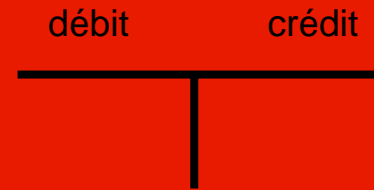


LES  
CONFÉRENCES  
de

**L'Académie**  
SCIENCES TECHNIQUES COMPTABLES FINANCIÈRES

# Convergence des Systèmes d'information et des Systèmes comptables :

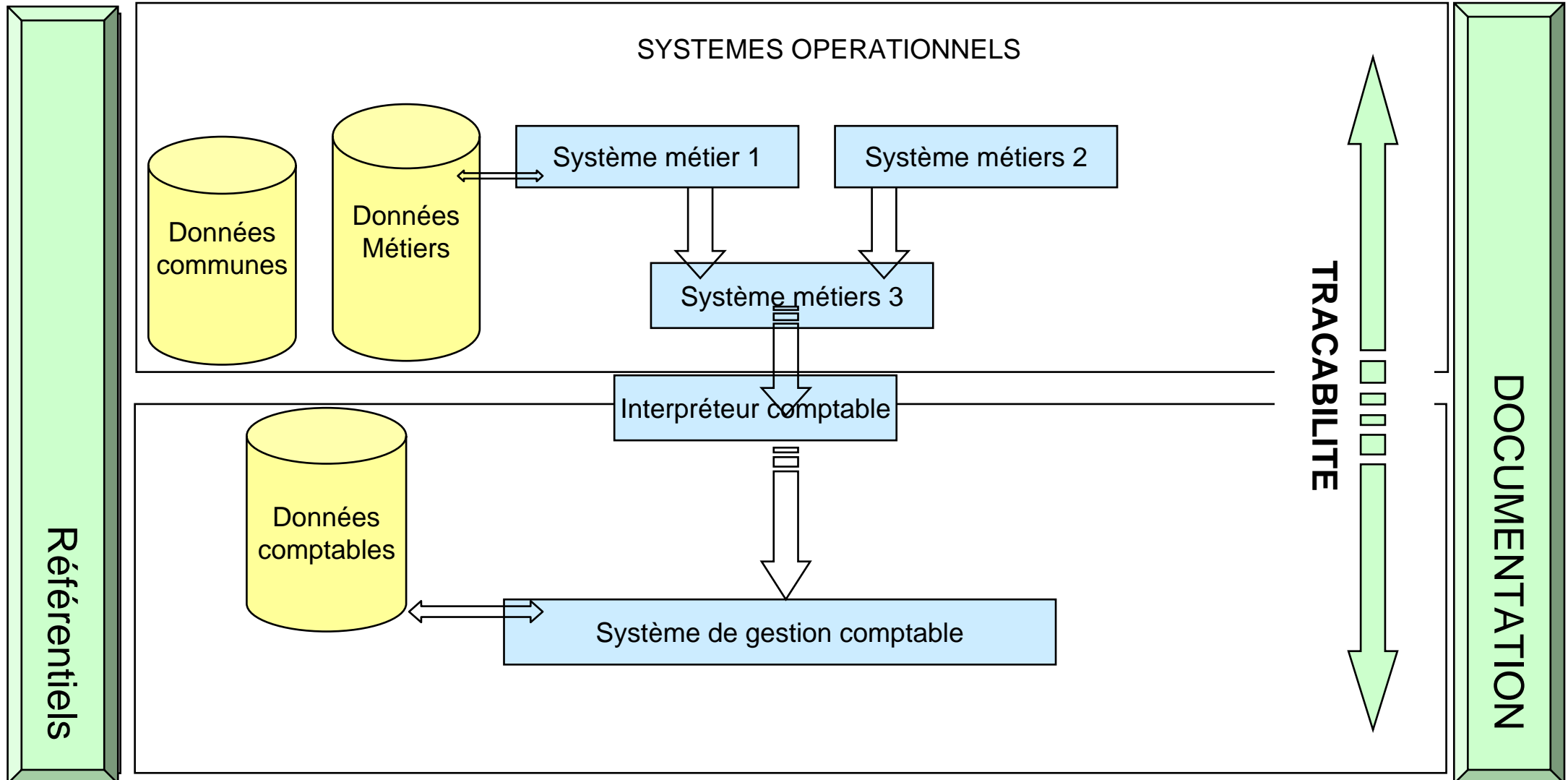
## Introduction : présentation des sujets d'étude



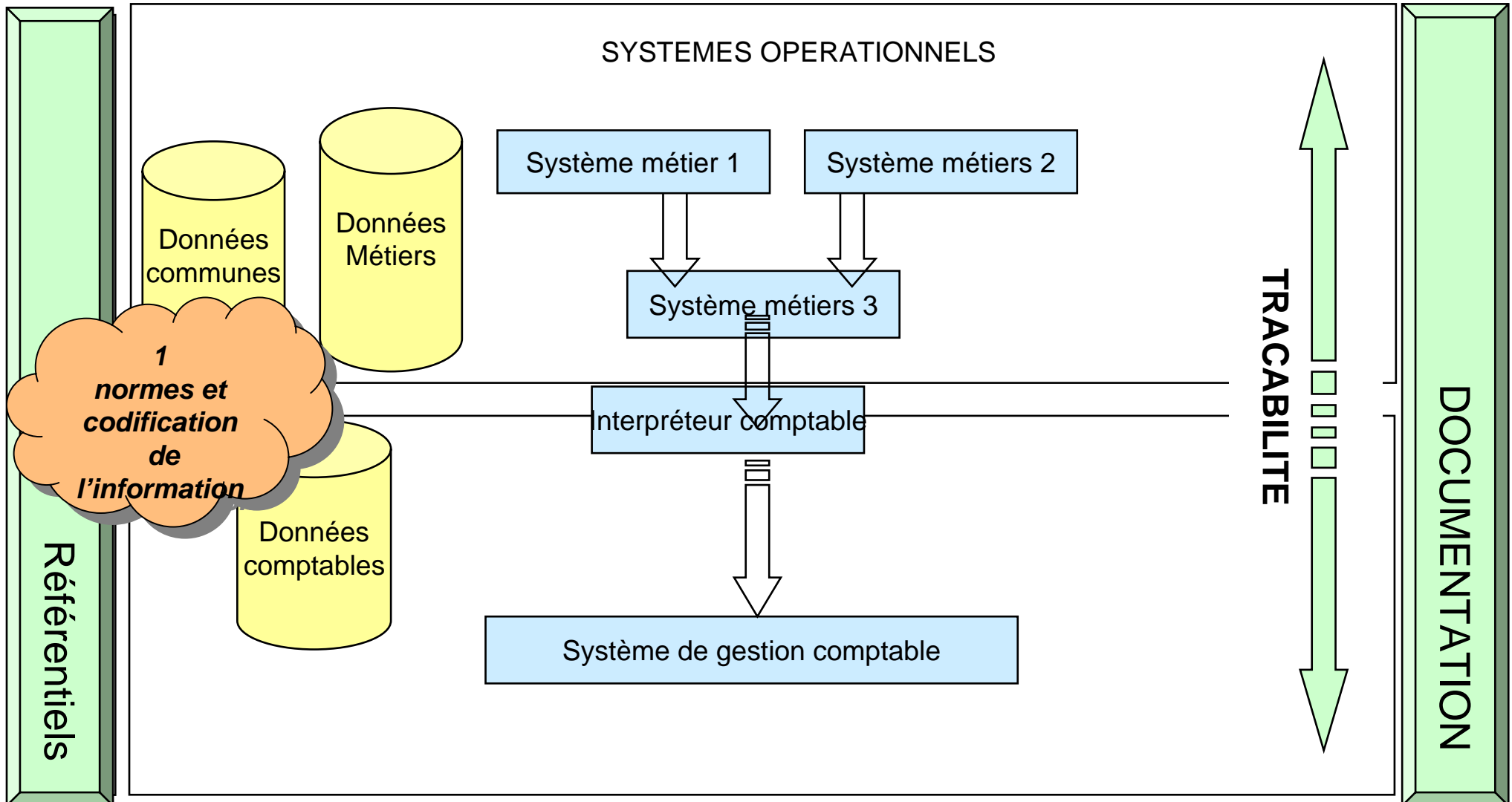
les systèmes d'information « externalisent » de plus en plus les informations économiques et financières en dehors des systèmes comptables et ont tendance à s'éloigner de la rigueur des normes comptables. Cette « externalisation » présente un risque majeur en matière de fiabilité du systèmes d'information et du contrôle interne des entreprises.

Comment, sans contraindre l'évolution technologique, intégrer dans la logique des systèmes d'information les principes fondamentaux qui garantissent la fiabilité du système comptable

