Gouvernance et contrôle des Systèmes d'Information

RÉFÉRENCE DSI

Jour 1 : Introduction et Concepts

Jean-Marc Montels
Maximilien Stebler
Philippe Tronc

Jean Marc Montels

jmmontels@referencedsi.com

- Directeur des Systèmes d'Information
- Temps partagé et Interim Management
- Responsable National de la Capitalisation

- Industrie et Service aux entreprises
- Prestataire de service depuis 1990
- Grands comptes, ETI et PME internationales

Programme

- J1 : Introduction - concepts
- J2 : 360° de la gouvernance : les hommes, les organisations, les budgets, la sécurité
- J3 : Les référentiels
- J4 : Les référentiels - Suite
- J5 : Les référentiels - Etude de cas : mise en place d'une démarche ITIL
- J6 : Organisation de la DSI - gouvernance des systèmes d'information-gouvernance d'entreprise
- J7 : Les indicateurs de la Direction des Systèmes d'informations
- J8 : Etude de cas - Elaboration d'un Plan Directeur Informatique

Introduction – Présentation

Entreprise et système d'information

- Le système d'information
- Les composants clés du S.I.
- Les contributeurs

Gouvernance : définition et enjeux

- La gouvernance
- Gouvernance d'entreprise
- Gouvernance du Système d'Information
- Illustration : The Sarbanes – Oxley Act

Entreprise et système d'information

- **Le Système d'informations**
- Les composants clés du S.I.
- Les contributeurs

Définition

SYSTEME D'INFORMATION DE QUOI PARLE-T-ON ?

A noter !

Le Système d'Information, c'est l'ensemble des ***ressources*** qui permettent de :

- ✓ Collecter
- ✓ Stocker
- ✓ Traiter : contrôler, transformer, supprimer
- ✓ Diffuser (restituer)

Les informations utiles au fonctionnement de l'entreprise

Questions subsidiaires :

- ✓ Une information, c'est quoi ?
- ✓ Une ressource, c'est quoi ?

Qu'est ce qu'une information utile au fonctionnement de l'entreprise ?

➔ Réflexion en groupes (10')

➔ Objectifs :

- A partir de la description d'entreprise donnée en exemple ci-après, identifier les informations utiles à l'activité de celle-ci
- Les informations peuvent être regroupées a priori ou a posteriori par domaines organisationnels ou fonctionnels : identifier des domaines possibles
- Deux approches possibles :
  - ✓ identifier des domaines, puis les informations qui les compose
  - ✓ Liste les informations, puis les regrouper par domaines d'appartenance

Exemple : AuBonFoieGras.com

AuBonFoieGras.com est une société qui fabrique et vend du foie gras de canard sur Internet et via la distribution spécialisée (épiceries fines).

- Comment fonctionne-t-elle ?

–AuBonFoieGras.com achète des canards à des agriculteurs, elle les cuisine, pour en faire des produits finis : du foie gras, des magrets, des confits.

–Ces produits sont commercialisés via son site internet.

–Des commerciaux visitent des épiceries fines pour que ces dernières deviennent des revendeurs.

–Les déchets sont revendus à des entreprises qui font de la nourriture pour chat.

AuBonFoieGras.com : Information

Quelles sont les informations utiles à AuBonFoieGras.com ?

- Les coordonnées des agriculteurs
- Les commandes passées aux agriculteurs
- Les réceptions des canards livrés par les agriculteurs
- Les factures des agriculteurs et le règlement de ces factures
- Les recettes pour faire les produits commercialisés
- Les coordonnées des fournisseurs des autres produits entrant dans la recette (y compris les emballages !)
- Les commandes passées à ces fournisseurs (et les réceptions des fournisseurs)
- …
- Les stocks des produits fabriqués
- Les commandes des clients à préparer
- Les coordonnées des clients
- Les commandes expédiées, et les règlements clients enregistrés ….

Le Système d'Information

AuBonFoieGras.com : Information utile

Une entreprise commerciale de ce type achète transforme et vend des produits. Pour assurer son fonctionnement elle gère des informations relatives à :

- Ses fournisseurs
- Ses clients
- Ses processus de transformation
- Ses produits et services

Une entreprise est composée de collaborateurs, elle gère donc aussi les informations nécessaire à la vie du collaborateur dans l'entreprise :

- Ses coordonnées
- Ses présences et absences
- Ses formations
- Et au moins sa paie !

Le Système d'Information

AuBonFoieGras.com : Information utile

Une entreprise industrielle telle que AuBonFoieGras.com peut utiliser des machines dont le fonctionnement automatisé est piloté.

Elle gère donc les informations nécessaires au pilotage des automates :

- Ordres à passer aux automates
- Compte rendu des ordres effectués
- Etat de l'automate, …

Enfin, et c'est une évolution plus récente, si certaines données ou informations sont crées, et / ou traitées, puis stockées par l'entreprise, d'autres lui échappent :

- Les informations sur les sites internet autres que ceux gérés par l'entreprise (avis de consommateurs, etc.)
- Les réseaux sociaux
- Les bases de collecte d'informations gérées par des tiers :
  - Opérateurs de télémarketing
  - Agences de notation : Dun & Bradstreet, Coface, …
  - L'Administration Fiscale
  - D'autres administrations comme dans notre cas l'ANSES, Agence National de SEcurité sanitaire et des aliments,
  - Les concurrents dans certains cas …

Entreprise et système d'information

- Le Système d'informations
- **Les composants clés du S.I.**
- Les contributeurs

Etude de cas : AuBonFoieGras.com

- Quelles sont les ressources nécessaires pour collecter, stocker, traiter (contrôler, transformer) et diffuser (restituer) les informations ?

➔ Réflexion en groupes (10')

➔ Objectifs :

- ❑ A partir de vos connaissances et expériences, lister les ressources composants le système d'information d'une entreprise telle que AuBonFoieGras.com
- ❑ A partir de cette liste, essayer d'établir une typologie de celles-ci

Le Système d'Information

Les ressources

Quelles sont les ressources nécessaires pour collecter, stocker, traiter (contrôler, transformer) et diffuser (restituer) les informations ?

Ces ressources sont de 4 types :

- **Les ressources matérielles** : ordinateurs, équipements réseaux, moyens d'impressions, moyens d'acquisition de données (capteurs, …)
- **Les ressources logicielles** : programmes permettant de collecter, transformer, publier et organiser le stockage des informations et programmes nécessaires pour piloter des matériels (OS des ordinateurs, systèmes embarqués, automates, …) ou d'autres ressources
- **Les ressources humaines** : les hommes et les femmes qui créent, opèrent et entretiennent les ressources matérielles et logicielles
- **Les procédures** : les règles à respecter pour garantir la bonne adéquation du système et de son fonctionnement avec les enjeux de l'entreprise. Les procédures sont l'expression contextuelles du processus d'entreprise.

