organisation peut identifier les zones à risques élevés qui pourraient nécessiter ultérieurement une revue plus détaillée.

- Dans un premier temps, le rôle de l'Audit Interne a bien souvent été de former les audités à s'auto évaluer.

- Les CSA ont pris de l'ampleur suite à SOX et le rôle des Auditeurs Internes consiste désormais à s'assurer du caractère objectif de ces autoévaluations.

Les Outils de description

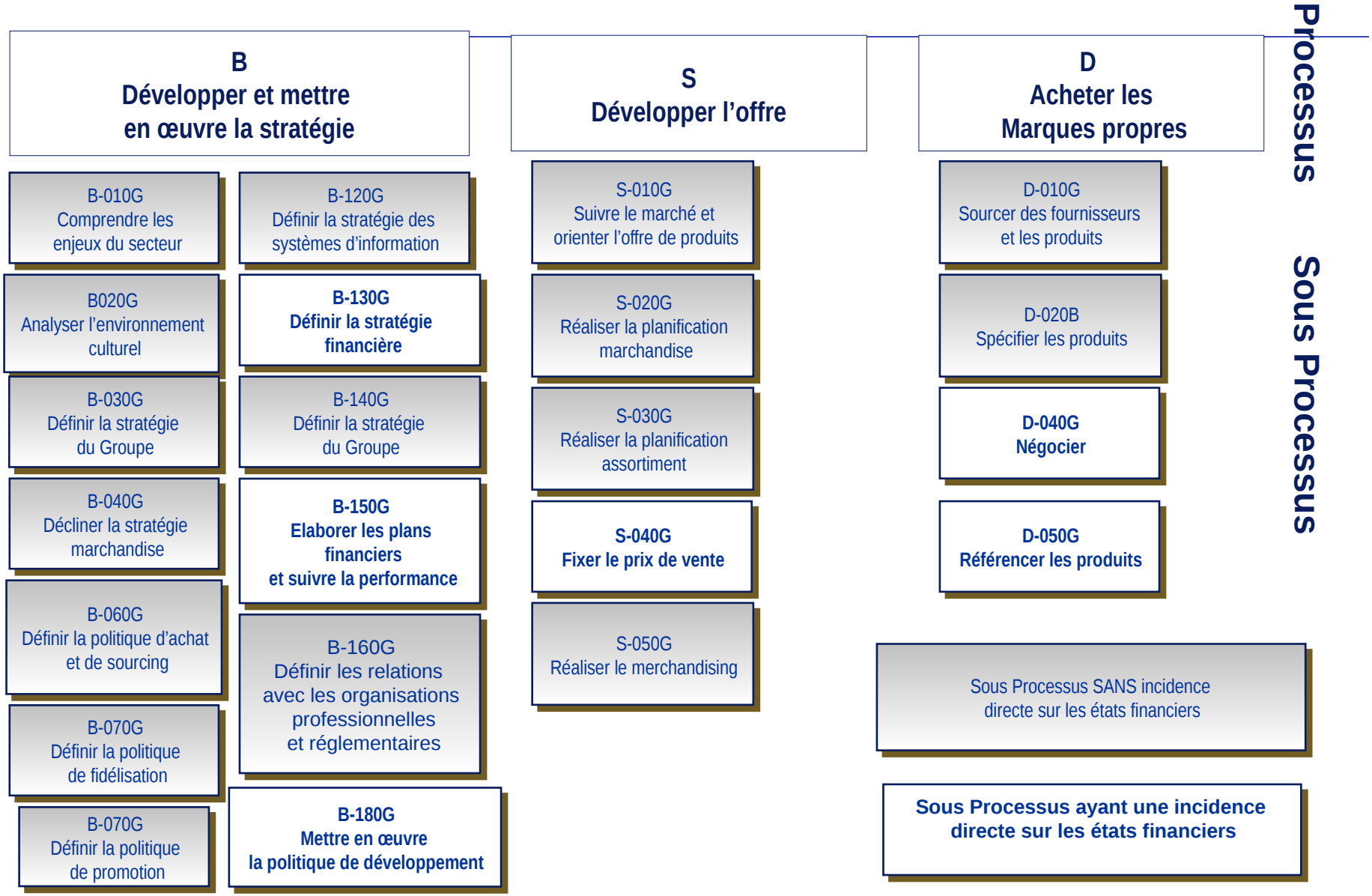


Documentation des processus : diagrammes de circulation des flux

- Le recours à des diagrammes de circulation de flux permet de faire apparaître très clairement :
  - quels sont les documents utilisés
  - quel est le nombre d'exemplaires
  - qui utilise le document et quelles sont les opérations effectuées
  - comment sont distribués et classés les différents exemplaires