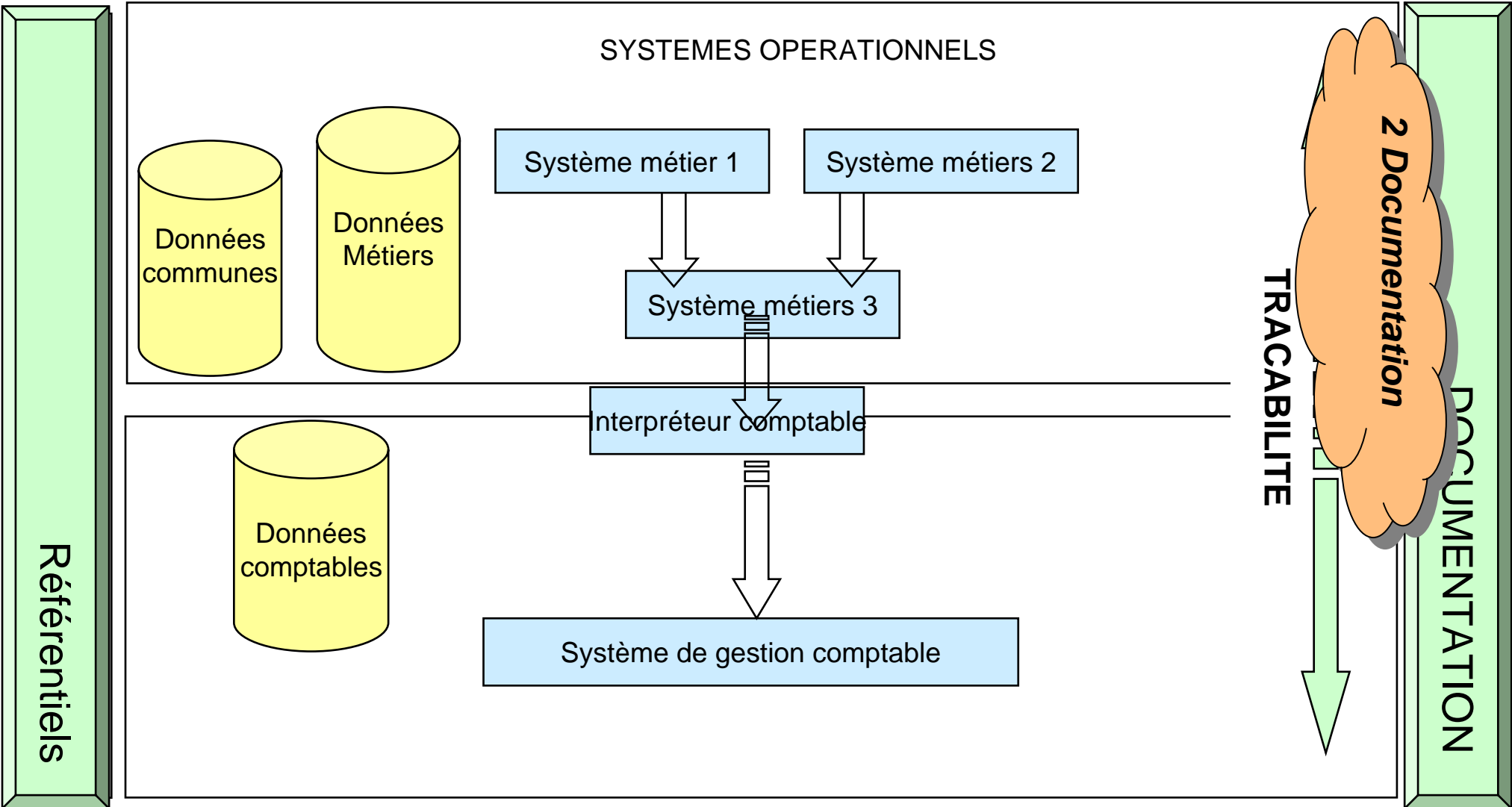
# GOUVERNANCE



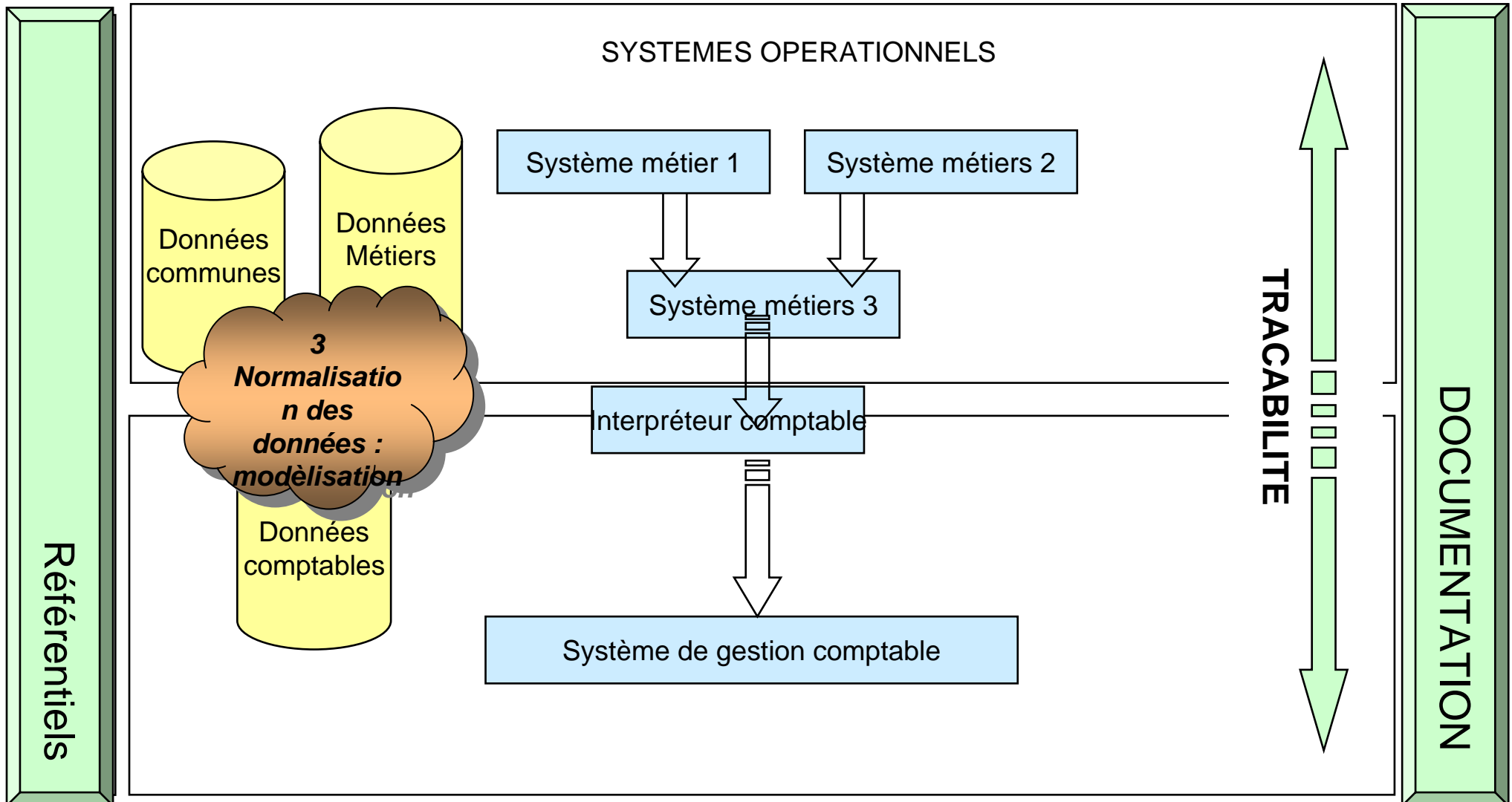
# GOUVERNANCE



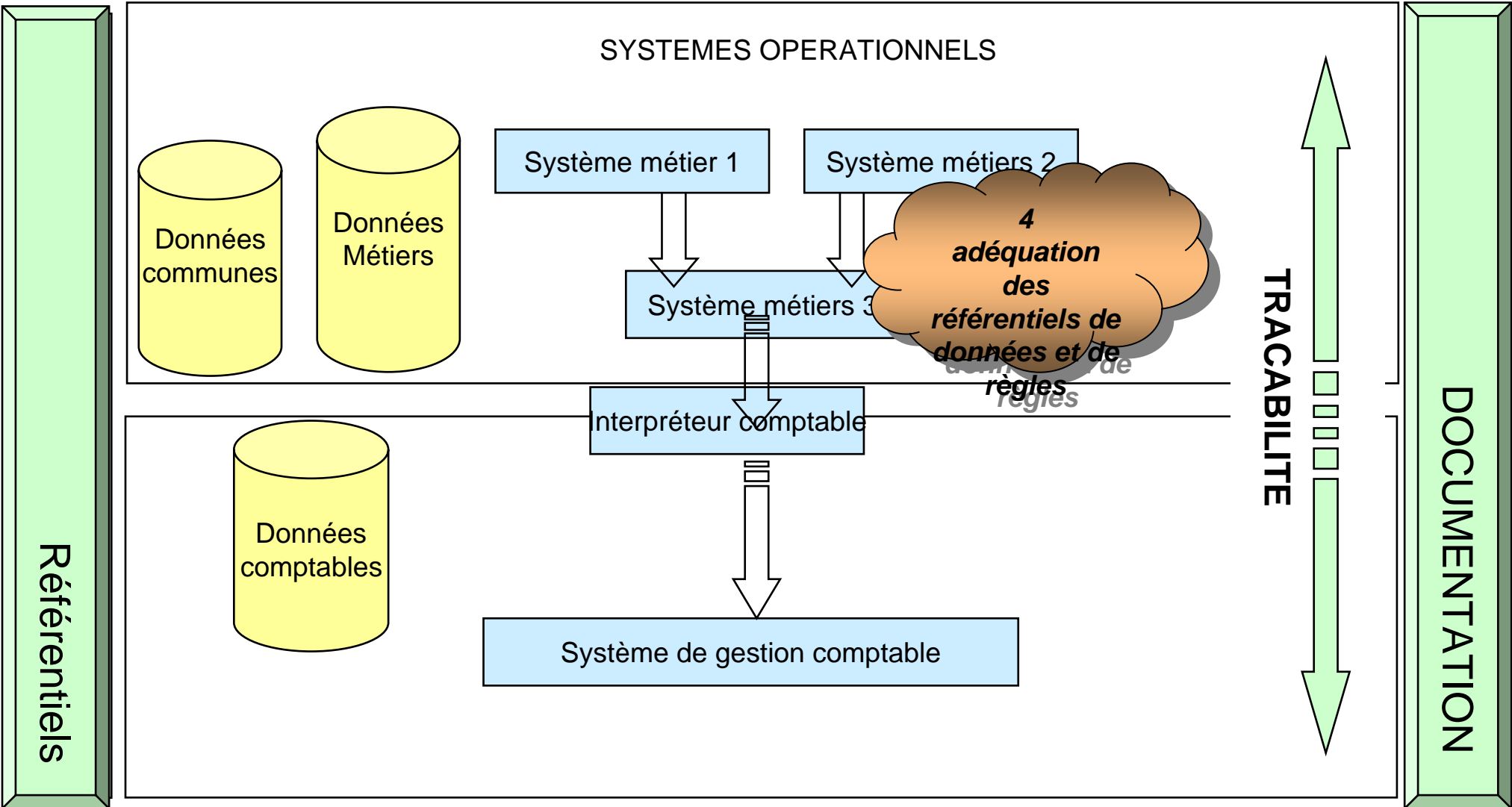
**GOUVERNANCE**



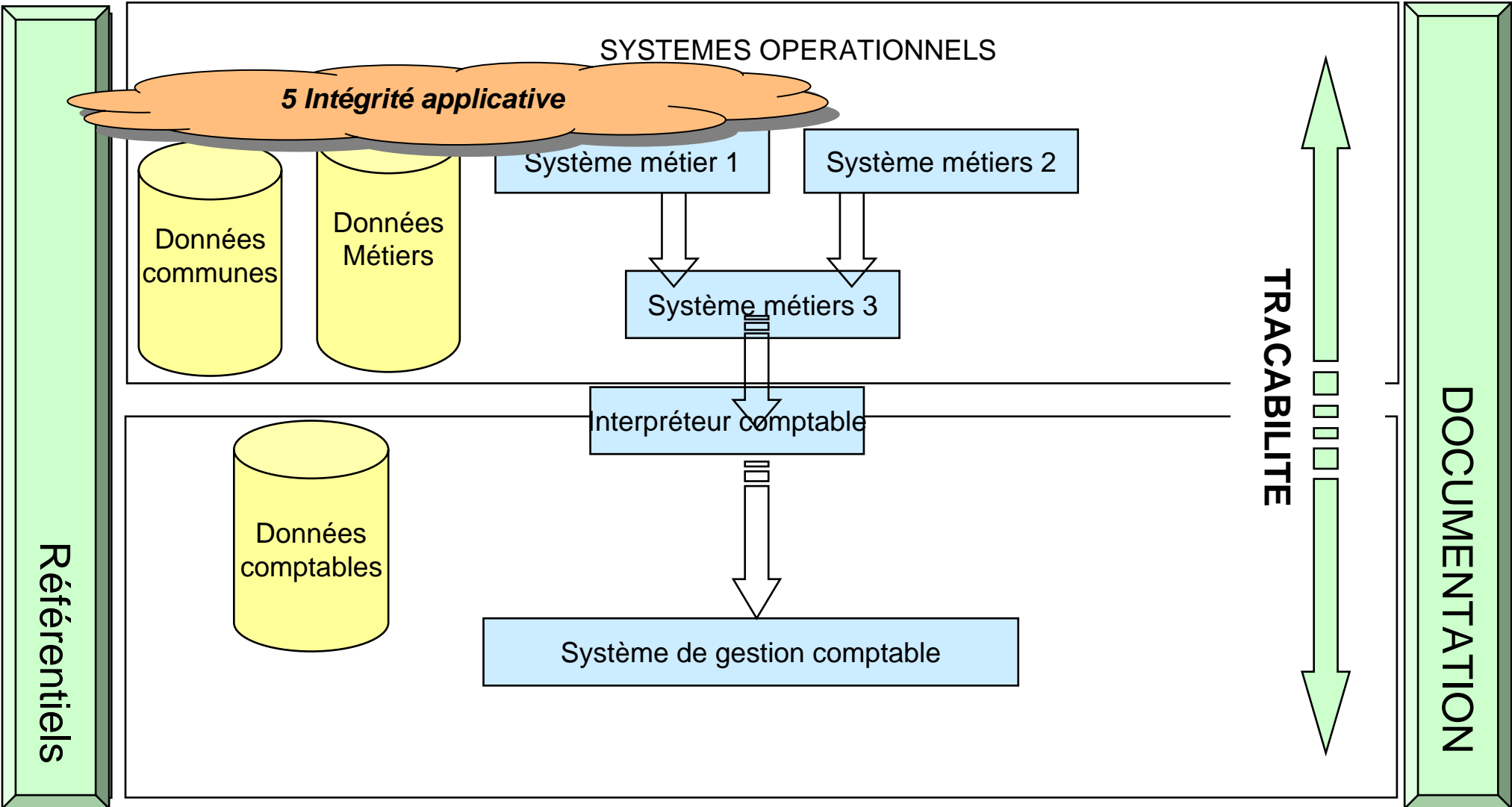
# GOUVERNANCE



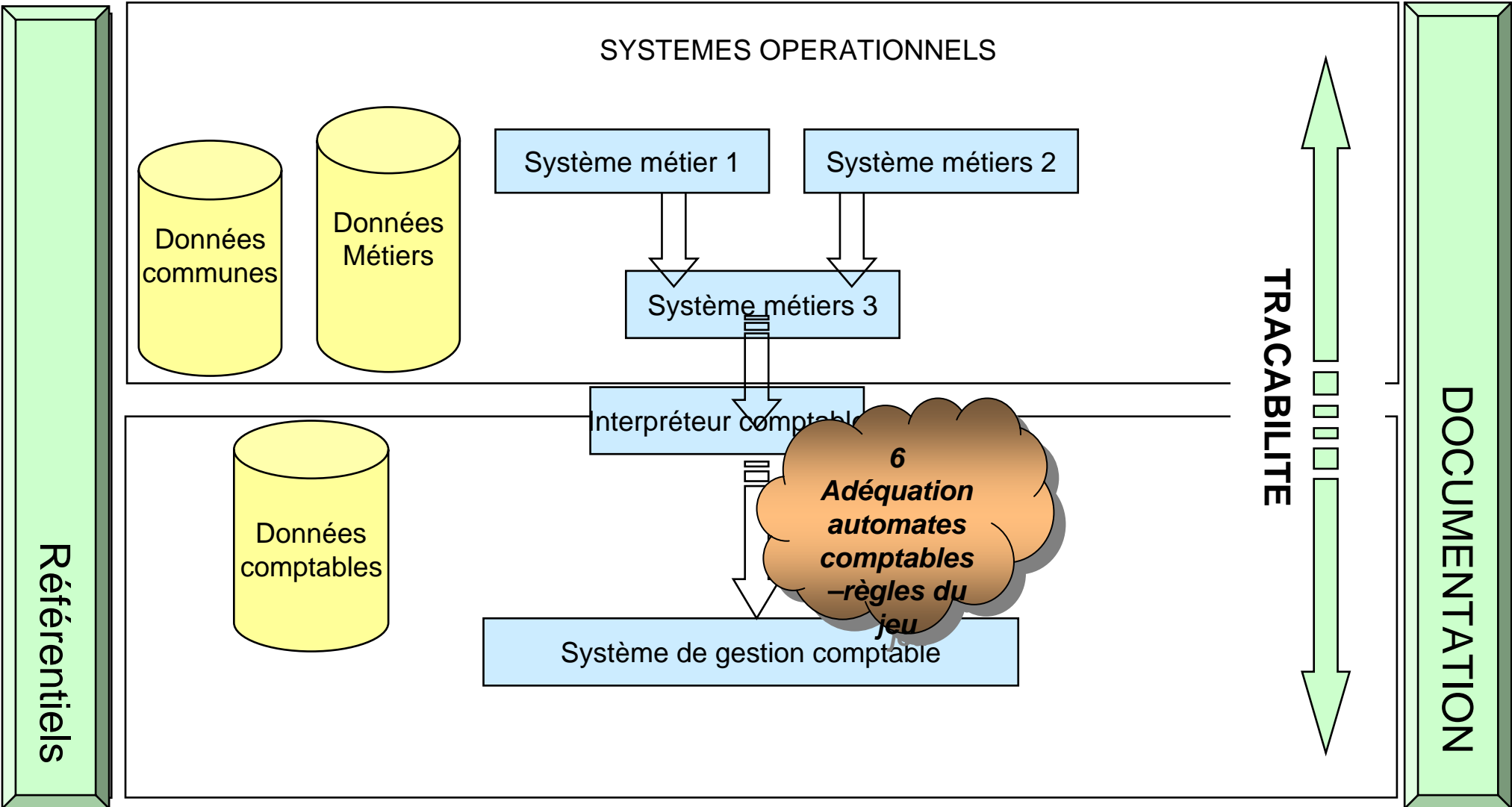
**GOUVERNANCE**



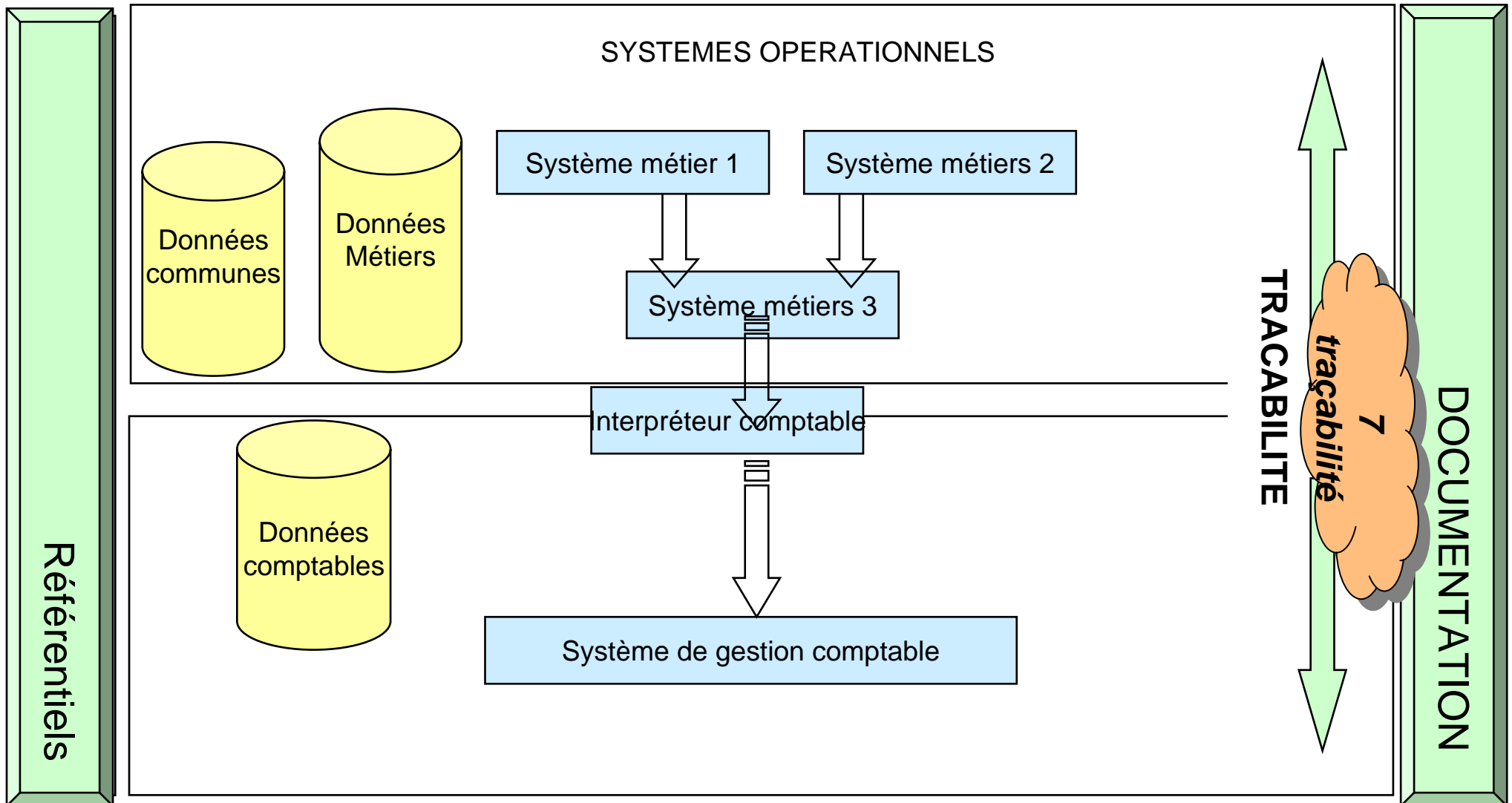
# GOVERNANCE

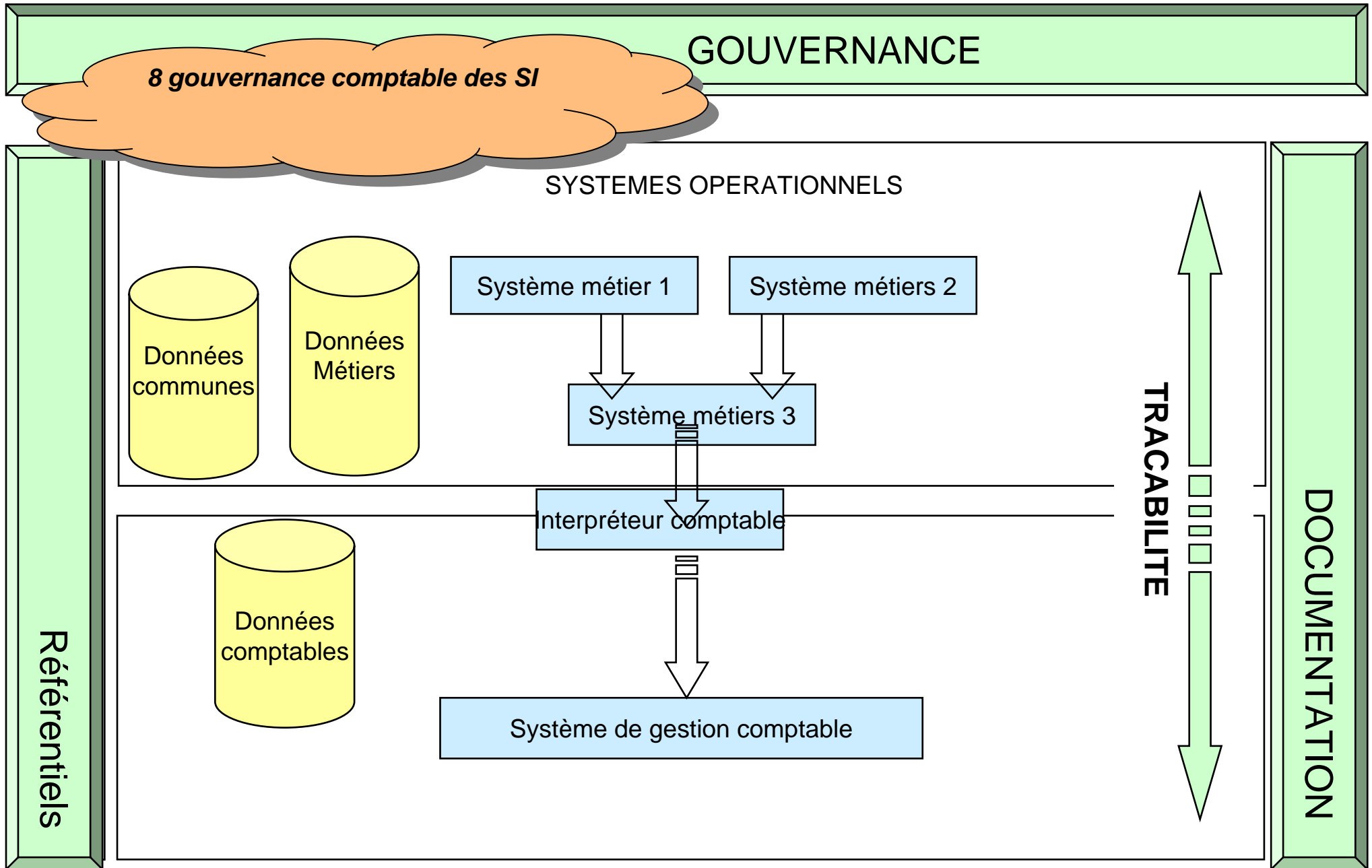


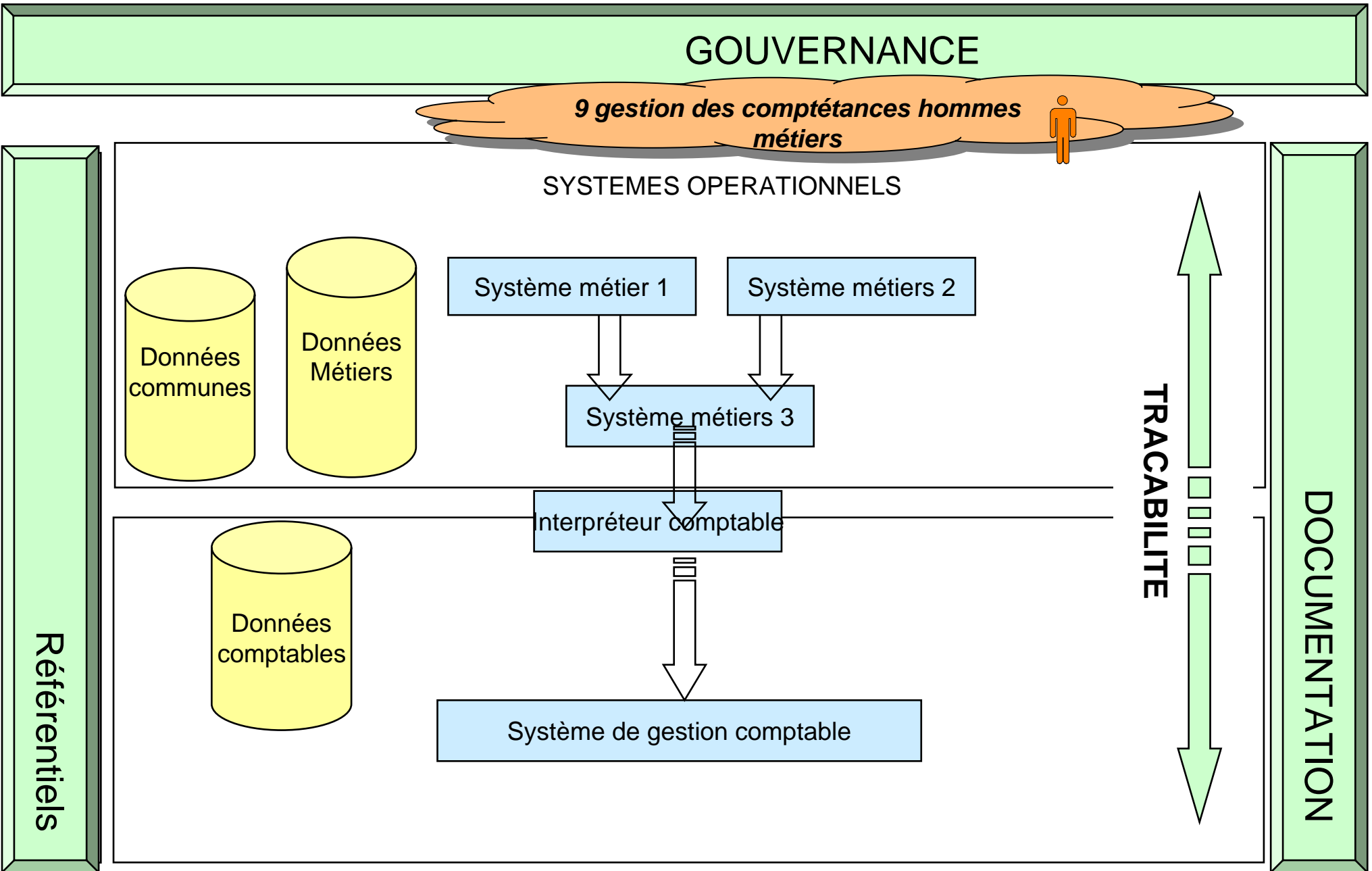
# GOVERNANCE

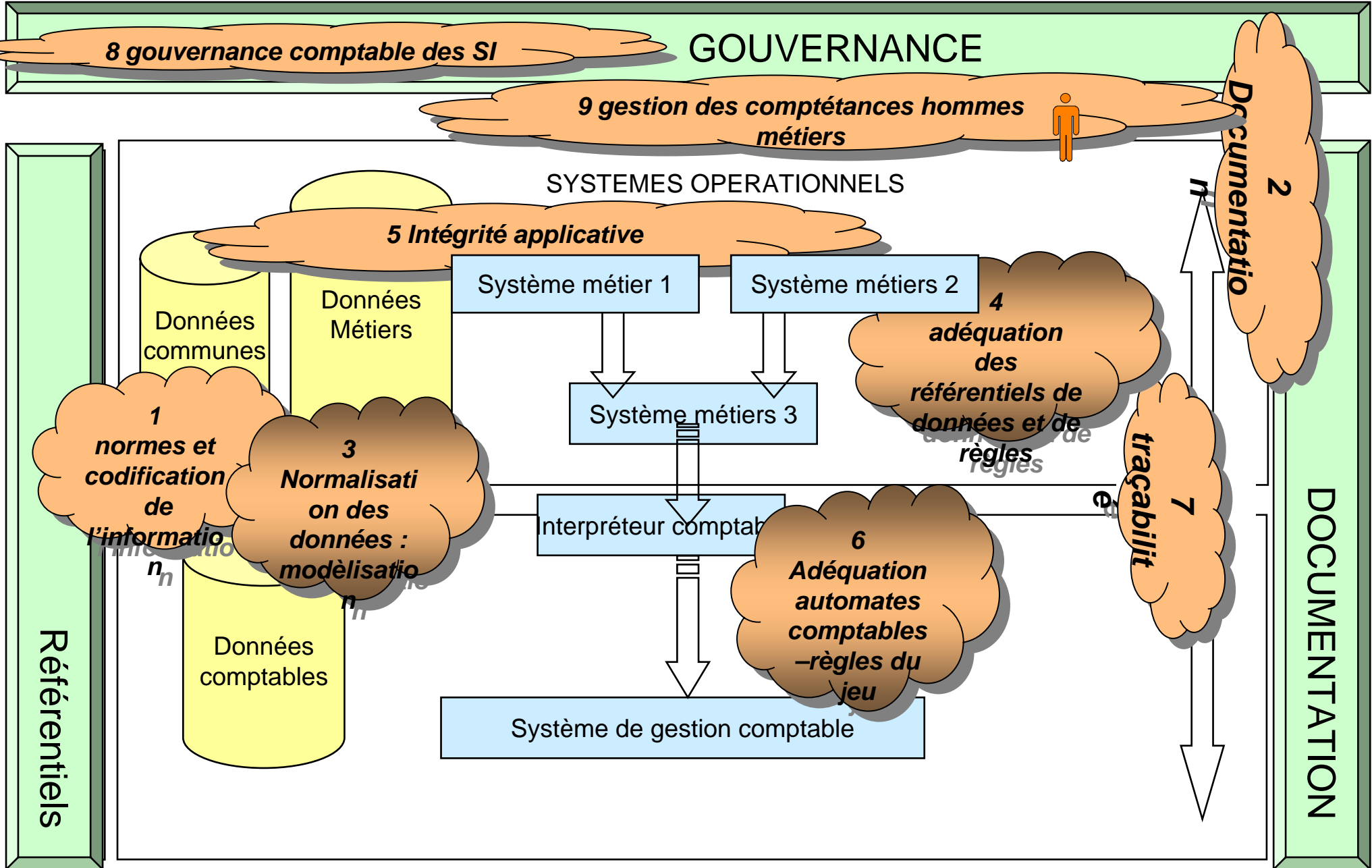


# GOVERNANCE









# Rôle du responsable comptable et financier dans la gouvernance du SI

**Serge Yablonsky**  
**Moore Stephens**  
**SYC**

## *Gouvernance d'Entreprise*

### Gouvernement d'Entreprise

- Direction Générale
- Conseil d'Administration et de Surveillance
- Comité d'Audit
- Comité des Rémunérations
- Gestion des Risques
- Audit Interne

**CONFORMITE  
CERTIFICATION**

### Gouvernance des activités métiers

- Vision et Alignement stratégique
- Processus de Décision Stratégique
- Tableau de bord, mesure de l'atteinte des objectifs stratégiques et de la performance
- Système d'information stratégique
- Amélioration continue

**CREATION DE VALEUR  
UTILISATION DES RESSOURCES**

La responsabilité du professionnel comptable et financier apparaît à trois niveaux :

- La garantie d'une information comptable et financière fiable ;
- L'organisation des systèmes ;
- La mesure des performances de l'entreprise.

## La garantie d'une information comptable et financière fiable

- Etre un interlocuteur incontournable et privilégié dans les projets informatiques
- Avoir accès à l'information et au système d'information pour la maintenance de ses paramètres

## L'organisation des systèmes

- Reconnaître sa légitimité dans tous les systèmes de l'entreprise
  - Bénéficier d'un accès permanent à tout type d'information
- Émettre des recommandations d'amélioration y compris Contrôle interne
  - Agir sur l'organisation, les tâches manuelles et les tâches informatisées

## La mesure des performances de l'entreprise

- Comprendre et maîtriser les outils d'Infocentre
- Assurer la maîtrise d'ouvrage de son système d'information décisionnel (Infocentre, *Business Intelligence*, etc.)
- Droit à recevoir l'information chiffrée, ou non, nécessaire pour la mesure de la performance par rapport à la stratégie de l'entreprise et aux objectifs par processus
- Nécessité de recevoir l'information sur la cartographie et l'évaluation chiffrée des risques

## Questions au responsable comptable et financier ? 1/2

- Avez-vous un tableau de bord de suivi de votre SI comptable couvrant notamment :
  - le bon déroulement des interfaces et le suivi des rejets ?
  - Le nombre d'appels pour maintenance en souffrance et depuis combien de temps?
  - la liste des projets en cours avec impact sur le SI Finance et la planification correspondante de la MOA finance
  - la mesure de la satisfaction des utilisateurs du SI finance (disponibilité, ergonomie, couverture fonctionnelle, ...) ?
  - la mesure de la satisfaction des clients de la Finance ?

## Questions au responsable comptable et financier ? 2/2

- Avez-vous des responsabilités affichées en matière de Gouvernance du SI Finance ?
- Participez-vous à des réunions formelles d'évolution du SI :
  - Finance ?
  - Métiers ?
- Avez-vous un processus d'analyse et d'information sur les impacts des nouveautés comptables sur le SI ?

## Conclusion

- Un rôle majeur pour la qualité de l'information
- Un rôle majeur pour la qualité du système d'information
- Un rôle majeur pour la qualité du contrôle interne
- Un rôle majeur pour la qualité de l'analyse des risques y compris informatiques

# La traçabilité

**Franck Saada**  
**Senior Manager Ernst & Young**

**Jean Florent Girault**  
**Associé Ernst & Young**

## La traçabilité : définition et vocabulaire

- Le dictionnaire « Le Petit Robert » définit la traçabilité comme la : « possibilité d'identifier l'origine et de reconstituer le parcours (d'un produit), depuis sa production jusqu'à sa diffusion ».
- La norme « NF EN ISO 8402 » et la norme française NF X50-120 définissent également la traçabilité : elle représente l'« aptitude à retrouver l'historique, l'utilisation ou la localisation d'une entité au moyen d'identifications enregistrées ».
  - ➔ **Toute la problématique de telles définitions appliquées aux informations porte sur l'immatérialité du « produit » information comptable et financière et la dématérialisation des pièces justificatives**
  - ➔ Sans compter que le format de cette donnée qu'elle véhicule varie en fonction du système qui la reçoit.
- **Traçabilité, piste d'audit, chemin de révision**, autant de mots pour définir un concept qui diffère uniquement selon l'acteur concerné :
  - ➔ la traçabilité utilisée par tous les professionnels dont le sujet est au cœur de leurs préoccupations (par exemple, le professionnel du secteur alimentaire utilise souvent ce terme car la traçabilité alimentaire est devenue un enjeu majeur de société).
  - ➔ la piste d'audit est souvent employée par l'auditeur,
  - ➔ le chemin de révision est plutôt le langage de par l'expert –comptable,
- Mais, quelque soit l'acteur concerné, le concept reste identique : nous emploierons donc indifféremment ces trois termes dans la suite de cette présentation.

## La traçabilité des informations comptables et financières

- La traçabilité a pris une importance significative dans les problématiques d'élaboration et de production de l'information comptable et financière compte tenu :
  - de la mondialisation des organisations, et par conséquent de la diversification des sources d'information
  - de la production de masse et de la complexité de l'information liées à l'utilisation de l'informatique à tous les échelons de l'entreprise,
  - De la forte automatisation du process de transformation des données de gestion en information comptable et financière (« phénomène de boîte noire »)
  - de l'évolution de la réglementation (notamment le Sarbanes Oxley Act aux Etats-Unis et la Loi de Sécurité Financière en France, les normes IFRS ainsi que Basle 2) et des impératifs de sécurité de l'information ;
  - de l'évolution du contexte concurrentiel supposant des prises de décision toujours plus rapides