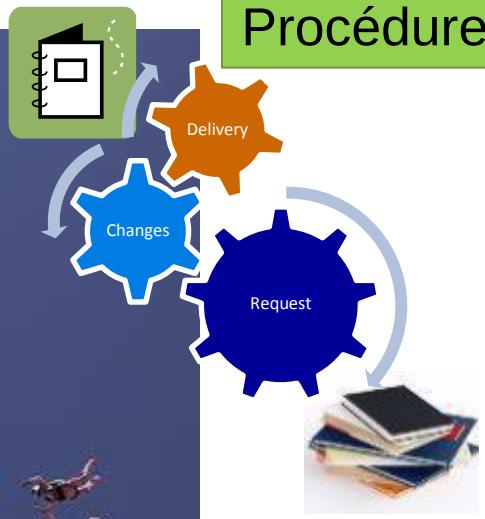
Définition du Système d'Information

Vue orientée Ressources

Processus d'Entreprise

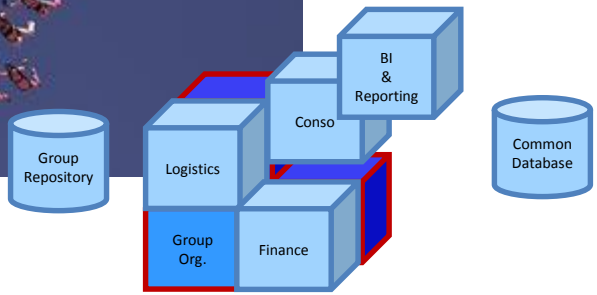
Acteurs & Contributeurs

Procédures



Matériels

Logiciels



DAUPHINE UNIVERSITÉ PARIS

RÉFÉRENCE DSI

Le Système d'Information

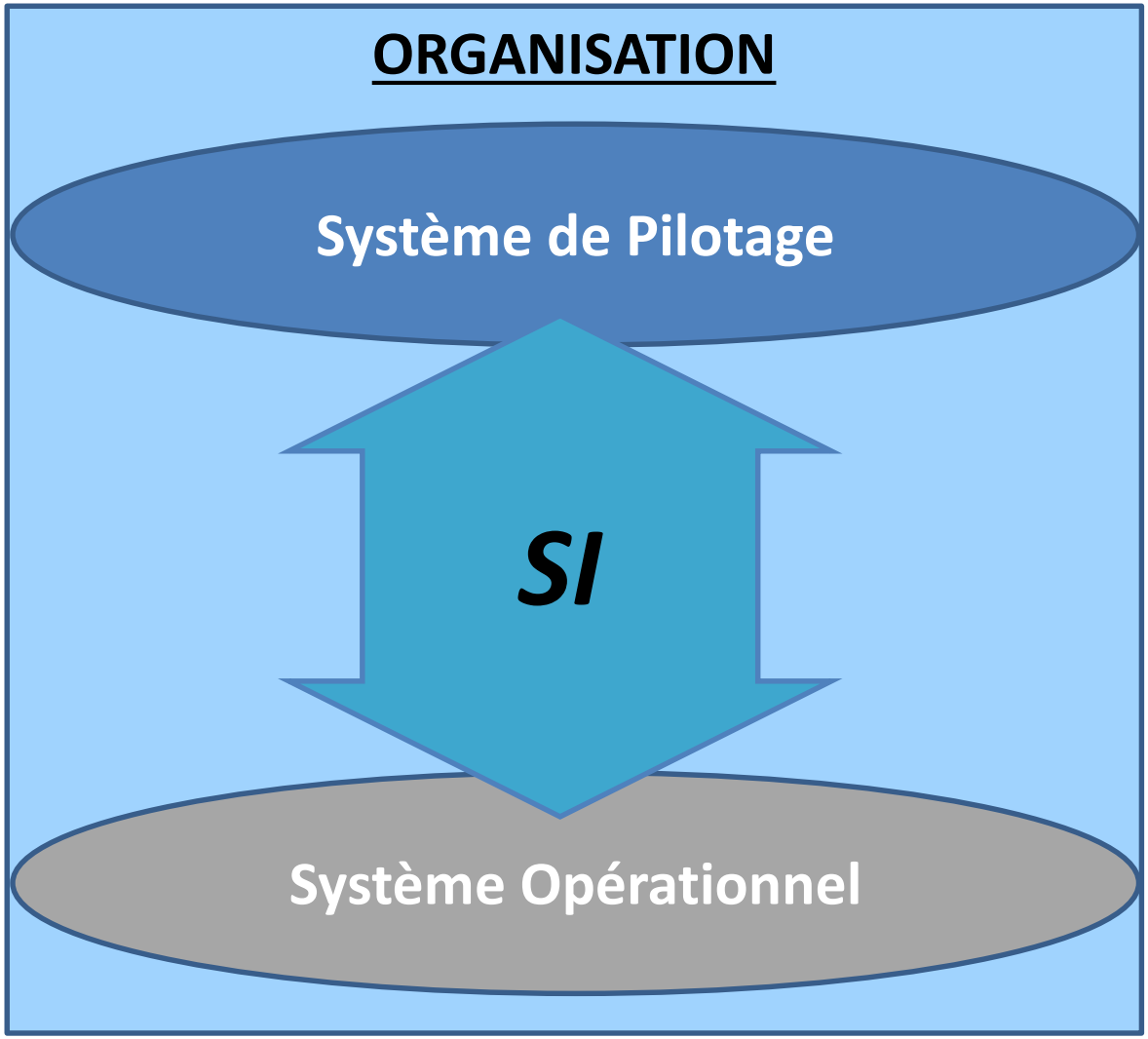
A noter !

1. Le Système d'Information contribue à fédérer les contributeurs d'une organisation et peut ainsi concourir à structurer leurs activité
2. Le Système d'Information est un vecteur de communication
3. Variantes du dessin précédent :
   - SI orienté « people » (le dessin présenté)
   - SI orienté « processus d'entreprise »
   - SI orienté « procédures »
   - SI orienté « hardware »
   - SI orienté « software »

… selon la culture de l'organisation ou le point de vue du DSI !

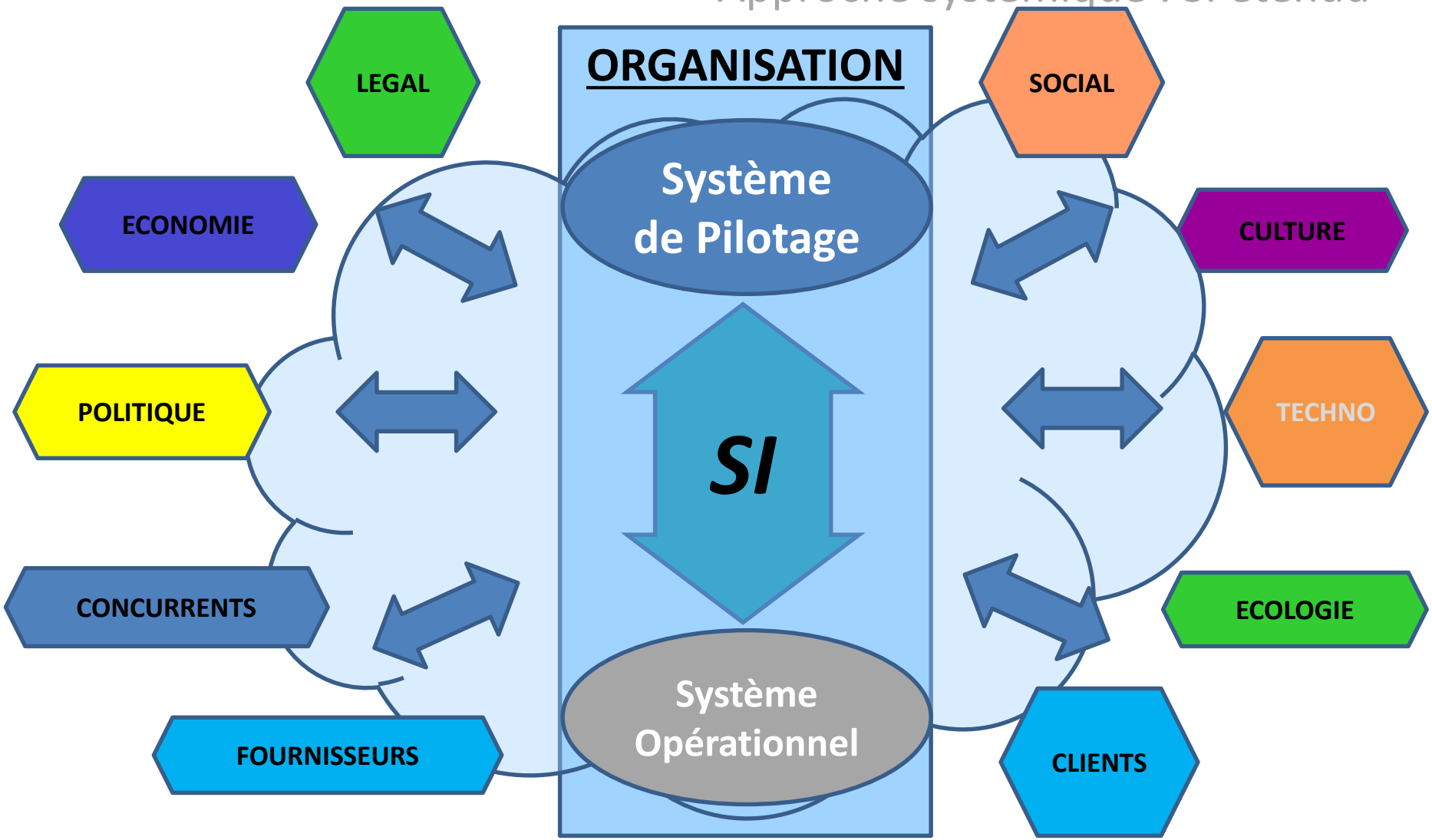
Définition du Système d'Information

Approche systémique



Définition du Système d'Information

Approche systémique : SI étendu



Les différentes informatiques :

- L'informatique de gestion
- L'informatique décisionnelle
- L'informatique industrielle
- Le Digital Marketing
- le Knowledge Management

La composition du SI : l'informatique de gestion

Gestion des données structurées :

- L'ERP (Enterprise Resource Planning ou Programme de Gestion Intégré) : le système central de l'entreprise (horizontal)
- Les logiciels Best Of Breed (verticaux)
- Les développements à façon
- La Business Intelligence

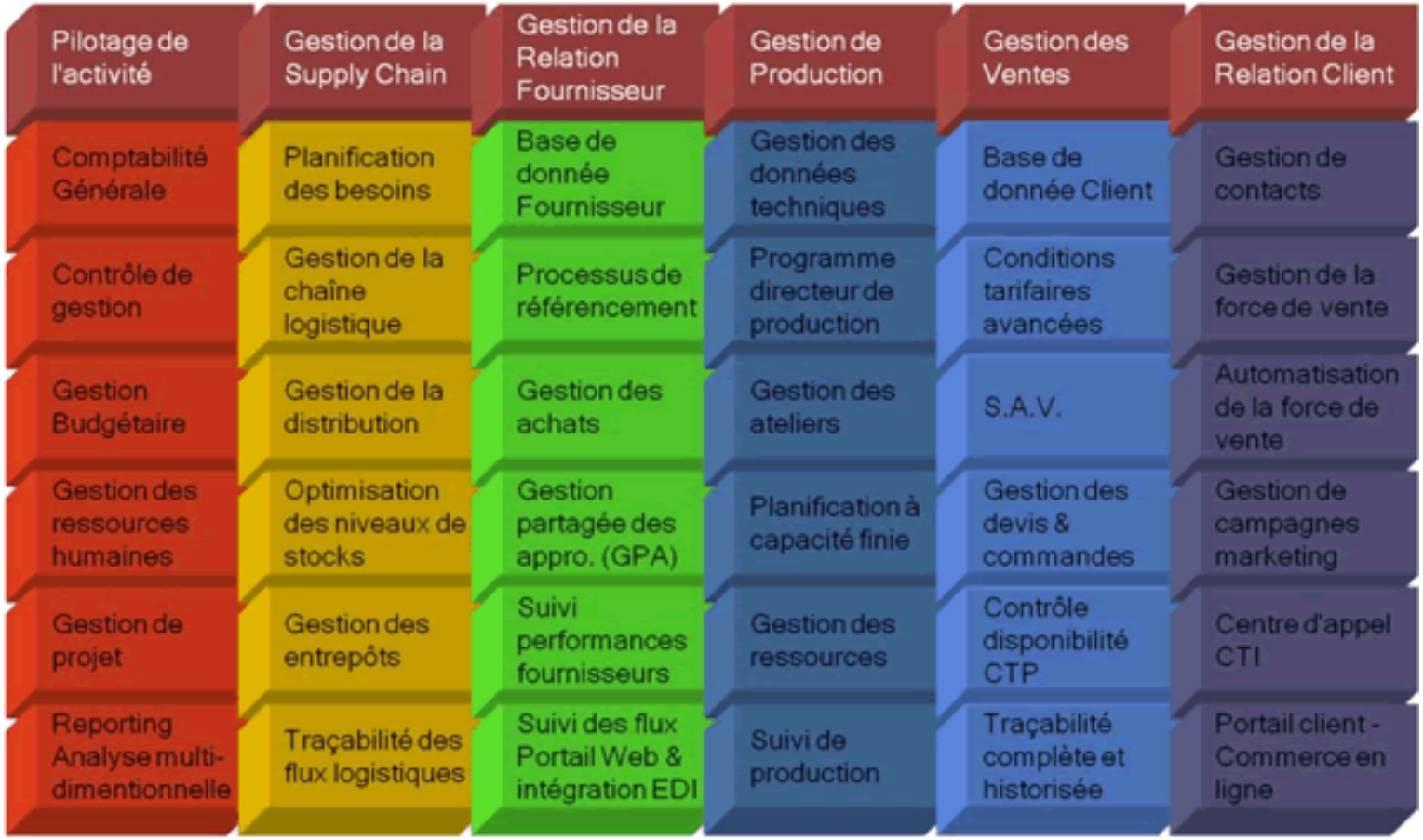
Gestion des données non structurées

- Les plates-formes collaboratives
- Les Réseaux Sociaux d'Entreprises
- Les intranets et extranets
- Les plates-formes de KM
- La BI ? (Big Data)

