



Gouvernance et contrôle des risques Systèmes d'Information

RÉFÉRENCE
DSI



Jour 2 : 360°

Jean-Marc Montels
Maximilien Stebler
Philippe Tronc

La gouvernance est très directement associée au contrôle du risque.


Quels sont les risques SI ?

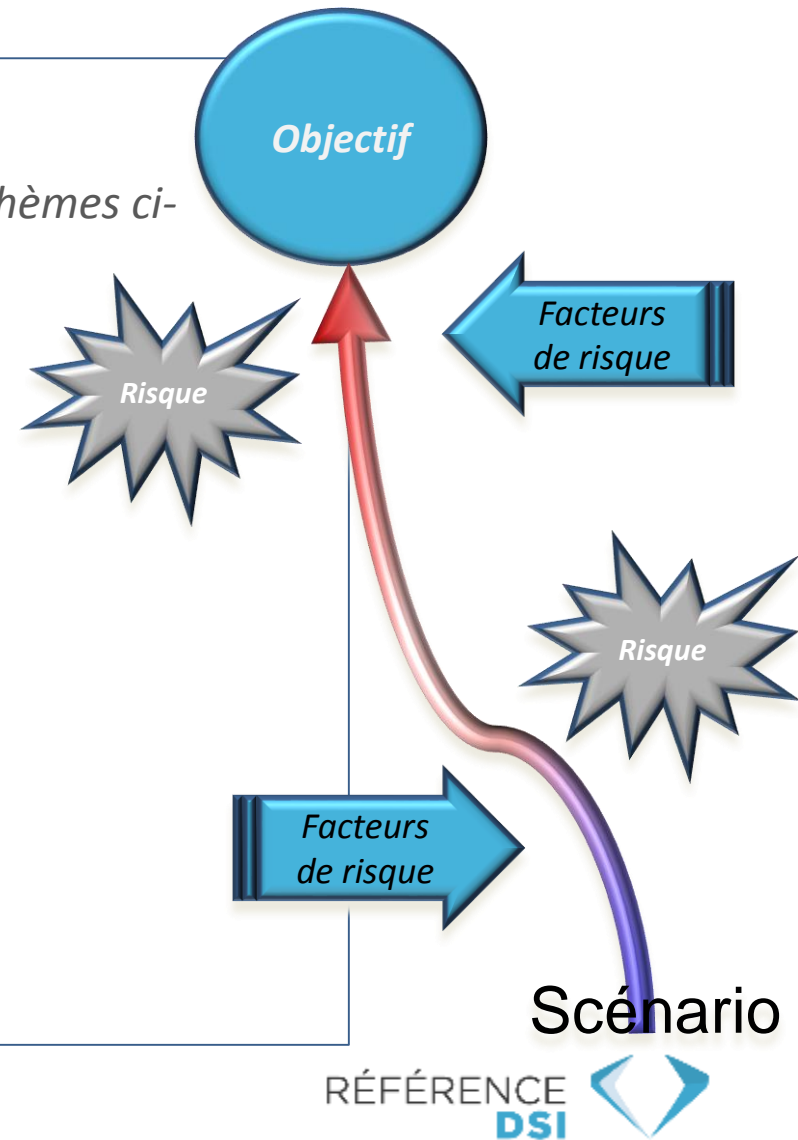


NOTION DE RISQUE

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*
- 



GOVERNANCE SI

Entre gestion du risque et opportunité :

Littérature, normes, modèles sur la gouvernance nous ramènent au contrôle du risque.

- Sa finalité est d'assurer aux dirigeants, actionnaires et autres parties prenantes (collaborateurs, partenaires) que la fonction SI est parfaitement gérée.

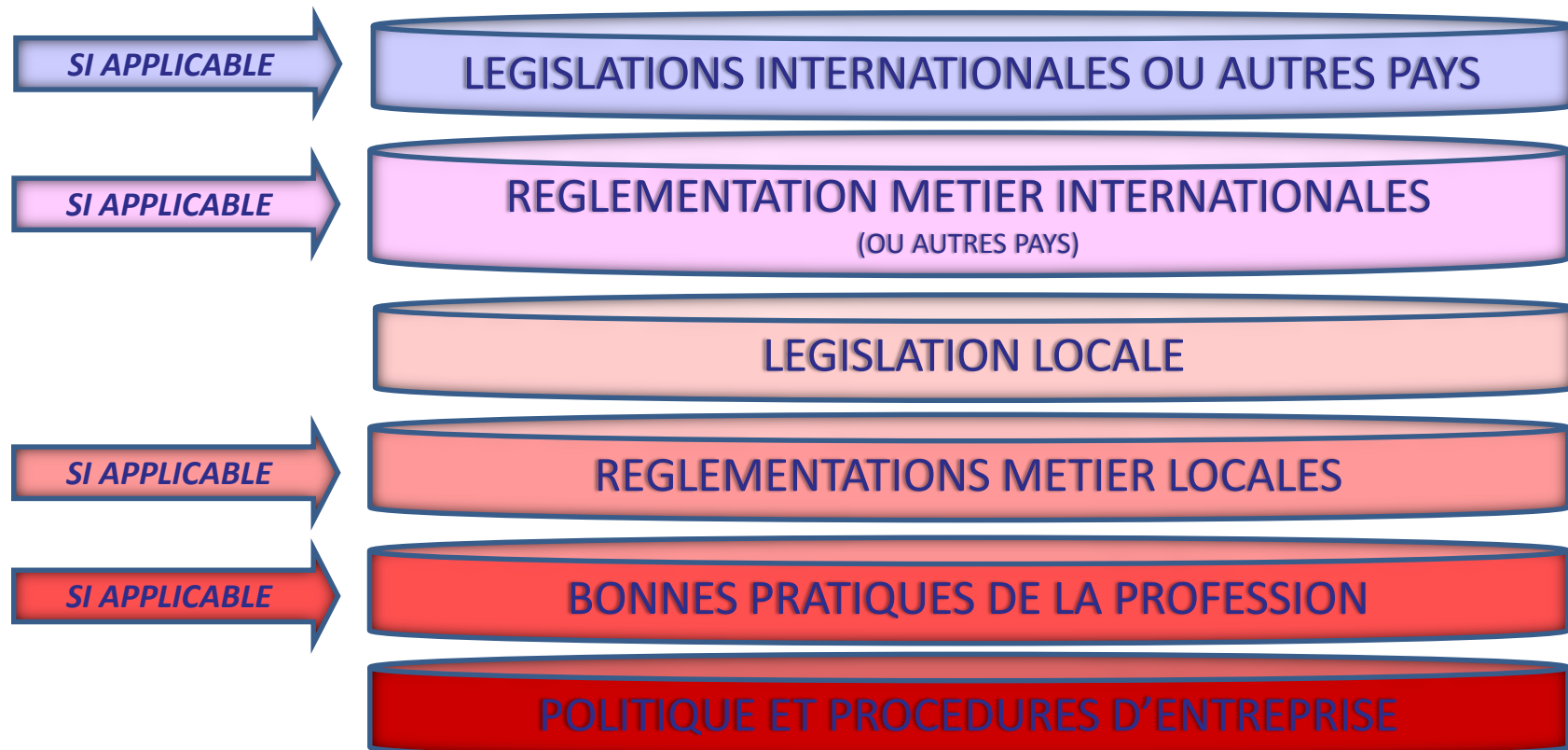
Quitte à être iconoclaste, veillons également à intégrer que gouverner, c'est aussi saisir des opportunités.