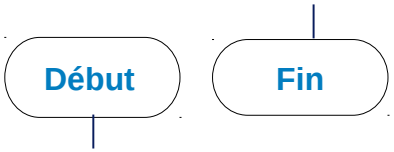
- Il doit être présenté le plus clairement possible et sa présentation est normée (cf «les diagrammes de circulations des flux» ci-après)
  - Le diagramme doit présenter toutes les catégories d'opérations traitées par le service ou le poste de travail concerné
  - Les informations sont recueillies auprès de différentes sources: documentation, interviews, organigrammes
  - **Parcourir le diagramme avec les collaborateurs du service pour s'assurer** que la procédure fonctionne bien selon le diagramme réalisé

Exemple de modélisation des processus

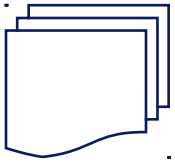


Les diagrammes de circulation des flux

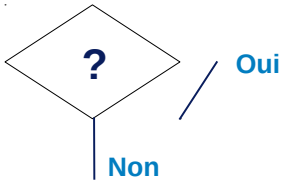
Symboles usuels



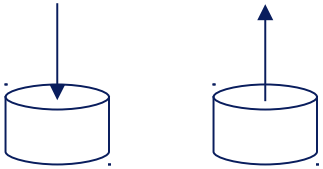
Début / Fin du processus



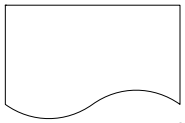
Documents liés au processus



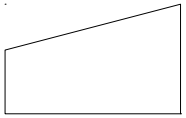
Procédure alternative, décision



Information venant ou partant vers un système d'information



Information fournit par le processus



Entrée manuelle d'une information

Etape / Action / Groupe de tâches

Point de control :