Le Système d'informations

La composition du SI : l'informatique de gestion

L'ERP

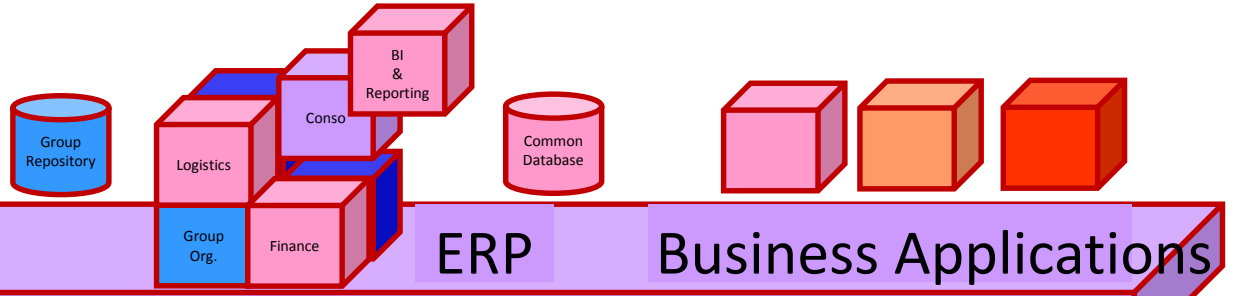


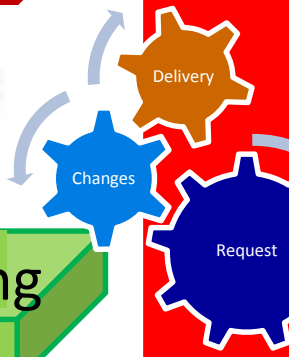
La composition du SI : l'informatique de gestion

- La BI
  - Datawarehouse
  - Datamart
  - Datamining
- Les niveaux de décisionnel :
  - Les décisions opérationnelles : requettes directes sur les données opérationnelles gérées par l'ERP notamment
  - Les décisions tactiques
  - Les décisions stratégiques
- Les outils et technologies :
  - OLAP
  - Multidimensionnel –
  - Datamining

Définition du Système d'Information

Vue orientée Architecture





Messaging | Intranet / Extranet | Phoning | Conferencing

PRODUCTIVITY

INFRASTRUCTURE

DAUPHINE UNIVERSITÉ PARIS

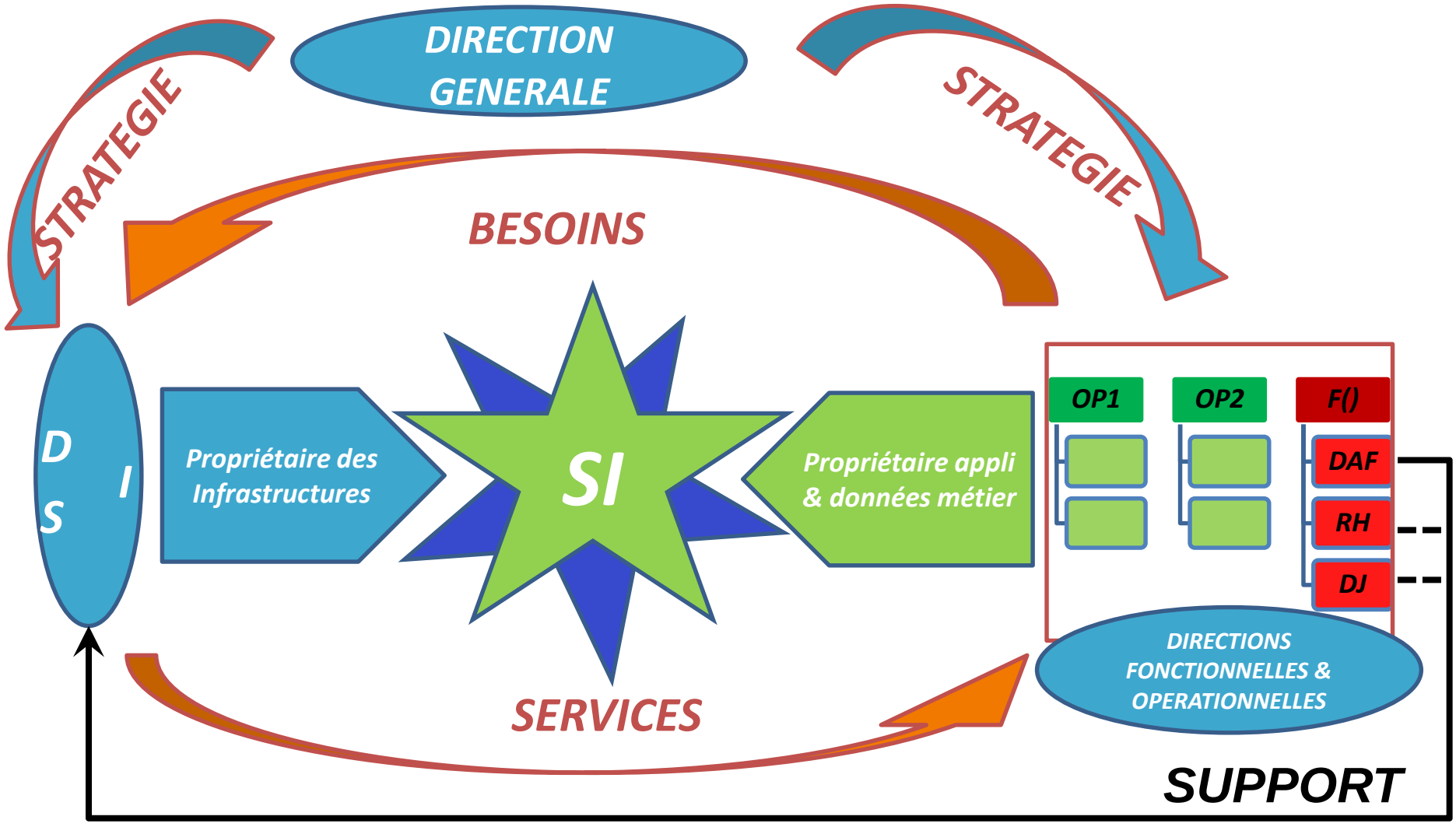
RÉFÉRENCE DSI

Entreprise et système d'information

- Le Système d'informations
- Les composants clés du S.I.
- **Les contributeurs**

Contributeurs du Système d'Information

Contributeurs internes



Contributeurs du Système d'Information

Contributeurs internes

❖ ***Direction Générale*** : représente ***les actionnaires***, donne les ***orientations stratégiques***

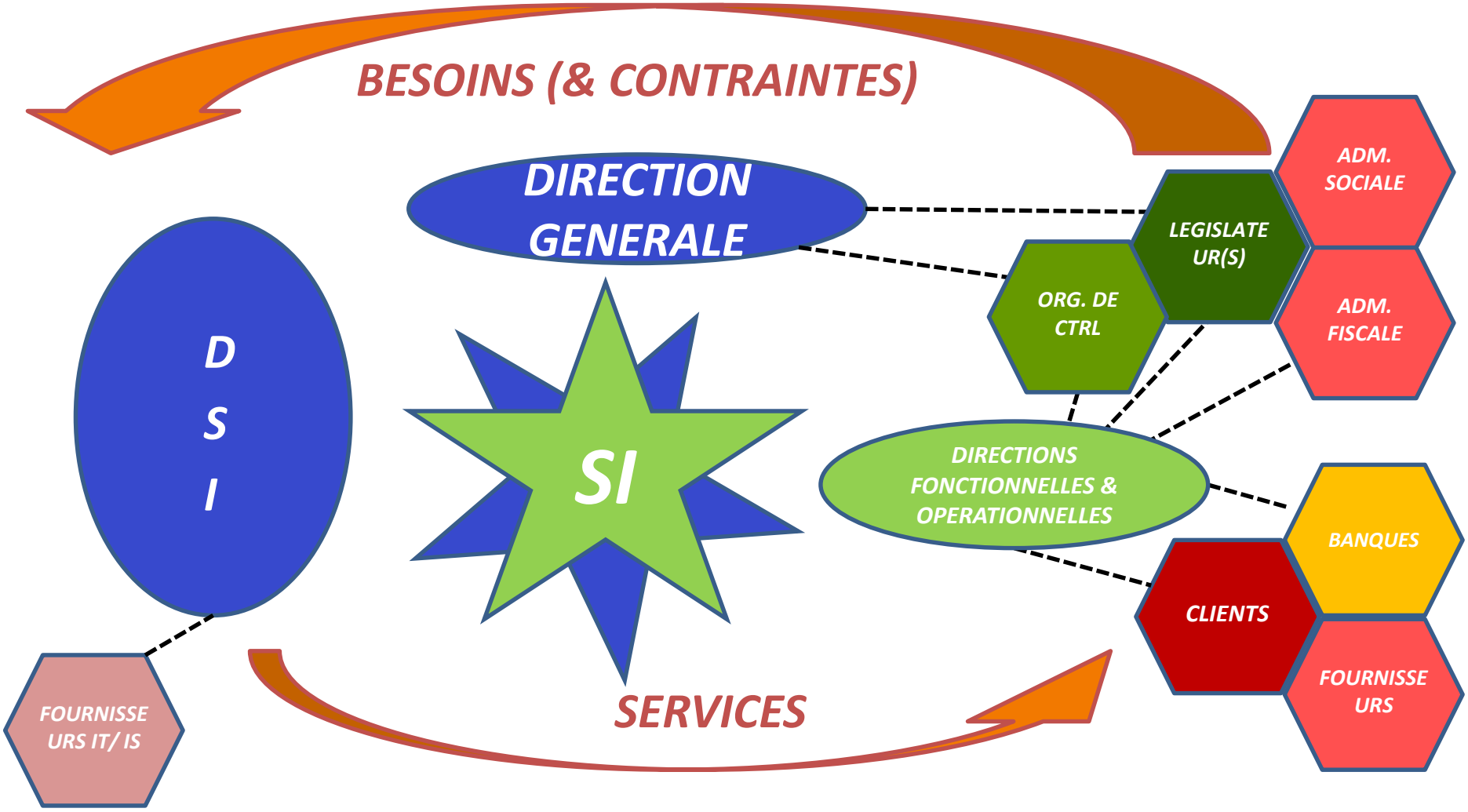
❖ ***Directions Fonctionnelles et Opérationnelles*** : ***les clients internes*** de la DSI, les ***utilisateurs*** des systèmes et ***propriétaires*** des ressources applicatives (données et traitements)

❖ ***La Direction des Systèmes d'Information*** agit selon un contrat implicite :

- ***met en œuvre*** le SI
- est ***responsable de la qualité du service*** délivré à l'organisation
- est ***propriétaire*** des ressources d'infrastructure et des services partagés : postes de travail, serveurs, stockages, routeurs, imprimantes, messagerie, téléphonie, intranet, etc.
- gère plusieurs sortes d'actifs :
  - matériels et logiciels ***(financement avec engagements à moyen terme enregistrés dans les comptes de l'entreprise en tant que coût),***
  - données et traitements ***(processus et procédures non valorisés en tant que tels dans les comptes de l'entreprise qui sont la réelle valeur du SI)***
  - les Directions (Fonctionnelles) Financières, Ressources Humaines et Juridiques sont de ce fait des fonctions supports essentielles pour le management du système d'information.