- Parlons alors d'un ensemble des moyens qui concourent à un pilotage efficient et une mise en synergie de toutes les composantes de son SI pour afin d'en tirer le profit maximum.

GOVERNANCE SI

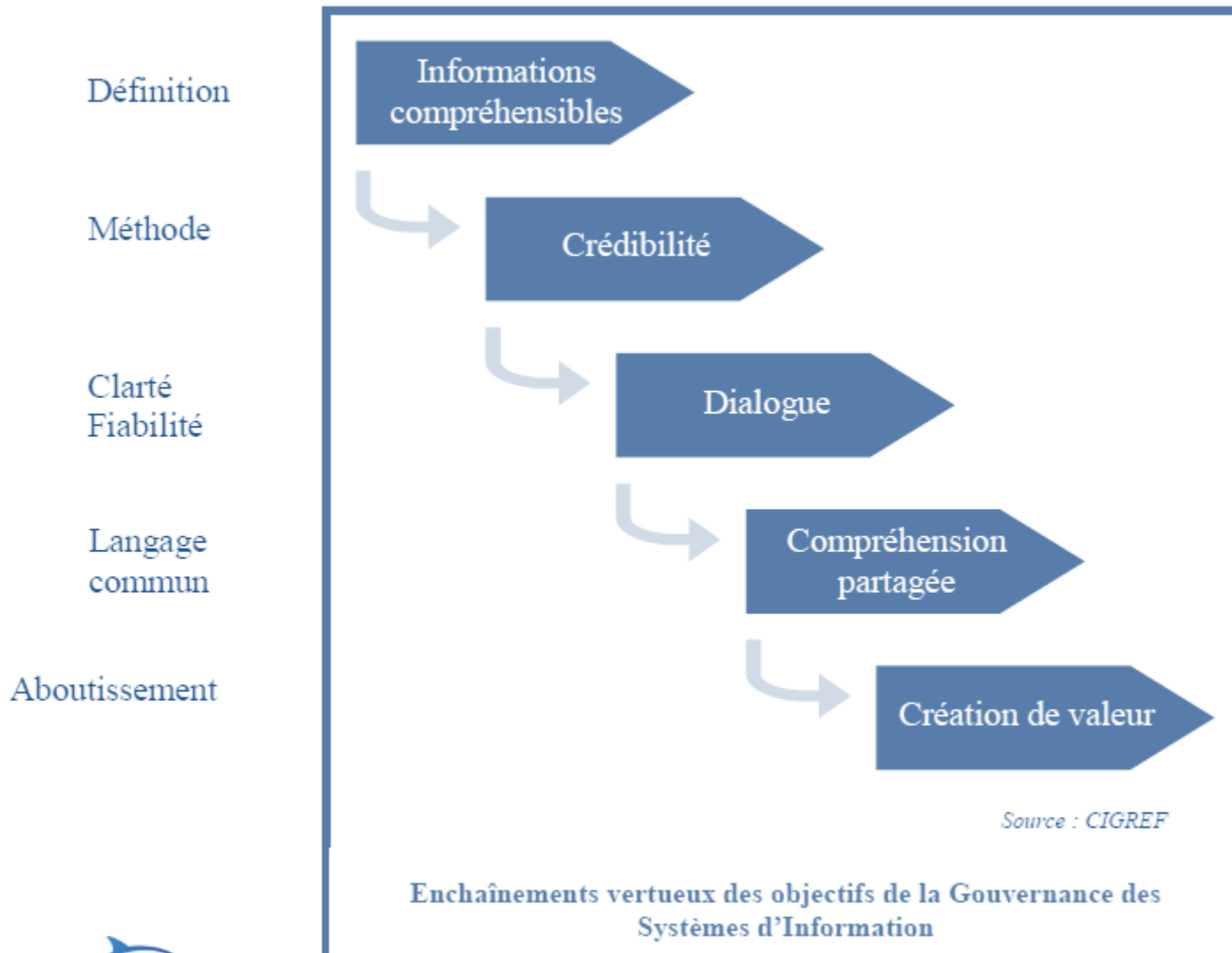
Contexte de la gouvernance - Compliance

- Terme anglo-américain (« Conformité ») qui s'est imposé pour désigner la somme des réglementations auxquelles l'entreprise (et par ricochet son SI) doivent se conformer



Gouvernance SI

Gouverner : comment et pourquoi ?



Gouvernance du SI

Les 5 piliers de la gouvernance :



Les 5 piliers de la gouvernance

Alignement stratégique

- Pour une meilleure gouvernance, le système d'information doit être aligné sur la stratégie générale de l'entreprise.
- En d'autres termes, les objectifs du SI doivent être en adéquation claire avec les grands objectifs stratégiques.
- Par conséquent, la stratégie du SI doit être la déclinaison de la stratégie globale à son niveau.
- La DSI est tenue alors de mobiliser ses ressources pour contribuer activement à l'atteinte des objectifs de l'entreprise.



Les 5 piliers de la gouvernance

Alignement stratégique et CoBit

- Le référentiel Cobit propose d'établir un cadre de pilotage orienté processus du Système d'Information afin de contribuer efficacement à l'alignement des technologies sur la stratégie d'entreprise.
- COBIT a pour ambition de placer en perspective les solutions techniques et les risques business dans une logique de contrôle et de management.
- La démarche s'inscrit dans une dynamique d'amélioration continue, généralise la pratique de l'audit et garantit la gestion des risques.

Les 5 piliers de la gouvernance

Alignement stratégique et CoBit

➤ Cobit est structuré selon 34 processus regroupés en 4 domaines :

- **Planning and Organization** : Planning et Organisation
Comment utiliser au mieux les technologies afin que l'entreprise atteigne ses objectifs ?
- **Acquisition and Implémentation** : Acquisition et Mise en place
Comment définir, acquérir et mettre en œuvre les technologies nécessaires en adéquation avec les business processus de l'entreprise ?
- **Delivery and Support** : Distribution et Support
Comment garantir l'efficacité et l'efficience des systèmes technologiques en action ?
- **Monitoring** : Surveillance
Comment s'assurer que la solution mise en œuvre corresponde bien aux besoins de l'entreprise dans une perspective stratégique ?



