

---

# Assises de la Sécurité 2009

## *Le Contrôle Interne du Système d'Information des Organisations*

Régis Delayat  
SCOR, DSI Groupe  
Administrateur du Cigref  
7 octobre 2009

# Agenda

---

- **Crise financière : faillite du contrôle interne et des systèmes d'information ?**
- **Des risques accrus pour l'entreprise**
- **Les SI au cœur des risques d'entreprise**
- **L'initiative conjointe Cigref/Ifaci pour renforcer le contrôle interne du système d'information**
  - Le contrôle interne du système d'information de l'entreprise
  - Le contrôle interne de la DSI
  - Illustrations SCOR
- **Conclusion**

# Crise financière : faillite du contrôle interne et des systèmes d'information ? (verbatim)

- « Les failles du contrôle interne portent indéniablement leur part de responsabilité dans la crise actuelle »
- « Le contrôle interne, que l'on pensait bien installé au sein des établissements bancaires, a montré au cours de la période récente des signes de grande faiblesse »
- « La crise a révélé des insuffisances dans les systèmes de gestion du risque et de gouvernance d'entreprise »
- « C'est la culture du contrôle et de la prudence qu'il paraît urgent d'approfondir au sein des établissements bancaires et financiers »
- « Trop de contrôle tue le contrôle : un trop plein de procédures pousse les salariés à les contourner »
- « Loin de jouer le rôle qu'on attendait d'eux, les systèmes d'information ont amplifié la crise financière »
- « Le SI aurait dû tirer la sonnette d'alarme et édicter des solutions prédictives prêtes à être déployées »
- « On ne peut s'empêcher de s'interroger sur les causes de l'incapacité des systèmes informatiques à détecter, prévenir et alerter les acteurs sur les risques encourus »
- « L'informatisation est la cause matérielle de la crise financière. A l'origine se trouve en effet une autre crise, l'inadéquation de nos comportements au monde nouveau qu'a ouvert l'informatisation »

# La juste place du contrôle interne et des systèmes d'information...(verbatim)

- « Les radars économiques ne fonctionnent plus, place aux intuitifs, aux détecteurs de signaux faibles et transdisciplinaires »
- « Les procédures de validation n'ont pas fonctionné car elles sont organisées verticalement, en silos étanches »
- « Le pilotage de l'entreprise et l'analyse des risques se sont cantonnés à une batterie de mesures prises isolément les unes des autres »
- « Pour certains experts, la crise est derrière nous, pour d'autres le pire est à venir. La réalité, c'est que personne n'y comprend rien »
- “Notre compréhension du monde s'érode, le lien entre ce qui se passe aujourd'hui et ce qui est à venir est de plus en plus nébuleux”
- “L'économique, science de la masse, basée sur les statistiques et le calcul du nombre, n'est plus en mesure de penser le monde ! Ses règles sont quantitatives ; elles reposent sur des projections linéaires qui ne tiennent pas compte des aléas alors que l'on est entré dans un monde de l'inédit.”
- « Si responsabilité de l'informatique il y a, elle réside dans le manque de discernement de ses utilisateurs »
- « Quand les réseaux suppriment la distance, quand on peut lancer d'un simple clic toute une cascade d'opérations, la simplicité de la procédure masque la complexité des choses »

# Un univers des risques en expansion et en mutation

---

- Des anciens risques plus présents et plus lourds que jamais
- Des nouveaux risques qui se multiplient
- Des risques de plus en plus complexes et de moins en moins contrôlables
- Des risques aux conséquences plus « durables » voire « irréversibles » (changement climatique)
- Des risques « moins visibles » et plus insidieux (terrorisme, virus informatiques)
- Des risques « globalisés » (crise financière, criminalité, pillage économique)
- Des risques dont nous n'avons aucune expérience (grippe A)
- Une perception aggravée des risques, un sentiment croissant de vulnérabilité
- Une aversion accrue au risque

# L'entreprise est devenue la grande gestionnaire des risques

---

- La remise en cause des protections traditionnelles
- L'entreprise « responsable de tout devant tous »
  - *Une responsabilité au-delà des frontières de l'entreprise (salariés, clients, fournisseurs, actionnaires, environnement, générations futures)*
  - *Une responsabilité de plus en plus étendue (contenu, rétroactivité, globalisation)*
  - *Une responsabilité de plus en plus sanctionnée (principe de précaution, sanctions pécuniaires, pénales et réputationnelles, multiplication des contrôles externes)*
- La nouvelle gestion des risques dans l'entreprise, le « risk management » global et intégré
- L'entreprise de plus en plus dépendante de ses systèmes d'information

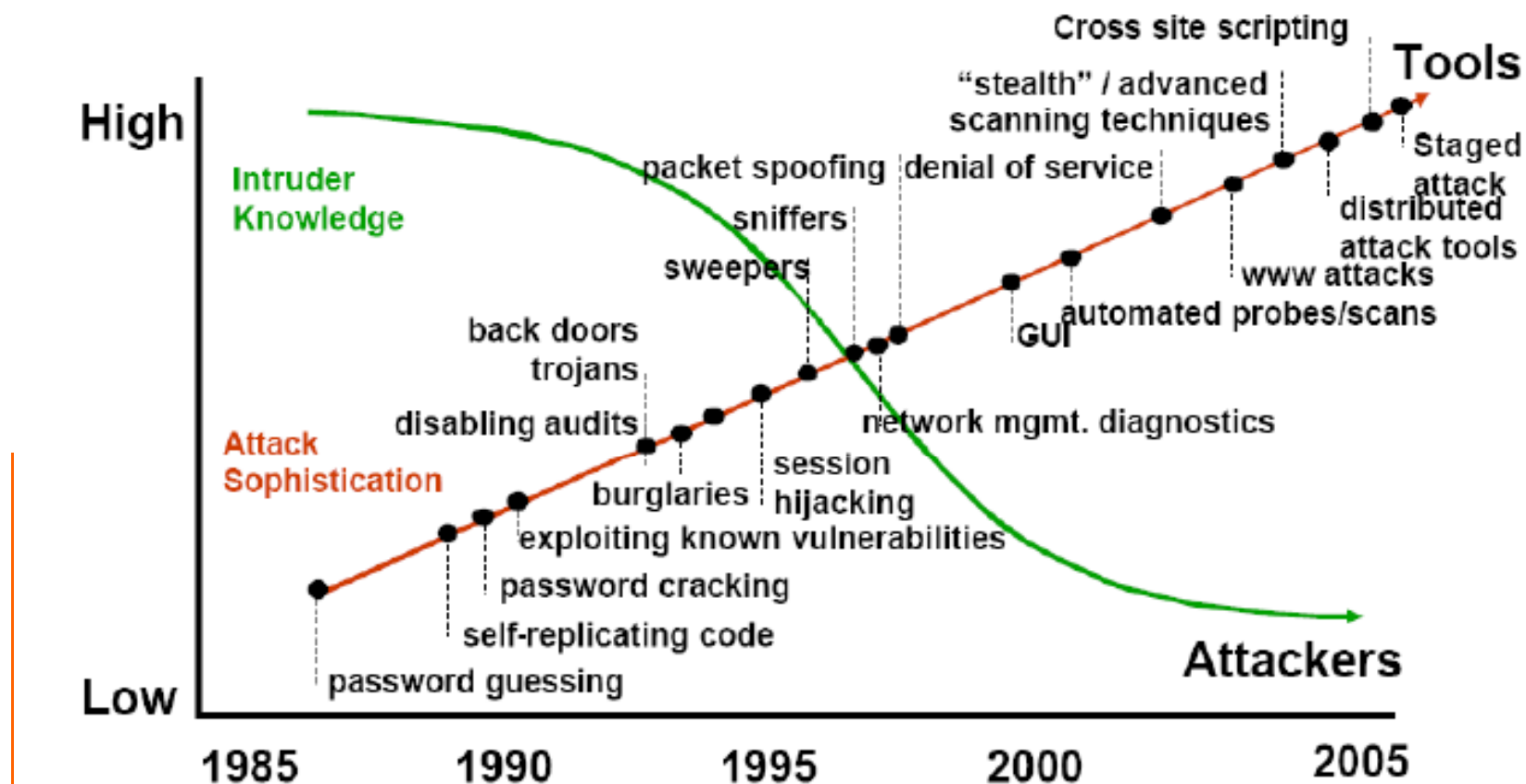
# Les SI au cœur des risques d'entreprise



Source: The Economist Intelligence Unit survey, 2008

# Les SI au cœur des risques d'entreprise

Des cyber-attaques de plus en plus sophistiquées et ouvertes au plus grand nombre !



Source : PricewaterhouseCoopers  
2008 Global State of Information Security Study

# Les SI au cœur des risques d'entreprise

---

- Rôle primordial des systèmes d'information dans la vie de l'entreprise
- Risques majeurs liés aux systèmes d'informations dans l'entreprise
- La protection des systèmes d'information est devenu un enjeu majeur de la politique des risques de l'entreprise
  - *Un enjeu de concurrence décisif*
  - *Des coûts de protection croissants*
- Le contrôle des risques d'entreprise repose aussi de plus en plus sur des systèmes d'information efficaces
  - *Le contrôle des risques suppose l'accumulation d'informations*
  - *La maîtrise des risques repose sur l'efficacité des systèmes d'information*

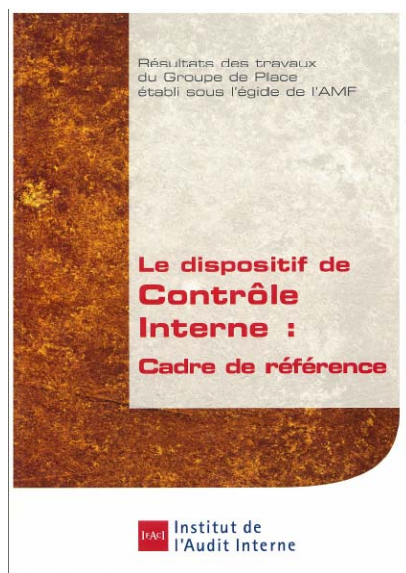
# Agenda

---

- **Crise financière : faillite du contrôle interne et des systèmes d'information ?**
- **Des risques accrus pour l'entreprise**
- **Les SI au cœur des risques d'entreprise**
- **L'initiative conjointe Cigref/Ifaci pour renforcer le contrôle interne du système d'information**
  - **Le contrôle interne du système d'information de l'entreprise**
  - **Le contrôle interne de la DSI**
  - **Illustrations SCOR**
- **Conclusion**