Control manuel

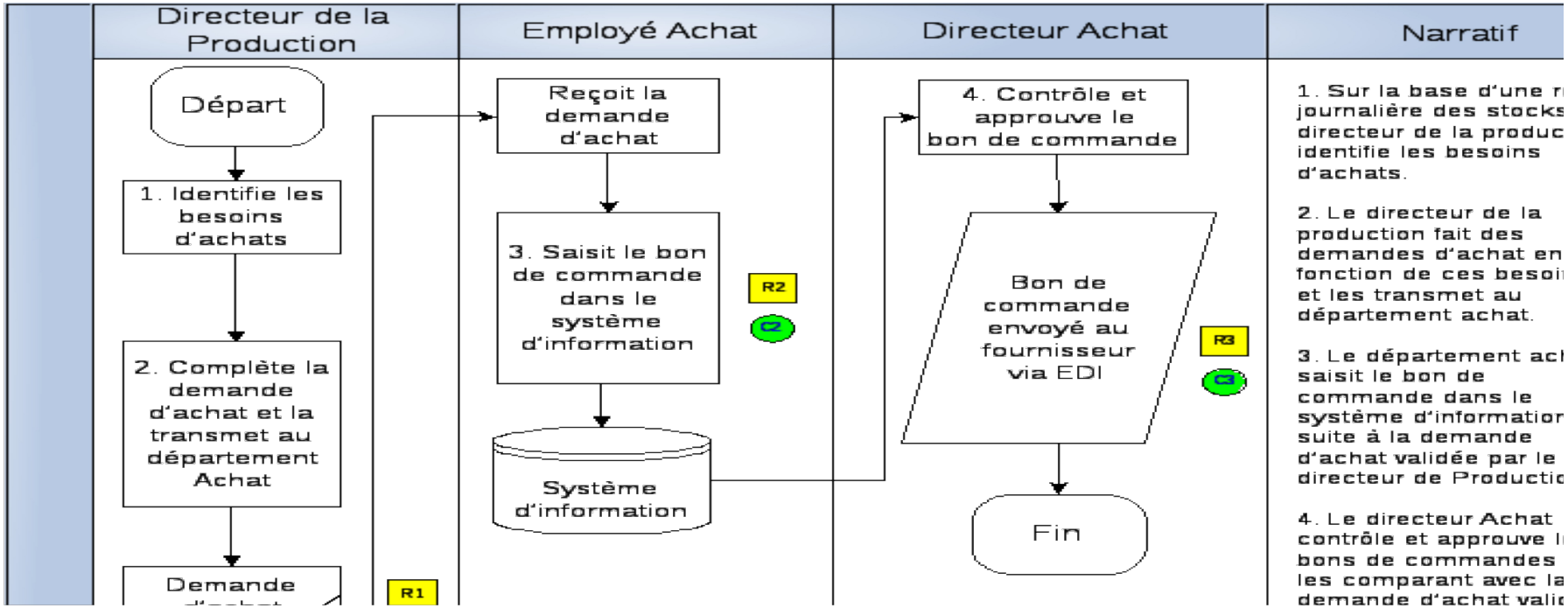
Control automatique

Exemple de diagramme de flux

Entité	TPI
Année fiscale	2008
Processus	Achat
Sous-processus	Achat - Production
Responsable processus	xxxxx
Responsable sous -processus	xxxxx

Version	Date de création	Rédacteur	Page
1	2008/01/20		1

Achat - Production



Exercice pratique

Exercice pratique « Diagramme de circulation des flux » 1/3

- Un auditeur interne élabore principalement un diagramme de flux pour :
    a. Détecter des erreurs et des anomalies.
    b. Analyser un système et identifier les contrôles internes.
    c. Déterminer les responsabilités fonctionnelles.
    d. Réduire le besoin d'interviewer les audités.

- Au cours de l'enquête préliminaire, quelle méthode d'évaluation des contrôles internes procure à l'auditeur la meilleure vue d'ensemble d'un système, ainsi qu'un moyen d'analyser les opérations complexes ?
    a. Un diagramme de circulation des flux.
    b. Un questionnaire.
    c. Une matrice.
    d. Une description détaillée.

Exercice pratique « Diagramme de circulation des flux » 2/3

- Un auditeur interne examine et adapte un diagramme de circulation relatif à des systèmes, afin de comprendre comment se déroule le flux d'informations lors du traitement des encaissements. Lequel des énoncés suivants est vrai en ce qui concerne l'utilisation de ces diagrammes de circulation ? Les diagrammes de circulation :

  a. Représentent les procédures de contrôle spécifiques mises en œuvre, telles que les contrôles d'édition ou les rapprochements des contrôles par lots.
  b. Donnent de bonnes indications sur l'éventuelle séparation des tâches.
  c. Sont généralement tenus à jour en cas de changements apportés aux systèmes.
  d. N'illustrent que le traitement informatique, pas le traitement manuel.

Exercice pratique « Diagramme de circulation des flux » 3/3

- Quel symbole est utilisé pour déterminer si la rémunération d'un salarié est supérieure ou inférieure au plafond relatif aux contributions sociales FICA ?

  a. 

  b. 

  c. 

  d. 