Les 5 piliers de la gouvernance

Alignement stratégique et CoBit

➤ 7 critères d'information pour qualifier le jugement :

1. Efficience
2. Efficacité
3. Confidentialité
4. Intégrité
5. Disponibilité
6. Conformité
7. Fiabilité

Les 5 piliers de la gouvernance

Alignement stratégique et CoBit

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure
Governance
Framework Setting
and Maintenance

EDM02 Ensure
Benefits Delivery

EDM03 Ensure
Risk Optimisation

EDM04 Ensure
Resource
Optimisation

EDM05 Ensure
Stakeholder
Transparency

Align, Plan and Organise

AP001 Manage
the IT Management
Framework

AP002 Manage
Strategy

AP003 Manage
Enterprise
Architecture

AP004 Manage
Innovation

AP005 Manage
Portfolio

AP006 Manage
Budget and Costs

AP007 Manage
Human Resources

AP008 Manage
Relationships

AP009 Manage
Service
Agreements

AP010 Manage
Suppliers

AP011 Manage
Quality

AP012 Manage
Risk

AP013 Manage
Security

Monitor, Evaluate and Assess

MEA01 Monitor,
Evaluate and Assess
Performance and
Conformance

MEA02 Monitor,
Evaluate and Assess
the System of Internal
Control

MEA03 Monitor,
Evaluate and Assess
Compliance With
External Requirements

Build, Acquire and Implement

BAI01 Manage
Programmes and
Projects

BAI02 Manage
Requirements
Definition

BAI03 Manage
Solutions
Identification
and Build

BAI04 Manage
Availability
and Capacity

BAI05 Manage
Organisational
Change
Enablement

BAI06 Manage
Changes

BAI07 Manage
Changes
Acceptance and
Transitioning

BAI08 Manage
Knowledge

BAI09 Manage
Assets

BAI010 Manage
Configuration

Deliver, Service and Support

DSS01 Manage
Operations

DSS02 Manage
Service Requests
and Incidents

DSS03 Manage
Problems

DSS04 Manage
Continuity

DSS05 Manage
Security
Services

DSS06 Manage
Business
Process Controls

Processes for Management of Enterprise IT



Gouvernance SI

Alignement stratégique

Stratégie d'entreprise

Marché

Finances

Innovation

ALIGNEMENT

- Quantitatif
- Qualitatif :
 - ✓ priorités,
 - ✓ cibles,
 - ✓ ...

Stratégie SI

Stratégie IT

Services et Applications

SI

RESSOURCES

C O U P L A T A G E

INFORMATIONS



Les 5 piliers de la gouvernance

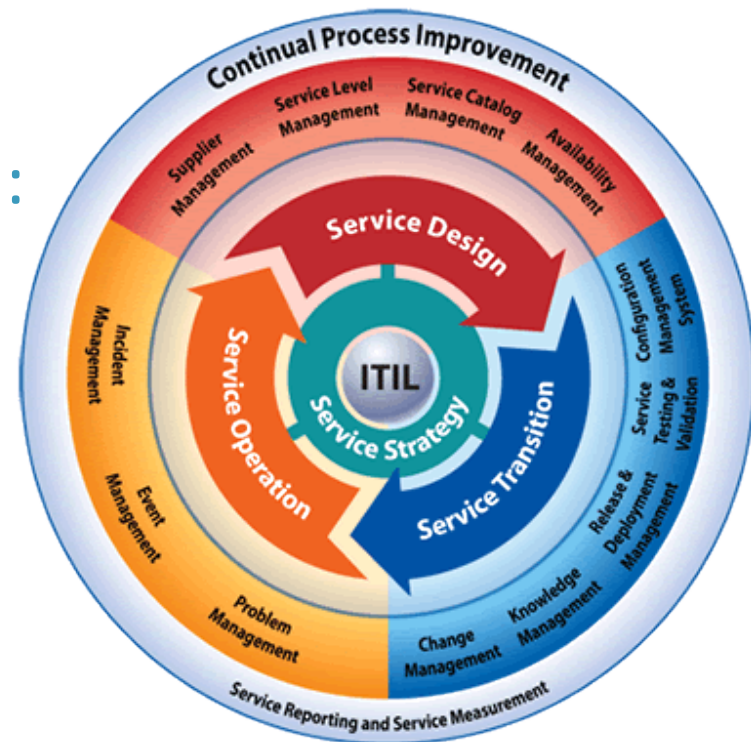
Alignement stratégique et ITIL

➤ La notion d'alignement stratégique apparaît à partir de la Version 3.

➤ Initialement, ITIL est centré sur :

- Le Service Support
- Le service Delivery

Itil V3



Les 5 piliers de la gouvernance

Modèles d'alignement stratégique

- Les 4 modes d'alignement stratégique : le modèle Henderson et Venkatraman
 - *MODE 1 : Exécution opérationnelle de la stratégie*
 - *MODE 2 : Les SI comme vecteurs de la transformation technologique*
 - *MODE 3 : Les SI à l'origine de la stratégie et source d'avantage concurrentiel*
 - *MODE 4 : Les SI comme prestataire de services opérationnels*

Les 5 piliers de la gouvernance

Modèles d'alignement stratégique

➤ Les 4 modes d'alignement stratégique : le modèle Henderson et Venkatraman

MODE 1 : Exécution opérationnelle de la stratégie

Dans ce premier mode, la Direction Générale et les Directions Métiers sont à l'origine de la stratégie. Une stratégie dictée pour assurer l'exécution opérationnelle des activités suivant des règles de gestion prédéfinies et persistantes.

La DSI s'adapte alors dans ce cas littéralement aux processus existants et sa tâche se résume à essayer de satisfaire, notamment, des besoins de disponibilité, rapidité, coûts et délais.

Ce type d'alignement se fait généralement dans le cas d'une entreprise qui a acquis une maturité relativement importante et dans laquelle la DSI n'intervient pas ou que peu dans la définition de son mode d'organisation.

Les 5 piliers de la gouvernance

Modèles d'alignement stratégique

➤ Les 4 modes d'alignement stratégique : le modèle Henderson et Venkatraman

MODE 2 : les SI comme vecteur de la transformation technologique

Dans ce mode, la Direction Générale définit une nouvelle stratégie qui va déclencher une redéfinition de la stratégie de la DSI. Autrement dit, la DSI est appelée à concrétiser une innovation exprimée par la Direction Générale.

Une fois la stratégie de la DSI redéfinie, il faut penser aux infrastructures et aux processus technologiques nécessaires à sa mise en place.

La DSI est évaluée dans ce cas par sa capacité de fournir une innovation technologique adaptée au besoin et les délais de réalisation.