  - des nouvelles normes professionnelles d'audit, notamment les normes NEP 315 et 330 dans le cadre de référence normatif du Commissaire Aux Comptes.

# SOMMAIRE

- LES ENJEUX DE LA TRACABILITE
- LA MISE EN ŒUVRE DE LA TRACABILITE
- LA MAITRISE DE LA TRACABILITE
- CONCLUSION

# 1. Les enjeux de la traçabilité

## Enjeux financiers et comptables

- **La traçabilité de l'information est une** garantie de la validité et de la qualité des informations comptables et financières **qui trouve ses fondements dans les principes comptables (norme française), notamment :**
  - ➔ le principe d'image fidèle,
  - ➔ le principe de permanence des méthodes,
  - ➔ le principe de continuité d'exploitation,
  - ➔ le principe de séparation des exercices,
  - ➔ Le principe d'intangibilité du bilan d'ouverture.
  
- >> **piste d'audit "statique" (traçabilité de l'information au travers des flux)**
  
- >> **piste d'audit "dynamique" (traçabilité d'un solde d'un exercice à l'autre).**

# 1. Les enjeux de la traçabilité

## Enjeux opérationnels

- Les enjeux opérationnels liés à la traçabilité portent sur trois éléments :
  - l'auditabilité **de l'information à travers les flux qu'elle génère** à l'aide d'attributs détaillant tout le parcours de l'information : de son point de départ (donnée d'origine), sa route empruntée (applications...), sa durée de parcours (datation), ses rencontres faites (identification des retraitements, processus, paramétrage...) à son point d'arrivée (Nom de l'état de restitution, nom de la donnée comptable...)
  - **la sécurisation de l'information en termes de qualité (contrôle d'accès aux données) et de protection des informations (plan de continuité informatique...),**
  - l'homogénéisation, de normalisation et l'optimisation **du système d'information**, en formant une cohérence des données (assurée par le "lien" qui est véhiculé tout au long du "fil rouge") dans des systèmes d'information de plus en plus complexes.

# 1. Les enjeux de la traçabilité

## Enjeux réglementaires

- La notion de « traçabilité » est issue du corpus réglementaire relatif à la piste d'audit comptable et également des nouvelles réglementations portant sur l'évaluation du contrôle interne du processus d'élaboration des états financiers
- Les principaux textes réglementaires traitant de la « traçabilité » de l'information sont : le Plan Comptable Général 2005, le Code du commerce, le Contrôle fiscal des comptabilités informatisées

### Plan Comptable Général 2005

Article 410-3 : Chemin de révision

L'organisation du système de traitement permet de reconstituer à partir des pièces justificatives appuyant les données entrées, les éléments des comptes, états et renseignements, soumis à la vérification, ou, à partir de ces comptes, états et renseignements, de retrouver ces données et les pièces justificatives

Article 420-2 : Mentions minimales d'un enregistrement

Tout enregistrement comptable précise l'origine, le contenu et l'imputation de chaque donnée, ainsi que les références de la pièce justificative qui l'appuie

### Code du commerce – Chapitre III, Des obligations générales des commerçants

Article L123-12

Toute personne physique ou morale ayant la qualité de commerçant doit procéder à l'enregistrement comptable des mouvements affectant le patrimoine de son entreprise. Ces mouvements sont enregistrés chronologiquement.

# 1. Les enjeux de la traçabilité

## Enjeux réglementaires

### Contrôle Fiscal des Comptabilités Informatisées

BOI 13 L-6-91

**« ... en vue de préserver la fiabilité du chemin de révision, les entreprises doivent conserver :**

- Les éléments d'information intégrés dans un système informatique sous une forme conventionnelle pour être conservés, traités ou communiqués ;
- L'ensemble des opérations réalisées par des moyens automatiques pour permettre l'exploitation de ces éléments et notamment leur collecte, leur saisie, leur enregistrement, leur modification, leur classement, leur tri, leur conservation, leur destruction, leur édition.

# 1. Les enjeux de la traçabilité

## Enjeux réglementaires

### Réglementation Bancaire

le CRBF 97-02 : Article 12  
– La piste d’audit, modifié par  
le CRBF 2001-01, 2004-02

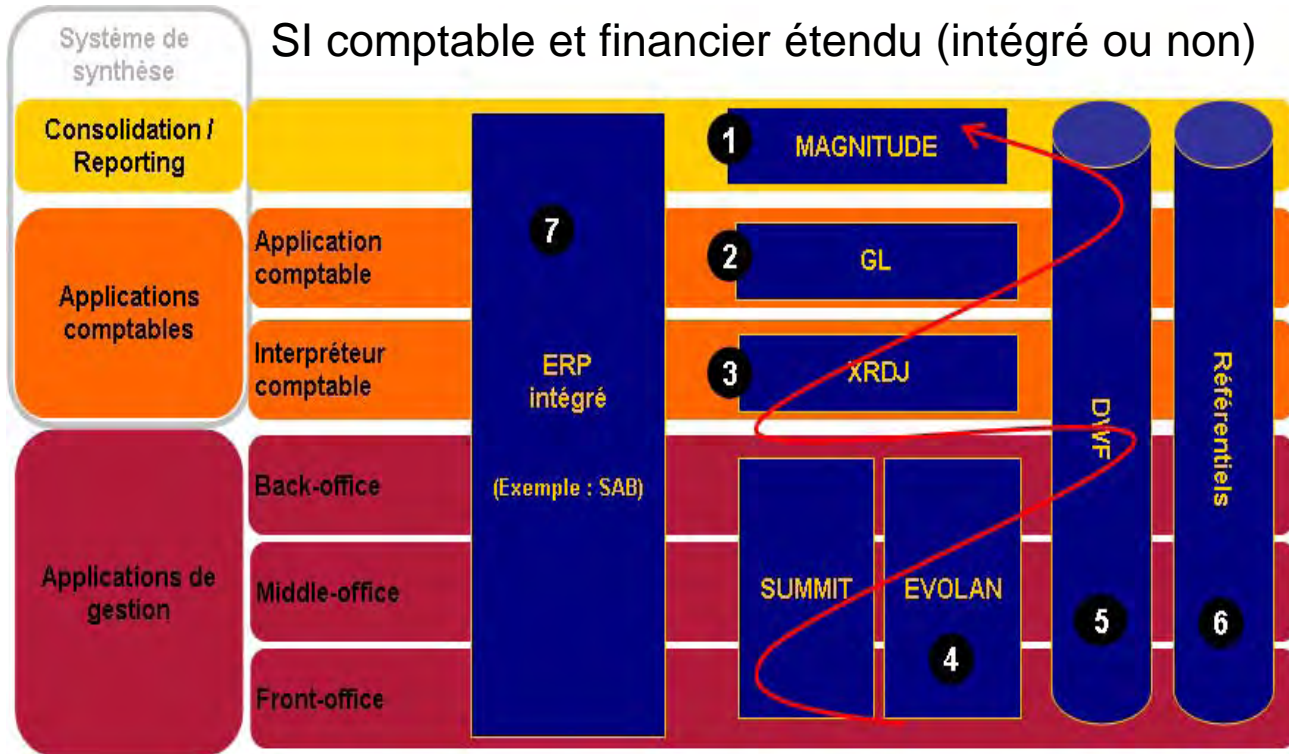
**« En ce qui concerne l'information comprise dans les comptes de bilan et de résultats publiés ainsi que les informations de l'annexe issues de la comptabilité, l'organisation mise en place doit garantir l'existence d'un ensemble de procédures, appelé piste d'audit, qui permet :**

- de reconstituer dans un ordre chronologique les opérations
- de justifier toute information par une pièce d'origine à partir de laquelle il doit être possible de remonter par un cheminement ininterrompu au document de synthèse et réciproquement
- d'expliquer l'évolution des soldes d'un arrêté à l'autre par la conservation des mouvements ayant affecté les postes comptables...»

- Ces textes traitent de la traçabilité de l'information contenue dans les états financiers. Ils induisent, au même titre que les enjeux comptables, financiers et opérationnels, la mise en œuvre de fonctionnalités obligatoires dans le système d'information des entreprises

## 2. Mise en œuvre de la traçabilité

La traçabilité au cœur de la logique de transformation de l'information comptable et financière



### ❶ Consolidation et reporting :

Construction et suivi des états financiers et réglementaires

### ❷ Application comptable :

Enregistrement des écritures comptables

### ❸ Interpréteur comptable :

Pont entre les applicatifs métier et les progiciels comptables

### ❹ Applications de gestion :

Points d'entrée des événements de gestion

### ❺ DataWarehouse Financier :

Outil d'aide à la décision

### ❻ Référentiels :

Ensemble de données de référence

### ❼ ERP :

Progiciel de gestion intégré couvrant différentes couches applicatives

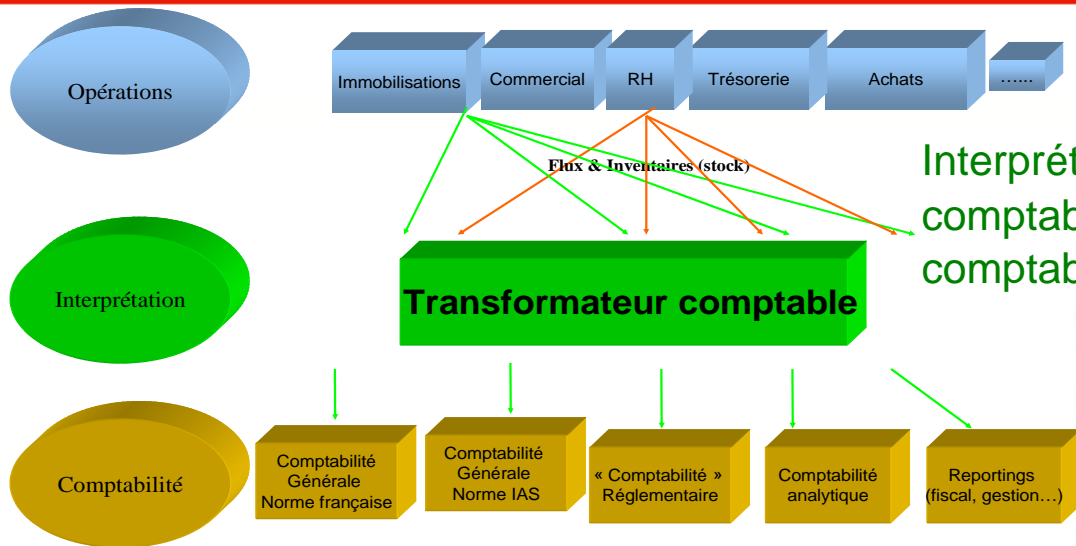
### Légende

Couches applicatives Applications Base de données

Fil rouge

## 2. Mise en œuvre de la traçabilité

La logique de transformation dans le cadre d'une architecture présentant un interpréteur comptable



Interpréteur transformant l'information de gestion en information comptable sur la base de référentiels (événements, comptes comptables, schémas...)