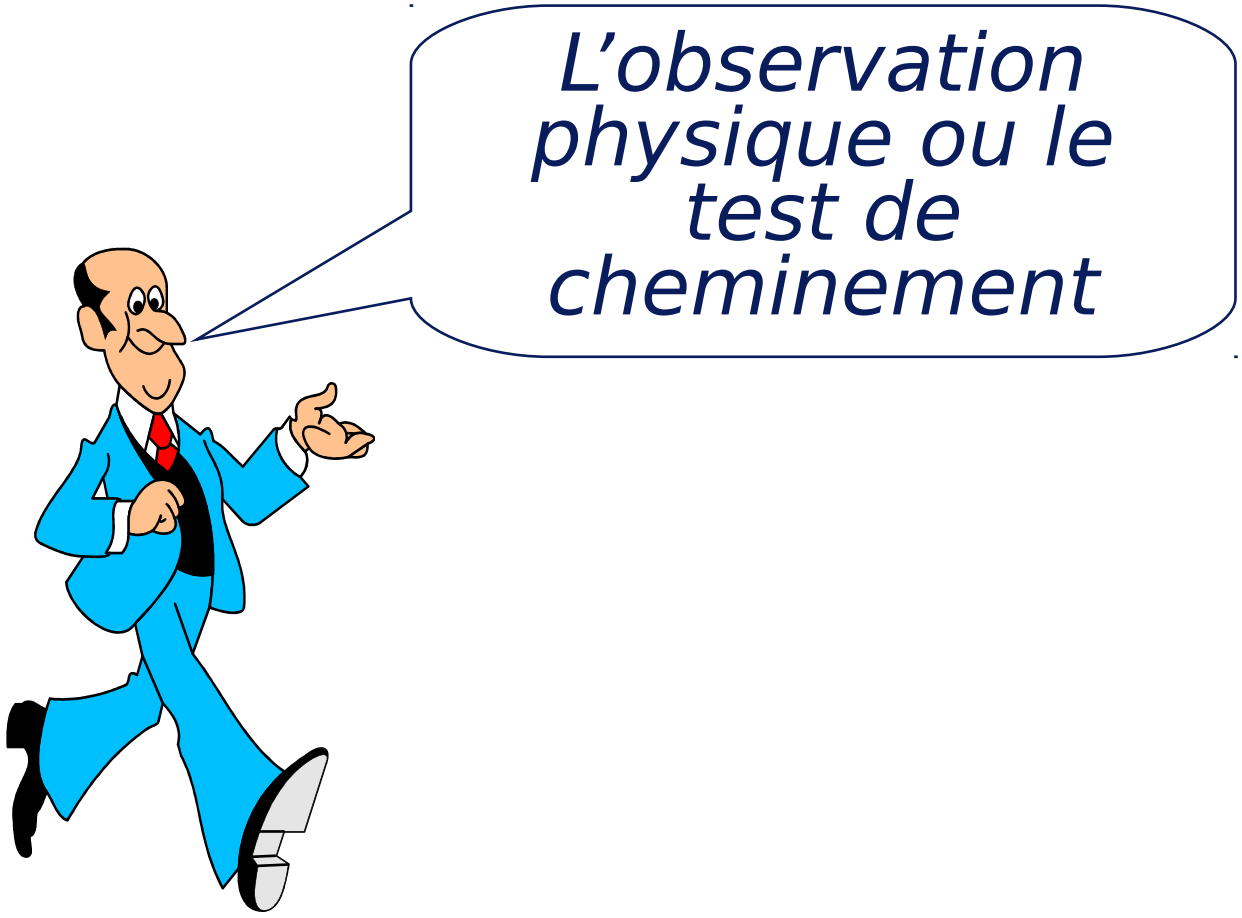
- Le symbole utilisé pour représenter les chèques du personnel imprimés à partir de l'ordinateur est ?

  a. 

  b. 

  c. 

  d. 



Les tests de cheminement (1/2)

- Définition
  - Ils sont aussi appelés "pistes d'audit" ou "chemins d'audit"
  - Il s'agit d'une méthode de test s'appuyant sur un document final ou sur le résultat d'une opération et permettant de remonter à la source en passant par toutes les phases intermédiaires
  - Les caractéristiques de cette méthode sont les suivantes :
    - elle ne concerne qu'une seule opération à la fois
    - elle part du document ou résultat final pour remonter à la source
    - elle permet de contrôler, pour l'opération choisie, tous les stades intermédiaires, leurs justificatifs et justifications

Les tests de cheminement (2/2)

- C'est un outil efficace pour s’assurer de la correcte compréhension du processus et pour matérialiser l’existence des dispositifs de contrôle interne tout au long du processus