Enfin, la DSI est un facteur primordial de différenciation dans ce genre de stratégies.

Les 5 piliers de la gouvernance

Modèles d'alignement stratégique

➤ Les 4 modes d'alignement stratégique : le modèle Henderson et Venkatraman

MODE 3 : les SI à l'origine de la stratégie et source d'avantage concurrentiel

Ce mode d'alignement est un mode qui règne dans des secteurs dominés par la technologie comme le secteur des télécommunications, l'industrie automobile, etc... . En effet, la stratégie de la DSI est dans ce cas le fait initiateur de la stratégie globale de l'entreprise.

La DSI adopte des innovations technologiques majeures en vue d'offrir à l'entreprise un avantage concurrentiel.

La stratégie d'entreprise et les processus métiers n'existent pas a priori mais découlent des opportunités technologiques.

La DSI est alors tenue de traduire les nouvelles tendances technologiques en stratégie d'offres de produits et service.

Les 5 piliers de la gouvernance

Modèles d'alignement stratégique

➤ Les 4 modes d'alignement stratégique : le modèle Henderson et Venkatraman

MODE 4 : les SI comme prestataire de services opérationnels

Dans ce mode, l'accent est mis sur la relation de la DSI vis-à-vis des Directions Métiers.

La DSI élabore une stratégie d'organisation des infrastructures et processus dans le but de fournir un excellent niveau de service.

Les processus de l'entreprise sont alors remis en question pour optimiser les performances (qualité de service, satisfaction des utilisateurs, etc...).

On rencontre ce mode souvent dans les entreprises qui voient leur rythme d'évolution des activités s'élever.

Alignement stratégique

Etude de cas : AuBonFoieGras.com

➤ AuBonFoieGras.com



AuBonFoieGras.com a pour stratégie de se développer à l'international, en propre aux USA et en Angleterre, en Joint Venture en Chine et en Russie

- Comment aligner SI et Stratégie d'entreprise ?
- Dans quel mode je me situe ?



Alignement stratégique

Etude de cas : Un Nez bien né

➤ UnNezbienNé.com



Un Nez bien né est une société de création de fragrance.

Le directeur informatique d'un Nez Bien Né a créé une application Android et IOS qui permet de qualifier et « liker » des parfums.

Chaque semaine, un utilisateur de la semaine est tiré au sort et gagne un parfum.

En quelques mois il a constitué une base unique des goûts et tendances de fragrances.



➤ Comment aligner SI et Stratégie d'entreprise ? Dans quel mode je me situe ?



Les 5 piliers de la gouvernance

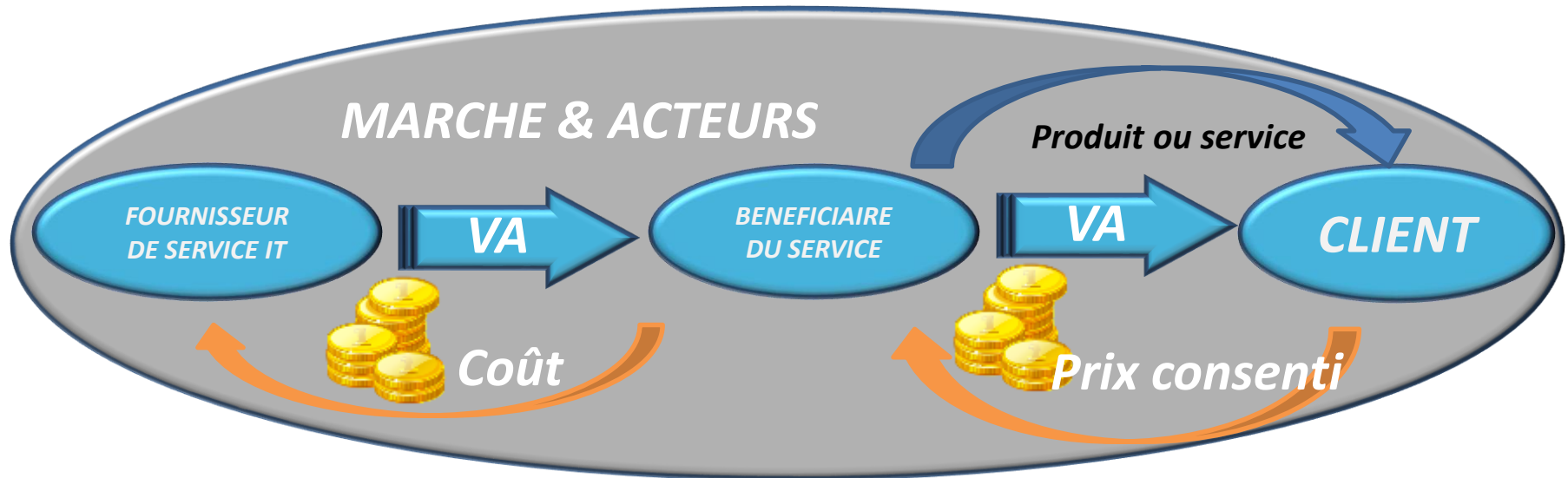
Création de valeur

- Le SI doit créer de la valeur et doit apporter des bénéfices à l'entreprise.
- La justification de son budget passe par la mise en évidence de la valeur créée et l'optimisation des coûts.
- La valeur ajoutée demeure quoique qu'il en soit abstraite et difficile à mesurer.



Les 5 piliers de la gouvernance

Création de valeur dans un marché



APPROCHE FINANCIERE DE LA VALEUR AJOUTEE

Valeur Ajoutée (VA) = Produits – Matières premières – Achats externes

💡 On peut approcher de la sorte l'apport interne à l'entreprise dans la constitution de la Valeur Ajoutée.

Valeur Ajoutée (VA) = Excédent Brut d'Exploitation (EBE) + Salaires

💡 L'EBE finance le remplacement des investissements et autres provisions, le fisc, les financiers, les actionnaires. La VA représente les engagements durables : investissements, collectivité, capital, personnel.

💡 La part moyenne de la masse salariale des logiciels et services IT est de l'ordre de 60 à 70% du Produit.

💡 Quelle valeur ajoutée représente la DSI pour chacun des acteurs ? Ou dit autrement, combien chacun des acteurs est-il prêt à payer le service apporté par la DSI ?