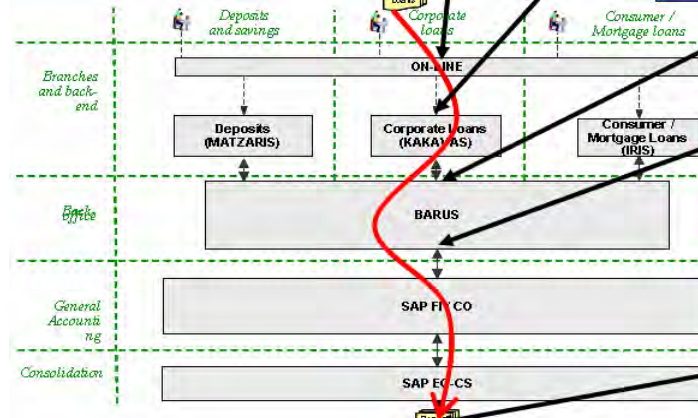
| Loan contract |           | Client Name      | Start date | Duration | Loan type | Currency | Rating   |                   |
|---------------|-----------|------------------|------------|----------|-----------|----------|----------|-------------------|
| AZE4356F      | 654376875 | M. Dupond        | 12032007   | 24032007 | 23032017  | 10 ZA2   | Conso 56 | 0 EUR 8500 A2 ... |
| Loan #        | Client #  | Transaction date | End date   | Agency # | Status    | Account  |          |                   |

| Operation: Principal reimbursement |                |          |         |
|------------------------------------|----------------|----------|---------|
| Operation #                        | Operation date |          |         |
| 234                                | AZE4356F       | 14042007 | 850 ... |
| Loan #                             | Amount         |          |         |

| Accounting entries |                |
|--------------------|----------------|
| Client 65437687501 | Loan 654376875 |
| 850                | 850            |

| Monthly aggregation    |          |             |
|------------------------|----------|-------------|
| -20312 personal loans. | 14042007 | 2511 Client |
| 3.344.324              |          | 3.344.324   |

| Financial statements |  |
|----------------------|--|
|                      |  |



Chaine complexe de production de l'information comptable et financière via des systèmes d'information intégrés ou non intégrés

## 2. Mise en œuvre de la traçabilité

### Piste d'audit – clé de voûte de la traçabilité

- La piste d'audit doit permettre de retracer les différentes transformations des flux de données de gestion en flux comptables et financiers et concrètement suivre le fil rouge.
- Pour cela, la piste d'audit doit couvrir quatre fonctions à mettre en œuvre dans le système d'information comptable et financier étendu de l'entreprise :
  - ➔ **Fonction 1** : la reconstitution de l'ordre chronologique des opérations
  - ➔ **Fonction 2** : la justification des informations présentes dans les comptes et états financiers par les informations de gestion à leur origine et inversement (piste d'audit statique)
  - ➔ **Fonction 3** : la justification de l'évolution des informations d'une date à une autre (piste d'audit dynamique)
  - ➔ **Fonction 4** : la reconstitution du chemin de révision, à partir des données conservées et la justification des données, à partir de l'historisation des règles de gestion

## 2. Mise en œuvre de la traçabilité

### Piste d'audit – clé de voûte de la traçabilité

#### Fonction 1 : Reconstitution de l'ordre chronologique des opérations

##### ■ Obligation

- La piste d'audit doit permettre de reconstituer dans un ordre chronologique les opérations (Code de Commerce – Art. L-123-12)

##### ■ Conséquence opérationnelle

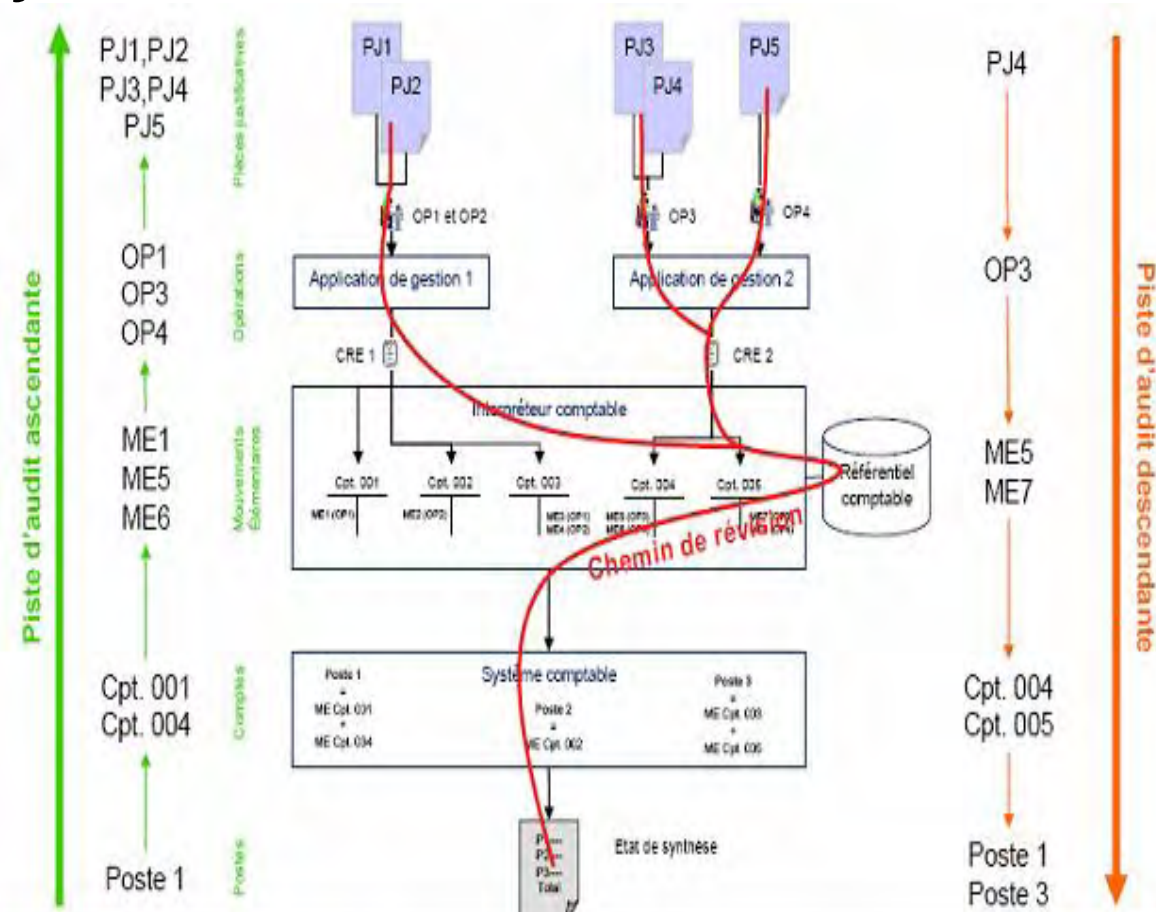
- La pièce d'origine doit contenir la date de la transaction
- Tous les mouvements doivent être datés et numérotés afin de pouvoir reconstituer les opérations dans leur ordre chronologique
- Toutes les transactions comptables doivent être journalisées chronologiquement
- Le SI comptable doit générer périodiquement des états récapitulatifs de toutes les données comptables. Ces états doivent être numérotés et datés

## 2. Mise en œuvre de la traçabilité

### Piste d'audit – clé de voûte de la traçabilité

#### Fonction 2 : Piste d'audit statique : Traçabilité ascendante et descendante

- **Obligation**  
L'organisation du système de traitement permet de reconstituer à partir des pièces justificatives appuyant les données entrées, les éléments des comptes, états et renseignements, soumis à la vérification, ou, à partir de ces comptes, états et renseignements, de retrouver ces données et les pièces justificatives (PCG – art. 410-3)
- **Conséquence opérationnelle**  
Le cheminement suivant doit être effectuable dans les deux sens (ascendant – des états financiers jusqu'aux pièces d'origine – et descendant – des pièces d'origine jusqu'au états financiers) comme illustré par le chemin de révision



## 2. Mise en œuvre de la traçabilité

### Piste d'audit – clé de voûte de la traçabilité

#### Fonction 2 : Piste d'audit statique : Traçabilité ascendante et descendante

| Audit trail scheme  | Example   |
|---|---|
| <p><b>Pièces justificatives<br/>(ex : factures)</b></p> <p style="text-align: center;">↑      ↓</p> | <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px; width: 40%;"> <p>Document<br/>001<br/>01/01/2006<br/>Deal A<br/>MM<br/>100 KEUR</p> </div> <div style="border: 1px solid black; padding: 5px; width: 40%;"> <p>Document<br/>002<br/>01/01/2006<br/>Deal B<br/>MM<br/>50 KEUR</p> </div> </div> |
| <p><b>Interpréteur comptable</b></p> <p style="text-align: center;">↑      ↓</p>                    | <p>01/01/2006; Deal A; MM; KEUR; 100; Document 001</p> <p>01/01/2006; Deal B; MM; KEUR; 50; Document 002</p>  |
| <p><b>Mouvements comptables</b></p>   | <p>ENTRY 1; 150; CREDIT; ACCT 000001</p> <p>ENTRY 2; 150; DEBIT; ACCT 000002</p>  |

## 2. Mise en œuvre de la traçabilité

### Piste d'audit – clé de voûte de la traçabilité

#### Fonction 3 : Piste d'audit dynamique : Justification par les flux

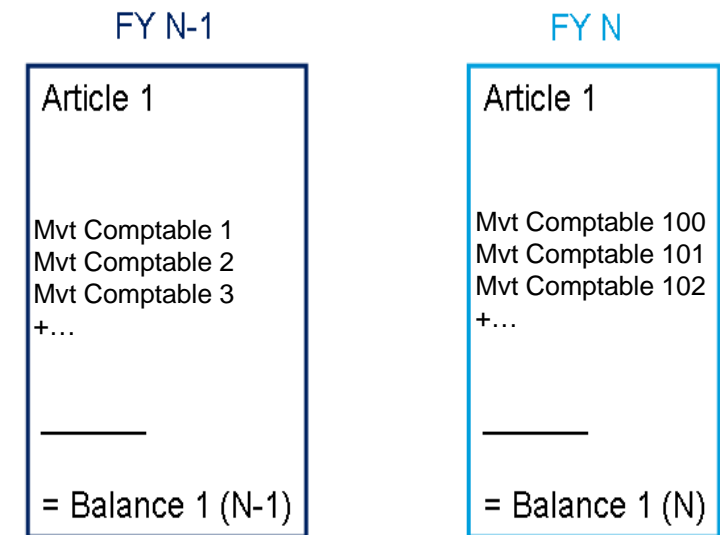
##### ■ Obligation

La piste d'audit (...) permet d'expliquer l'évolution des soldes d'un arrêté à l'autre par la conservation des mouvements ayant affecté les postes comptables (CRBF 97-02 : art. 12)

##### ■ Conséquence opérationnelle

→ Cette obligation implique la conservation de la trace de tous les mouvements comptabilisés entre deux arrêts afin de pouvoir justifier l'évolution des soldes entre ces deux arrêts.

→ Solde N = Solde N-1 +/- mouvements



$$\text{Balance 1 (N)} = \text{Balance 1 (N-1)} + \sum \text{Mvt Comptable (N)}$$

Piste d'audit dynamique



## 2. Mise en œuvre de la traçabilité

### Piste d'audit – clé de voûte de la traçabilité

#### Fonction 3 : Piste d'audit dynamique : Justification par les flux

Exemple simplifié (Immobilisation)

Au 31/12/2006

→ Total du poste immobilisation (Actif du bilan) = 1500K€

Au cours de l'exercice 2007

- Acquisition d'un terrain pour 1200K€
  - Acquisition d'un bâtiment pour 1300K€
  - Cession d'un entrepôt pour 1700 K€
- Soit un mouvement total de 800K€**

Au 31/12/2007

→ Total du poste immobilisation (Actif du bilan) = 3200K€ soit (1500K€ + 1700K€)

FY N-1

|                   |
|-------------------|
| Article 1         |
|                   |
| Mvt Comptable 1   |
| Mvt Comptable 2   |
| Mvt Comptable 3   |
| +...              |
| _____             |
| = Balance 1 (N-1) |

FY N

|                   |
|-------------------|
| Article 1         |
|                   |
| Mvt Comptable 100 |
| Mvt Comptable 101 |
| Mvt Comptable 102 |
| +...              |
| _____             |
| = Balance 1 (N)   |

$$\text{Balance 1 (N)} = \text{Balance 1 (N-1)} + \sum \text{Mvt Comptable (N)}$$

Piste d'audit dynamique

|      |      |       |      |
|------|------|-------|------|
| N-1  | Acq. | Cess. | N    |
| 1500 | 2500 | 800   | 2000 |

## 2. Mise en œuvre de la traçabilité

### Piste d'audit – clé de voûte de la traçabilité

#### **Fonction 4 : Conservation des données**

##### ■ Obligation

« ... en vue de préserver la fiabilité du chemin de révision, les entreprises doivent conserver : les éléments d'information intégrés dans un système informatique sous une forme conventionnelle pour être conservés, traités ou communiqués (BOI 13L-6-9)

##### ■ Informations et documents visés par le contrôle :

- Les informations, données et traitements informatiques concourant directement ou indirectement à la formation des résultats comptables et fiscaux ainsi qu'à l'élaboration des déclarations fiscales,
- La documentation informatique (conception, réalisation, maintenance, utilisation, exploitation).
- Obligation de conservation sur support informatique jusqu'à l'expiration de la troisième année suivant celle à laquelle l'imposition est due, puis sur support libre jusqu'à l'expiration du délai de six ans

##### ■ Conséquence opérationnelle

- La conservation des données réalisée par des moyens automatiques doit permettre l'exploitation de ces éléments (récupération, interprétation, modification, restitution ...)
- La conservation des éléments concourant à la détermination des données comptables et financières (historisation des valeurs de paramètres)

## 2. Mise en œuvre de la traçabilité Complexité et responsabilité

- **La mise en œuvre de la traçabilité devient un exercice complexe qui suppose la capacité à traiter des lots d'informations qui peuvent :**
  - provenir de sources d'information géographiquement dispersées,
  - être similaires en apparence mais en réalité différents,
  - être véhiculés par une variété d'outils et traversés différents couches applicatives,
  - avoir évolué de manière spécifique au gré des traitements qui les modifient.
- **Cette mise en œuvre est de la responsabilité**
  - Dans le cas d'un SI comptable et financier intégré de bout en bout de l'éditeur de l'application
  - Dans le cas d'un SI comptable et financier non intégré de l'entreprise elle-même (problématique complexe de clés de réconciliation de piste d'audit).

## 3. Maîtrise de la traçabilité Contraintes

- Un système d'information historiquement bâti dans le temps, d'où une hétérogénéité croissante à gérer,
- Des formats de données différents entre les différentes couches applicatives,
- Une multiplicité des référentiels du SI (plans de comptes, référentiel comptable français et international...),
- Une complexité accrue des produits et des opérations qui en découlent,
- Des ruptures de chaînes entre les différentes applications dues à des saisies manuelles d'opérations non standardisées,
- L'externalisation de certains services et/ou de certaines opérations,
- La synchronisation des opérations initiées dans des lieux géographiques différents (plateforme technique différente) et sur des versions applicatives différentes etc.

## 3. Maîtrise de la traçabilité Stratégie de mise en oeuvre

- La stratégie de mise en place de la traçabilité en partant d'un existant doit être la suivante :
  - Recensement de toutes les applications couvertes par la piste d'audit,
  - Mise en place d'un transcodificateur en aval de ceux-ci,
  - Mise en place d'une base opération,
  - Mise à niveau des applications non couvertes par la traçabilité,
  - Mise en place des modèles de données (relationnel ou document),
  - Mise en place d'un bus pour la structuration des échanges,
  - Éventuellement mise en place d'outils / base de données permettant de gérer la piste d'audit.

Par exemple :

La mise en œuvre de cette stratégie est favorisée dans un contexte d'externalisation ou encore de changements d'application

## 3. Maîtrise de la traçabilité

### Outils d'optimisation de la piste d'audit

- EAI : Architecture intergicielle permettant à des applications hétérogènes de gérer leurs échanges. L'objet de l'EAI (Enterprise Application Integration, traduisez intégration des applications de l'entreprise) est l'interopérabilité et l'organisation de la circulation de l'information entre des applications hétérogènes, c'est-à-dire faire communiquer les différentes applications constituant le système d'information de l'entreprise, voire même celles des clients, des partenaires ou des fournisseurs.  
*Exemple d'éditeurs* : TIBCO, WebMethod, Seebeyond, Sybase (NEON), BEA, Vitria, uMercator...
- ETL : Technologie informatique intergicielle (comprendre middleware) permettant d'effectuer des synchronisations massives d'information d'une base de données vers une autre.  
*Exemple d'éditeurs* : Informatica, Sunopsis...
- XBRL : est un standard émergent basé sur XML pour définir de l'information financière performante. De surcroît, il est le fluidificateur par excellence de l'échange de données décisionnelles, quelle que soit l'infrastructure informatique et technologique. In fine, en donnant le pouvoir à l'utilisateur final, XBRL contribue à l'ubiquité logique à savoir la disponibilité des données et des outils de traitement, quel que soit l'endroit où l'on se trouve.
- ISIE : est une solution d'interprétation mise en œuvre par Artaud Courthéaux & Associées (ACA) permettant la gestion de tous les échanges entre applications.
- EDI : échange informatisé de données structurées d'application à application selon des messages préétablis et normalisés via un mode de communication électronique.
- GED : Gestion électronique de documents.
- xRDJ : est une solution d'interprétation mise en œuvre par Axway permettant la gestion de tous les échanges entre applications.