- L’importance de garder une trace des pistes d’audit :
  - L’existence de traces permet de signaler et de corriger les erreurs et les exceptions. L’audit interne doit contribuer à l’incorporation de traces concernant les transactions.
  - Aujourd’hui les systèmes d’information ont rendu la traçabilité des transactions invisibles, ce qui constitue un inconvénient pour les auditeurs qui effectuent leurs tests autour du système d’information. Ils sont dépendants de l’intégrité et de la traçabilité à travers le système d’information. De ce fait, ils ne peuvent pas conclure que les données entrées dans le système sont sorties non contaminées. L’audit doit être capable d’analyser les systèmes d’information et ses contrôles. Il doit se faire assister par un expert s’il n’est pas expert dans la matière.

Compréhension des processus et des systèmes

- Réalisation de tests de cheminement (Walkthrough)
  - Consistent à suivre une transaction de son origine jusqu'à sa transcription dans les livres comptables en passant par toutes les étapes intermédiaires
  - Permettent une compréhension en profondeur des flux documentaires
  - Conduisent à la réalisation de diagramme de flux (flowcharts) permettant une représentation schématique précise des flux documentaires

Les pistes d’audit

- Exemples de pistes d’audit :

Objectif de l’existence de la piste d’audit	Exemples de pistes d’audit
S’assurer de l’application des contrôles manuels	• Les factures payées sont tamponnées « Payée ». • Les factures payées sont classées avec la demande d’achats, le bon de commande et le bon de réception.
Identifier les erreurs et les exceptions	• Un état reprenant les écarts (quantité et valeur) entre les factures et les bons de commande. • Une réconciliation bancaire documentée et validée.
S’assurer de l’application des contrôles automatisés.	• Le demandeur d’achats valide la réception des achats sous informatique. • Des contrôles visant à prévenir la saisie de factures en double

La grille de séparation de fonction

- La grille d’analyse est construite afin de :
  - relier l’organigramme fonctionnel à l’organigramme hiérarchique
  - justifier les analyses de postes
  - déceler les manquements à la séparation des tâches
  - Identifier tout conflit ou cumul de tâches traduisant un risque élevé d’erreurs ou de fraude