Les 5 piliers de la gouvernance

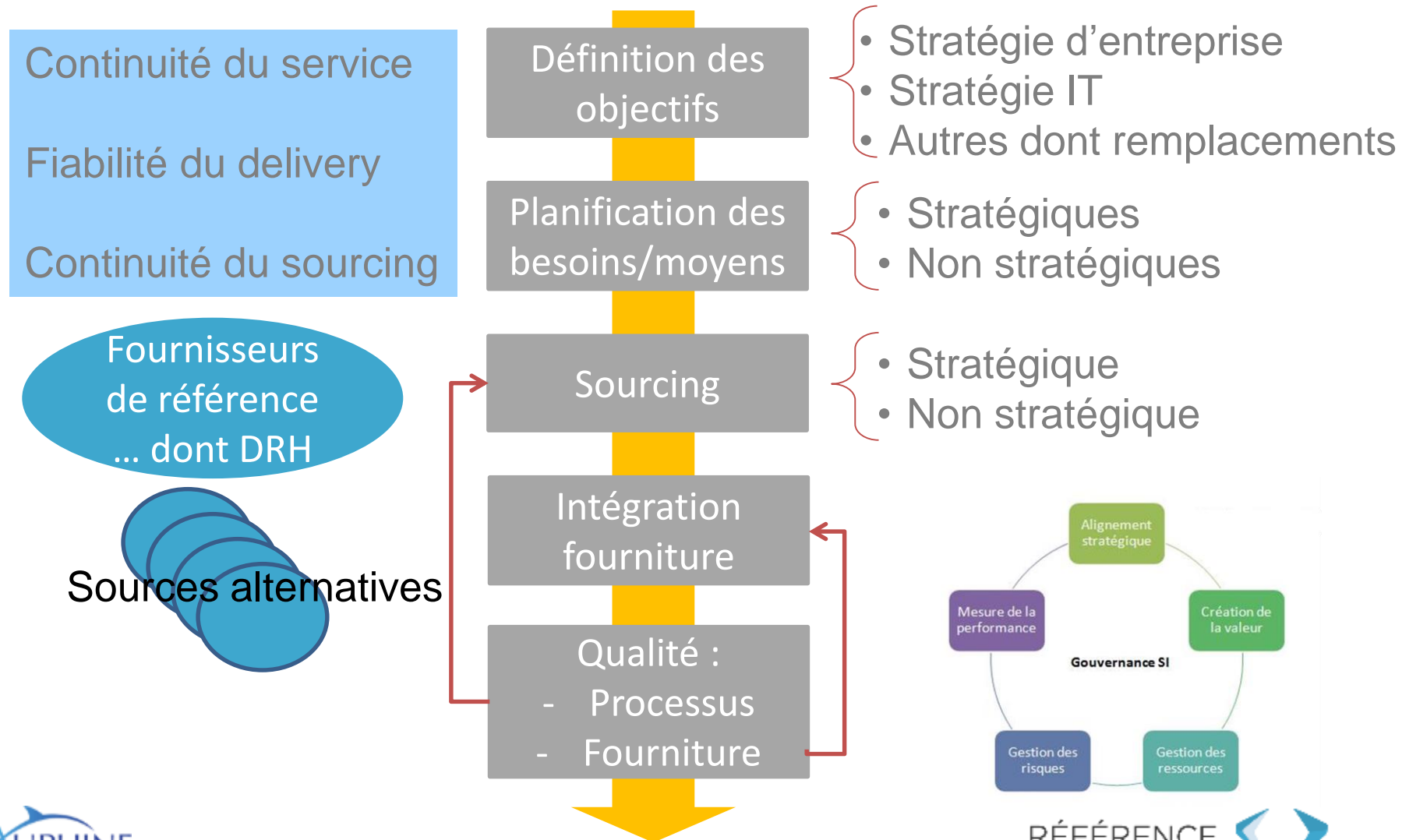
Gestion des ressources

- Ce pilier de la gouvernance vise à optimiser et à rationaliser les investissements dans les ressources informatiques (infrastructures, applications, compétences,...).
- L'optimisation financière des ressources est pilotée par la démarche budgétaire.



Les 5 piliers de la gouvernance

Gestion des ressources : Supply Chain IT



Les 5 piliers de la gouvernance

Gestion des ressources : priorités de gouvernance

	<i>INTERNE</i>	<i>EXTERNE</i>
<i>STRATEGIQUE</i>	<ul style="list-style-type: none"> Adéquation Disponibilité Coût et Charge vs. Valeur Capitalisation connaissances 	<ul style="list-style-type: none"> Adéquation Sourcing Contrat Réversibilité
<i>NON STRATEGIQUE</i>	FLEXIBILITE	

CONTRAT

Type d'engagement
 Disponibilité/ Remplacement
 Evaluation
 Pérennité structure/compétence
 Coût & Charges vs. Valeur



➤ COBIT

- COBIT fait référence aux coûts dans le processus DS6 « Identifier et imputer les coûts » qui a pour objectif d' « assurer une connaissance exacte des coûts imputables aux services informatiques ».
- COBIT donne une liste de coûts alloués à toutes les ressources informatiques à recenser mais sans les définir précisément :
 - le matériel d'exploitation
 - les périphériques
 - l'utilisation des télécommunications
 - le développement des applications et leur maintenance
 - les frais généraux administratifs
 - les coûts des prestations des fournisseurs externes
 - l'assistance aux utilisateurs (help desk)
 - les installations et leur maintenance
 - les coûts directs/indirects
 - les charges fixes et variables
 - les coûts à fonds perdus et discrétionnaires

Le Budget IT vu par les référentiels

> ITIL

- ITIL a défini un processus « Gestion financière pour les services IT » qui a pour but d' « assurer une administration rentable des biens IT et des ressources financières utilisées pour la fourniture des services IT ».
 - ITIL propose un exemple de catégorisation des coûts informatiques :
 - - Matériel (grands systèmes, stockage sur disques, réseaux, PC, portables, serveurs locaux)
 - - Logiciel (systèmes d'exploitation, applications, bases de données, outils de contrôle de gestion)
 - - Ressources humaines (salaires, primes, coûts de transfert, frais, conseils)
 - - Locaux (bureaux, réserve, lieux sécurisés)
 - - Services externes (services de sécurité, de récupération en cas de sinistre, d'approvisionnement à l'extérieur)
 - - Transfert (dépenses internes provenant d'autres centres de coûts au sein de l'organisation)
 - ITIL précise que d'autres catégorisations peuvent être choisies ; **l'important est que tous les coûts soient identifiés.** La catégorisation dans un « Cost Model » ("Budget" ou "Plan de comptes informatiques") doit permettre :
 - d'analyser l'évolution dans le temps de ses propres dépenses
 - de comparer ses coûts avec ceux d'autres organisations (internes ou externes)
- de servir de simple base pour l'ABC (Activity Based Costing)