Contributeurs du Système d'Information

Contributeurs externes



Contributeurs du Système d'Information

Contributeurs externes

❑ Les contributeurs externes

❖ ***Tiers*** : clients, fournisseurs, banques, … et leurs SIs (EDI, extranet, …)

❖ ***Législateur(s) et organismes de contrôle*** : législation commerciale, droit des entreprises, droit de l'information (CNIL, ARCEP, …), réglementations sanitaires et professionnelles (ANSES, AIEA, FDA, …)

❖ ***Administrations publiques*** :

- ***Sociales (URSSAF, …)***
- ***Fiscales***
- ***Douanes***
- ***…***

❖ ***Fournisseurs IT/IS*** : fournisseurs de matériels, logiciels et services, peuvent agir comme Maître d'Œuvre délégué

GOUVERNANCE DEFINITION ET ENJEUX

- **La gouvernance**
- Gouvernance d'entreprise
- Gouvernance du Système d'Information
- Illustration : The Sarbanes – Oxley Act

GOUVERNER = GOUVERNEMENT OU GOUVERNANCE ?

Gouvernement ou Gouvernance ?

➔ Réflexion en groupes (10')

➔ Objectifs :

- ❑ A partir de vos connaissances et expériences, donner une définition de chacun des termes
- ❑ Mettez en évidence les différences d'acceptation ou d'utilisation de chacun d'eux, si elles existent

Quelques jalons historiques

Etymologie

Du Latin, gubernare, gouverner

Il y a très longtemps

- ***Gouvernance et Gouvernement sont synonymes : Art ou manière de gouverner, en ancien français.***

Au XIVème siècle

- ***Gouvernement supplante Gouvernance en Français, mais Governance passe dans la langue anglaise.***

Au XXème siècle, dans les années 70

- ***Gouvernance réapparaît en France au travers de l'expression Corporate Governance.***

Quelques jalons historiques

Généalogie

A partir des années 80, le concept issu de l'entreprise est repris par la sphère politique autour du rôle de l'Etat.

L'Etat moderne démocratique est au carrefour de multiples influences : pouvoir central et décentralisé, délégations, lobbies, contre-pouvoirs

La gouvernance a trait aux interactions de ces parties prenantes dans l'action de gouvernement.

Le sens moderne de Gouvernance inclut donc cette notion de régulation sociale à tous les niveaux de gouvernement : gouvernance mondiale, européenne, locale, etc.

Il n'y a donc pas un modèle unique de gouvernance, mais bien des systèmes de gouvernance

Quelques jalons historiques

Etymologie

Gouvernance *désigne l'action de gouverner (nominalisation),*

quand

Gouvernement *renvoie le plus souvent à l'organisation prévue à cette fin, voire au groupe de personnes qui sont en charge de gouverner*

GOUVERNANCE DEFINITION ET ENJEUX

- La gouvernance
- **Gouvernance d'entreprise**
- Gouvernance du Système d'Information
- Illustration : The Sarbanes – Oxley Act

Gouvernance au niveau de l'entreprise

Généalogie

Lorsqu'on parle de Gouvernance d'entreprise, on évoque les mécanismes de direction d'une société et de responsabilité des dirigeants dans leur conduite des affaires sociales

Ce concept concerne les règles et principes édictés par le gouvernement et les professionnels dans le souci de rétablir la confiance des investisseurs et d'assurer la transparence

Quelques définitions 1/2

Gouvernement d'entreprise en Europe

Corporate governance …

- *… is the system by which companies are directed and controlled (Cadbury report, UK)*
- *… refers to the set of rules applicable to the direction ad control of a company (Cardon report, Belgium)*
- *… is the organization of the administration and management of companies (Recommendations of the Federation of Belgian Companies, Foreword)*
- *… describes the legal and factual regulatory framework for managing and supervising a company (Berlin Initiative Code, Preamble)*
- *…, in the sense of the set of rules according to which firms are managed and controlled, is the result of norms, traditions and patterns of behaviour developed by each economic and legal system (Preda Report, Italy)*
- *… is used to describe the system of rules and procedures employed in the conduct and control of listed companies (Securities Market Commission Recommendations, Portugal)*

Quelques définitions 2/2

Gouvernement d'entreprise en Europe

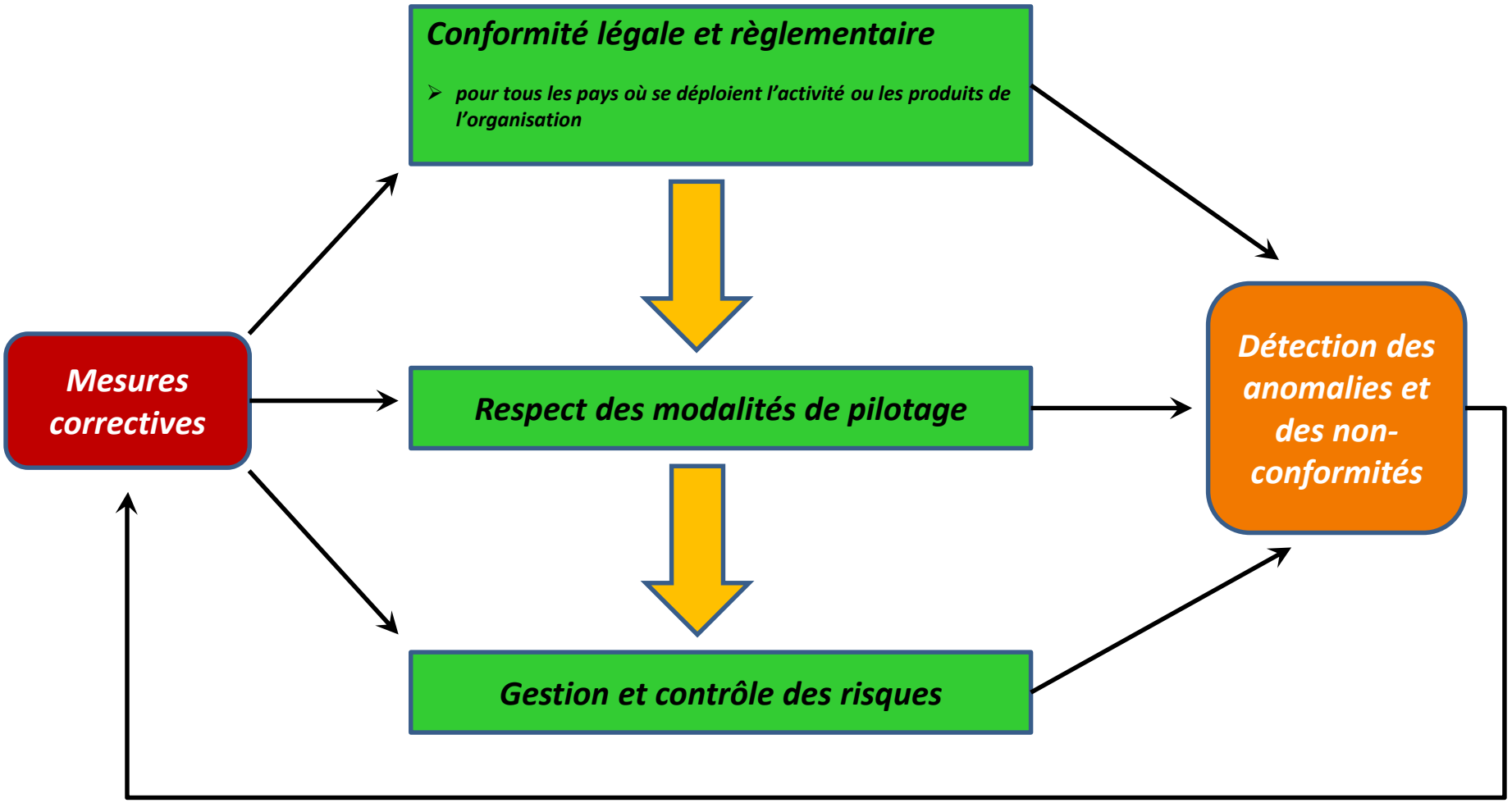
Corporate governance …

- *… is the goals, according to which a company is managed, and the major principles and frameworks which regulate the interaction between the company's managerial bodies, the owners, as well as other parties who are directly influenced by the company's dispositions and business (is this context jointly referred to as the company's stakeholders). Stakeholders include employees, creditors, suppliers, customers and the local community (Norby Report and Recommendations, Denmark)*

- *The concept of Corporate Governance has been understood to mean a code of conduct for those associated with the company … consisting of a set of rules for sound management and proper supervision and for a division of duties and responsibilities and powers effecting the satisfactory balance of influence of all the stakeholders (Peters Report, Netherlands)*