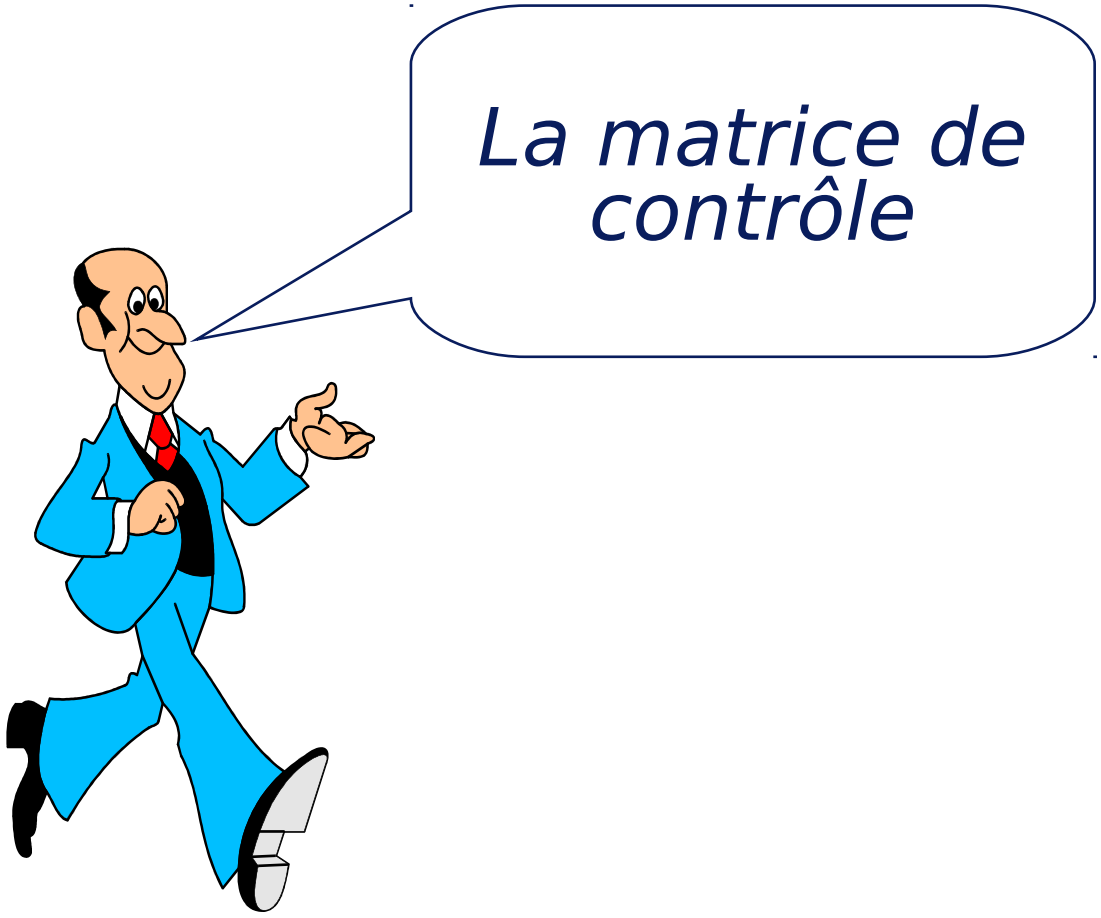
La grille de séparation de fonction

- Les moyens :
  - Utiliser les diagrammes de flux pour identifier les points de contrôles
  - Identifier toute fonction cumulant une combinaison de tâches incompatibles
    - Autorisation + exécution + contrôle + enregistrement

- Les séparations de fonctions et de tâches doivent être correctement reflétées dans les systèmes intégrés (ERP); toutefois leur analyse nécessite l'utilisation d'outils dédiés qui permettent d'interroger les bases et tables dans lesquelles sont contenues les informations / données relatives aux profils utilisateurs (ex: CSI Authorization Auditor pour SAP R/3). Ces analyses sont généralement impossibles à réaliser manuellement
- Cas des organisations de petites tailles
  - Leurs tailles ne permettent pas une séparation des fonctions/tâches appropriée
  - Mise en place de contrôles compensatoires (type supervision) afin de prévenir le risque de fraude et d'erreurs.

Matrice de Séparation des Tâches: Un exemple

Action	Responsable					
	Opérationnel demandeur	Acheteur	Magasinier	Délégataire	Comptable	Autre intervenant
Etablissement des commandes	Non	**Oui**	Non	Non	Non	Non
Autorisation des commandes	Non	Non	Non	**Oui**	Non	Non
Réception	Non	Non	**Oui**	Non	Non	Non
Comparaison commande /facture	Non	Non	**Oui**	Non	Non	Non
Comparaison bon de réception /facture	Non	**Oui**	Non	Non	Non	Non
Imputation comptable	**Oui**	**Oui**	Non	Non	Non	Non
Vérification de l'imputation comptable	Non	**Oui**	Non	Non	**Oui**	Non
Bon à Payer	**Oui**	Non	Non	Non	Non	Non
tenue du journal des achats	Non	Non	Non	Non	**Oui**	Non
tenue du compte fournisseurs	Non	Non	Non	Non	Non	**Oui**
Rapprochement relevés fournisseurs avec les comptes	Non	Non	Non	Non	**Oui**	Non
Rapprochement de la balance fournisseurs avec le compte collectif	Non	Non	Non	Non	**Oui**	Non
Signature des chèques	Non	Non	Non	**Oui**	Non	Non
Envoi des chèques	Non	Non	Non	Non	Non	**Oui**
Acceptation des traites	Non	Non	Non	**Oui**	Non	Non
Tenue du journal des effets à payer	Non	Non	Non	Non	**Oui**	Non
Accès à la comptabilité générale	Non	Non		Non	**Oui**	Non