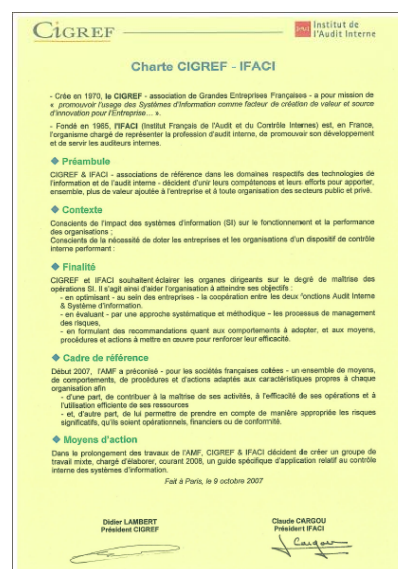
# Contrôle Interne : du Cadre de Référence AMF au Guide Opérationnel Cigref/Ifaci

## Cadre de Référence AMF



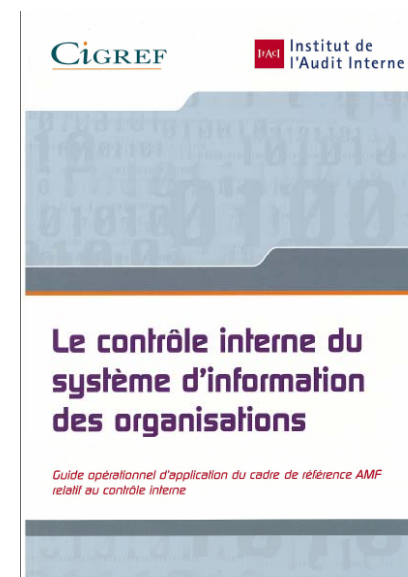
2007  
Janvier

## Charte Cigref/Ifaci



2007  
Octobre

## Le Contrôle Interne du SI : Guide opérationnel Cigref/Ifaci



2009  
Mars

# Objectifs de l'étude CIGREF/IFACI

---

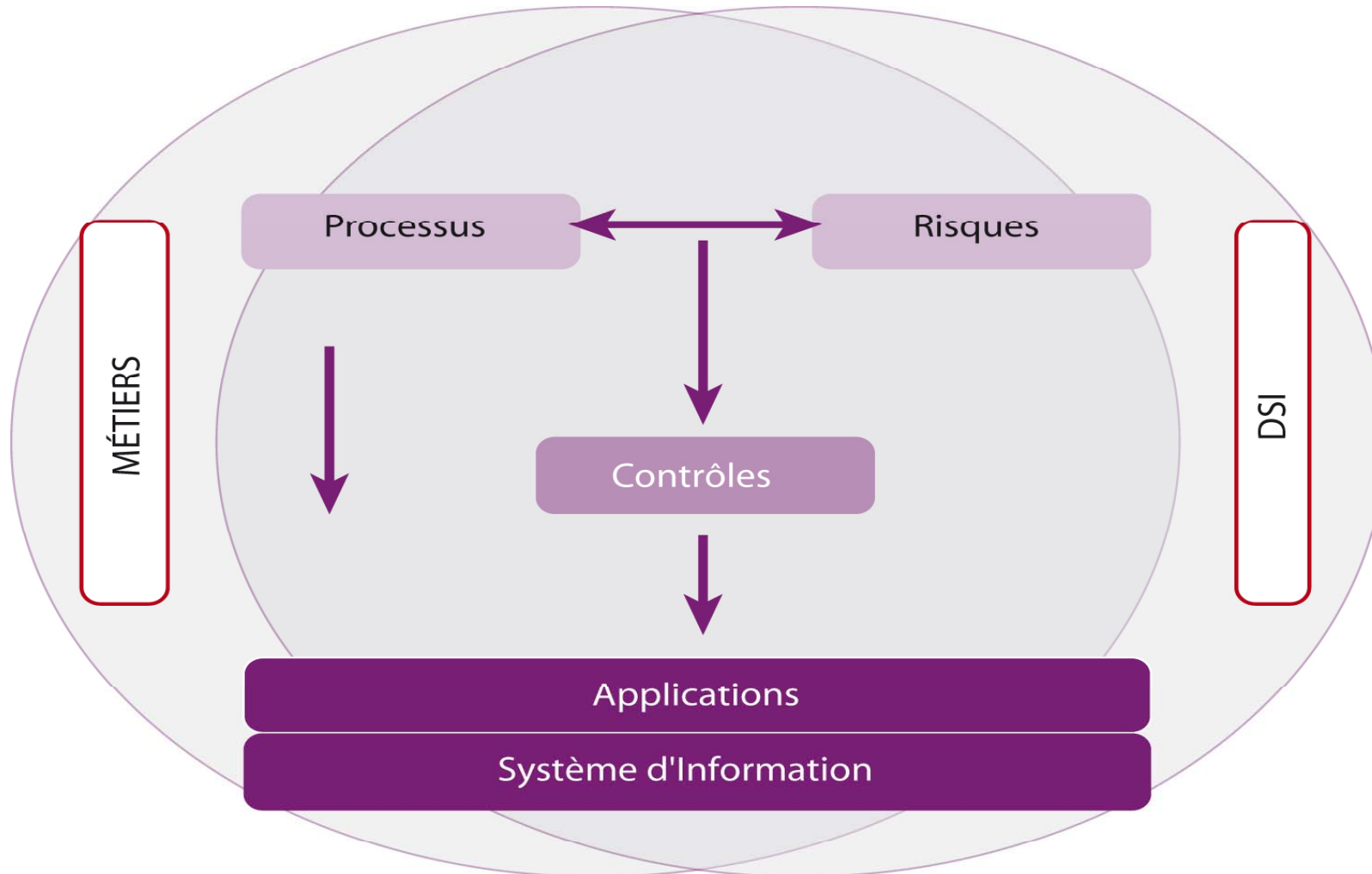
- Sensibiliser les Directeurs Généraux, Directeurs des Systèmes d'Information, Directeurs Audit et Contrôle, Directeurs Métiers, Consultants, etc...
- Enrichir la dimension SI du cadre AMF et mieux le relier aux référentiels existants
- Elaborer un guide d'application relatif au contrôle interne des systèmes d'information, incluant des listes de bonnes pratiques
- Aider les fonctions SI et Audit à mieux collaborer pour renforcer l'efficacité du contrôle interne de l'entreprise
- Avoir une approche sélective et réaliste des risques

# Les 5 principes du contrôle interne

---

1. Le management doit instaurer une culture et une dynamique du contrôle
2. Le contrôle interne doit être intégré dans les processus de l'entreprise
3. Les systèmes d'information jouent un rôle clé, ils sont à la fois objet et instrument du contrôle interne
4. Le principe de proportionnalité et granularité doit s'appliquer
5. Il faut être conscient de la non-exhaustivité et des limites du dispositif de contrôle

# Le contrôle interne du système d'information : deux parties distinctes et complémentaires



# Typologie des points de contrôle

## Contrôles métier

Tout contrôle (tel que les vérifications d'autorisations de transaction, les rapprochements exhaustifs ou non, ...) effectué par les entités opérationnelles dans le cadre des processus métier. Ce sont souvent des contrôles manuels qui s'appuient sur des états produits par les applications.

## Contrôles généraux informatiques

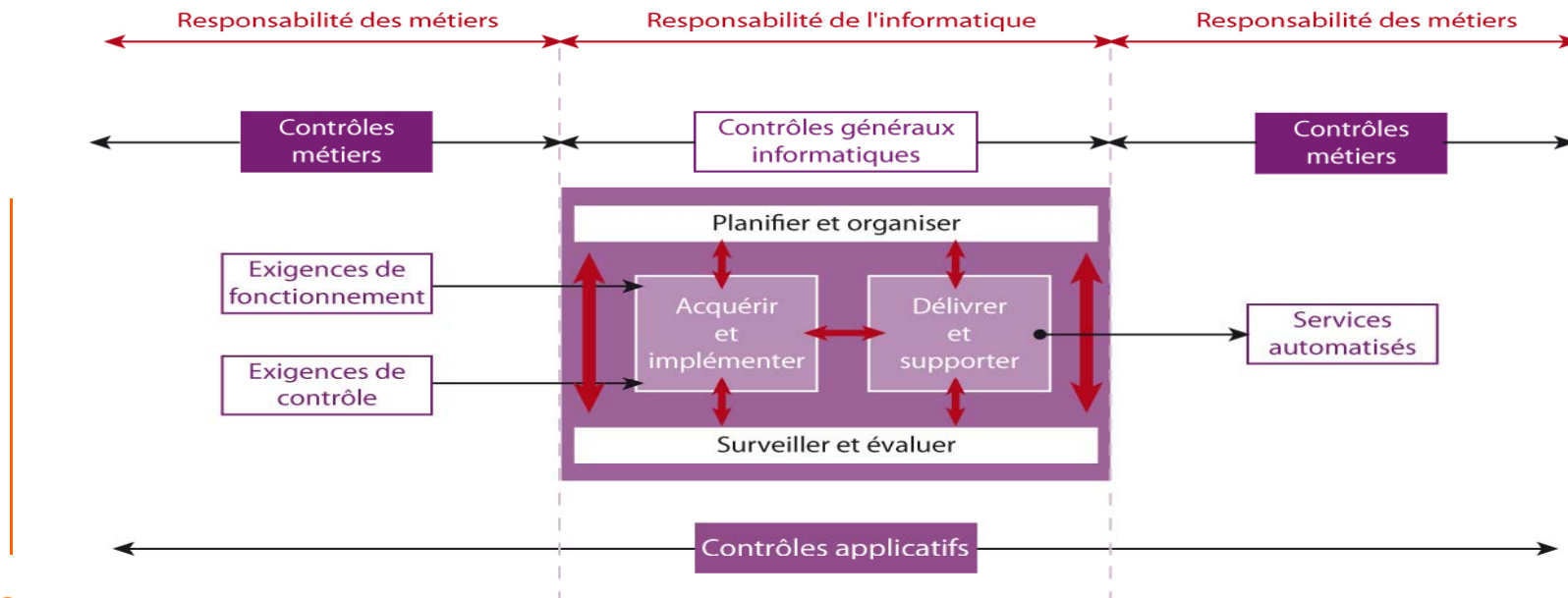
Les contrôles généraux sont ceux qui sont intégrés aux processus et aux services informatiques. Ils concernent, par exemple :

- le développement des systèmes,
- la gestion des changements,
- la sécurité,
- l'exploitation.

## Contrôles applicatifs

On appelle communément "contrôles applicatifs" les contrôles intégrés dans les applications métier. Ils concernent, par exemple :

- l'exhaustivité,
- l'exactitude,
- la validité,
- l'autorisation,
- la séparation des tâches.