## 3. Maîtrise de la traçabilité

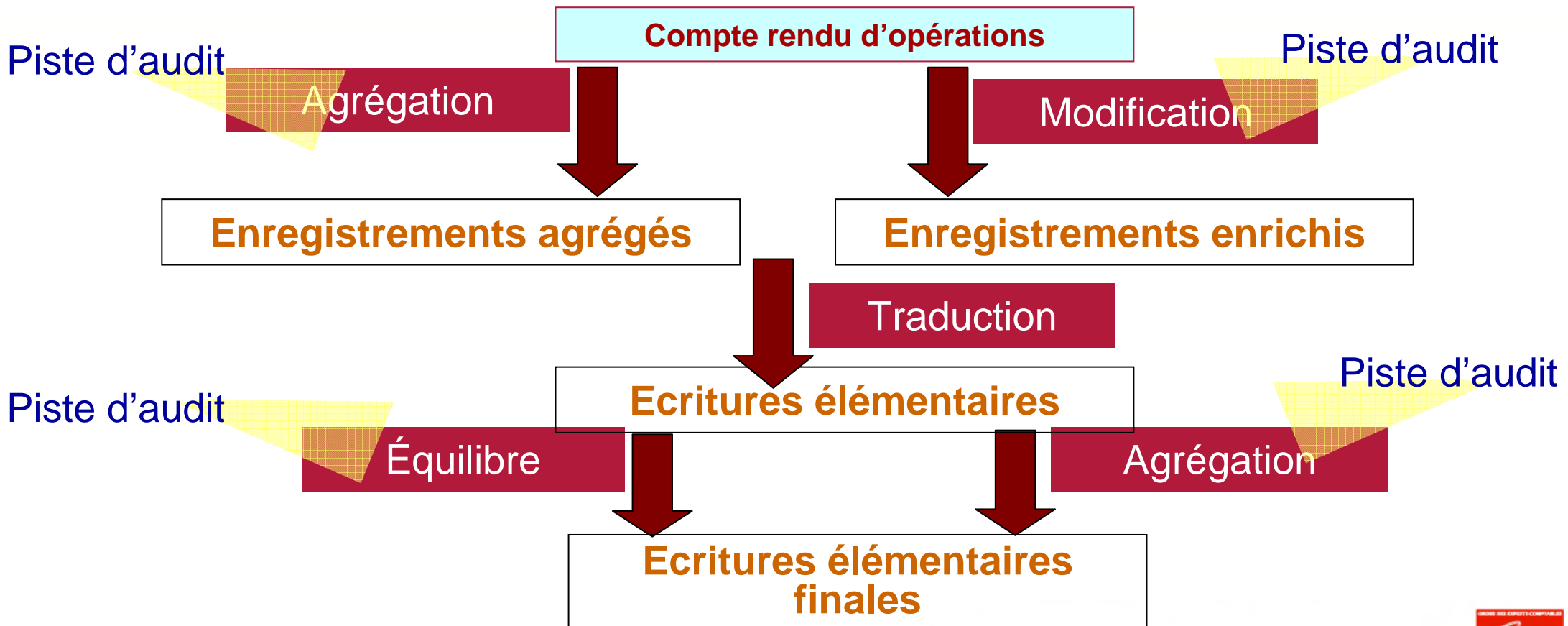
### Outils de gestion de la piste d'audit

- Sentinel : est une solution de gestion de la piste d'audit mise en œuvre par Axway :
- Système d'audit performant
  - Améliore la productivité et la qualité des données
  - Traçabilité des opérations
- Système de suivi performant
  - Gestion d'alertes sur dépassement de seuils
  - Statistiques sur les traitements
  - Gestion du non-événement, Corrélation entre événements
  - Suivi de Bout-en-bout
  - Opérations sensibles (blanchiment d'argent, ...)
- Exemples
  - A partir d'un événement, retrouver les écritures comptables générées selon leur norme respective dans un contexte multi-norme – Cf. schéma page suivante
  - A partir d'une écriture comptable, retrouver les autres écritures générées selon leur norme respective, qui correspondent à l'écriture sélectionnée

## 3. Maîtrise de la traçabilité

### Outils de gestion de la piste d'audit

Un exemple :



## Conclusions

- La tracabilité est un sujet à la croisée de nombreuses réglementations
- La tracabilité, c'est la possibilité de remonter/descendre les flux d'informations mais c'est également la reconstitution chronologique des opérations, la conservations des données et la justification des soldes d'une date à une autre.
- Le challenge de la tracabilité ne réside pas tant dans la mise en œuvre et l'application des textes référents mais dans la capacité à faire inter-opérer les blocs fonctionnels de manière à définir une clef de réconciliation entre les différentes pistes d'audit appartenant aux différentes applications impactées dans les échanges.
- Un outil de gestion de piste d'audit concourt à la mise en place d'une traçabilité au sein des systèmes mais ne peut pas être le seul élément pour satisfaire pleinement aux exigences requises
- C'est un ensemble d'outils, de clés dans les systèmes et de principes (homogénéité des référentiels, structuration des données...) qui le permettront.

# Analyse de l'intégrité applicative dans l'audit des SI

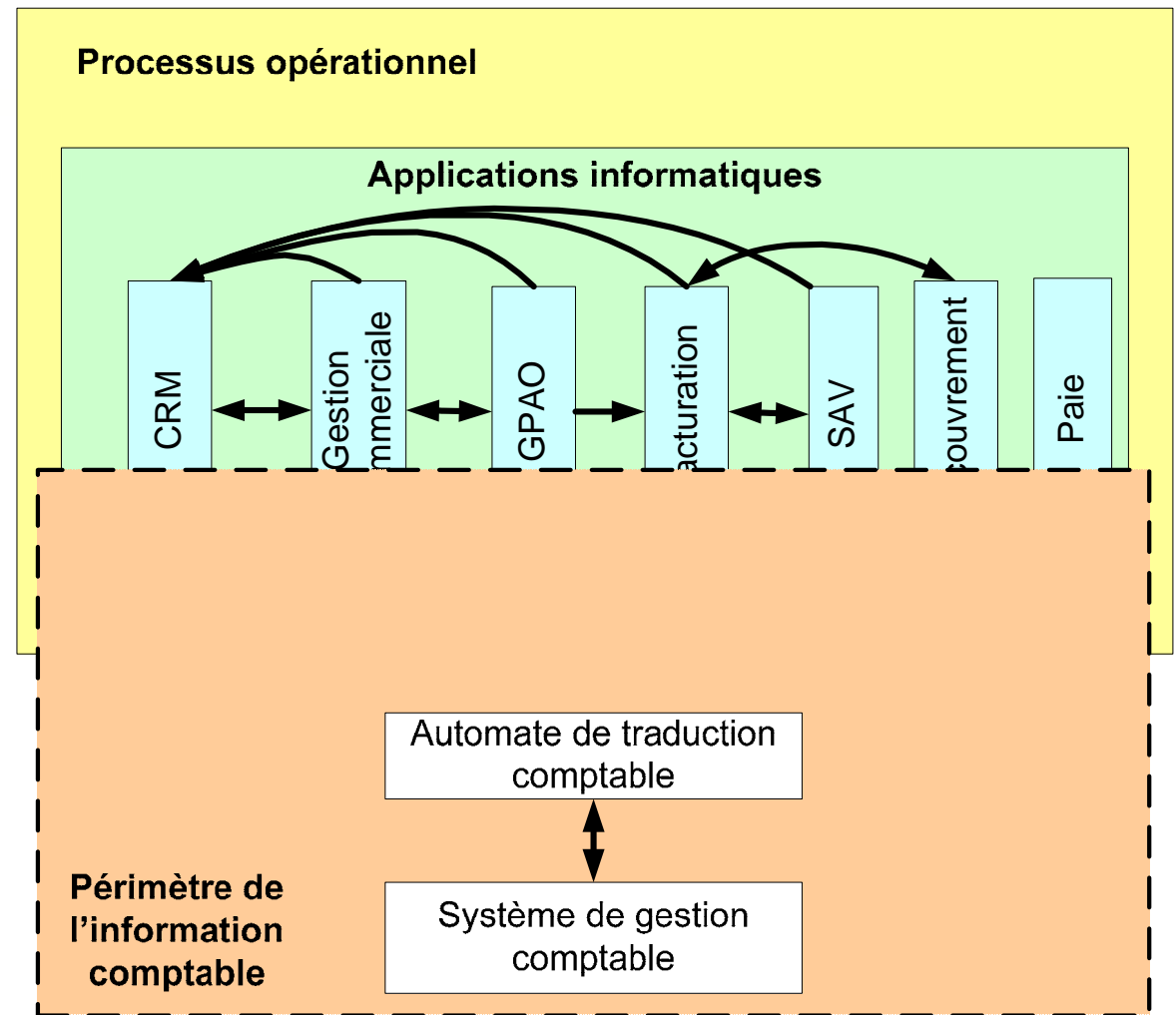
**Jean-Pierre Veyrier**  
**Bellot Mullenbach & Associés**

# SOMMAIRE

- 1** Une forte évolution réglementaire
- 2** Impacts
  - 2.1** Impact sur la localisation des contrôles
  - 2.2** Impact sur la nature des contrôles
  - 2.3** Impact sur la nature des contrôles : l'intégrité référentielle
  - 2.4** Impact sur la nature des contrôles : l'intégrité transactionnelle
- 3** Où sont les zones à risque ?
  - 3.1** Où sont les zones à risque dans les progiciels du marché ?
  - 3.2** Où sont les zones à risque dans les logiciels spécifiques ?
  - 3.3** Les interfaces sont toujours des zones à risque majeures
- 4** Impact sur la stratégie d'audit : exemple de démarche
- 5** Conclusion

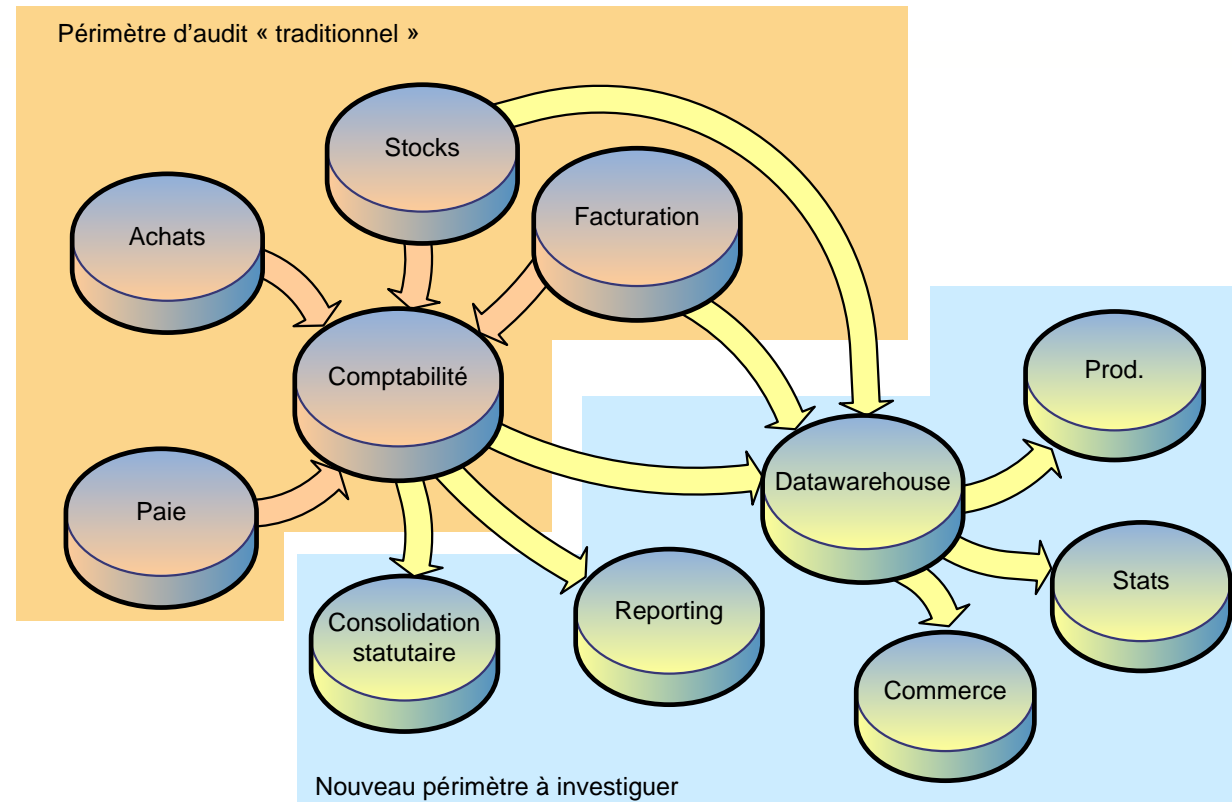
# Une forte évolution réglementaire

- Les nouvelles réglementations (SOX et notamment sa section 404, LSF) confirment la tendance amorcée depuis plusieurs années consistant à faire porter de manière approfondie le regard de l'auditeur :
  - non seulement sur le progiciel comptable
  - mais aussi vers les applications opérationnelles qui produisent les écritures comptables
- La norme d'exercice professionnel NEP-315 a remplacé la norme 2-202



# Impact sur la localisation des contrôles

- De nouvelles applications assurant la mise à disposition d'informations financières sont souvent exploitées directement ou indirectement dans les annexes financières des rapports de gestion publiés :
  - ➔ datawarehouse
  - ➔ reportings spécifiques
  - ➔ application de consolidation
  
- Ces outils informatiques assurent des rôles tels que :
  - ➔ l'application de règles de retraitements (Exemple : changement de normes)
  - ➔ la création d'agrégats financiers
  - ➔ la production d'indicateurs de gestion

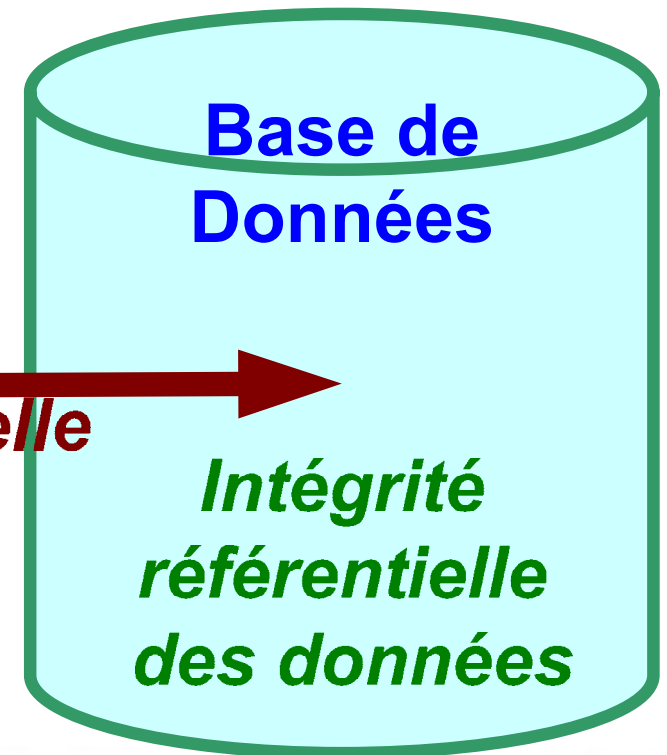
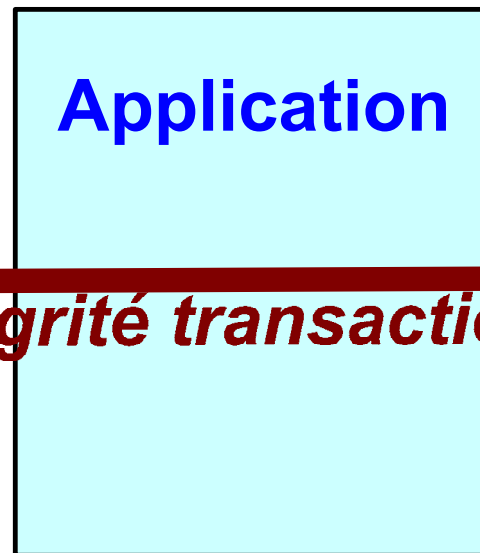
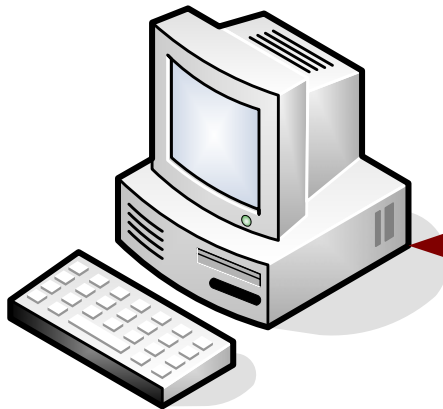


# Impact sur la nature des contrôles

- L'auditeur doit s'assurer qu'il n'y pas de risques d'altération des données financières ou que s'ils existent, ces risques sont sous contrôle.
- Un des axes de ces contrôles consistera à vérifier que les données sont intègres et cohérentes du point de vue du métier en s'assurant notamment que :
  - ➔ les applications auditées ont mis en œuvre les principes techniques permettant de garantir cette intégrité
  - ➔ l'entreprise dispose des moyens de contrôle adéquats :
    - requêtes de contrôle spécifiques au sein des applications ou entre applications
    - organisation dédiée aux corrections identifiées et procédure de correction formalisée
    - outils dédiés : indicateurs de qualité des données
- Cette vérification s'appuiera sur le principe fondamental d'intégrité applicative, dont la mise en œuvre permet de réduire fortement les risques d'altération des données

# Impact sur la nature des contrôles

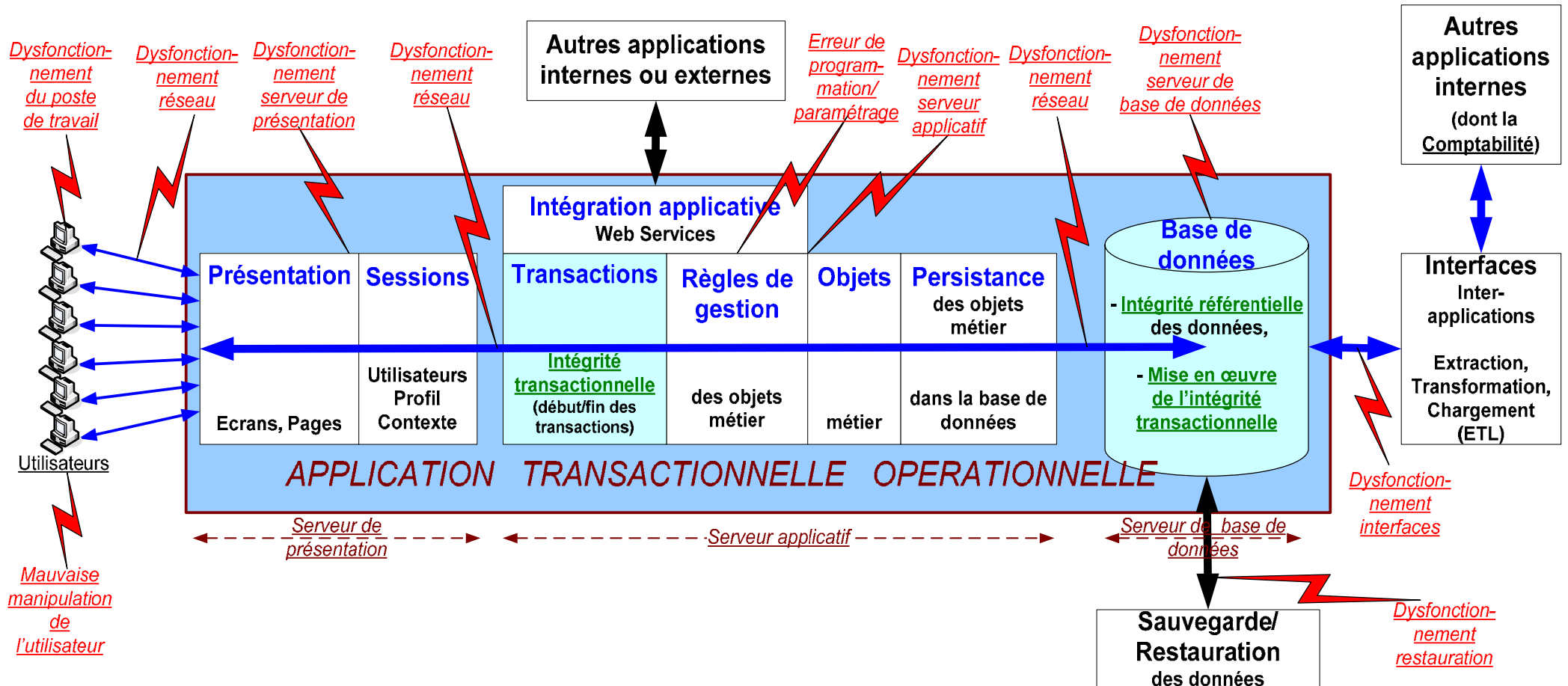
- L'intégrité applicative se décompose en :
  - L'intégrité transactionnelle
  - L'intégrité référentielle



***Intégrité transactionnelle***

# Impact sur la nature des contrôles

- L'intégrité applicative assure un « bouclier de protection » des données de la piste d'audit afin de protéger les données contre :
  - les erreurs d'utilisation des logiciels
  - les anomalies de programmation et de paramétrage
  - les dysfonctionnements des infrastructures techniques : postes de travail, réseaux, serveurs, stockage disque, etc...