La matrice de contrôle

- Outil essentiel dans le cadre de SOX section 404
- La matrice de contrôle décrit de manière méthodologique et structurée les contrôles mis en œuvre destinés à réduire les risques identifiés
- Pour chaque cycle/processus la matrice de contrôle comprend les éléments clé suivants:
  - Risque inhérent
  - Activité de contrôle et objectif de contrôle (inverse du risque inhérent)
  - Type de contrôle: manuel ou automatisé (application control), transactionnel ou de supervision, préventif ou détectif
  - Documentation du contrôle (input/output) et personnes en charge de le réaliser
- La matrice découpe les processus/cycles en objets/étapes auditables qui suivent le cheminement des opérations

Exemple de matrice des contrôles et des risques

Processus	Sous-processus	Assertions						N°du risque	Description du risque	N°de contrôle	Description de l'activité de contrôle	Contrôle préventif ou détectif? (P/D)	Contrôle manuel ou par le système? (M/S)	Niveau de risque	Fréquence
		Occurrence	Exhaustivité	Droits et obligations	Evaluation	Rattachement	Présentation								
Achat	1			•				R1	Les bons de commande sont préparés sans de demandes d'achats validées	C1	Les demandes d'achats sont revues et approuvées par le directeur de la production avant d'être saisies en bons de commandes dans le système d'informations	P	M		sur occurrence
Achat	1		•					R2	Omission de la saisie d'un bon de commande sous le système d'informations	C2	Vérification que chaque demande d'achat a un bon de commande correspondant	P	M		sur occurrence
Achat	1		•					R3	L'exhaustivité des bons de commandes n'ont pas été envoyés aux fournisseurs	C3	Un rapport informatique heddomadaire alerte le Directeur Achat sur les écarts entre les bons de commande saisis et ceux envoyés aux fournisseurs	D	S		hebdomadaire

Les Outils Informatiques

Les outils informatiques : Formalisation

- 3 outils de bureautique essentiels constituent la trousse à outils quotidienne de l'auditeur
  - **Un traitement de texte (de type Word)**
    - C'est l'outil des échanges formalisés de courrier : lettre de mission, échanges divers
  - **Un tableur (de type Excel)**
    - Elaboration de tableaux d'analyse, représentations graphiques, tris des données
  - **Un logiciel de présentation (de type Powerpoint)**
    - Pour la synthèse et la présentation des résultats

Outils informatiques : Présentation d’ACL

- ACL (Audit Command Language) est un produit canadien conçu au début des années 70 comme outil d’enseignement.

- Depuis, diverses améliorations ont été apportées à l’application. Un grand nombre de celles-ci ont été le fruit des tests réalisés par Deloitte & Touche et les cabinets du réseau DTT qui est fondamentalement indépendant d'ACL et réciproquement.

Outils informatiques : ACL
Ses points forts

- Logiciel sous Windows avec 3 modes de fonctionnement :
  - Menus déroulants
  - Interactif
  - Batch (automatisation des tâches récurrentes)

- Analyse sur des "copies" de bases/fichiers
  - Pas d'interférences possible avec et sur les applications

- Résultats quasi immédiat pour des analyses simples

Outils informatiques : ACL
Ses points forts

- Fonctionnalités d'audit et d'analyse de données prédéfinies
  - Contrôler les séquences (ruptures et doublons)
  - Importer / Exporter et extraire
  - Totaliser -Stratifier – Classifier des champs clés
  - Echantillonner /Statistiques simples
  - Effectuer des calculs simples et complexes
  - Joindre - Fusionner - Trier - Nettoyer des fichiers

Outils informatiques : ACL
Ses points forts

- Modification des données sources impossible
  - Outil en lecture seule
  - Traçabilité et auditabilité parfaite
  - Existence d'un fichier LOG
  - Capacités d'interrogation interactive et visuelle
  - Rapidité de déploiement et de traitement
  - Taille de fichier illimitée
  - Lecture de types de données multiples et sans conversion
  - SAP, Micro, Mainframe, Mini, délimitée, dbase, ODBC...
  - Fonctions de génération de rapports de qualité et rapide
  - Réutilisable dans tous les domaines d'applications d'une entreprise
  - Utilisable par des "non informaticiens"

Outils d'audit et de contrôle interne
Base de données des risques et contrôles

Rack Knowledge Base