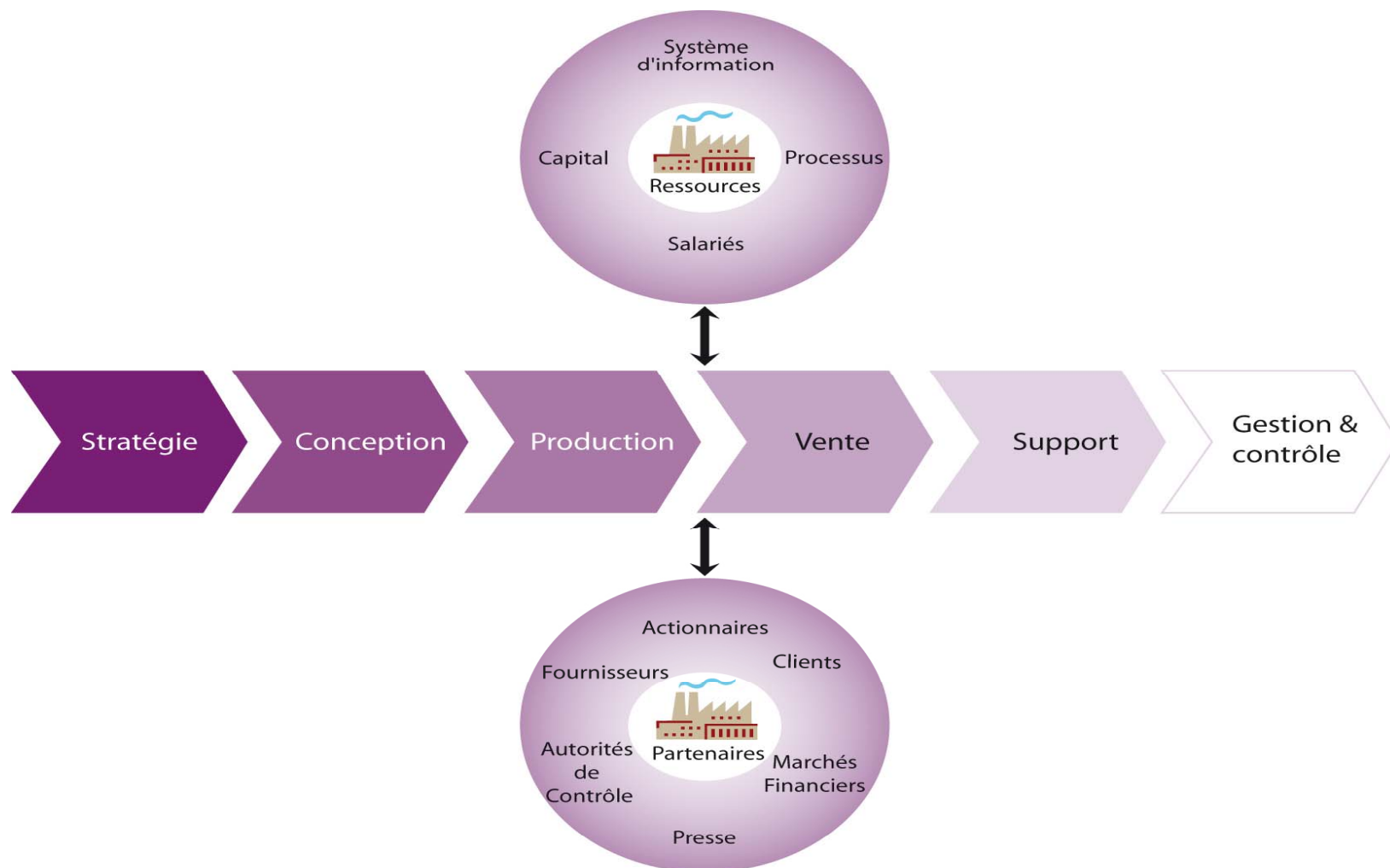


Source: CobiT®

# Les acteurs du risque (RACI)

	Identification des risques	Evaluation des risques	Traitement des risques	Surveillance
<b>Direction générale</b>	Approbateur	Approbateur	Informé	Approbateur
<b>Directeur métier *</b>	Approbateur	Approbateur	Approbateur	Approbateur
<b>Opérationnels métier</b>	Réalisateur	Réalisateur	Réalisateur	Consulté
<b>Direction des systèmes d'information</b>			Réalisateur	Consulté
<b>Risk Manager Groupe</b>	Réalisateur	Réalisateur / Approbateur	Informé	Informé
<b>Responsable Sécurité SI</b>	Informé	Informé	Réalisateur	
<b>Responsable du contrôle interne</b>	Consulté	Consulté	Consulté	Réalisateur
<b>Audit interne</b>	Informé / Réalisateur **	Informé / Réalisateur **	Informé	Réalisateur

# Chaîne de valeur de l'entreprise



# Les processus de l'entreprise

Processus de direction	Processus opérationnels	Processus support
<ul style="list-style-type: none"><li>• Stratégie</li><li>• Organisation</li><li>• Déontologie</li><li>• Conformité</li><li>• Gestion des Risques</li><li>• Communication financière</li><li>• Audit interne</li><li>• Affaires Publiques</li><li>• Communication interne</li><li>• Relations sociales</li></ul>	<ul style="list-style-type: none"><li>• Recherche &amp; Développement</li><li>• Achats</li><li>• Fabrication</li><li>• Contrôle qualité</li><li>• Distribution / Logistique</li><li>• Marketing</li><li>• Vente</li><li>• Après-vente</li></ul>	<ul style="list-style-type: none"><li>• Contrôle de gestion</li><li>• Trésorerie</li><li>• Comptabilité</li><li>• Investissements</li><li>• Consolidation</li><li>• Fiscalité</li><li>• Juridique</li><li>• RH</li><li>• Services généraux</li><li>• Informatique</li></ul>



# Les risques de l'entreprise

Risques financiers	Risques opérationnels	Risques de conformité
<ul style="list-style-type: none"><li>• Risques de contrepartie</li><li>• Risques de taux</li><li>• Risques de change</li><li>• Risques de marché</li><li>• Risques de liquidité</li></ul>	<ul style="list-style-type: none"><li>• Risques pays</li><li>• Catastrophe naturelle</li><li>• Fraudes, corruption</li><li>• Failles de sécurité</li><li>• Accidents de travail</li><li>• Arrêts de production</li><li>• Dommages aux actifs corporels</li><li>• Défaillances dans l'exécution et la gestion des processus et des systèmes</li><li>• Autres dysfonctionnements de l'activité</li></ul>	<ul style="list-style-type: none"><li>• Aspects légaux et réglementaires</li><li>• Risques de sanctions (administrative, judiciaire, disciplinaire)</li><li>• Risques de réputation et d'image</li><li>• Risques déontologiques</li><li>• Risques contractuels</li></ul>

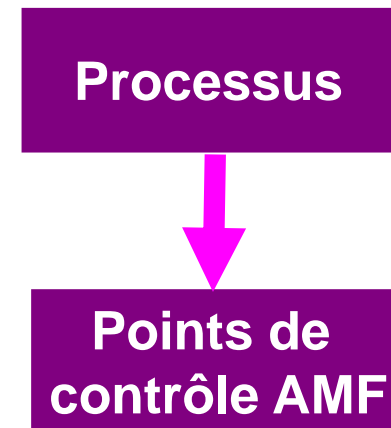
# Démarche des travaux sur le contrôle interne du système d'information de l'entreprise

---

- Une approche par les processus et par les risques
- Pour chaque processus, identification des étapes, des acteurs, des risques, et des contrôles à intégrer dès la conception de l'application
- Une illustration sur trois processus communs à un grand nombre d'entreprises : Achats, Ventes et Consolidation Financière
- Un rapprochement avec le Cadre de Référence AMF

# Le guide d'application AMF

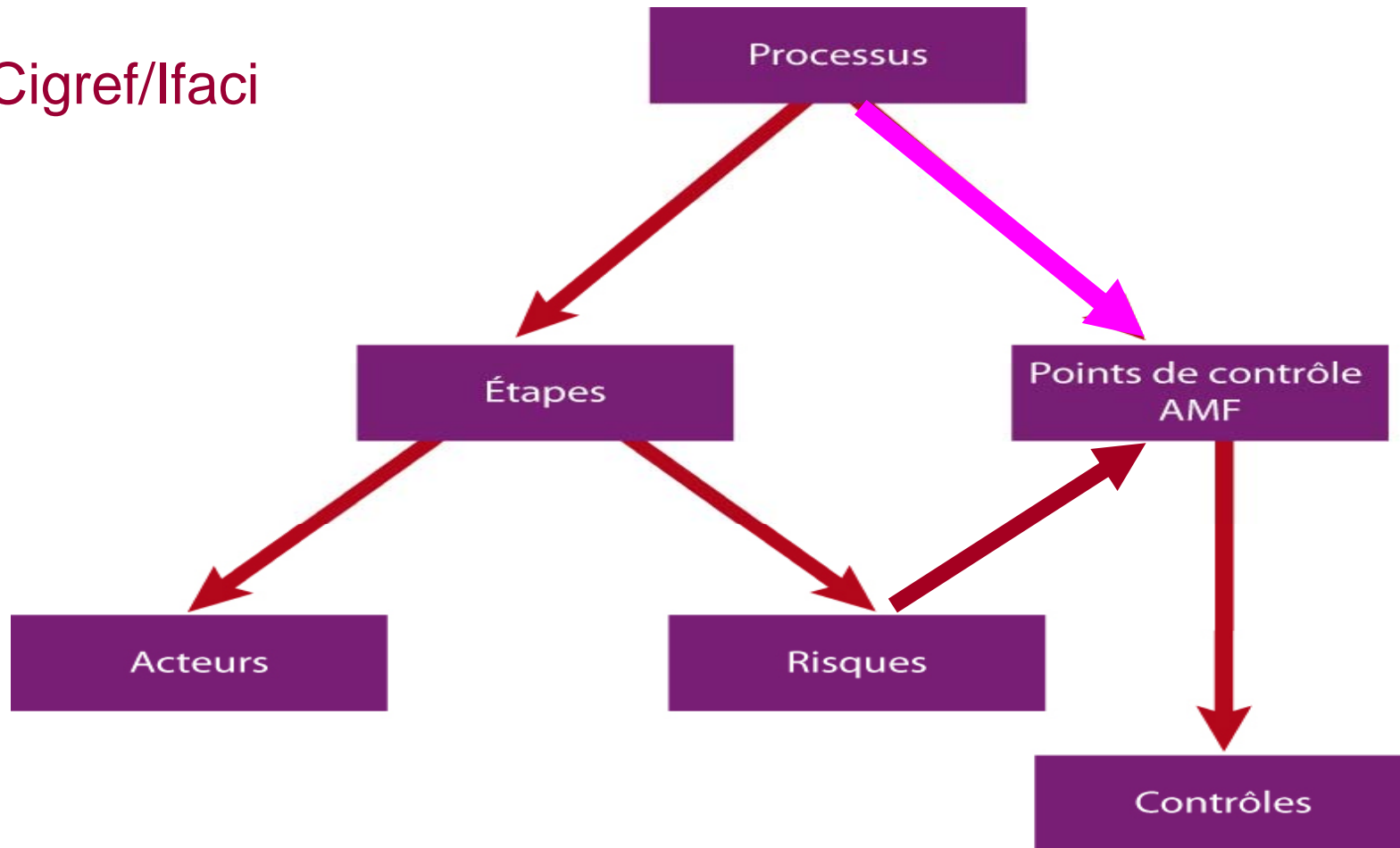
N° de §	Nom de l'opération
2.3.1	Investissement / désinvestissement / R&D
2.3.2	Immobilisations incorporelles, corporelles et goodwill
2.3.3	Immobilisations financières
<b>2.3.4</b>	<b>Achats fournisseurs et assimilés</b>
2.3.5	Coût de revient / stocks et encours / Contrats à long terme ou de construction
<b>2.3.6</b>	<b>Produits des activités ordinaires / Clients et Assimilés</b>
2.3.7	Trésorerie / financement et instruments financiers
2.3.8	Avantages accordés au personnel
2.3.9	Impôts, taxes et assimilés
2.3.10	Opérations sur le capital
2.3.11	Provisions et engagements
<b>2.3.12</b>	<b>Consolidation</b>
2.3.13	Information de gestion nécessaire à l'élaboration des informations comptables et financières publiées
2.3.14	Gestion de l'information financière externe