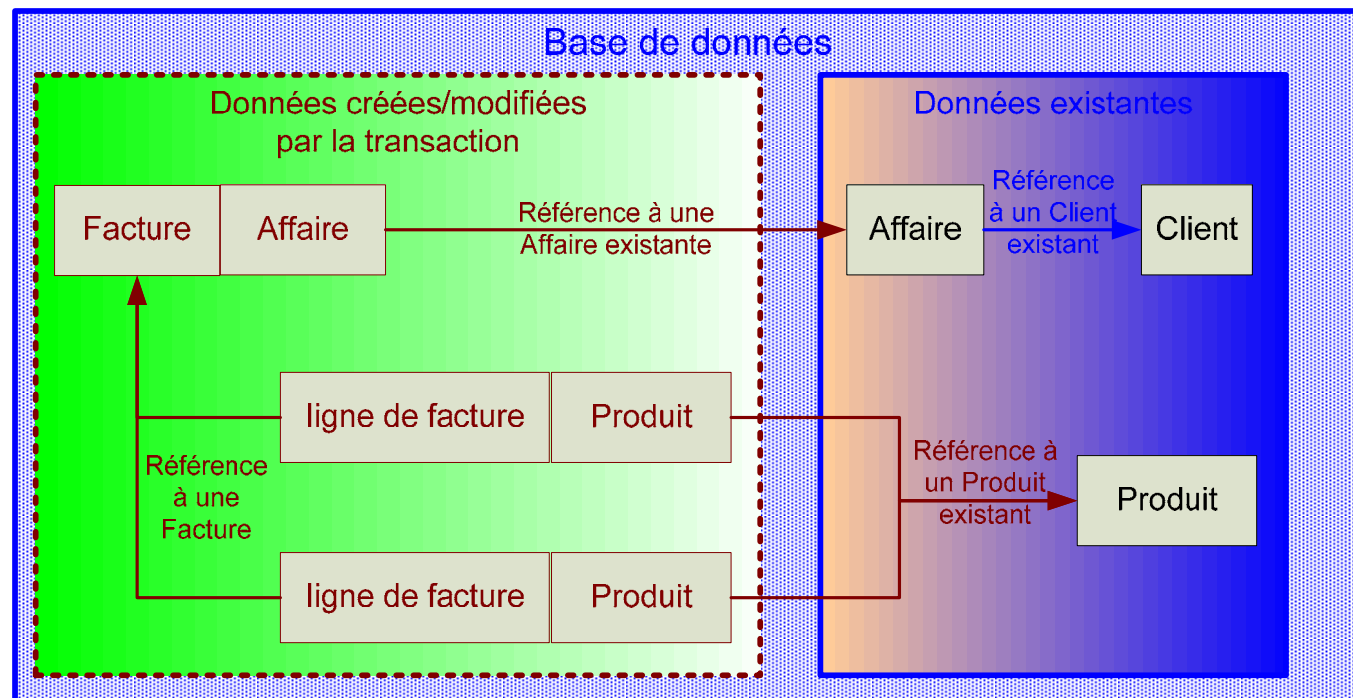


# Impact sur la nature des contrôles : l'intégrité référentielle

- L'intégrité référentielle se définit comme le respect des règles métier régissant les relations\_entre données
  - ces règles existent dans le métier, que celui-ci soit informatisé ou non
- L'objet de l'intégrité référentielle est d'interdire à tout moment la création ou la mise à jour de données qui ne respectent pas ces relations définies entre les données
  - Ces relations expriment des règles de gestion très structurantes qui imposent qu'une donnée soit nécessairement rattachée à une autre donnée

– Dans notre illustration, présentée à titre d'exemple :

- une ligne de facture doit obligatoirement être rattachée à une seule facture existante et à un produit existant,
- une facture doit obligatoirement être rattachée à une affaire existante,
- une affaire doit obligatoirement être rattachée à un client existant



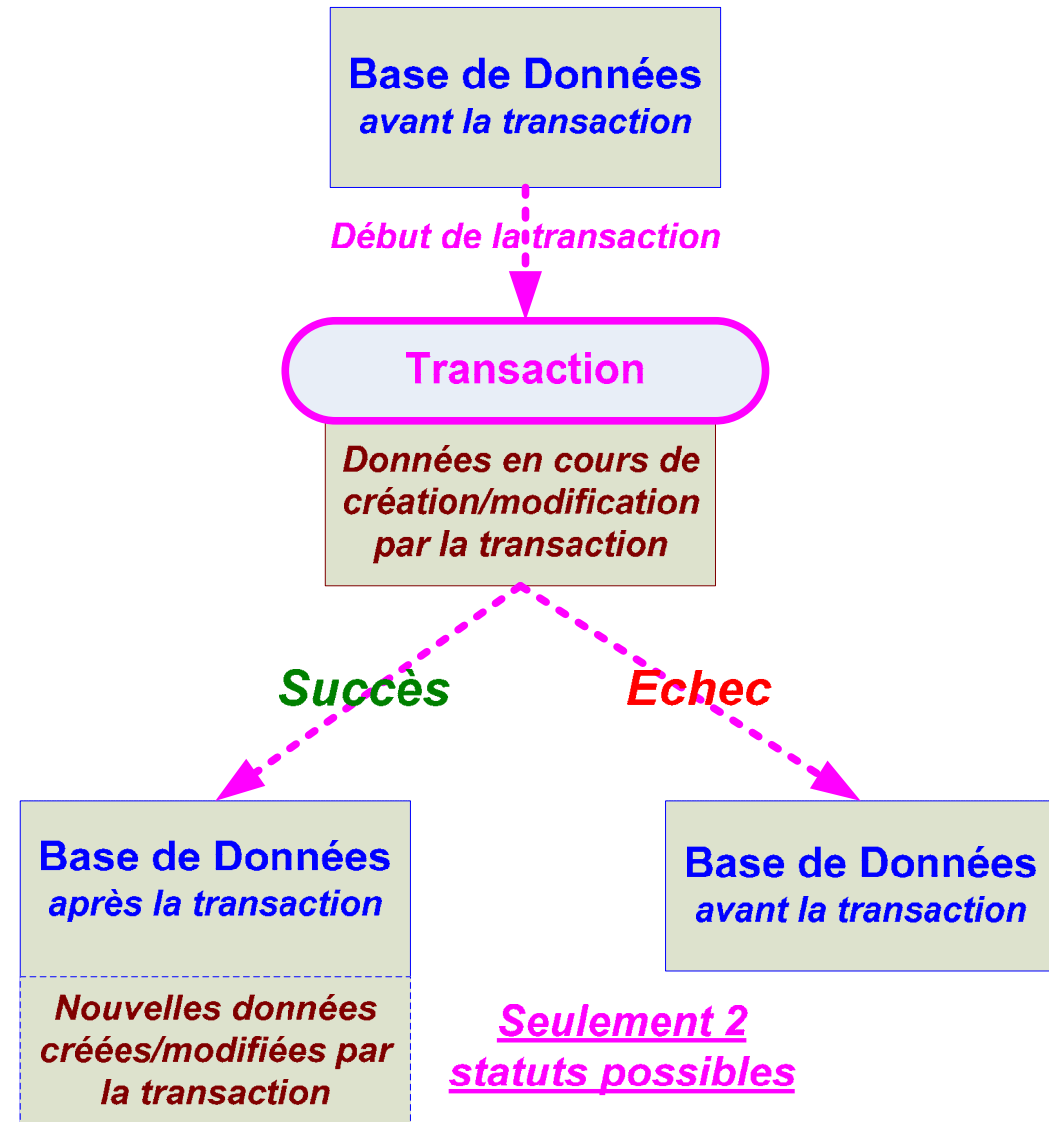
# Impact sur la nature des contrôles : l'intégrité référentielle

- Application pratique à nos travaux d'audit :
  - ➔ La vérification, au sein des applications, de l'existence des mécanismes techniques permettant de s'assurer de l'intégrité référentielle des données est relativement aisée
  - ➔ La complexité réside :
    - dans le périmètre d'investigation : beaucoup de tables à contrôler
    - dans l'adéquation des règles techniques mises en place par rapport aux besoins métier : nécessite une connaissance approfondie du métier
  - ➔ Son absence totale ou quasi-totale est remédiable uniquement dans des contextes techniques équipés de bases de données mais se traduit par un véritable projet informatique lourd et complexe
  - ➔ Son absence plus ponctuelle est aisément remédiable mais constitue toujours un mini projet délicat du fait des données historiques qui ont une forte probabilité d'être non intègres

# Impact sur la nature des contrôles : l'intégrité transactionnelle

L'objet de l'intégrité transactionnelle est d'interdire toute mise à jour partielle de la base de données, si la transaction ne s'est pas correctement déroulée ou si elle a été interrompue pour quelque raison que ce soit :

- ainsi, les données d'une transaction ne peuvent se trouver que dans deux situations possibles :
  - soit mises à jour en totalité dans la base de données
  - soit non mises à jour dans la base de données si la transaction ne se déroule pas correctement jusqu'au bout.
- par exemple, la création d'une facture ne peut pas être incomplète ou incohérente (lignes sans entête, lignes manquantes, lignes en double, etc...), la création d'une écriture comptable ne peut pas être déséquilibrée



# Impact sur la nature des contrôles : l'intégrité transactionnelle

## ■ Application pratique à nos travaux d'audit :

- ➔ Du point de vue pratique, la vérification de la mise en œuvre de l'intégrité transactionnelle est difficilement applicable dans un contexte d'audit car elle nécessite pour identifier les zones à risque d'examiner le code applicatif.  
elle reste néanmoins possible par des experts applicatifs notamment dans des contextes où la cause est clairement identifiée et nécessite la correction d'une transaction existante défectueuse.
- ➔ Une autre solution consiste, par sondage, à identifier les données corrompues :  
la problématique réside alors dans la démonstration que la corruption provient d'un défaut d'intégrité transactionnelle puis dans la mise sous contrôle des anomalies.
- ➔ Les risques d'altération de l'intégrité des données proviennent majoritairement :
  - soit d'anomalies matérielles essentiellement techniques (qui sont relativement faibles et ponctuelles et portent sur un nombre limité de données)
  - soit d'anomalies logicielles
- ➔ Nous verrons que dans ce dernier cas des contrôles compensatoires tels que des tests techniques poussés, une recette fonctionnelle formalisée, et un suivi maîtrisé des évolutions applicatives peuvent limiter le risque.

# Où sont les zones à risque ?

- L'intégrité applicative qui paraît être un principe technique appliqué et maîtrisé depuis 20 ans, ne l'est pas en pratique pour diverses raisons
- Son absence est potentielle, que nous nous ayons à faire face à un environnement progiciel ou développement spécifique

|   | Probabilité de non respect de l'intégrité relationnelle | Probabilité de non respect de l'intégrité transactionnelle |
|---|---|--|
| <b>Progiciels</b>   |   |  |
| •Mainframe : technologie fichiers séquentiels indexés   | +++   | +  |
| •Client Serveur : Base de données relationnelle   | + / -   | ++   |
| •Architecture N Tiers   | + / -   | + / -  |
| <b>Développement spécifique</b>   |   |  |
| •Mainframe : technologie fichiers séquentiels indexés   | +++   | +  |
| •Client Serveur : Base de données relationnelle   | + / -   | ++   |
| •Client Serveur : Base de données relationnelle Cas des applications jetables ou développées en méthode RAD | + / -   | ++   |
| •Architecture N Tiers   | + / -   | + / -  |

# Où sont les zones à risque dans les progiciels du marché ?

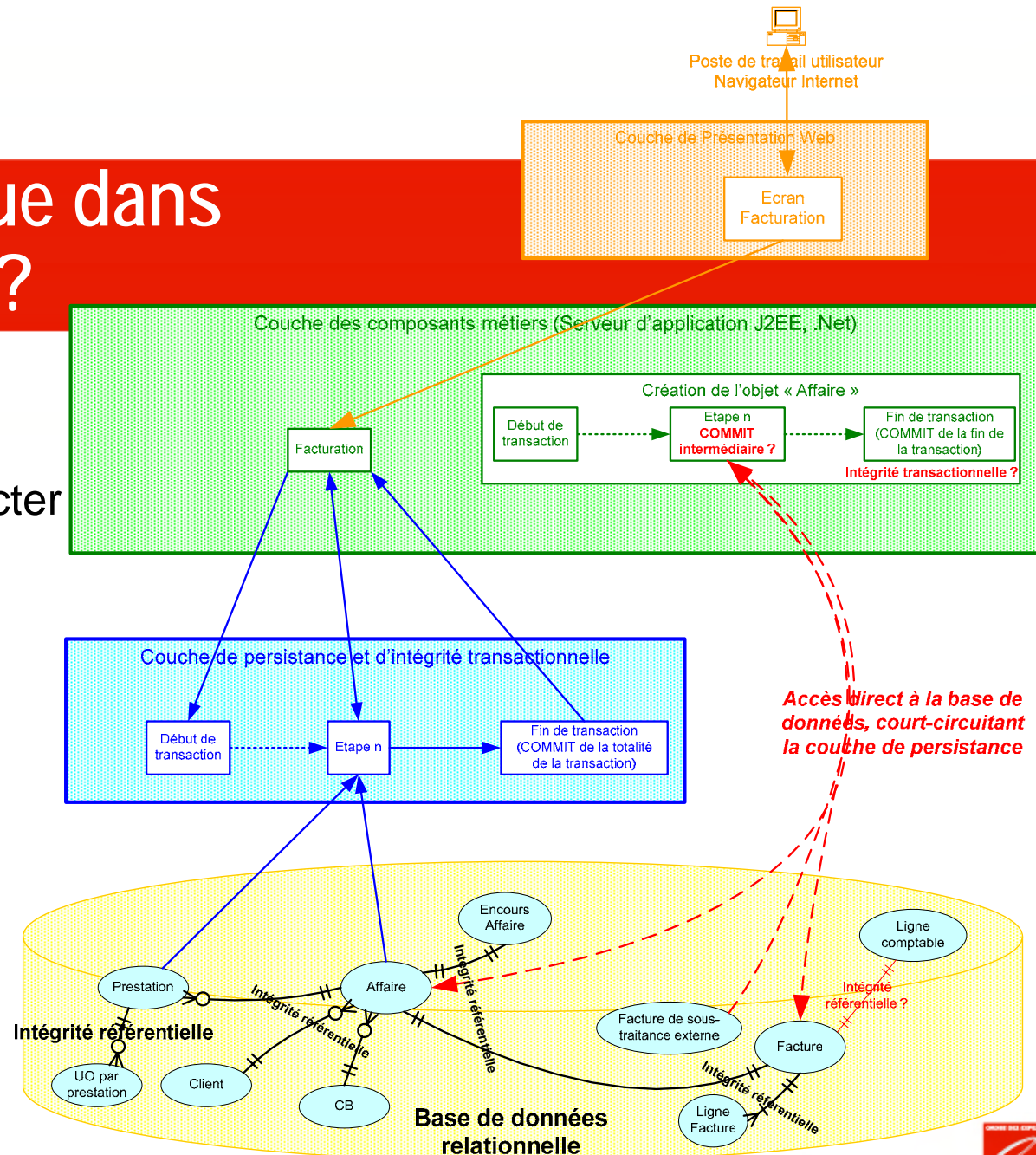
- La sélection des progiciels aborde rarement l'intégrité applicative  
Il n'est pas d'usage courant de demander à l'éditeur de communiquer la structure interne de son progiciel pour vérifier si l'intégrité applicative est bien mise en œuvre. Les choix de progiciels sont fréquemment basés sur de simples comparaisons de fonctionnalités, en omettant de mesurer la pertinence de l'architecture technique
- L'intégrité applicative est encore un sujet tabou  
Les comportements actuels que nous rencontrons sont d'une part ceux des éditeurs qui n'abordent pas ou ne communiquent pas sur ce sujet pour les raisons suivantes :
  - ➔ ce sont plutôt des sujets qui ralentissent le processus de vente et peuvent mettre en évidence des faiblesses structurelles des produits. En effet, la plupart certains des progiciels intégrés sont dérivés d'anciennes versions de progiciels ne s'appuyant pas sur des bases relationnelles et n'implémentent pas l'intégrité référentielle. Certains progiciels utilisent les bases relationnelles à des simples fins de stockage sans tirer parti des possibilités offertes par ces outils pour garantir l'intégrité des données.
  - ➔ certains éditeurs considèrent leur modèle de données et leurs règles de validation des transactions comme un secret technologique, et refusent de les communiquer.
  - ➔ le manque d'intégrité des données existantes peut être un frein important à la reprise des données dans un progiciel respectant l'intégrité référentielle, et donc là aussi retarder pour un intégrateur la réception de l'application.
- L'intégrité applicative est considérée à tort comme respectée de fait  
Les opérationnels et les auditeurs considèrent souvent que, s'agissant de progiciels, les règles de l'art sont respectées par tout et par conséquent que le correct fonctionnement de l'intégrité applicative est un postulat de travail.

# Où sont les zones à risque dans les logiciels spécifiques ?

- Principes techniques (ACID) non systématiquement appliqués  
Les quatre lettres de l'acronyme ACID renvoient à un moyen mnémotechnique pour se souvenir de chacune de ces caractéristiques essentielles : Atomicity (atomicité), Consistency (cohérence), Isolation, Durability (durabilité) :
  - Atomicité signifie que les mises à jour de la base de données doivent être "atomiques", à savoir qu'elles doivent être totalement réalisées ou pas du tout. On rejoint ici les principes d'intégrité transactionnelle évoqués précédemment.
  - Cohérence signifie que les modifications apportées à la base doivent être valides, en accord avec l'ensemble de la base et de ses contraintes d'intégrité. On rejoint ici les principes d'intégrité référentielle évoqués précédemment
  - Isolation signifie que les transactions lancées au même moment ne doivent jamais interférer entre elles, ni même agir selon le fonctionnement de chacune. Par exemple, si une requête est lancée alors qu'une transaction est en cours, le résultat de celle-ci ne peut montrer que l'état original ou final d'une donnée, mais pas l'état intermédiaire.
  - Durabilité signifie que toutes les transactions sont lancées de manière définitive. Une base ne doit pas afficher le succès d'une transaction, pour ensuite remettre les données modifiées dans leur état initial. On rejoint de nouveau les principes d'intégrité transactionnelle évoqués précédemment.