En résumé

Objectifs affichés de la gouvernance d'entreprise



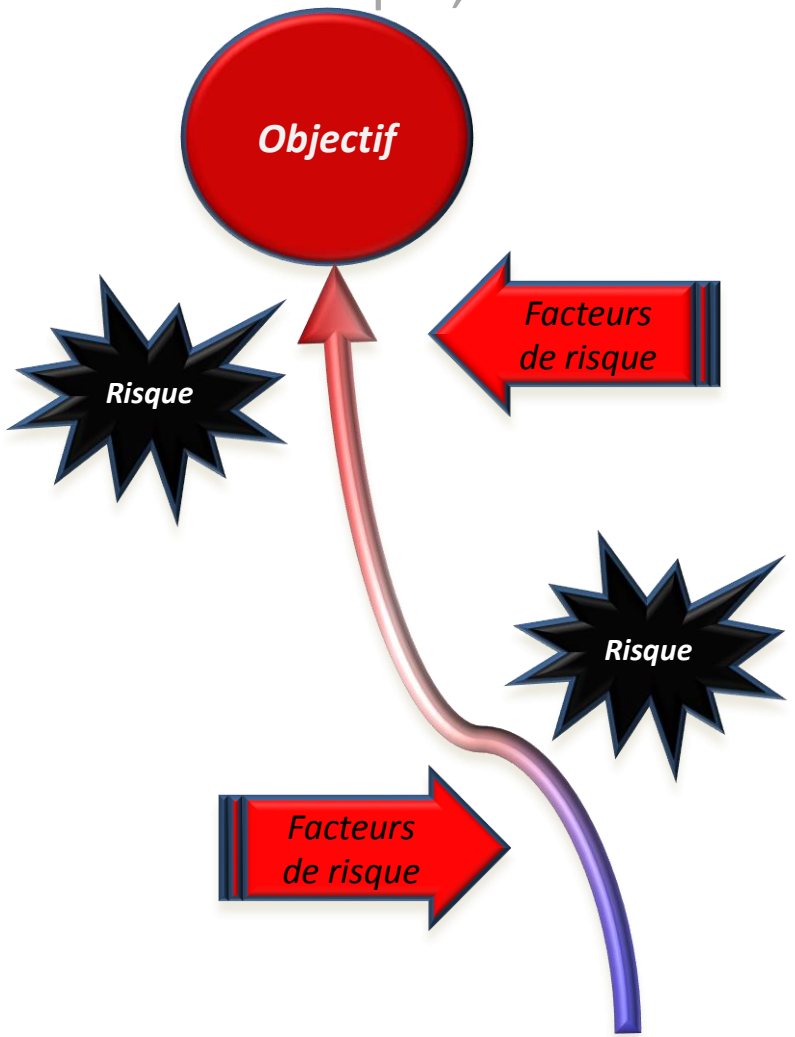
GOUVERNANCE DEFINITION ET ENJEUX

- La gouvernance
- Gouvernance d'entreprise
- **Gouvernance du Système d'Information**
- Illustration : The Sarbanes – Oxley Act

Notion de risque

Risque, facteurs de risque, contrôle

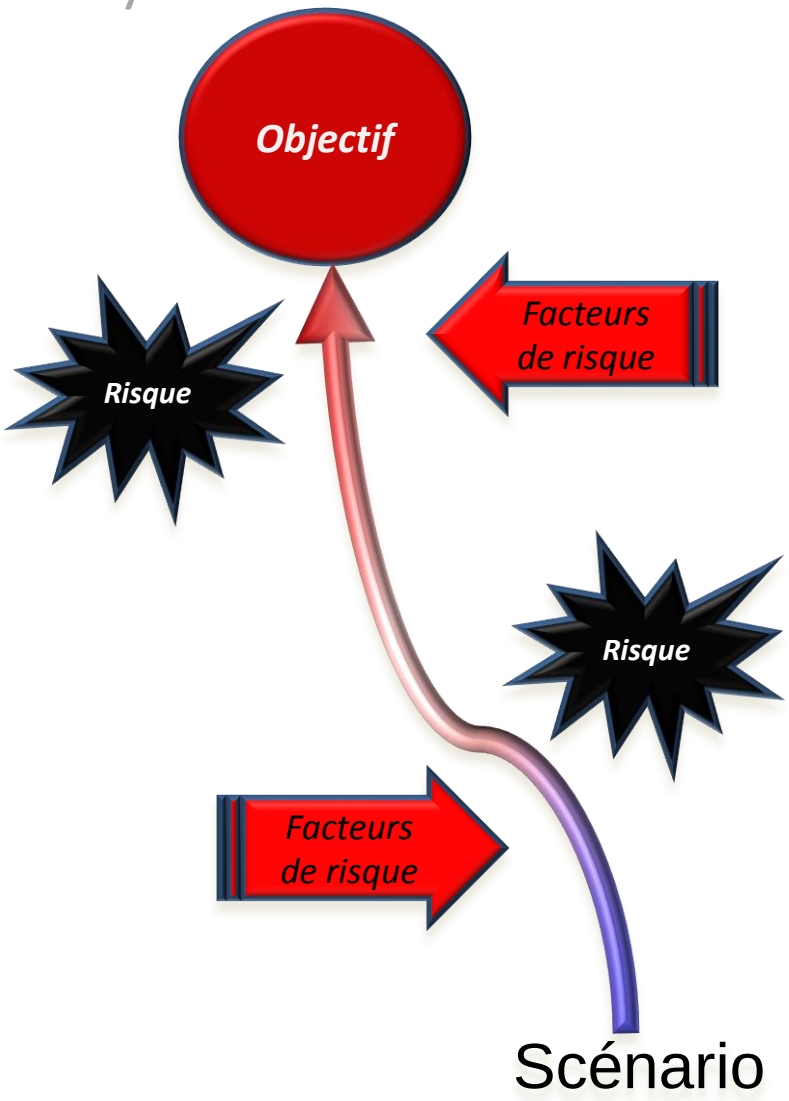
- *Les facteurs de risques sont des événements ou des circonstances qui rendent la probabilité de survenance du risque plus importante.*
- *Le risque en tant que tel n'a que deux états : actif ou inactif.*
- *Il faut donc maîtriser (contrôler) les facteurs qui peuvent activer le risque.*
- *Il est possible de transférer les risques (contrats commerciaux, assurances, réassurances) voire de les déléguer (sous-traitance avec engagements)*
- *Exemple : Organiser l'Arbre de Noël de l'entreprise*
  - *3 risques ?*
  - *Quels sont les facteurs de risques ?*
  - *Comment les contrôler ? Les transférer ?*



Notion de risque

Risques pour le Système d'Information

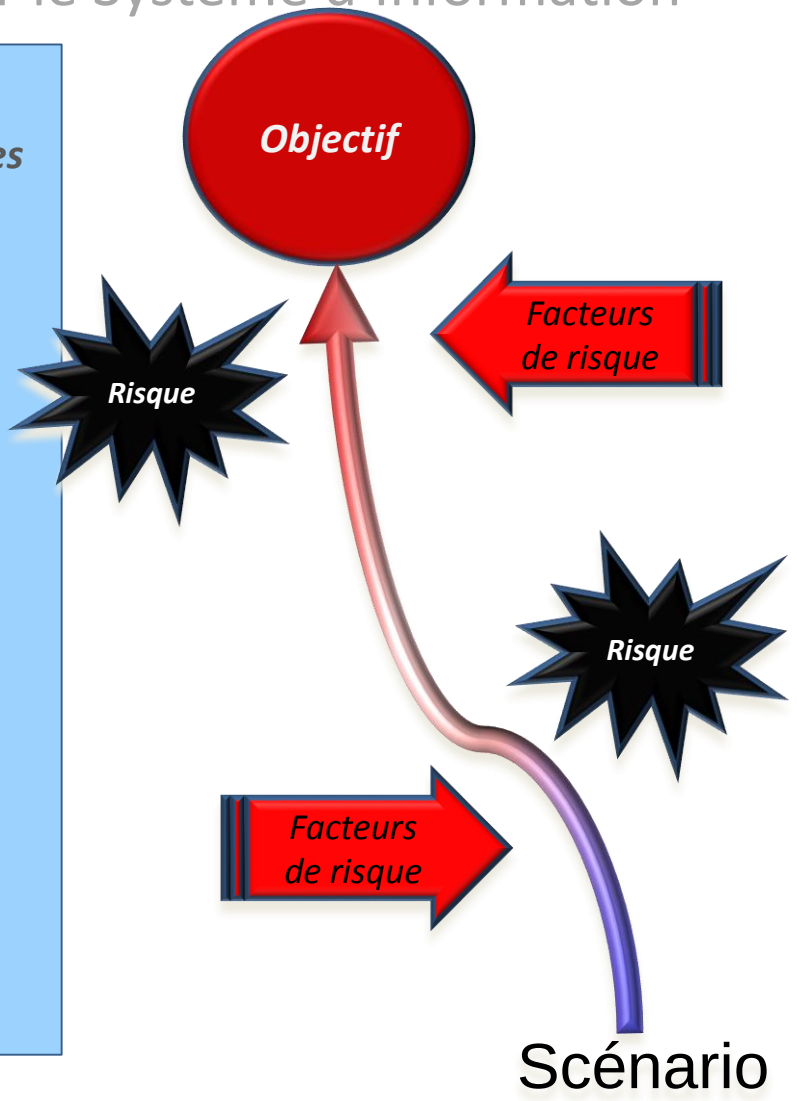
- *Risques sur les moyens*
  - *Risque de non opportunité*
  - *Risque de non aboutissement*
  - *Risque commercial et financier*
  - *Risque technologique*
- *Risque sur les applications et les données*
  - *Risque stratégique : non opportunité, non aboutissement, non alignement financier ou commercial*
  - *Fiabilité : non qualité de l'information, corruption, falsification, pertes, …*
  - *Non-conformité*
  - *Vol*