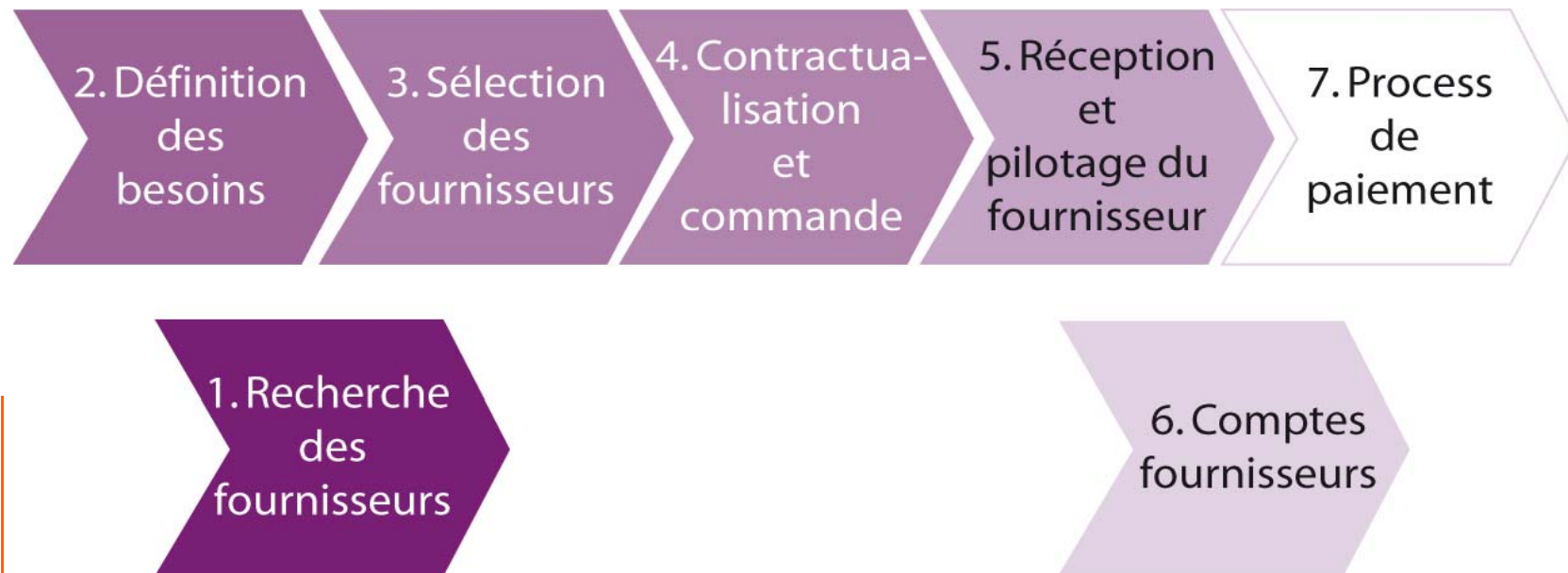
# Les travaux Cigref/Ifaci

➔ AMF

➔ Cigref/Ifaci

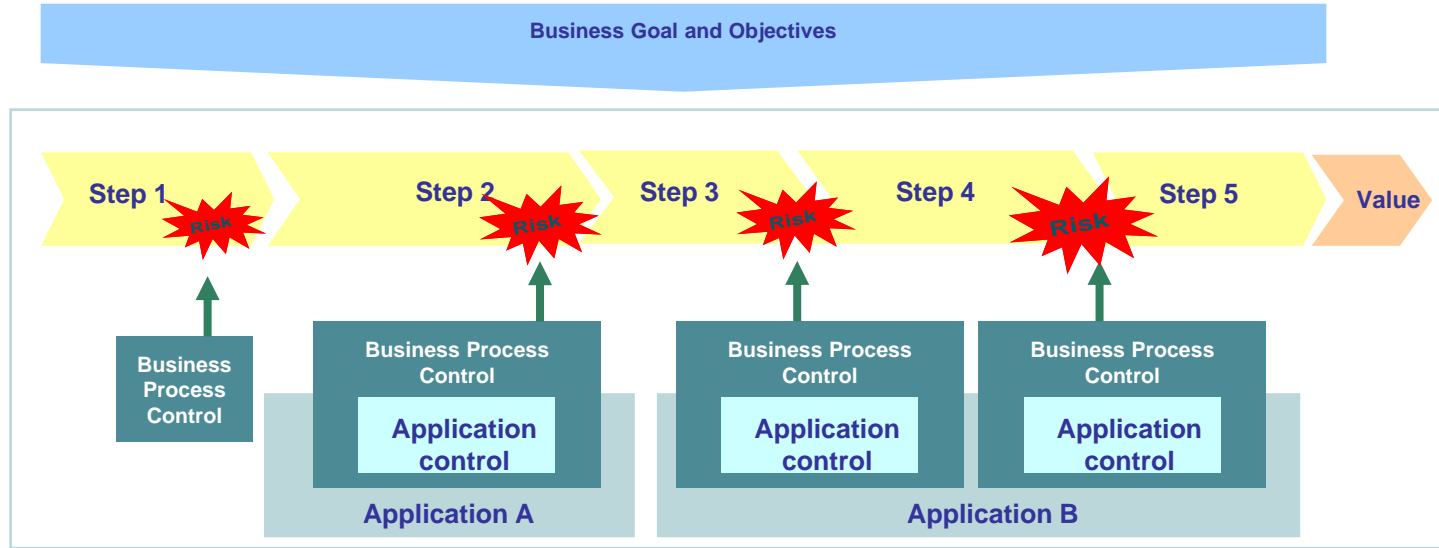


# Exemple : Processus Achats

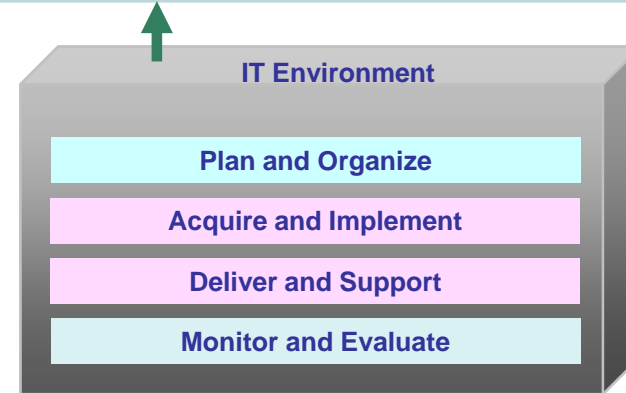


# L'intégration des contrôles lors du développement des applications

**Integrating Application Controls into Software Development/ Acquisition**



- AI1 Identify Relevant Control Objectives
- AI2 Design Application Control
- AI3
- AI4 Document Controls and Train Users
- AI7 Test and approve application controls