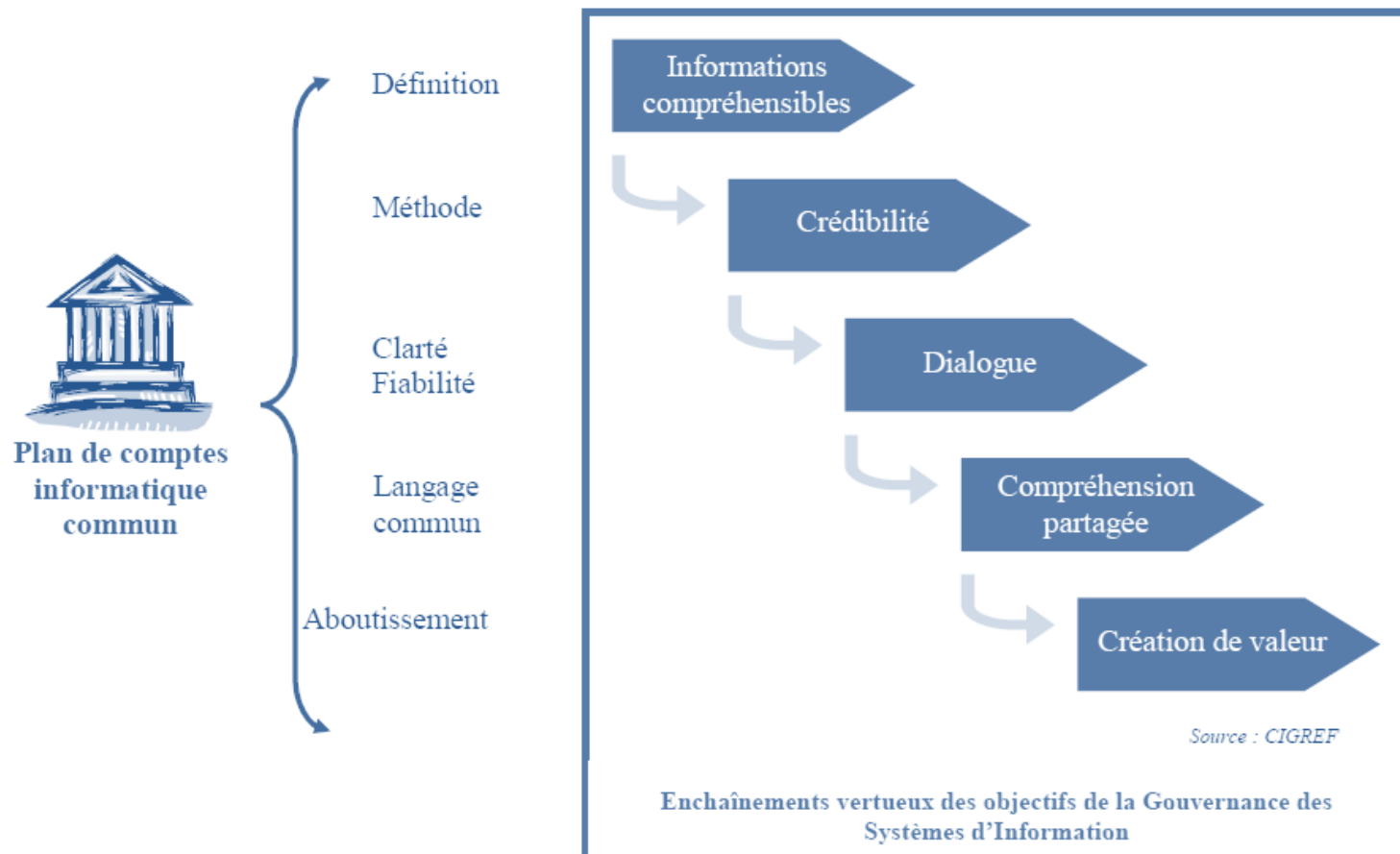


Démarche budgétaire : Point clé de la gouvernance

- **Rappel :** « La gouvernance décrit comment un système est dirigé et contrôlé. Ainsi définie, la gouvernance est l'association du pilotage, c'est-à-dire s'assurer que les décisions d'aujourd'hui préparent convenablement demain, et du contrôle, c'est-à-dire mesurer l'écart par rapport à ce qui était prévu. »
- **Etablir un plan de comptes informatique commun contribue aux objectifs de base de la gouvernance :**
 - Informations compréhensibles
 - La gouvernance est bien une demande de plus de transparence. Pour trop de décideurs, le système d'information reste obscur dans sa définition, son étendue, sa terminologie et au final son coût et son apport.
 - Crédibilité
 - Pour construire sa crédibilité, il faut non seulement fournir des informations, mais aussi montrer et démontrer la nature rationnelle, contrôlée et prédictible des méthodes qui les produisent.

Le budget IT

Démarche budgétaire : Point clé de la gouvernance



Le budget IT

Un maîtrise insuffisante

- Beaucoup d'entreprises aujourd'hui encore ne savent pas ce que leur informatique leur coûte. Et plus aujourd'hui qu'hier d'ailleurs du fait de l'imbrication, voire de la fusion des systèmes d'information dans le fonctionnement de l'entreprise. A l'extrême, on trouve encore des cas où il n'y a pas de budget informatique à proprement parler.
- Le plus souvent les dépenses centrales directes sont suivies, parfois des études ponctuelles de coût complet sont réalisées.
- Au total, on constate très souvent un suivi synthétique très insuffisant de la dépense informatique.

Le budget IT

Quel périmètre ?

- Réflexion : quels couts en prendre en compte dans le budget informatique.



Le budget IT

Quel périmètre ?

- Le cout de l'informatique ne se limite pas aux seuls achats de matériel et de logiciels !
- Les 3 notions de couts à prendre en compte :
 1. Les dépenses du seul service informatique : ce sont les dépenses faites sous l'autorité du chef de service
 2. Les dépenses de la fonction informatique : c'est la somme du coût du service informatique et de l'informatique décentralisée
 3. Les dépenses du système d'information : c'est le coût de l'ensemble des tâches liées au fonctionnement de ces systèmes

Le budget IT

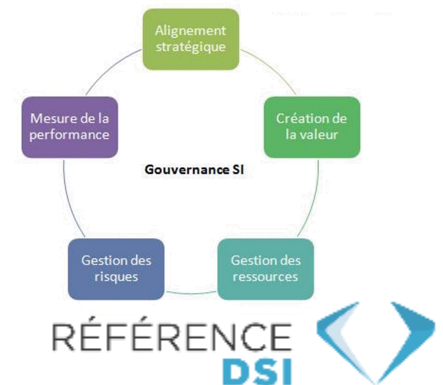
Quel périmètre ?

- **Les coûts d'investissement** (liés à une décision qui aboutit à une dépense) sont les dépenses effectuées en vue d'acquérir, de construire, de développer, de mettre en valeur ou d'améliorer une partie du SI et qui lui procureront des avantages au cours d'un certain nombre d'exercices.
- **Les coûts de fonctionnement** (liés à l'activité quotidienne et permettant un fonctionnement continu) sont les dépenses courantes informatiques, correspondant à l'ensemble des activités informatiques, qui relèvent de la marche normale des services informatiques, et qui concernent la réalisation de l'objet dominant que le service s'est donné.