Notion de risque

Risques pour le Système d'Information

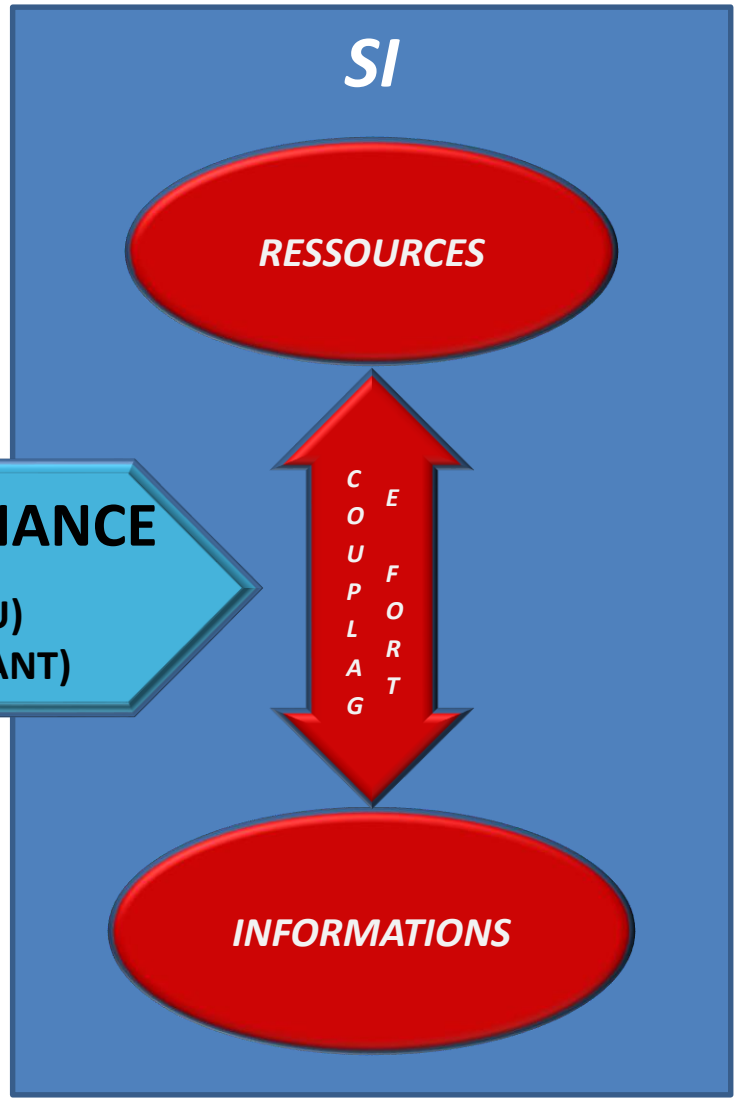
- *Risques SI*
  - *Alignement stratégique (combine plusieurs des thèmes ci-dessous)*
  - *Non opportunité (risque projet)*
  - *Non aboutissement (risque projet ou processus)*
  - *Commercial*
  - *Financier*
  - *Technologie(s)*
  - *Qualité de l'information (processus d'entreprise)*
  - *Protection de la donnée et de son cycle de vie*
  - *Protection des traitements et de leur conformité*
  - *Réglementations applicables*
  - *Protection juridique*



Gouvernance SI

Une gouvernance complexe

- *Risques SI*
  - *Alignement stratégique (combine plusieurs des thèmes ci-dessous)*
  - *Non opportunité (risque projet)*
  - *Non aboutissement (risque projet ou processus)*
  - *Commercial*
  - *Financier*
  - *Technologie(s)*
  - *Qualité de l'information (processus d'*
  - *Protection de la donnée et de son cycl*
  - *Protection des traitements et de leur*
  - *Réglementations applicables*
  - *Protection juridique*

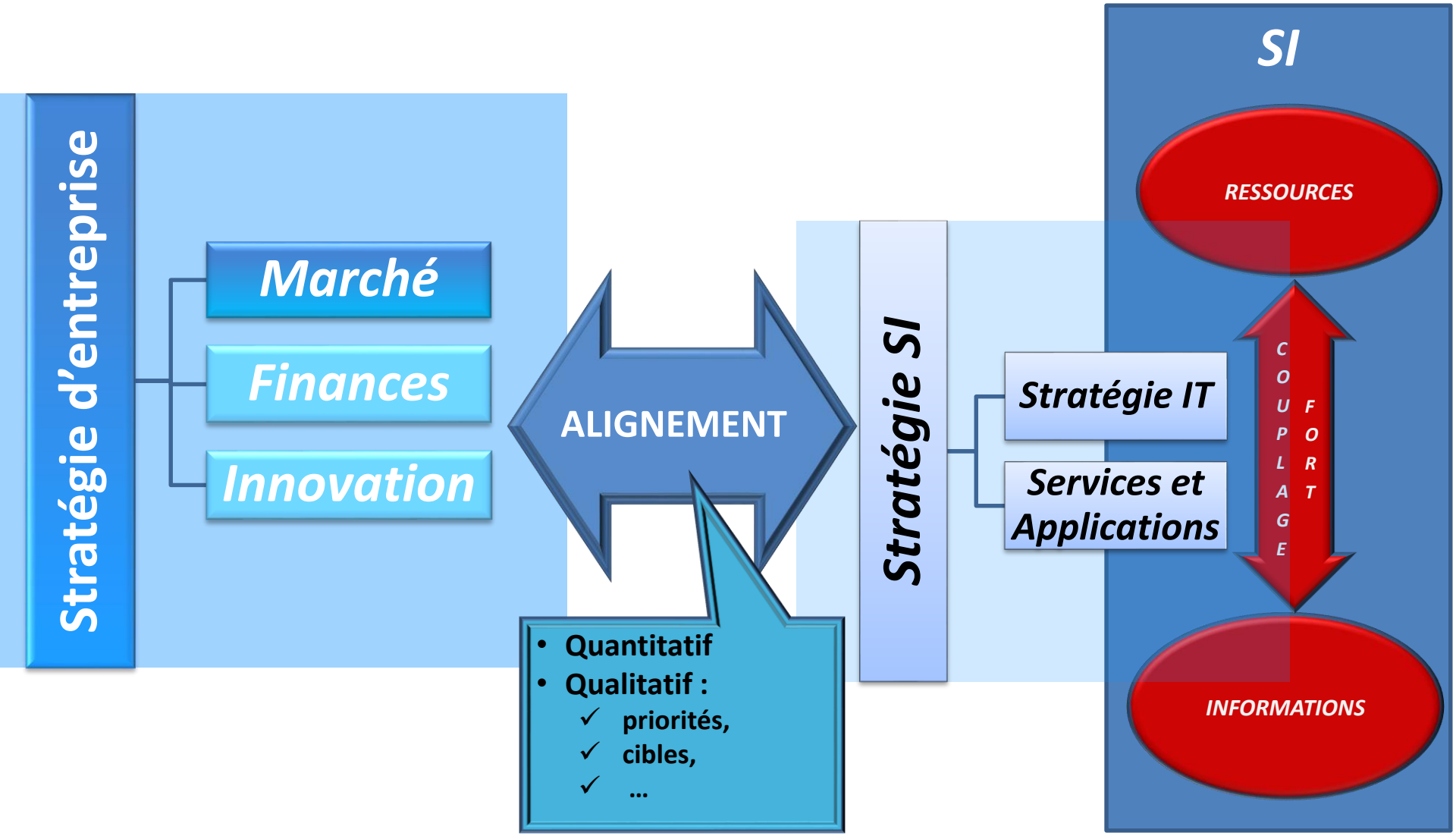


GOUVERNANCE

- **IS (CONTENU)**
- **IT (CONTENANT)**

Gouvernance SI

Alignement stratégique



Quelques références

Sources & Références

Gouvernance d'entreprise

- Viviane de Beaufort *Gouvernance d'entreprise en Europe* Economica
- *http://fr.wikipedia.org/wiki/Gouvernance*

Gouvernance du SI

- *http://www.piloter.org/blog/maitriser/gouvernance-du-SI.htm*
- *http://fr.wikipedia.org/wiki/Gouvernance_des_syst%C3%A8mes_d'information*

Gouvernance IT

- Frédéric Georgel *IT Gouvernance* Dunod

GOUVERNANCE DEFINITION ET ENJEUX

- La gouvernance
- Gouvernance d'entreprise
- Gouvernance du Système d'Information
- **Illustration : The Sarbanes – Oxley Act**

Illustration

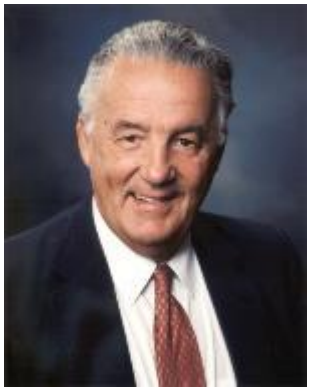
Loi de Sécurité Financière Sarbanes – Oxley (USA)

Illustration

Loi de Sécurité Financière Sarbanes – Oxley (USA)

La loi Sarbanes – Oxley, promulguée en 2002, doit son nom à ses promoteurs

- Le sénateur démocrate Paul Sarbanes



- Le député républicain M[illegible],

On la désigne également comme :

- ✓ *Public Company Accounting Reform and Investor Protection Act* (au Sénat)
- ✓ *Corporate and Auditing Accountability and Responsibility Act* (à la Chambre)

et plus couramment :

- ✓ *Sarbanes–Oxley*
- ✓ *Sarbox*
- ✓ *Sox*

Illustration

Loi de Sécurité Financière Sarbanes – Oxley (USA)

- Par cette loi, le top management ("principal officers" : Chief Executive Officer, PDG, et Chief Financial Officer, Directeur Financier) des entreprises concernées doit certifier personnellement l'exactitude des informations financières publiées
- Elle a été approuvée :
  - À la Chambre : par 423 voix pour, 3 contre et 8 abstentions
  - Au Sénat : par 99 voix pour et 1 abstention
- La loi règlemente des aspects comme :
  - ✓ L'indépendance des auditeurs
  - ✓ La gouvernance d'entreprise
  - ✓ Le contrôle interne
  - ✓ L'amélioration de la communication financière

Loi de Sécurité Financière Sarbanes – Oxley (USA)

- La loi Sarbanes-Oxley s'impose aux entreprises cotées sur le marché principal de la bourse de New-York (NYSE, New York Stock Exchange).
- Elle vise à fiabiliser les communications financières des entreprises et à redonner confiance aux investisseurs en réaction aux scandales financiers majeurs ayant impliqué des entreprises comme Enron, Tyco International ou WorldCom.
- A la suite des USA, d'autres pays ont édicté des lois comparables :
  - ✓ En Asie et Océanie : Japon, Australie et Inde,
  - ✓ En Europe : Allemagne, France et Italie,
  - ✓ En Afrique et Moyen-Orient : Israël,, Afrique du Sud et Turquie

Illustration

Loi de Sécurité Financière Sarbanes – Oxley (USA)

- La loi a amené l'organisme de régulation des opérations en bourse, la SEC (Securities and Exchange Commission) à édicter de nombreuses règles de conformité.