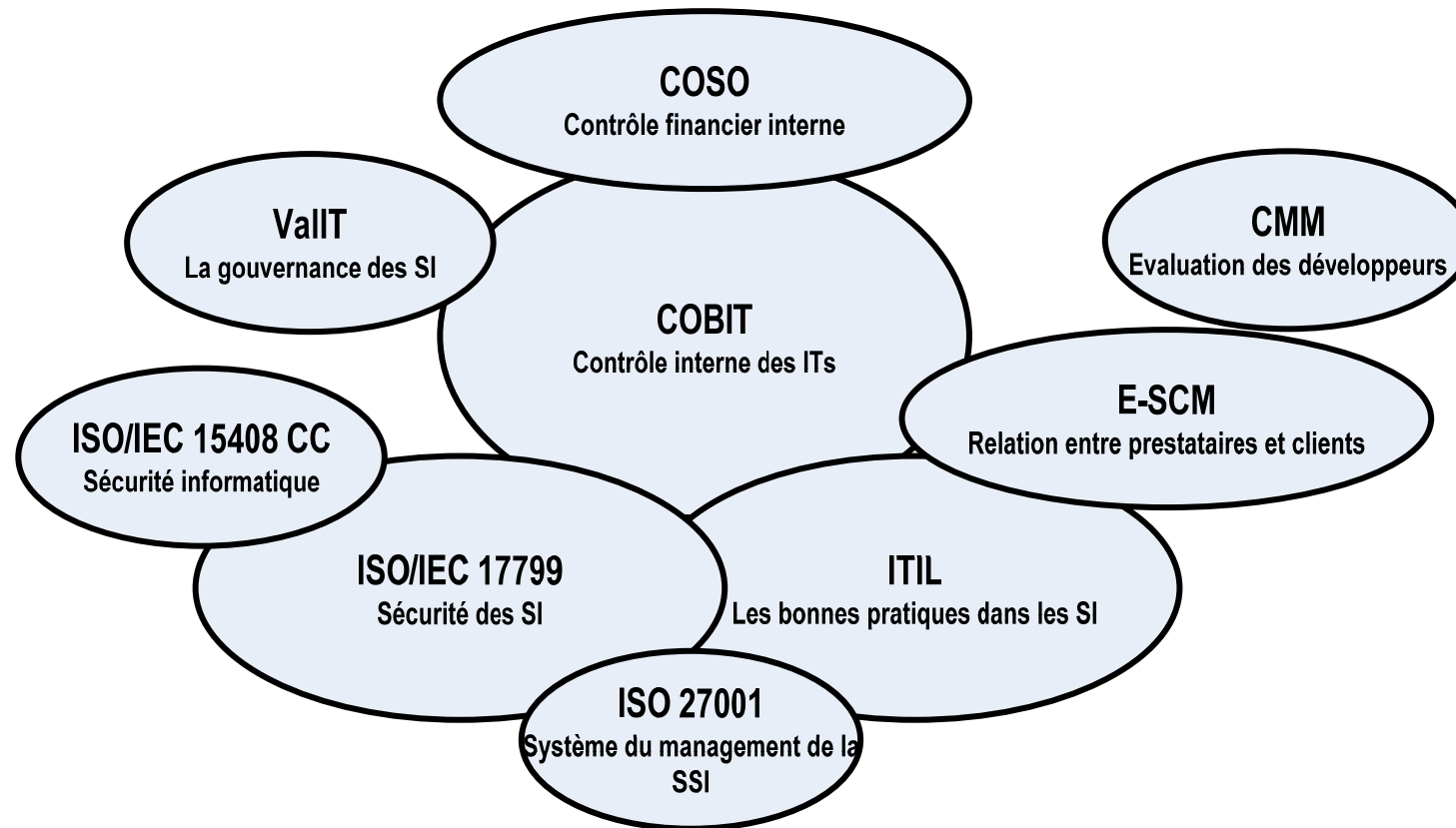
Source: CobiT® and Application Controls

# Agenda

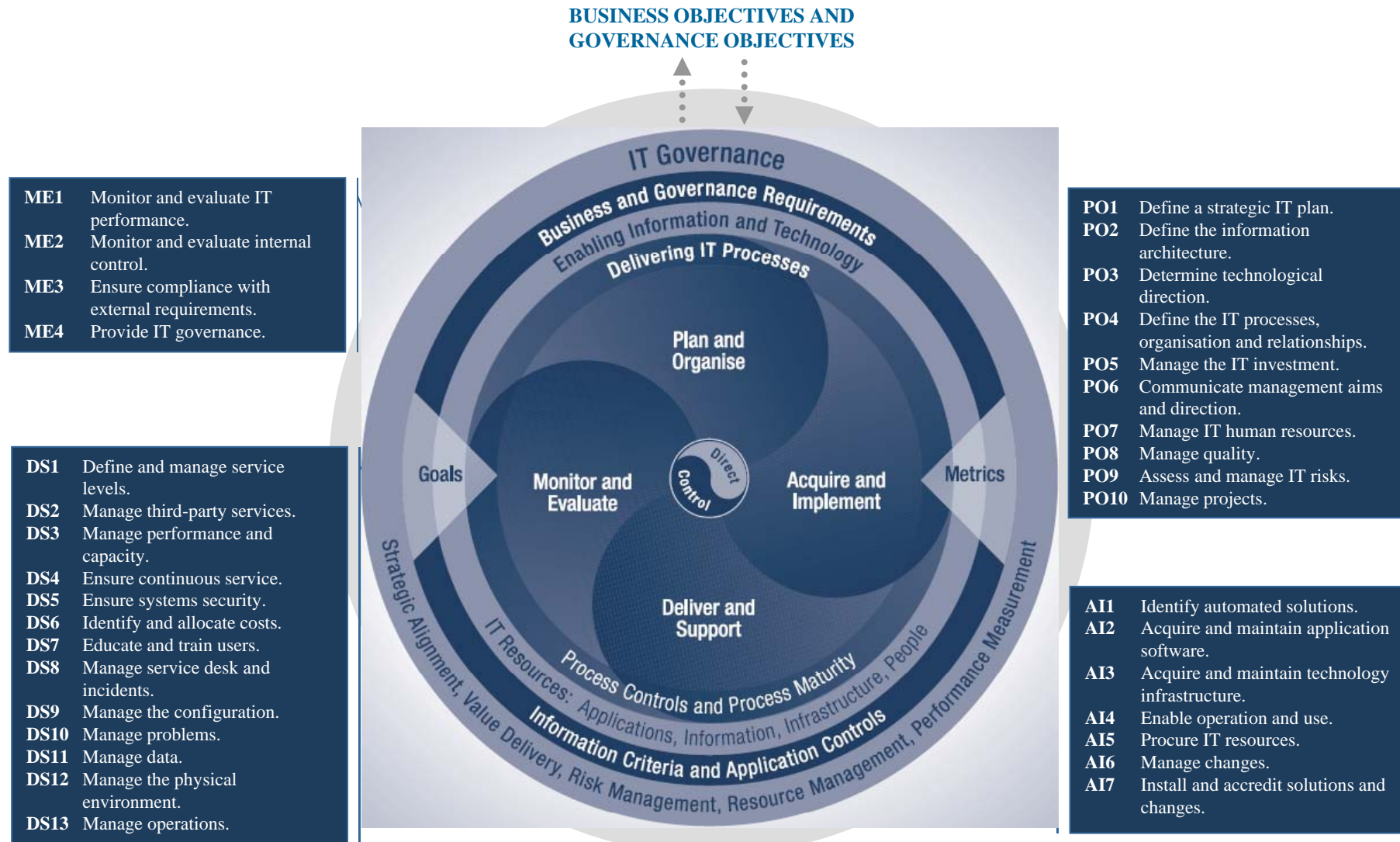
---

- **Crise financière : faillite du contrôle interne et des systèmes d'information ?**
- **Des risques accrus pour l'entreprise**
- **Les SI au cœur des risques d'entreprise**
- **L'initiative conjointe Cigref/Ifaci pour renforcer le contrôle interne du système d'information**
  - **Le contrôle interne du système d'information de l'entreprise**
  - **Le contrôle interne de la DSI**
  - **Illustrations SCOR**
- **Conclusion**

# Le contrôle interne de la DSI : Référentiels



# COBIT, la référence du contrôle interne de la DSI



# Démarche

---

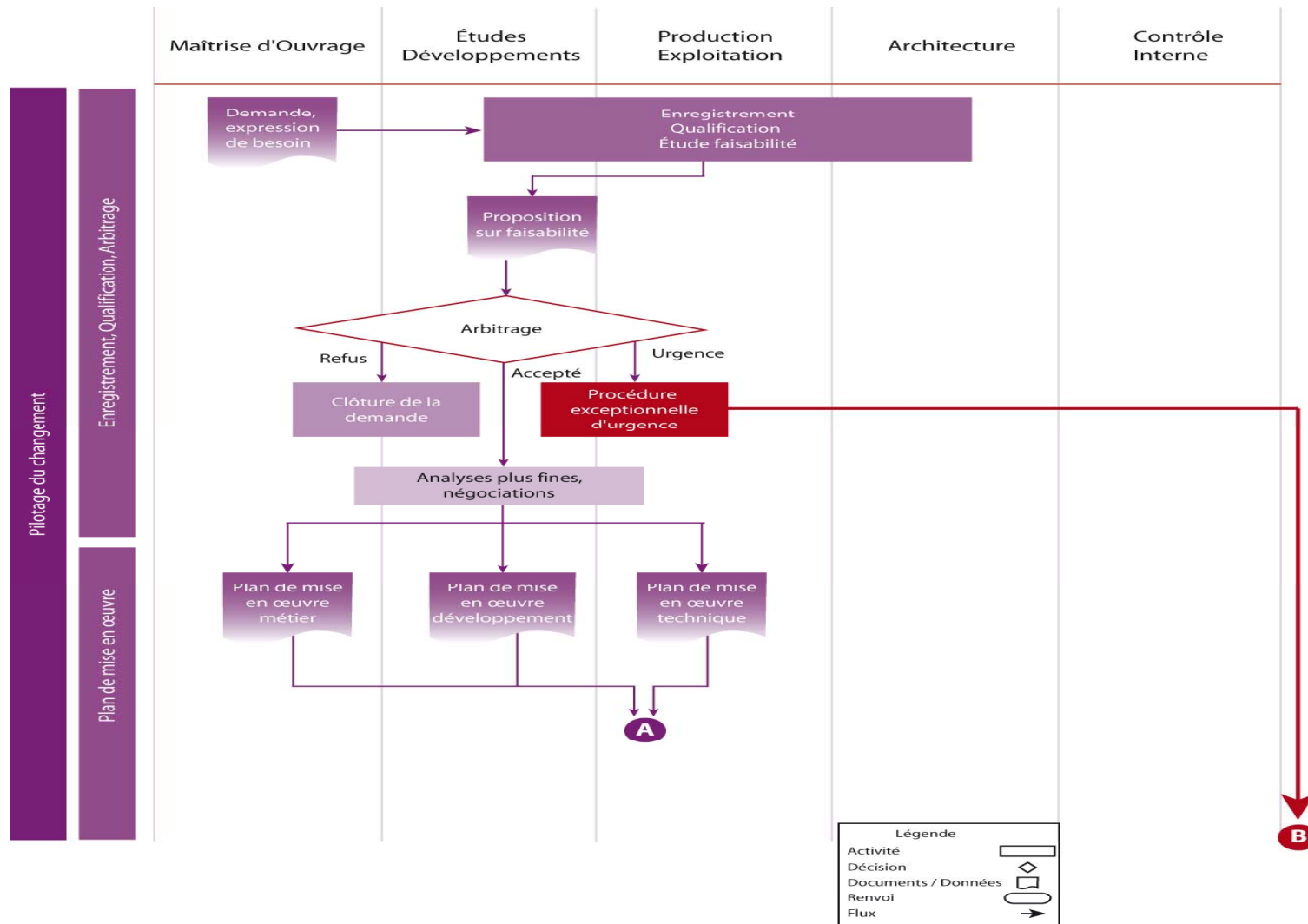
## ● Principes

- Utiliser les référentiels existants, et notamment COBIT
- Sélectionner quelques processus clés : gestion des compétences, de la sous-traitance, des changements, des accès, des projets, des incidents
- Produire un livrable concret, utile à la DSI et à l'audit interne