Les 5 piliers de la gouvernance

Mesure de la performance

- Le SI doit être capable de mesurer la performance ou autrement dit surveiller l'activité et contrôler l'aboutissement à l'atteinte des objectifs stratégiques de l'entreprise par le biais de tableaux de bords et d'indicateurs pertinents afin d'apporter de la visibilité par rapport à une situation quelconque.
- La méthode du Balance Scorecard présente une façon standardisée de construire des tableaux de bord de mesure de la performance.



La mesure de la performance

Balance Scorecard

➤ L'ensemble des indicateurs opérationnels et économiques de la DSI peuvent être regroupés dans les 5 volets du Tableau de Bord de pilotage global (IT scorecard) :

- Contribution au Business
- Performance Economique
- Performance des processus informatiques
- Orientation « Clients »
- Apprentissage et préparation du Futur
- Un volet supplémentaire concernant la qualité de la « Gestion du risque » a été rajouté.

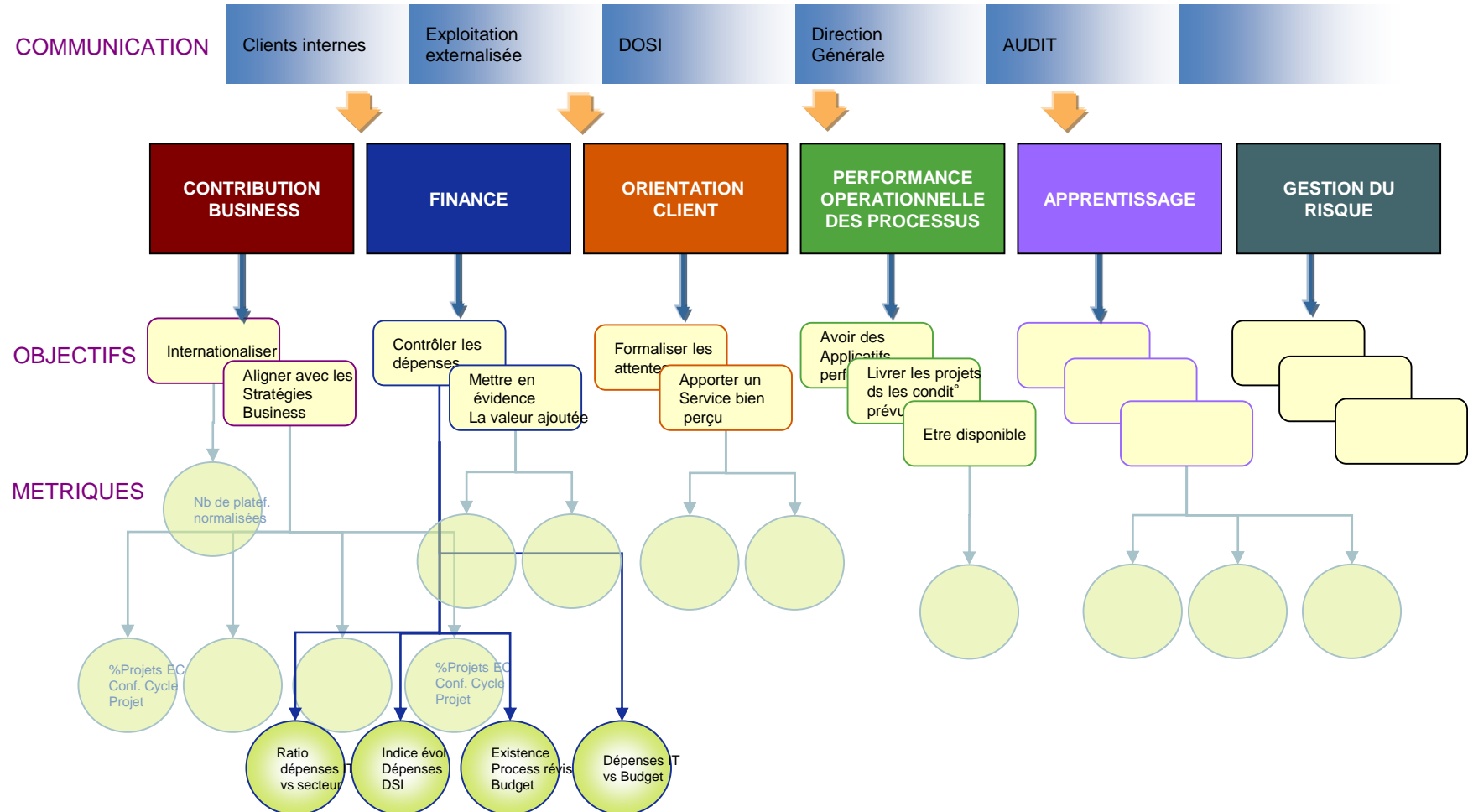
La mesure de la performance

Balance Scorecard

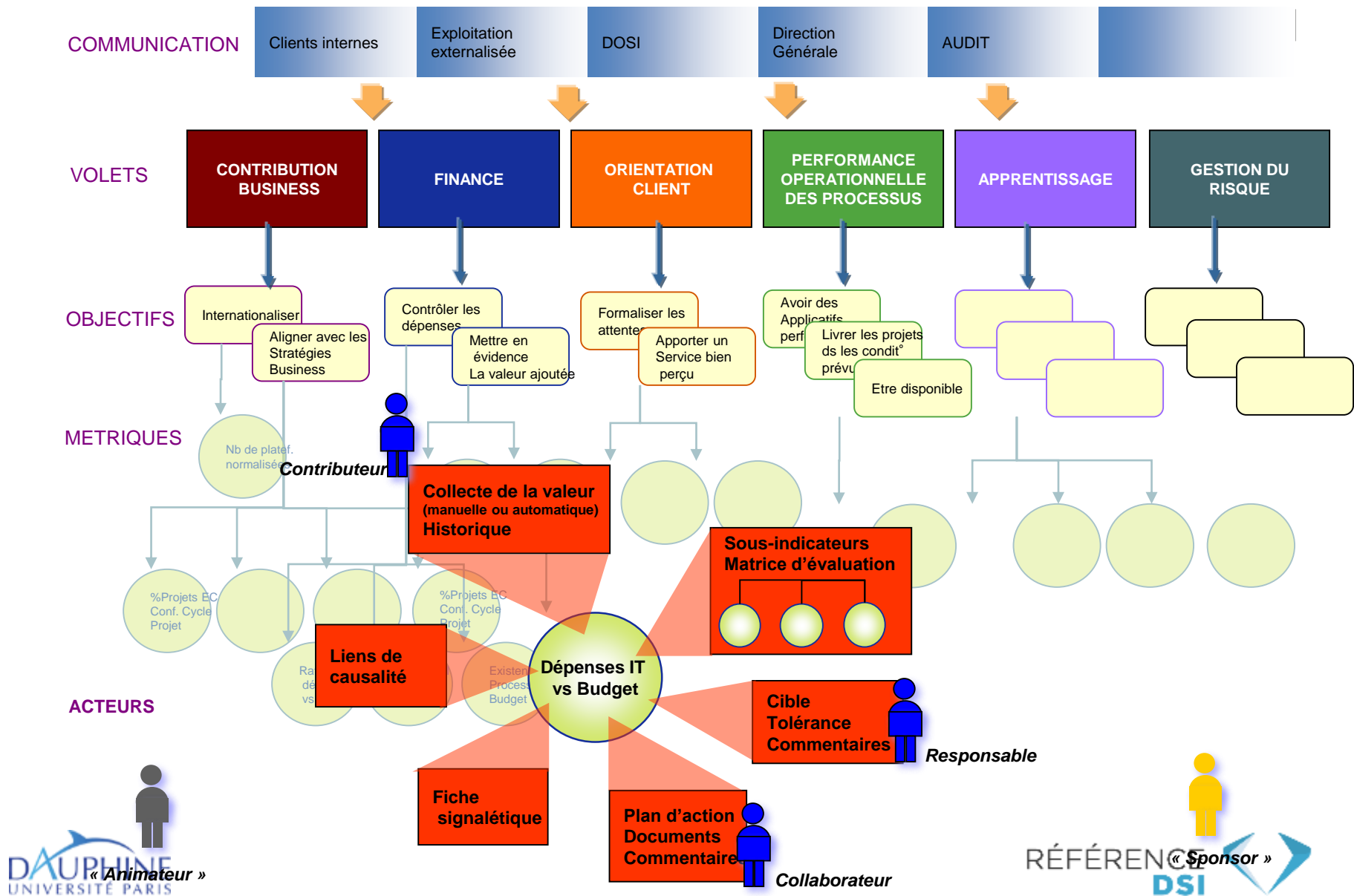
- L'objectif principal de ce tableau de bord est de faciliter la déclinaison des objectifs stratégiques de l'Entreprise en termes opérationnels et de suivre la progression des « réalisations » pour l'atteinte des objectifs fixés à chaque niveau.