- Elle a conduit à la création d'un organisme quasi-public, le PCAOB (Company Accounting Oversight Board)

en charge de la supervision, la régulation et l'inspection des entreprises comptables dans leur rôle d'auditeur.

Loi Sarbanes – Oxley (USA)

Les onze titres de la loi

1. Rôle et responsabilités du PCAOB (Public Company Accounting Oversight Board)
2. Indépendance des auditeurs
3. Responsabilité d'entreprise
4. Amélioration de la communication financière
5. Conflit d'intérêts des analystes
6. Autorité et moyens de la Commission (des opérations de bourse, SEC)
7. Etudes et rapports
8. Responsabilité de fraude criminelle et d'entreprise
9. Augmentation des sanctions criminelles à l'égard des cols blancs
10. Déclaration d'impôts des entreprises
11. Responsabilité de la fraude d'entreprise

Loi Sarbanes – Oxley (USA)

Implications de certains titres de la loi

2. Indépendance des auditeurs

- Limite la fourniture de services autres que les audits aux sociétés auditées

3. Responsabilité d'entreprise

- Le management porte une responsabilité individuelle concernant l'exactitude et la complétude des rapports financiers d'entreprise

6. Augmentation des sanctions criminelles à l'égard des cols blancs

- Augmentation des pouvoirs de la SEC pour censurer ou interdire certains professionnels

7. Etudes et rapports

- Entre autres, rôle des agences de notation

8. Responsabilité de la fraude d'entreprise

- Entre autres, protection des donneurs d'alerte (whistle blowers)

10. Déclaration d'impôts des entreprises

- Notamment, le Chef d'Entreprise doit signer personnellement la déclaration d'impôts de l'entreprise

Loi Sarbanes – Oxley (USA)

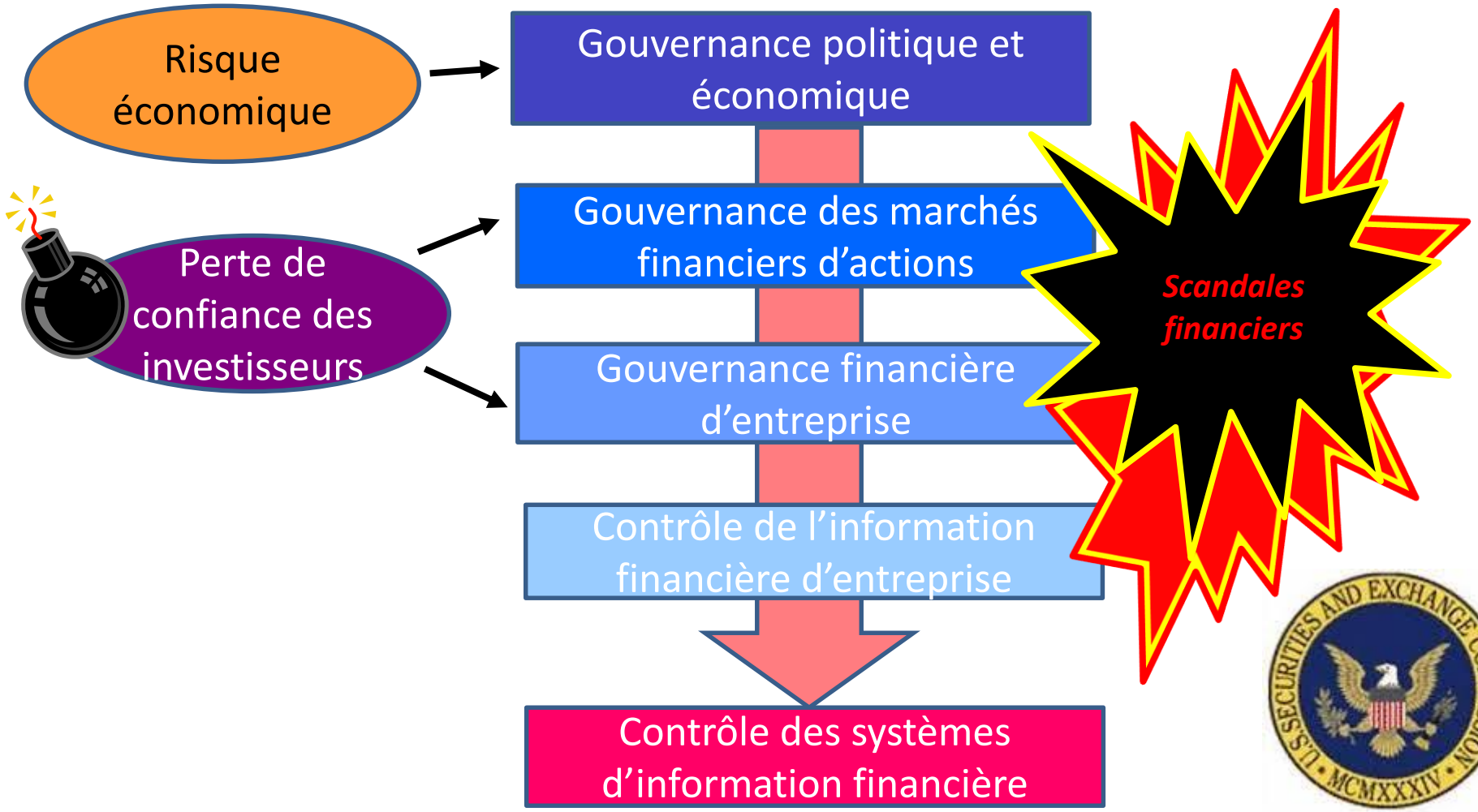
Impacts sur le Système d'Information : l'Article 404

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

- (a) RULES REQUIRED- The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
  - ***(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and***
  - ***(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting***.
- (b) INTERNAL CONTROL EVALUATION AND REPORTING- With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

Loi Sarbanes – Oxley (USA)

Pourquoi le SI est-il concerné ?



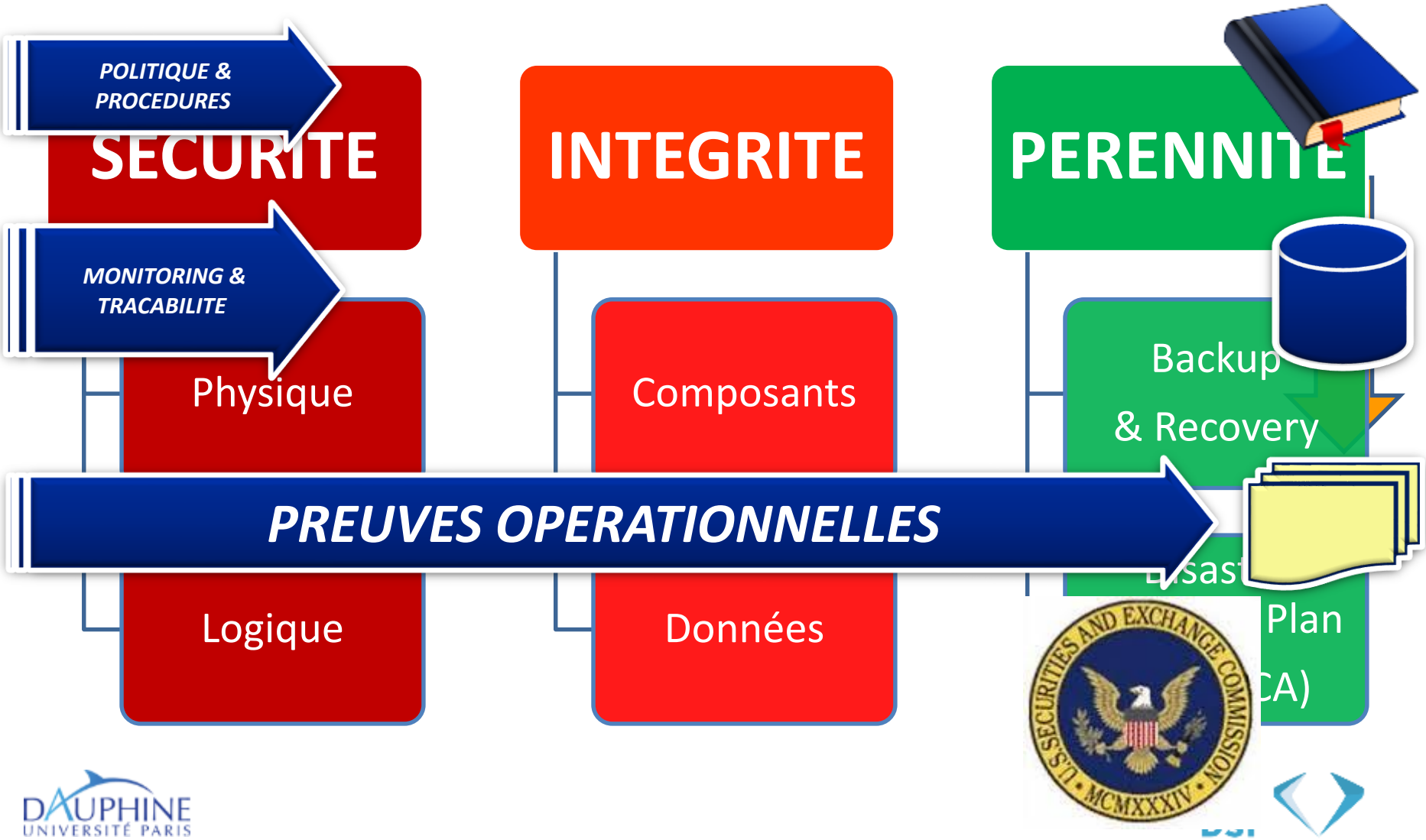
Loi Sarbanes – Oxley (USA)

Impacts sur la gouvernance du SI

- L'audit hérite d'un volet de contrôle supplémentaire
- Offres de consulting adaptées
- Version spécifiques de référentiels de contrôles
  - ✓ En général, Cobit Sox
  - ✓ Description formelles des contrôles (politiques et procédures)
  - ✓ Enregistrements des évènements ou/et des exceptions
  - ✓ Traçabilité de la chaîne de décision
  - ✓ Fournitures de preuves pour les décisions et les exceptions
  - ✓ Audit de certification par Commissaires aux Comptes