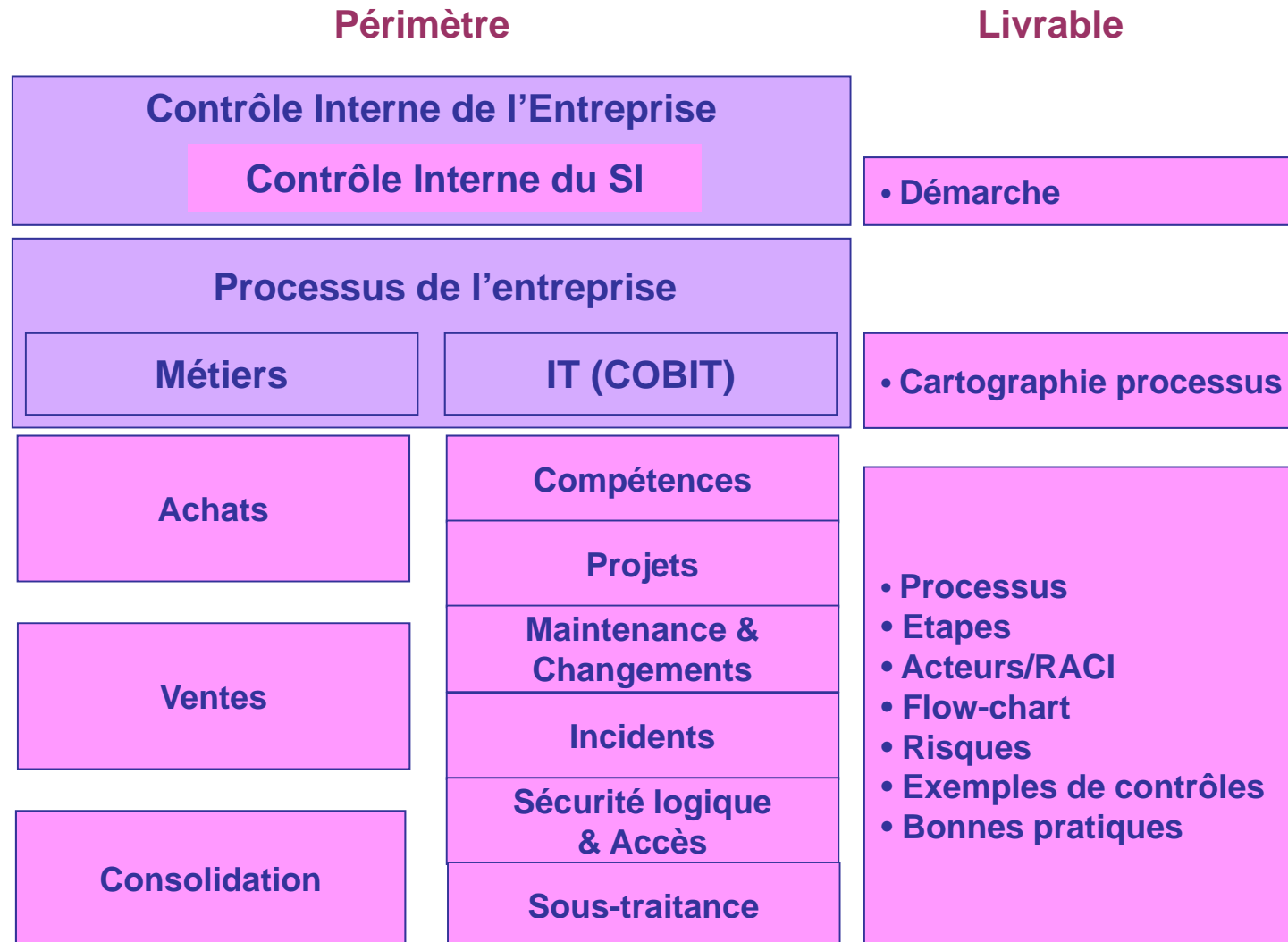
## ● Pour chacun des 6 processus choisis

- Identification des risques et points de contrôle associés
- Proposition de bonnes pratiques issues de l'expérience et du savoir-faire des rédacteurs
- Libre adaptation spécifique au contexte de chaque entreprise

# Exemple : Projet et Développement, & Maintenance et Gestion du changement



# Etude Cigref/Ifaci : synthèse

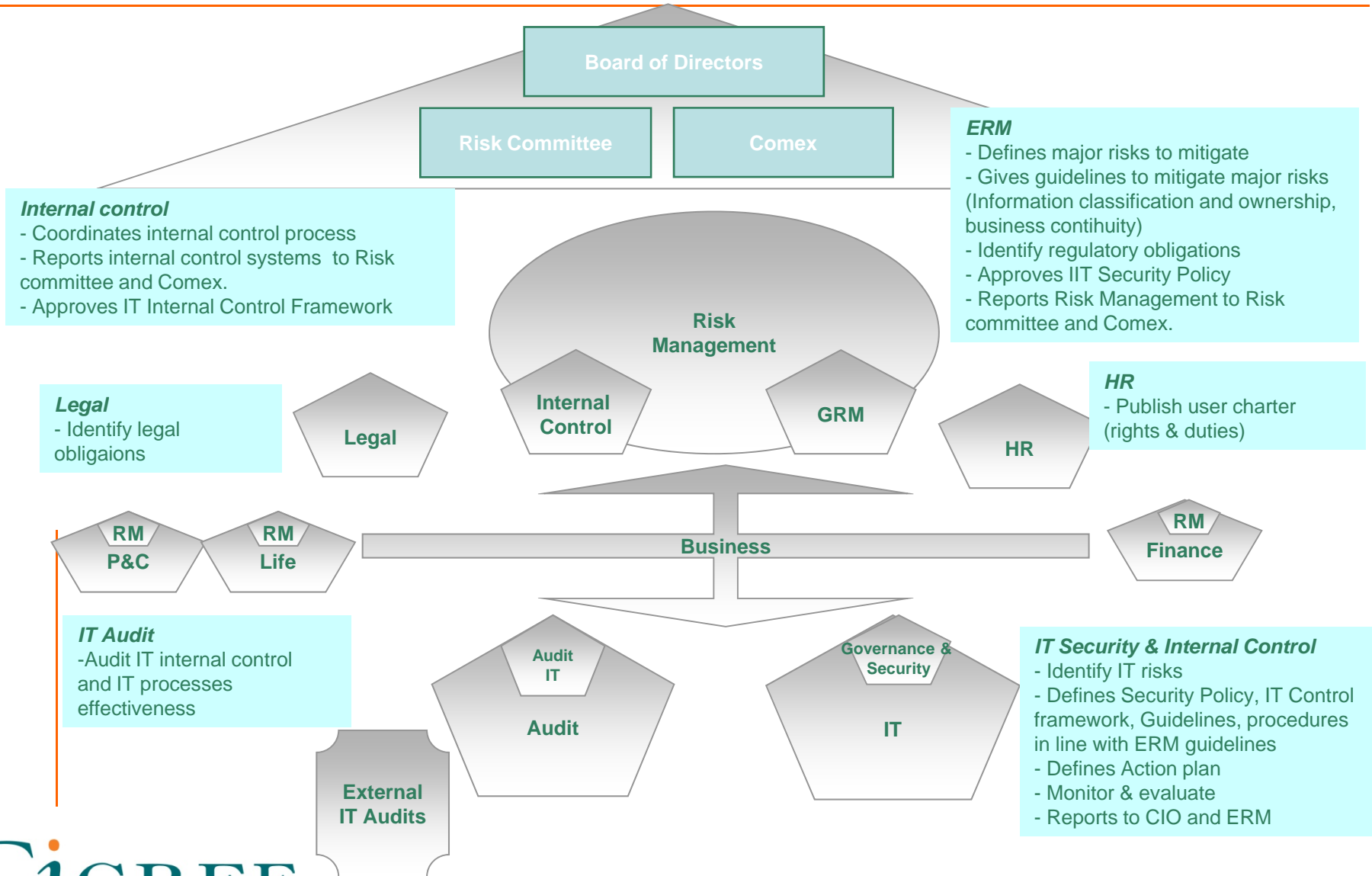


# Agenda

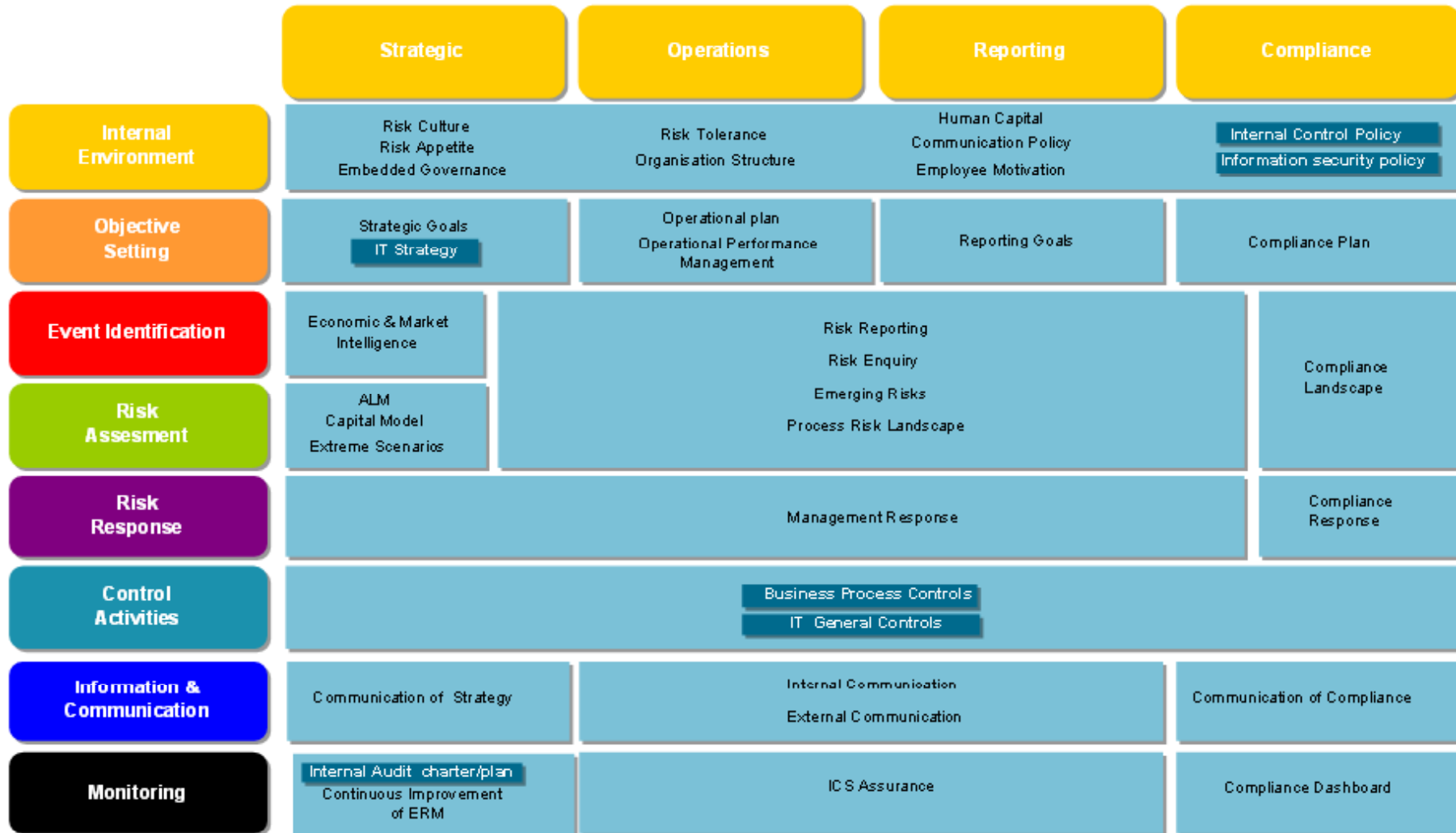
---

- **Crise financière : faillite du contrôle interne et des systèmes d'information ?**
- **Des risques accrus pour l'entreprise**
- **Les SI au cœur des risques d'entreprise**
- **L'initiative conjointe Cigref/Ifaci pour renforcer le contrôle interne du système d'information**
  - Le contrôle interne du système d'information de l'entreprise
  - Le contrôle interne de la DSI
  - **Illustrations SCOR**
- **Conclusion**