# Où sont les zones à risque dans les logiciels spécifiques ?

- Application au cas d'une architecture applicative moderne n-tiers : Il est aussi possible de ne pas respecter l'intégrité transactionnelle dans une architecture moderne.



# Les interfaces sont toujours des zones de risque majeures

- Malheureusement, dans la plupart des systèmes d'informations que nous rencontrons, les transferts d'information par lot (batch) entre applications, voire les duplications de données sont encore extrêmement fréquents et devront être considérés comme des points d'attention particulier par les auditeurs.
- En effet les interfaces sont des sources d'anomalies importantes en terme :
  - d'intégrité référentielle :  
au même titre que lors d'un flux intra applicatif, on devra contrôler que les principes d'intégrité référentielle sont bien respectés.
  - d'intégrité transactionnelle :  
l'intégrité transactionnelle est beaucoup plus critique que dans le cadre d'une transaction élémentaire où les risques de perte de données ne portent que sur un faible volume. Dans le cas d'interfaces, une anomalie technique peut entraîner la non exhaustivité de données sur plusieurs jours voire plusieurs semaines.

# Impact sur la stratégie d'audit : Exemple de démarche

| Etape  | Objet  | Moyens mis en œuvre   |
|--|--|---|
| Identification des zones à risques               |  |   |
|  | Identification des applications critiques du point de vue métier ; celles qui contribuent à la production d'éléments financiers et avec des montants significatifs                     | <ul style="list-style-type: none"> <li>• Représentation schématique et haut niveau des processus métier</li> <li>• Mise en évidence des sous systèmes contributeurs à l'information financière : architecture métier</li> <li>• Détermination de la couverture des sous systèmes par les différentes applications : architecture applicative</li> <li>• Compréhension du fonctionnement des différents composants logiciels,</li> </ul>   |
|  | Parmi celles-ci, identification des applications à risque : l'objet est de détecter, selon des critères techniques, les applications où un risque peut survenir de façon structurelle. | <ul style="list-style-type: none"> <li>• Analyse des solutions techniques mises en œuvre et notamment l'aspect intégrité applicative :               <ul style="list-style-type: none"> <li>○ Contrôle de la mise en œuvre des contraintes d'intégrité référentielle dans la structure de la base de données</li> <li>○ Revue du fonctionnement et du contenu des transactions critiques</li> </ul> </li> </ul>   |
|  | Analyse particulière des interfaces  | <ul style="list-style-type: none"> <li>• Mise en évidence des interfaces véhiculant de l'information financière</li> </ul>  |
| Qualification du risque                          |  |   |
|  | Analyse de la criticité et de la fréquence   | Qualification d'un niveau de criticité et d'une fréquence de survenance pour chacune des transactions examinées   |
|  | Analyse des moyens existants de mise sous contrôle des risques significatifs :   | Consiste à lister et analyser :<br>Les procédures existantes,<br>Les exploitations de requêtes standards permettant la détection d'anomalies,<br>Les requêtes spécifiques de traçabilité des données,<br>les travaux systématiques effectuant des contrôles de cohérence toutes les nuits   |
|  | Analyse de la criticité : cas particulier des interfaces   | Existence d'un environnement de traitement des anomalies métier (cas de l'intégrité référentielle) : <ul style="list-style-type: none"> <li>• Identification des rejets</li> <li>• Suivi de leur retraitement ou de leur recyclage automatique</li> <li>• Existence d'un système de traçabilité et de piste d'audit</li> <li>• Etats de gestion appropriés</li> <li>• Existence de processus d'arbitrage et d'amélioration, etc...</li> </ul> Existence d'un de traitement des anomalies techniques (cas de l'intégrité transactionnelle) : <ul style="list-style-type: none"> <li>• Identification des transferts en échec</li> <li>• Identification des transferts non exécutés</li> <li>• Existence de procédure de remise à niveau, etc...</li> </ul> |
|  | Analyse des risques résiduels à l'issue des contrôles existants  | L'analyse et la criticité des risques peuvent être confortés par un sondages des fiches incidents enregistrés au niveau de chaque application.  |
|  | Arbitrage  | Il faut en effet être conscient que dans de nombreux cas, il est techniquement impossible de sécuriser rapidement (un trimestre) le déroulement d'une transaction. Alors, un ensemble de solutions de contournement devra être mise en place.   |
| Préconisations de mise sous contrôle des risques |  |   |
|  |  | Construction d'un calendrier détaillant la mise sous contrôle des zones à risques   |

# Impact sur la stratégie d'audit : Exemple de démarche

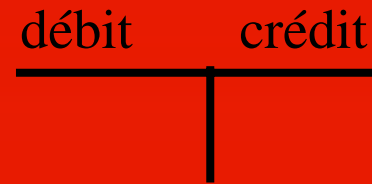
- Exemple de tableau des risques et de leur criticité :

| Module                        | Un seul COMMIT, à la fin de la transaction (O/N) | COMMIT(s) partiel(s) intermédiaire(s) (O/N) | Impact, en terme d'intégrité/cohérence des données, d'une interruption de la transaction (coupure réseau, déconnexion session, etc..) avant le dernier COMMIT ?   | Fréquence d'apparition d'anomalie                         | Criticité | Statut/Action (Version projet v6.1 du 7 Janvier 2006)  |
|-------------------------------|--|---|---|---|-----------|--|
| ImportationFact               | NON  | OUI (Factures)                              | Cette transaction réalise l'importation de factures spéciales. L'import se fait ligne après ligne, avec un commit à la fin de chaque ligne. Chaque ligne est donc intègre.<br><b>Si une ligne n'est pas importée, l'import continue a la ligne d'après</b>  | Faible  | Forte     | Factures spéciales très peu utilisées.   |
| ImportationFichierClient      | NON  | OUI (Clients)                               | Cette transaction réalise l'importation de fichiers clients externes. L'import se fait ligne après ligne, avec un commit à la fin de chaque ligne. Chaque ligne est donc intègre.<br><b>Si une ligne n'est pas importée, l'import continue a la ligne d'après</b>   | Faible  | Faible    | Son utilité semblerait limitée à des tests lors de la mise en place de l'accès à la base de clients COFACE.  |
| ValidationEncours             | NON  | OUI (Affaires, encours_A, encours_B)        | Cette transaction a pour objet d'insérer le résultat du calcul des encours, avec trois commits partiels au niveau de chaque affaire,<br><b>1. Il se peut que les données dans la table encours_A et encours_B soit incohérentes (commit indépendants).</b><br>Le calcul des encours n'est pas impacté.<br><b>2. Le calcul des encours de certaines affaires peut ne pas être effectué (commit par affaire).</b>   | Déjà détectée en 2005                                     | Forte     | Les fichiers Logs de la Base de données gardent trace des affaires dont l'encours n'a pas été calculé. Un outil de contrôle par requête sur ces logs est nécessaire                  |
| ValidationEncoursB            | NON  | OUI   | Cette transaction prépare un fichier externe, qui est ensuite importé dans le système comptable.<br><b>Si la transaction échoue le fichier est incohérent.</b><br><b>En cas de facturation en devise autre qu'euro, le taux de conversion de devise transféré à la comptabilité peut être faux (mais pas les montants en euro). Problème détecté en 12/2005 par le processus de contrôle de la comptabilité, en cours d'investigation.</b>  | 1 fois par an. Détectée la dernière fois en Novembre 2005 | Forte     | Le contrôle d'exhaustivité mis en place permet de détecter une éventuelle incohérence lors de l'importation du fichier. (Cf schéma de description du fonctionnement de l'applicatif) |
| FormAffaire                   | NON  | OUI (Client, complément Client)             | Cette transaction permet de modifier les caractéristiques d'une affaire. Des commits partiels sont utilisés lorsque les données modifiées proviennent de plusieurs tables en plus de la table affaire (par exemple les informations client, qui sont réparties dans deux tables distinctes)<br><b>Problème potentiel de mise à jour du rattachement de l'affaire à un client. On pourrait se retrouver avec une affaire rattachée à un client (l'ancien) pour laquelle les données connexes (adresse, contacts, référence client des prestations/interventions, documents) sont rattachées au nouveau client.</b> | Pas d'anomalie identifiée à ce jour                       | Faible    | N/A  |
| FormInterventionSousTraitance | OUI  | NON   | La création ou la modification d'une sous-traitance ne comporte qu'une transaction : création ou modification ==> pas de problème   | N/A   | N/A       | N/A  |

## Conclusion

- A. L'intégrité applicative : une règle de l'art :
  - sur laquelle personne ne communique,
  - qui est souvent « passée à la trappe »
  
- B. L'intégrité applicative est un facteur de risque important :
  - pouvant impacter l'exhaustivité des flux
  - que ce soit pour les progiciels ou les logiciels spécifiques
  
- C. L'auditeur ne doit pas emboîter le pas, et contrôler sa correcte mise en place :
  - Les contrôles internes pouvant être dans le cas le plus défavorable des batchs de contrôle a posteriori mis en œuvre toutes les nuits, dont les anomalies détectées sont corrigées à la main le lendemain

## Convergence des systèmes d'information opérationnels et comptables : normes et codification de l'information comptable



CRC 99-03 – IFRS – CNCC NEP315 et 330 – Sarbox 404 -  
BALE2 – ISO 17799 – COSO EDI – XBRL-  
Et un raton laveur !...

présentation par Thierry  
Trompette



## Normes et codification de l'information comptable la problématique :

- Il existe de nombreuses normes et référentiels réglementaires ou qualitatifs grâce ou à cause desquels il est nécessaire de codifier valider et communiquer l'information comptable. D'autres servent à concevoir et maîtriser les systèmes qui produisent cette information.
  
- L'objet de cette présentation :
  1. Cartographier et synthétiser ces référentiels
  2. les classer selon leur usage
  3. Analyser les convergences majeures et en dégager les tendances futures.

## Inventaire des référentiels normatifs

### ■ Famille comptable :

- Plan comptable – CNC CRC 99-03
- Règles fiscales (circulaire du 16 janvier 2006)
- Normes comptables internationales : IFRS – IAS -SARBOX 404
- Normes d'audit : IAS (international) - NEP France

### ■ Famille systèmes :

- Référentiels d'analyse : coso - cobit –itil– mehari
- Référentiels Qualité : ISO-17799-BS7799- SysTrust
- Méthodologiques : BPM approches par processus : UML 2.0 – BPMN – ISO 9000 – BPDM

### ■ Famille communication/ codification des données :

- ASCII (TXT) – EDI - XBRL

# La source des normes : quelles Institutions

|                                     | <i>Audit interne</i>  | <i>Audit informatique</i>  | <i>Audit externe</i>  |
|-------------------------------------|---|--|---|
| <i>Normes internationales</i>       | Divers normes et standards IIA, COSO ( <a href="http://www.coso.org">www.coso.org</a> )         | CobiT, (download depuis <a href="http://www.isaca.ch">www.isaca.ch</a> ) divers normes et standards                | ISA (International standards on auditing)<br><br>IRFS – NEP   |
| <i>Institutions internationales</i> | IIA Institute of internal auditors ( <a href="http://www.theiia.org">www.theiia.org</a> )       | ISACA Information systems audit and control association ( <a href="http://www.isaca.org">www.isaca.org</a> )       | IFAC International federation of accountants ( <a href="http://www.ifac.org">www.ifac.org</a> )<br><br>IASB |
| <i>Institutions françaises</i>      | IFACI Institut français de l'audit interne ( <a href="http://www.ifaci.com">www.ifaci.com</a> ) | AFAI Association française de l'audit et du conseil informatiques ( <a href="http://www.afai.fr">www.afai.fr</a> ) | CNCC Compagnie nationale des commissaires aux comptes ( <a href="http://www.cncc.fr">www.cncc.fr</a> )      |

# La loi Française : outils réglementaires

## ■ La responsabilité pénale du chef d'entreprise :

→ Délit de manquement à la sécurité : obligation de diligence

- Art. 226-17 CP = **5 ans** d'emprisonnement et **300 000 euros** d'amende.  
( *loi Godfrain du 5 janvier 1988* )

## ■ La responsabilité civile de l'entreprise :

- Dommages et intérêts au profit de l'entité qui prouve avoir subi un préjudice indirect (perte de fichiers, diffusion de données sensibles la concernant...)

## ■ Le respect de la confidentialité :

→ Délit d'intrusion : la connaissance de l'information

- Art. 323-1 CP = **1 an** d'emprisonnement et **15 000 euros** d'amende.

→ Délit d'utilisation frauduleuse de l'information

- Art. 226-18 CP (Loi informatique et libertés du 6 janvier 1978) = **5 ans** d'emprisonnement et **30 000 euros** d'amende.

## ■ Le respect de l'intégrité des données:

→ Délit de piratage : l'atteinte aux données

- Art. 323-3 CP (Loi Godfrain) = **3 ans** d'emprisonnement et **45 000 euros** d'amende.

→ Délit d'entrave : l'atteinte aux systèmes

- Art. 323-2 CP = **3 ans** d'emprisonnement et **45 000 euros** d'amende.

# Plan comptable

Règlement n° 99-03 du 29 avril 1999 du Comité de la réglementation comptable

## TITRE IV TENUE, STRUCTURE ET FONCTIONNEMENT DES COMPTES

410-2. – **Une documentation décrivant les procédures et l'organisation** comptables est établie en vue de permettre la compréhension et le **contrôle du système de traitement** ; cette documentation est conservée aussi longtemps qu'est exigée la présentation des documents comptables auxquels elle se rapporte.

410-3. – L'organisation du système de traitement permet de **reconstituer à partir des pièces justificatives** appuyant les données entrées, les éléments des comptes, états et renseignements, soumis à la vérification, ou, à partir de ces comptes, états et renseignements, de **retrouver ces données** et les pièces justificatives.

410-4. – L'organisation de la comptabilité tenue au moyen de systèmes informatisés implique **l'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements, en vue, notamment, de procéder aux tests nécessaires à la vérification des conditions d'enregistrement et de conservation des écritures.**

Toute donnée comptable entrée dans le système de traitement est enregistrée, sous une forme directement intelligible, sur papier ou éventuellement sur tout support offrant toute garantie en matière de preuve.

## CRC 99-03 suite

**420-2.** – Tout enregistrement comptable précise **l'origine**, le contenu et l'imputation de chaque donnée, ainsi que les **références de la pièce justificative** qui l'appuie.

**420-3.** – Chaque écriture s'appuie sur une pièce justificative datée, établie sur papier ou sur un **support assurant la fiabilité, la conservation et la restitution en clair de son contenu** pendant les délais requis. Les pièces justificatives sont classées dans un ordre défini dans la documentation prévue à l'article 410-2 décrivant les procédures et l'organisation comptables.

**420-5.** – **Le caractère définitif des enregistrements du livre-journal et du livre d'inventaire est assuré:**  
1 – pour les comptabilités tenues au moyen de systèmes informatisés, par une **procédure de validation, qui interdit toute modification ou suppression de l'enregistrement**

**420-6.** – **Une procédure de clôture destinée à figer la chronologie et à garantir l'intangibilité des enregistrements est mise en oeuvre au plus tard avant l'expiration de la période suivante.**

La procédure de clôture est appliquée au total des mouvements enregistrés conformément à l'article 420-4. Pour les comptabilités informatisées lorsque la date de l'opération correspond à une période déjà figée par la clôture, l'opération concernée est enregistrée à la date du premier jour de la période non encore clôturée, avec mention expresse de sa date de survenance.

## les normes d'audit comptables : un tronc commun se dégage !

- USA : loi Sarbanes-Oxley Contrôle interne du SI (section 404)
- International : IAS (norme d'audit)
- France :
  - ➔ LSF (idem SarBox)
  - ➔ NEP (normes d'exercice professionnel définies par le H3C et CNCC)

Tous portent sur les aspect suivants :

- ➔ les contrôles généraux informatiques (liés aux processus informatiques)
- ➔ les contrôles applicatifs (liés aux processus métiers et aux applications qui les supportent)
- ➔ les contrôles au niveau des données (cohérence – recoupements – exhaustivité ...)

voir notamment « IT Control objectives for Sarbanes-Oxley », IT Governance Institute®, [www.itgi.org](http://www.itgi.org)

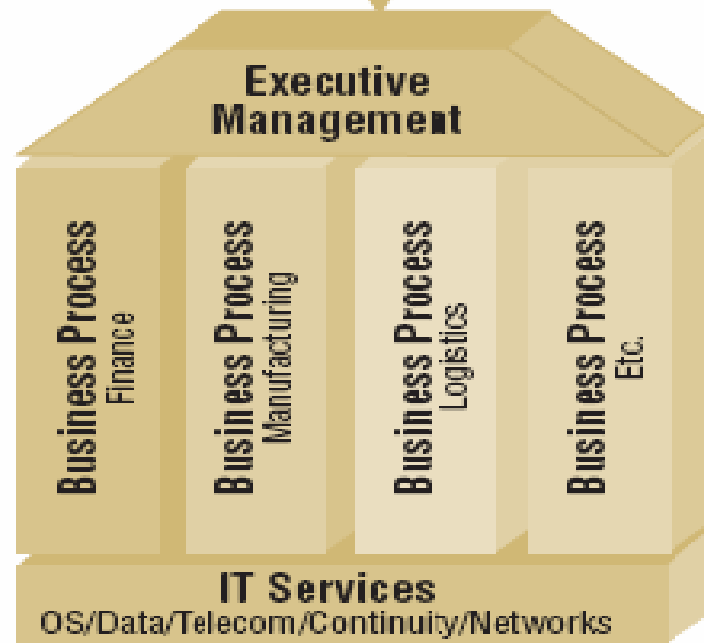
# SarBox 404 = Evaluation du contrôle interne : une approche transversale

## Elle ne se limite pas à la sphère comptable

### Company-level Controls

Company-level controls over the IT control environment set the tone for the organization. Examples include:

- Operating style
- Enterprise policies
- Governance
- Collaboration
- Information sharing



### Application Controls

Controls embedded in business process applications, such as large ERP systems and smaller best-of-breed systems, are commonly referred to as application controls. Examples include:

- Completeness
- Accuracy
- Validity
- Authorization
- Segregation of duties

les contrôles des processus applicatifs

les contrôles généraux informatiques

### General Controls

Controls embedded in IT services form general controls. Examples include:

- Program development
- Program changes
- Computer operations
- Access to programs and data

## Loi sur la Sécurité financière

- Art 120 de la LSF inséré dans l'article L.225-235 du code de commerce prévoit que :
  - « les CAC de la société doivent établir un nouveau rapport, joint au rapport général, qui doit contenir leurs observations sur le rapport du président pour celles des procédures de contrôle interne qui sont relative à l'élaboration et au **traitement de l'information comptable et financière** ».
  - « dans ce rapport, les CAC devront **vérifier la sincérité et la concordance avec les comptes des informations relatives aux procédures de contrôle interne** touchant au domaine comptable et financier données par le président dans son rapport de l'article 117 ».
- Ce rapport ne concerne plus, depuis 2005, que les SA faisant Appel Public à l'Épargne (APE). Toutefois toute personne morale faisant APE a l'obligation de publicité des informations relevant du contrôle interne.