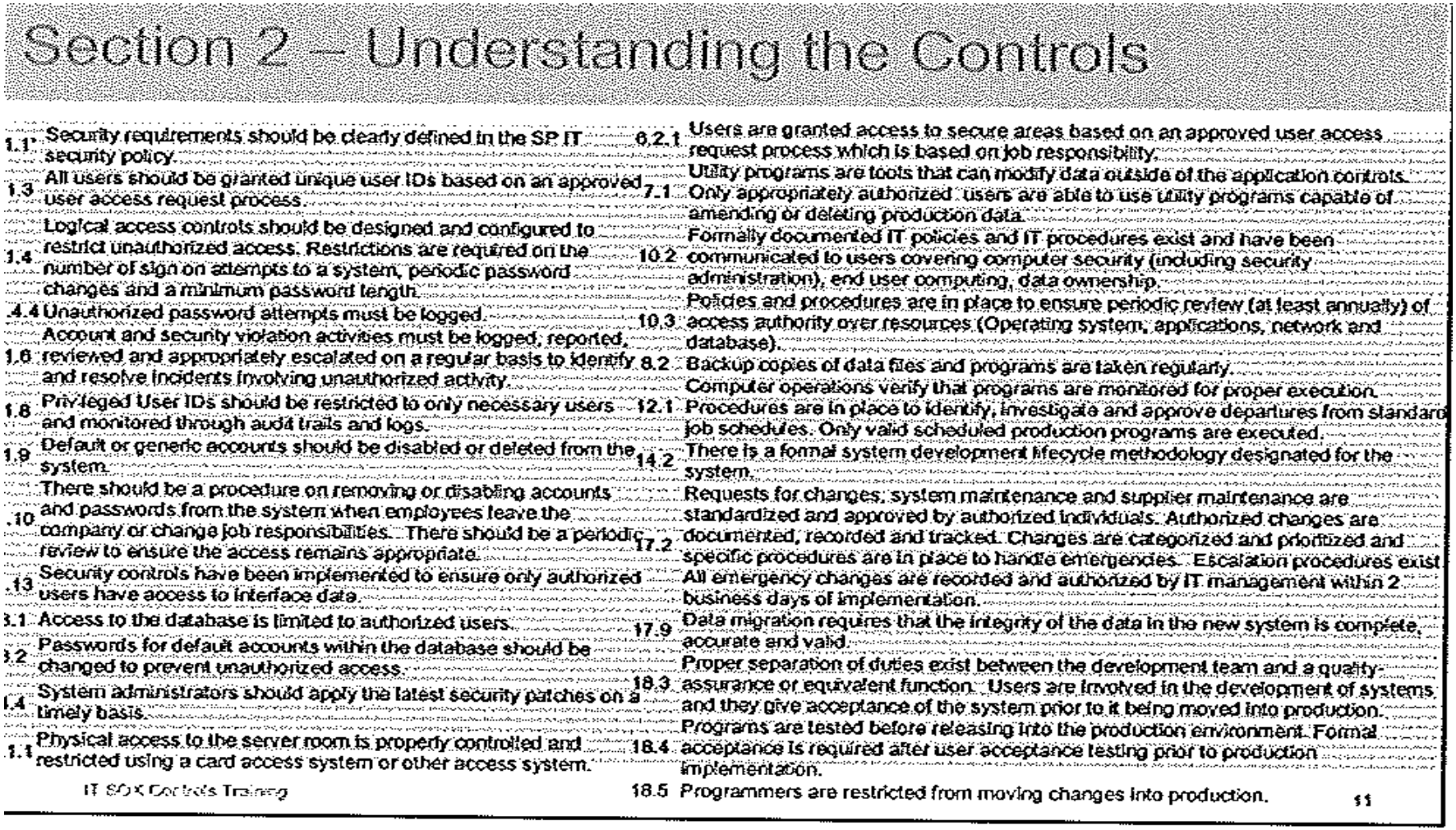
Loi Sarbanes – Oxley (USA)

Impacts sur la gouvernance du SI



Loi Sarbanes – Oxley (USA)

Exemples de contrôles IT Sox

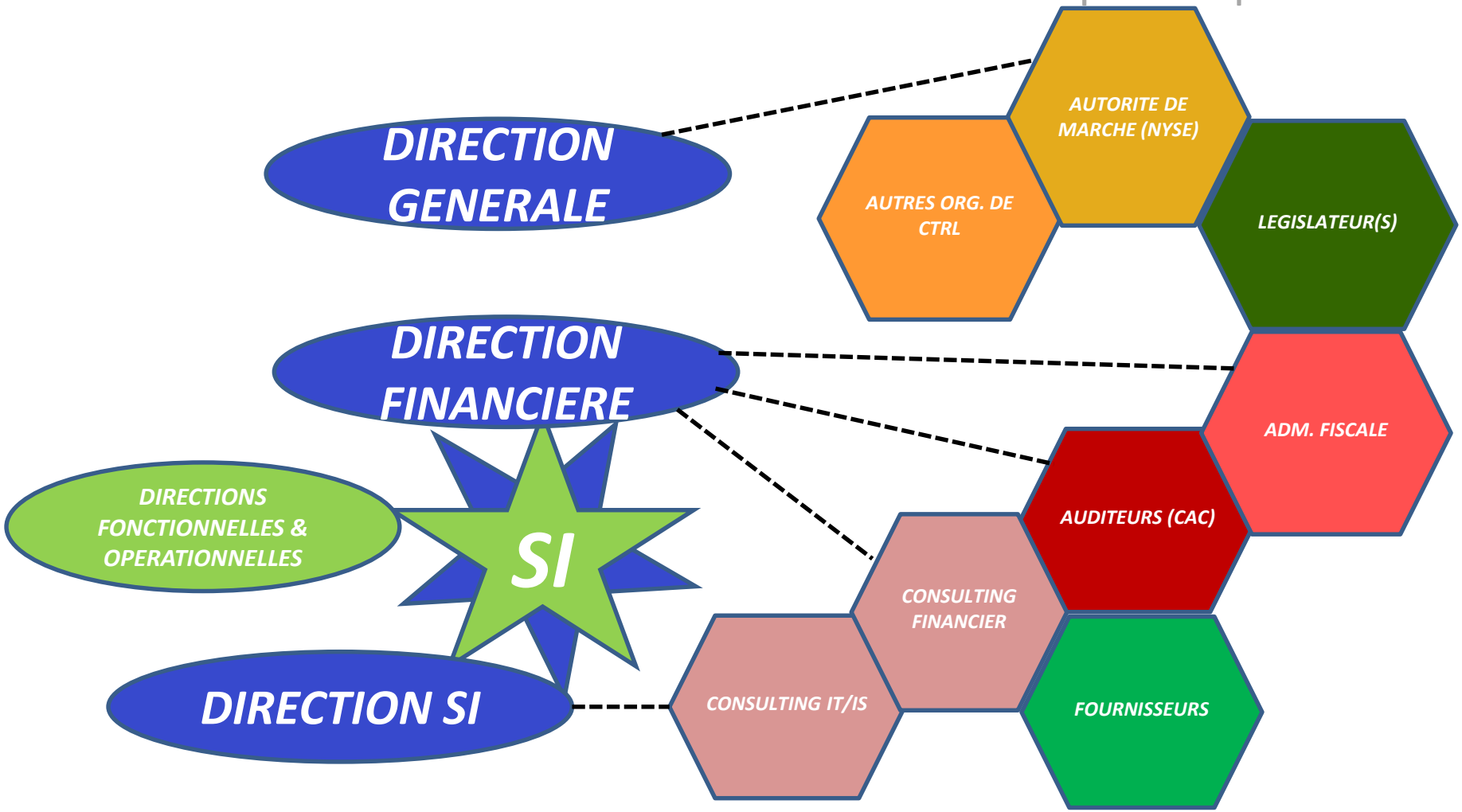


Section 2 – Understanding the Controls

1.1	Security requirements should be clearly defined in the SP IT security policy.	6.2.1	Users are granted access to secure areas based on an approved user access request process which is based on job responsibility.
1.3	All users should be granted unique user IDs based on an approved user access request process.	7.1	Utility programs are tools that can modify data outside of the application controls. Only appropriately authorized users are able to use utility programs capable of amending or deleting production data.
1.4	Logical access controls should be designed and configured to restrict unauthorized access. Restrictions are required on the number of sign on attempts to a system, periodic password changes and a minimum password length.	10.2	Formally documented IT policies and IT procedures exist and have been communicated to users covering computer security (including security administration), end user computing, data ownership.
.4.4	Unauthorized password attempts must be logged.	10.3	Policies and procedures are in place to ensure periodic review (at least annually) of access authority over resources (Operating system, applications, network and database).
1.6	Account and security violation activities must be logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity.	8.2	Backup copies of data files and programs are taken regularly.
1.8	Privileged User IDs should be restricted to only necessary users and monitored through audit trails and logs.	12.1	Computer operations verify that programs are monitored for proper execution. Procedures are in place to identify, investigate and approve departures from standard job schedules. Only valid scheduled production programs are executed.
1.9	Default or generic accounts should be disabled or deleted from the system.	14.2	There is a formal system development lifecycle methodology designated for the system.
.10	There should be a procedure on removing or disabling accounts and passwords from the system when employees leave the company or change job responsibilities. There should be a periodic review to ensure the access remains appropriate.	17.2	Requests for changes, system maintenance and supplier maintenance are standardized and approved by authorized individuals. Authorized changes are documented, recorded and tracked. Changes are categorized and prioritized and specific procedures are in place to handle emergencies. Escalation procedures exist. All emergency changes are recorded and authorized by IT management within 2 business days of implementation.
.13	Security controls have been implemented to ensure only authorized users have access to interface data.		
3.1	Access to the database is limited to authorized users.	17.9	Data migration requires that the integrity of the data in the new system is complete, accurate and valid.
3.2	Passwords for default accounts within the database should be changed to prevent unauthorized access.	18.3	Proper separation of duties exist between the development team and a quality assurance or equivalent function. Users are involved in the development of systems and they give acceptance of the system prior to it being moved into production. Programs are tested before releasing into the production environment. Formal acceptance is required after user acceptance testing prior to production implementation.
4.4	System administrators should apply the latest security patches on a timely basis.		
4.1	Physical access to the server room is properly controlled and restricted using a card access system or other access system.	18.4	
	IT SOX Controls Training	18.5	Programmers are restricted from moving changes into production. 11

Loi Sarbanes – Oxley (USA)

Les parties prenantes



FIN

DE LA

PREMIERE JOURNEE