# La DSI partie intégrante du dispositif ERM de SCOR

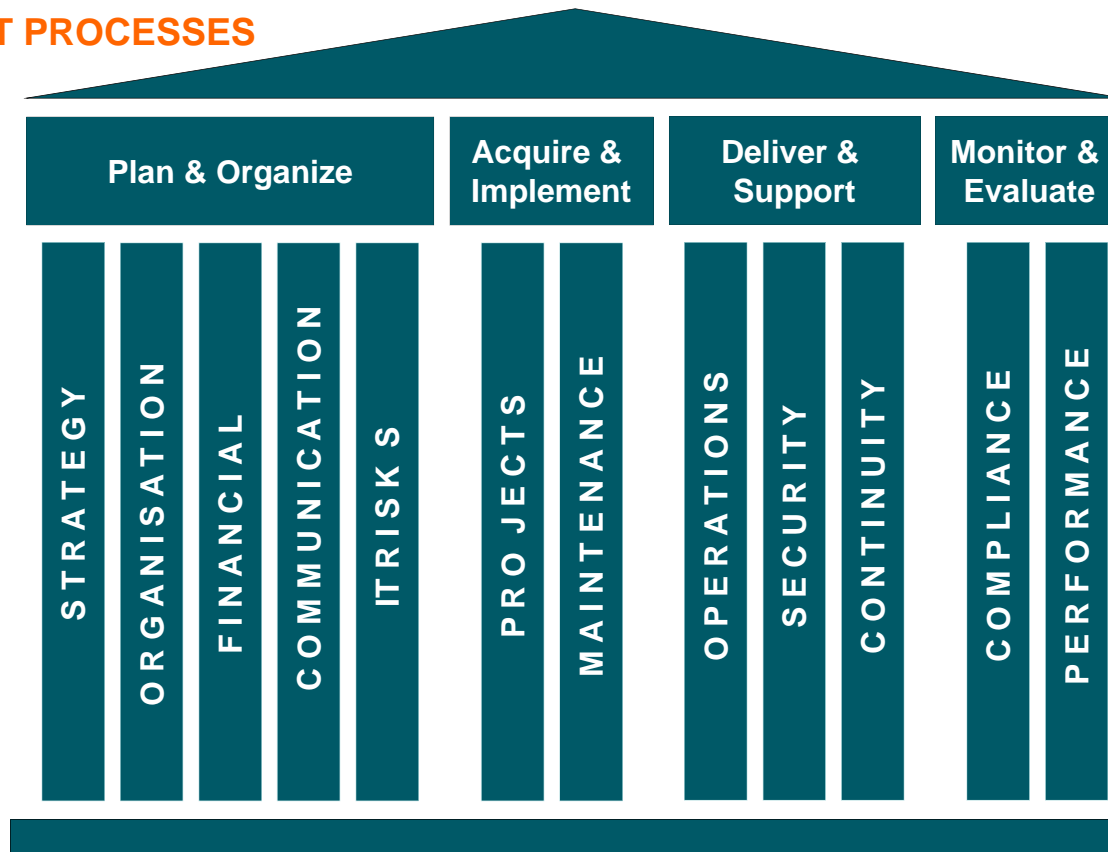


# La DSI partie intégrante du dispositif ERM de SCOR



# SCOR IT Governance

## IT PROCESSES

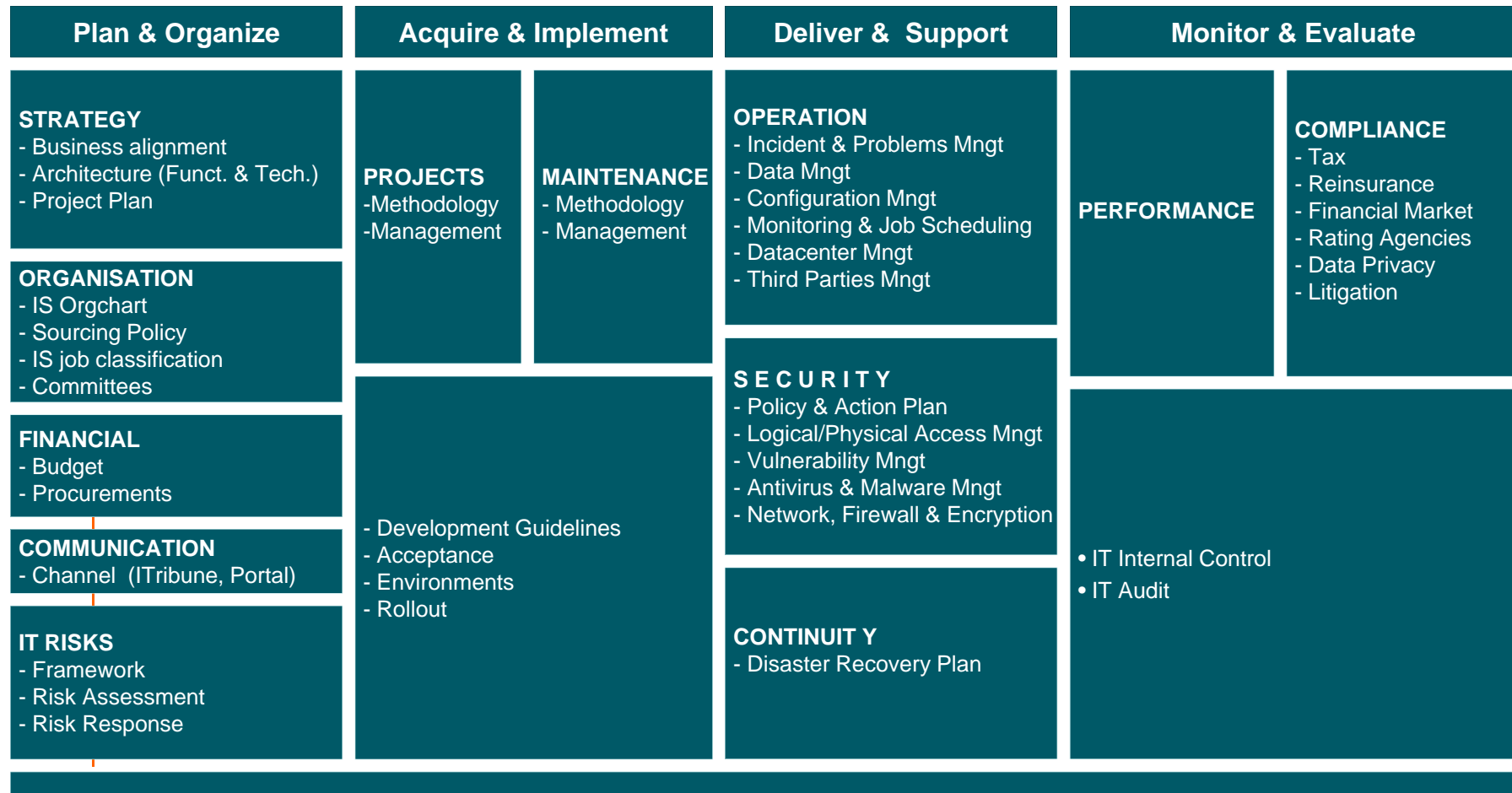


## IT RISKS



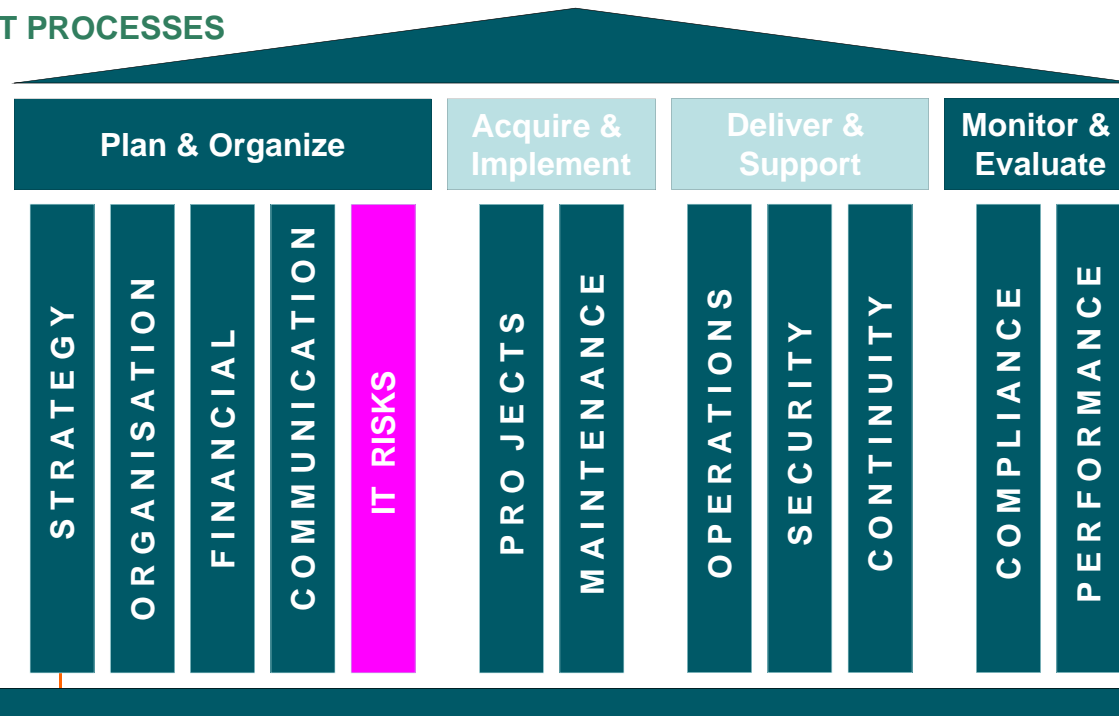
# SCOR IT Governance

## IT PROCESSES

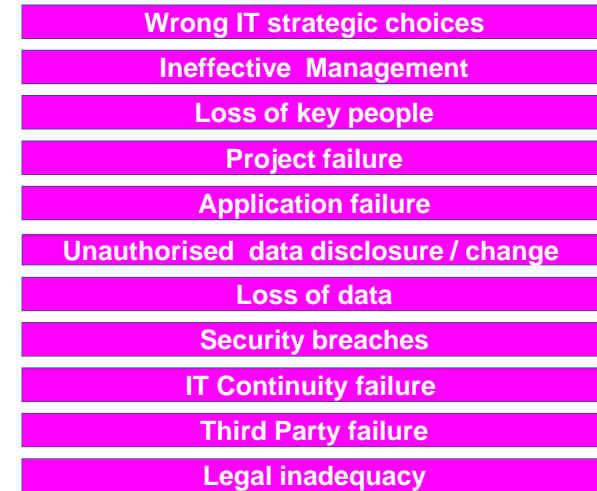


# SCOR IT Governance

## IT PROCESSES



## IT RISKS



## KEY IT CONTROLS

### IT Projects/Maintenance

- Software Development and Change Management life cycle Guidelines exist, are communicated and applied.
- New Development or changes are authorized, tested and approved
- New development or changes are monitored
- Segregation of incompatible duties exists

### IT Security

- IT Security policy exist, is communicated and applied
- General Security Settings are adequate
- Authentication settings are appropriate
- Access to privileged IT functions are managed
- Access to system resources and utilities are managed. Authorization and granting are appropriate
- Physical Access to computer hardware is managed
- Logical access process is monitored
- Segregation of incompatibles duties exists

### IT Operations

- Data is backed-up & restoration tested
- Scheduled processing is monitored
- IT incidents and problems are resolved timely

### IT Continuity

- Disaster Recovery Plan is tested

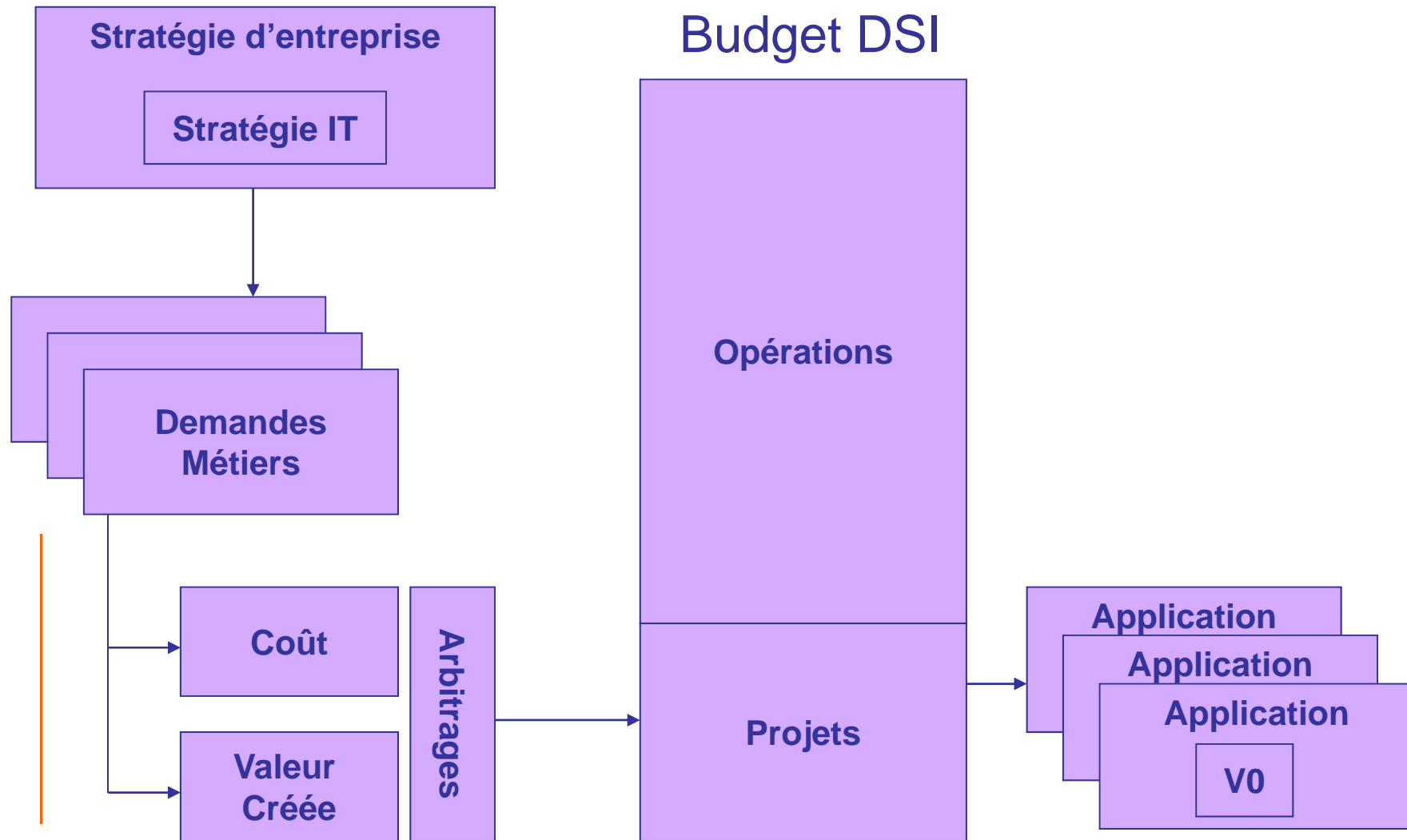
# Illustration sur l'alignement stratégique et le pilotage des projets

---

## La stratégie IT :

- Est partie intégrante de la stratégie d'entreprise
- Est révisée régulièrement en fonction de l'évolution des besoins des métiers
- Se décline en projets dont la présentation et l'arbitrage occupent l'essentiel des discussions budgétaires
- Est encadrée par les ressources mobilisables
- Prend en compte les risques associés aux fonctions automatisées
- Tient compte des contraintes réglementaires
- S'appuie sur une formalisation de politiques, processus, procédures, etc...

# La gestion du portefeuille de projets



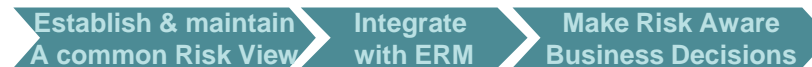
# Illustration sur les risques IT

**Objective:** The Risk IT framework explains IT risks and enables to :

- Integrate the management of IT risks into the overall enterprise risk management of the organization
- Make well-informed decisions about the extent of the risk, risk appetite and risk tolerance of the enterprise