## Les NEP 315 et 330 (2/3)

Ces 2 normes nouvelles font la synthèse de 3 anciennes (2-202, 2-301, 2-302)

### ■ NEP 315

Définition des modalités de prise de connaissance de l'entité, notamment du point de vue du contrôle interne :

- « Risque résultant de l'utilisation des traitements informatisés »
- « prise de connaissance du SI relatif à l'élaboration de l'information financière »

### ■ NEP 330

Procédures mises en place à l'issue de l'évaluation des risques

- « recours à un expert »
- « test de procédure, test de substance ou approche mixte »
- Précision sur la nature des tests de procédure et des contrôles de substance

### ■ NEP 240

- Présomption de risque d'anomalies significatives résultant de fraudes dans la comptabilisation des produits.
- Cette nouveauté dans la norme implique d'accorder une attention particulière au **CI du SI assurant la facturation**

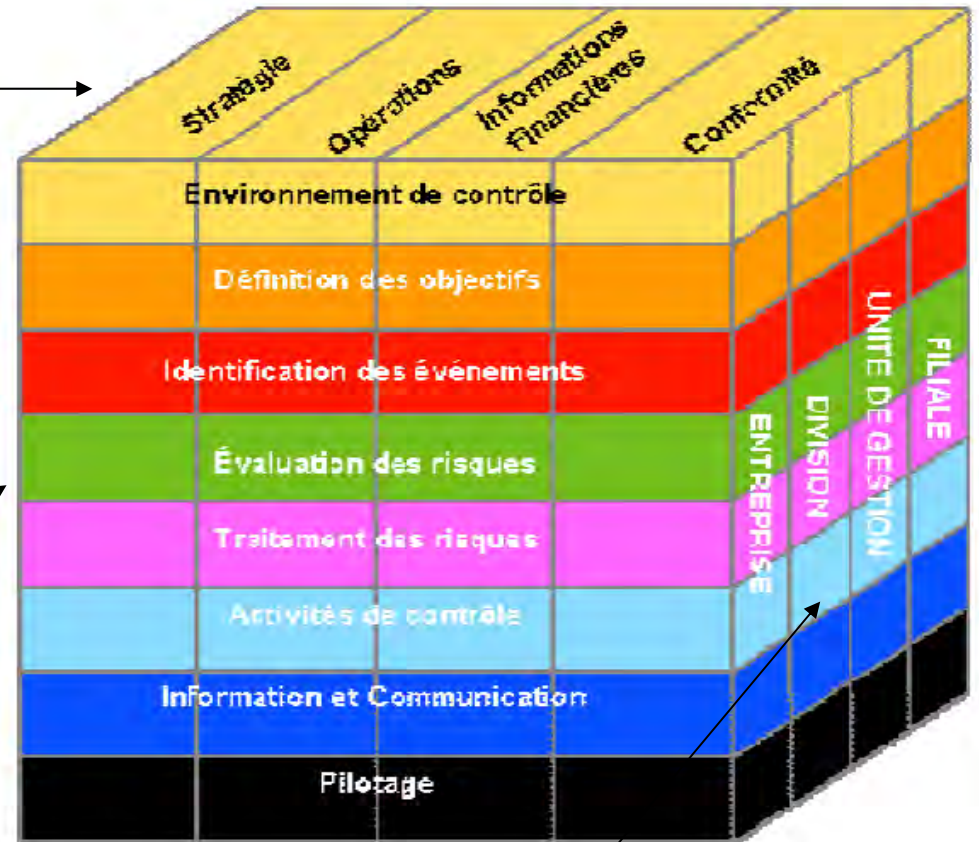
## Quels outils pour répondre aux nouvelles exigences : Présentation des principaux référentiels systèmes

- COSO : contrôle interne
- COBIT : analyse et contrôle system
- ITIL : contrôle system
- MEHARI : analyse des risques – pilotage sécurité
- ISO 17799 : idem
- SYSTRUST : certification de conformité

# COSO : le contrôle interne selon une approche multidimensionnelle

## ■ Colonnes : Objectifs :

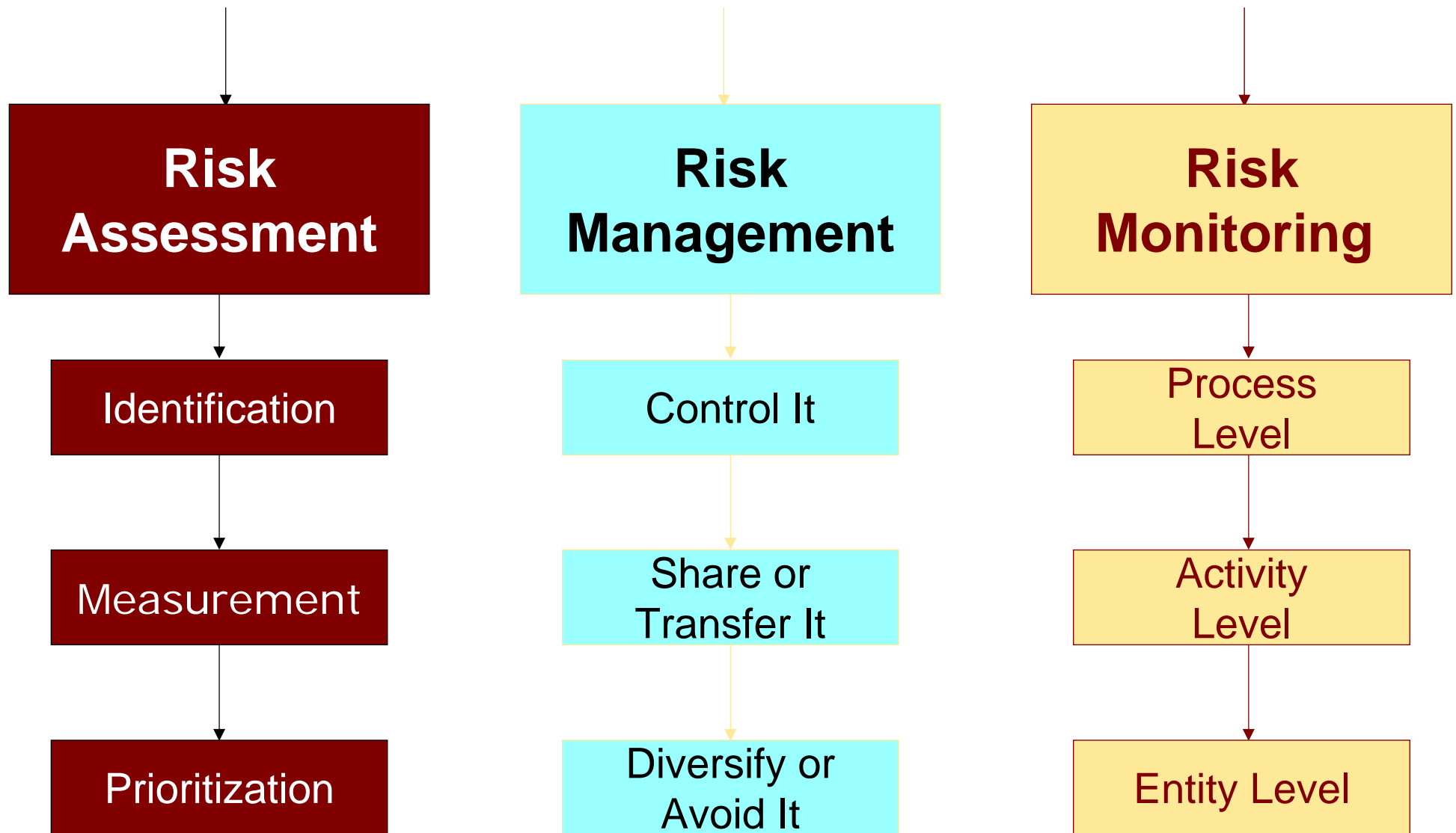
- Stratégiques
- Opérationnels
- Reporting
- Conformité



## ■ Lignes : Management des risques

## ■ Profondeur : unités de l'organisation

# Matrice des risques coso



# COBIT Framework

## Business Objectives

### Criteria

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

## IT RESOURCES

- Data
- Application systems
- Technology
- Facilities
- People

- PO1 Define a strategic IT plan  
 PO2 Define the information architecture  
 PO3 Determine the technological direction  
 PO4 Define the IT organisation and relationships  
 PO5 Manage the IT investment  
 PO6 Communicate management aims and direction  
 PO7 Manage human resources  
 PO8 Ensure compliance with external requirements  
 PO9 Assess risks  
 PO10 Manage projects  
 PO11 Manage quality

## MONITOR AND EVALUATE

- M1 Monitor the process  
 M2 Assess internal control adequacy  
 M3 Obtain independent assurance  
 M4 Provide for independent audit

## PLAN AND ORGANISE

## ACQUIRE AND IMPLEMENT

## DELIVER AND SUPPORT

- DS1 Define service levels  
 DS2 Manage third-party services  
 DS3 Manage performance and capacity  
 DS4 Ensure continuous service  
 DS5 Ensure systems security  
 DS6 Identify and attribute costs  
 DS7 Educate and train users  
 DS8 Assist and advise IT customers  
 DS9 Manage the configuration  
 DS10 Manage problems and incidents  
 DS11 Manage data  
 DS12 Manage facilities  
 DS13 Manage operations

- AI1 Identify automated solutions  
 AI2 Acquire and maintain application software  
 AI3 Acquire and maintain technology infrastructure  
 AI4 Develop and maintain IT procedures  
 AI5 Install and accredit systems  
 AI6 Manage changes

### Processus

### Commentaire

#### Gestion des niveaux de services

Définit la démarche de gestion des contrats de service, avec pour objectif de gérer les attentes en matière de prestations au regard des ressources allouées.

#### Gestion des configurations

Détail la manière d'inventorier actifs et configurations, en vue d'évaluer les risques, les besoins de mise à jour et les coûts d'équipements.

#### Gestion des changements

Recommande de passer en revue l'ensemble des conséquences que peuvent engendrer des changements sur les infrastructures informatiques.

#### Gestion des incidents

Renvoie à la manière d'identifier les causes des incidents, puis de les gérer en fonction de leur degré d'impact sur l'activité de l'entreprise.

#### Gestion des problèmes

Décrit une démarche comparable à la précédente en vue de gérer les incidents récurrents.

#### Gestion des mises en production

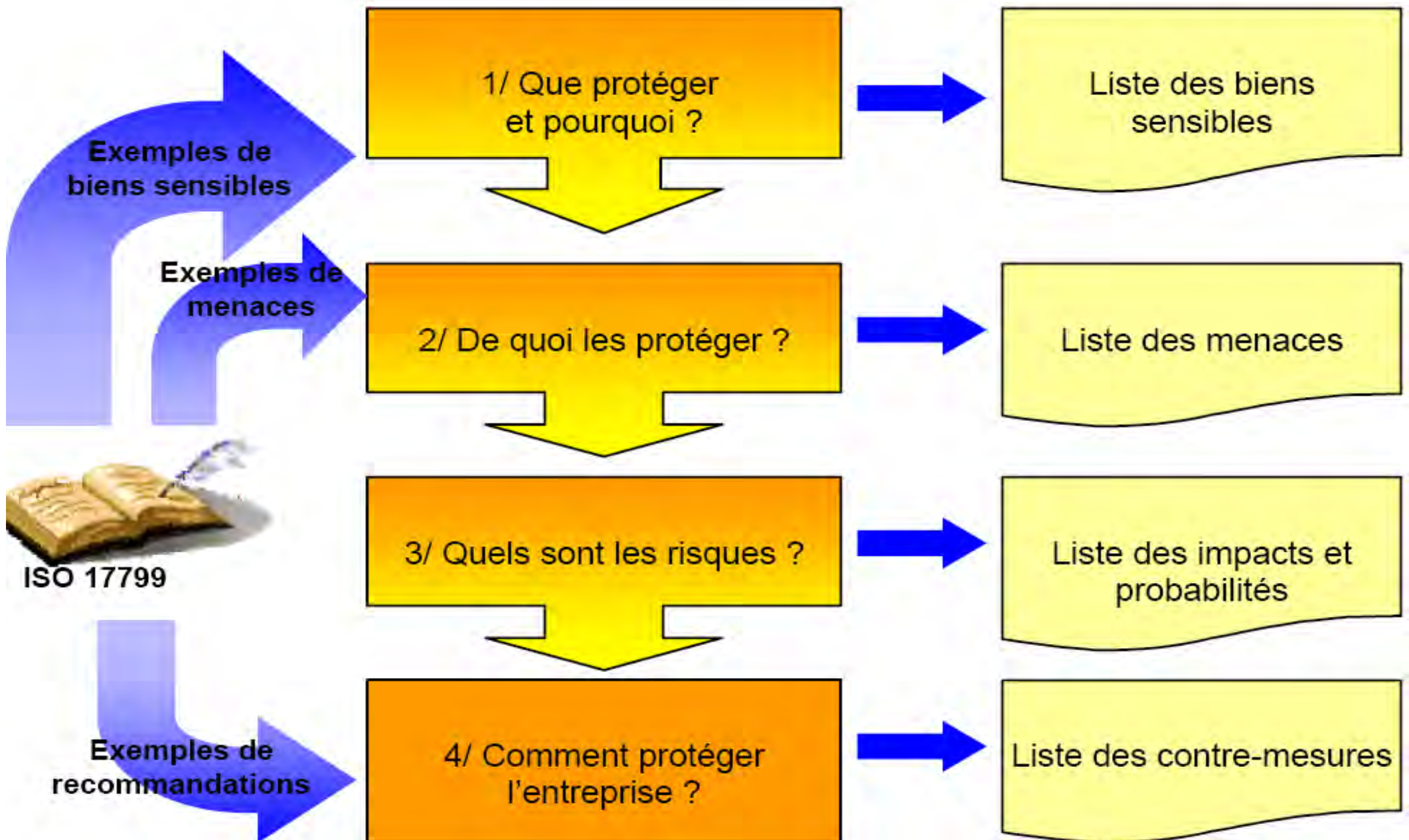
Fait le lien entre les activités du département production et les métiers, en vue d'appliquer des règles de déploiement en adéquation avec les exigences de ces derniers.

- gestion de la disponibilité
- gestion de la capacité
- continuité de services
- gestion financière des services

# MEHARI : Cadre - méthodes - base de connaissance

- Définition des enjeux
- Inventaire des vulnérabilités
- Inventaires et niveau de risques
- Pilotage de la sécurité

# ISO 17799 : principes - objectifs – bonnes pratiques



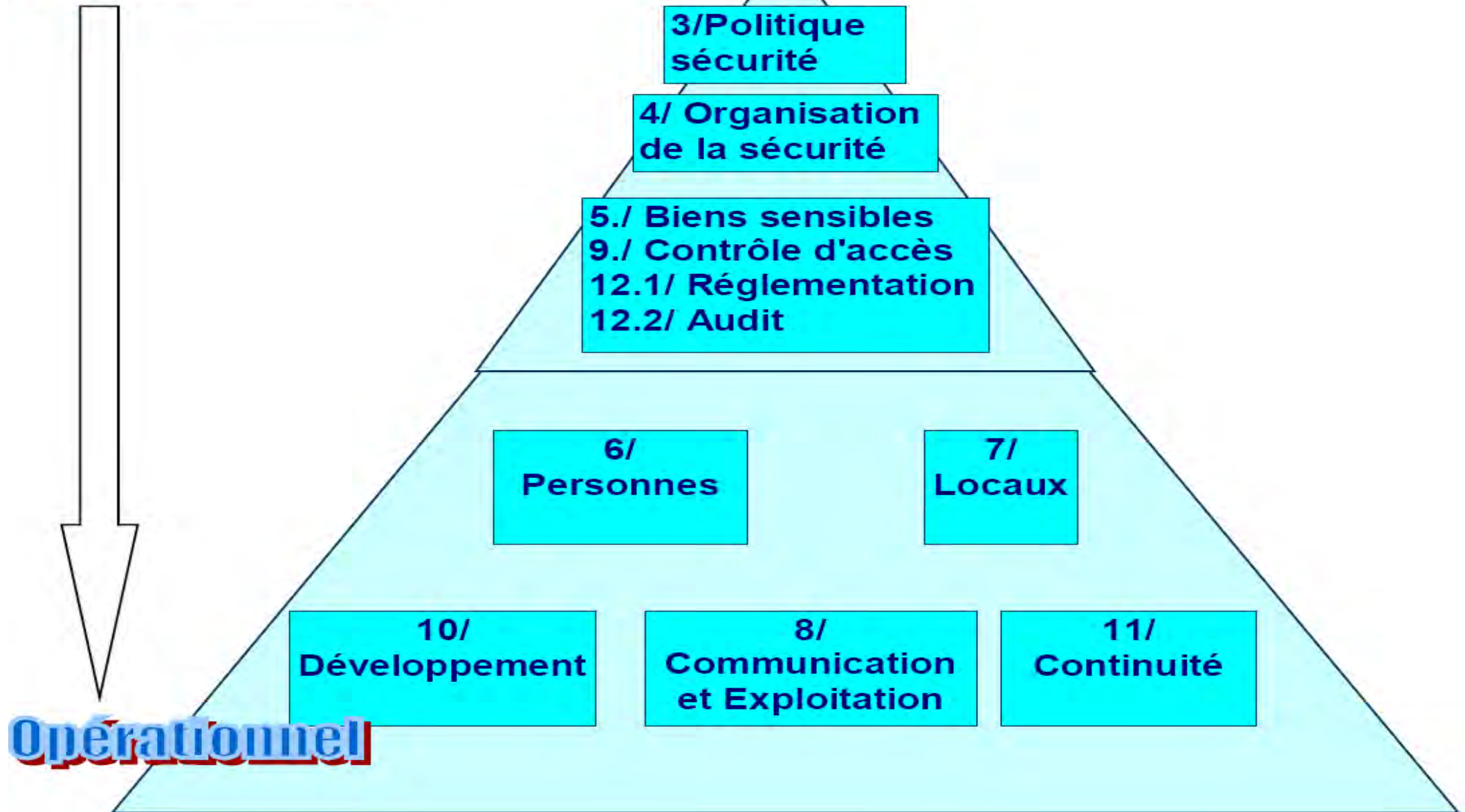
# ISO 17799

## Les onze thèmes clés de ISO 17799 : 2005



# ISO 17799 : Structure de la norme

**Organisationnel**



**Opérationnel**

## Convergences et tendances

Un constat : On retrouve une analyse commune dans les normes comptables et dans les référentiels systèmes

### ■ Objectifs et Principes :

→ fiabilité – disponibilité – confidentialité - Exhaustivité intégrité – échange ... de l'information financière

### ■ Règles :

→ Inaltérabilité – contrôle interne - Piste d'audit ...

### ■ Méthodologie et processus :

→ Sécurité - Contrôles accès – historisation – archivage...

### ■ Codification et communication

→ UML – XML - ASCII (TXT) – EDI – XBRL

## Conclusion

- La gouvernance d'entreprise doit intégrer la gouvernance du SI.
  - ➔ Pour raisons stratégiques
  - ➔ Par obligations réglementaires
- La mise en place d'un système de Contrôle Interne du SI est indispensable.
- Les audits externes vont évaluer le CI régulièrement

**L'ensemble de la présentation  
sera disponible sur le site**

**[www.lacademie.info](http://www.lacademie.info)**

**Nos prochains Petits déjeuners de l'Académie :**

- Dominique LAMIOT, Directeur Général de la Comptabilité Publique **le 15 janvier 2008**
- Philippe DANJOU, Membre du board de l'IASB **le 6 février 2008**

**L'Académie remercie ses partenaires**

**La Tribune**

**sage**

**2SI** SYSTEMES  
**comptalia**  
tv