- Understand how to respond to the risk

## 3 sub-processes:

### • IT Risk Governance



### • IT Risk Evaluation



### • IT Risk Response



## IT Controls

- IT Risks framework exists
- Annual IT Risks Report is communicated to CRO and head of Internal Control



IT Risks



IT value

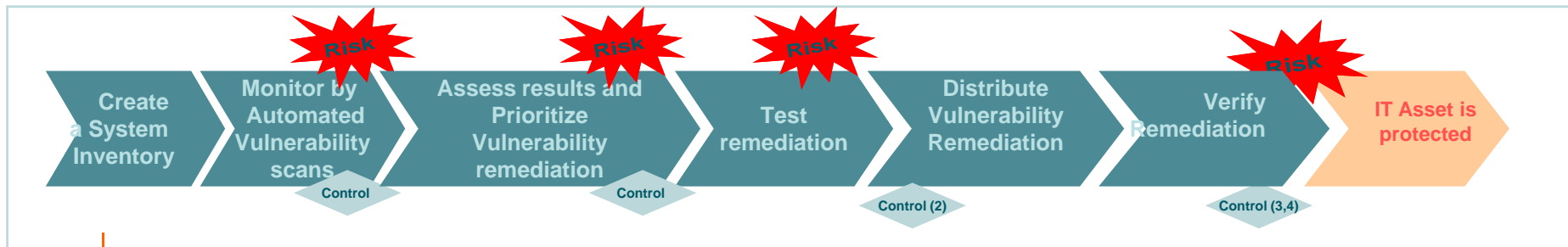
# Illustration sur les risques de vulnérabilité

**Objective:** Test and monitor the IT security implementation in a proactive way to reaccredit IT Security in a timely manner and to ensure that the approved enterprise information security baseline is maintained. Logging and monitoring function enable early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.



Tenable Security Center

## IT Process



### Key IT Controls

- Vulnerabilities are monitored, assessed, tested and remediated

mitigate

### IT Risks

- Security breaches - Unauthorised data disclosure/change -
- Application failure - IT Continuity Failure

- Undetected security breaches
- Lack of information for performing counterattacks
- Missing classification of security breaches

### IT Value

- Proactive security incident detection
- Reporting of security breaches at a defined and documented level
- Identified ways of communication for security incidents

Source: Cobir - Control practice

# Conclusion

---

- L'univers des risques est en expansion et en mutation. Il crée un sentiment diffus de vulnérabilité qui induit une demande de protection accrue
- L'entreprise est devenue la grande gestionnaire des risques, responsable de tout devant tous. Et, la liste de ses responsabilités s'accroît chaque jour
- Cette responsabilité de l'entreprise constitue un défi auquel elle a répondu en développant des stratégies sophistiquées de « risk management »
- La protection et l'optimisation des systèmes d'information sont de fait devenus des éléments clés du « risk management » de l'entreprise
- Les systèmes d'information sont au cœur de la gestion des risques, comme source de risque et comme moyen de maîtrise des risques
- Le contrôle interne du système d'information est clé, et doit porter à la fois sur les processus DSI et sur les processus métiers dont l'efficacité dépend des contrôles applicatifs définis dès la conception

---

# Assises de la Sécurité 2009

## *Le Contrôle Interne du Système d'Information des Organisations*

7 octobre 2009