- Dans ce but, chaque « volet » comprendra :
 - des Objectifs : description, enjeux,...
 - des Plans d'Action associés aux Objectifs : description, résultats attendus, délais, moyens alloués, responsable,....
 - des Indicateurs associés aux Plans d'Action permettant de mesurer la progression des résultats vers la « cible » à atteindre

Mesure de la performance

IT Scorecard



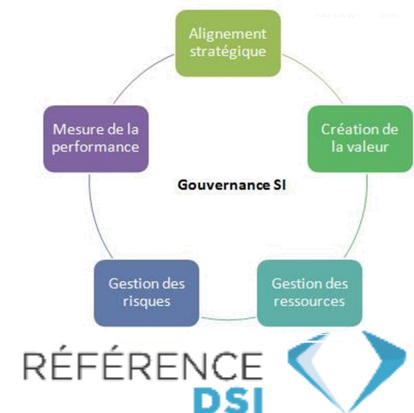
Mesure de la performance



Gouvernance du SI

Gestion des risques

- La gestion des risques consiste à prendre d'abord conscience de l'ensemble des menaces auxquelles est exposé le SI et essayer dans la mesure du possible de les contrôler.
- Dans ce contexte, le référentiel des bonnes pratiques ISO 27002 fournit les bonnes pratiques pour implémenter un système de management de la sécurité de l'information.
- D'une manière générale l'ensemble des référentiels ISO 27000 s'intéressent au management de la sécurité du système d'information.

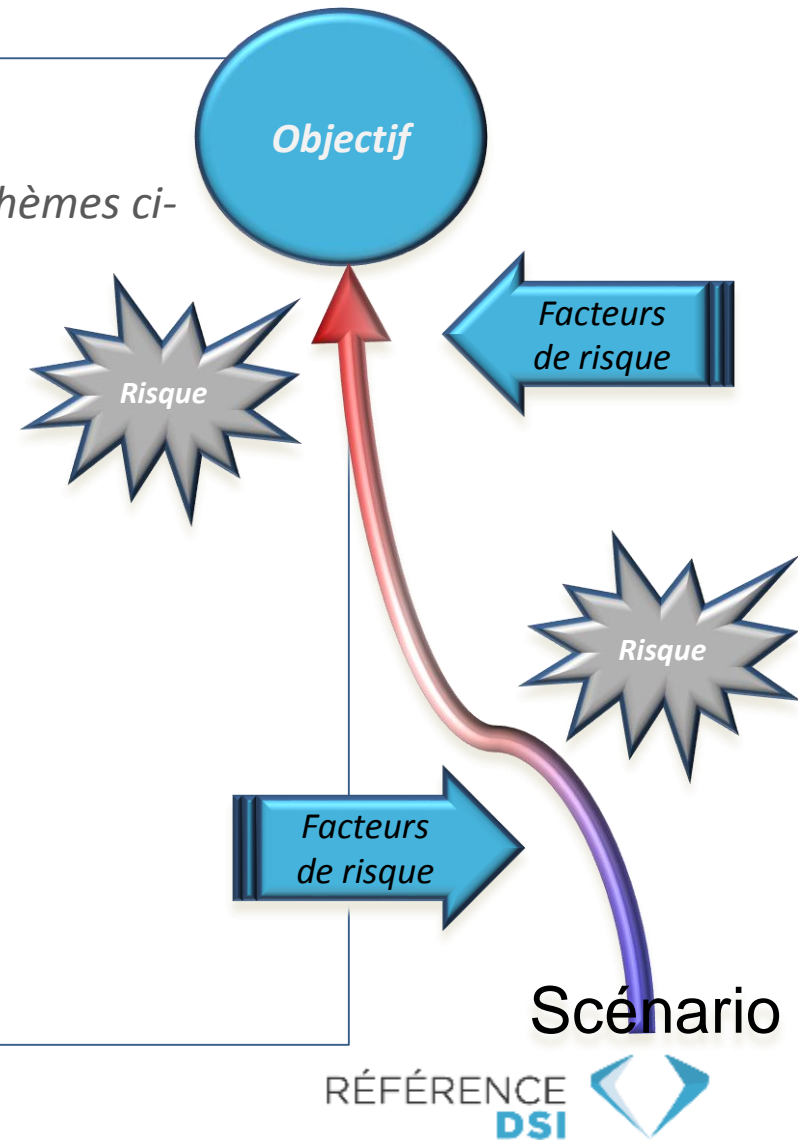


NOTION DE RISQUE

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*



La sécurité du Système d'Information

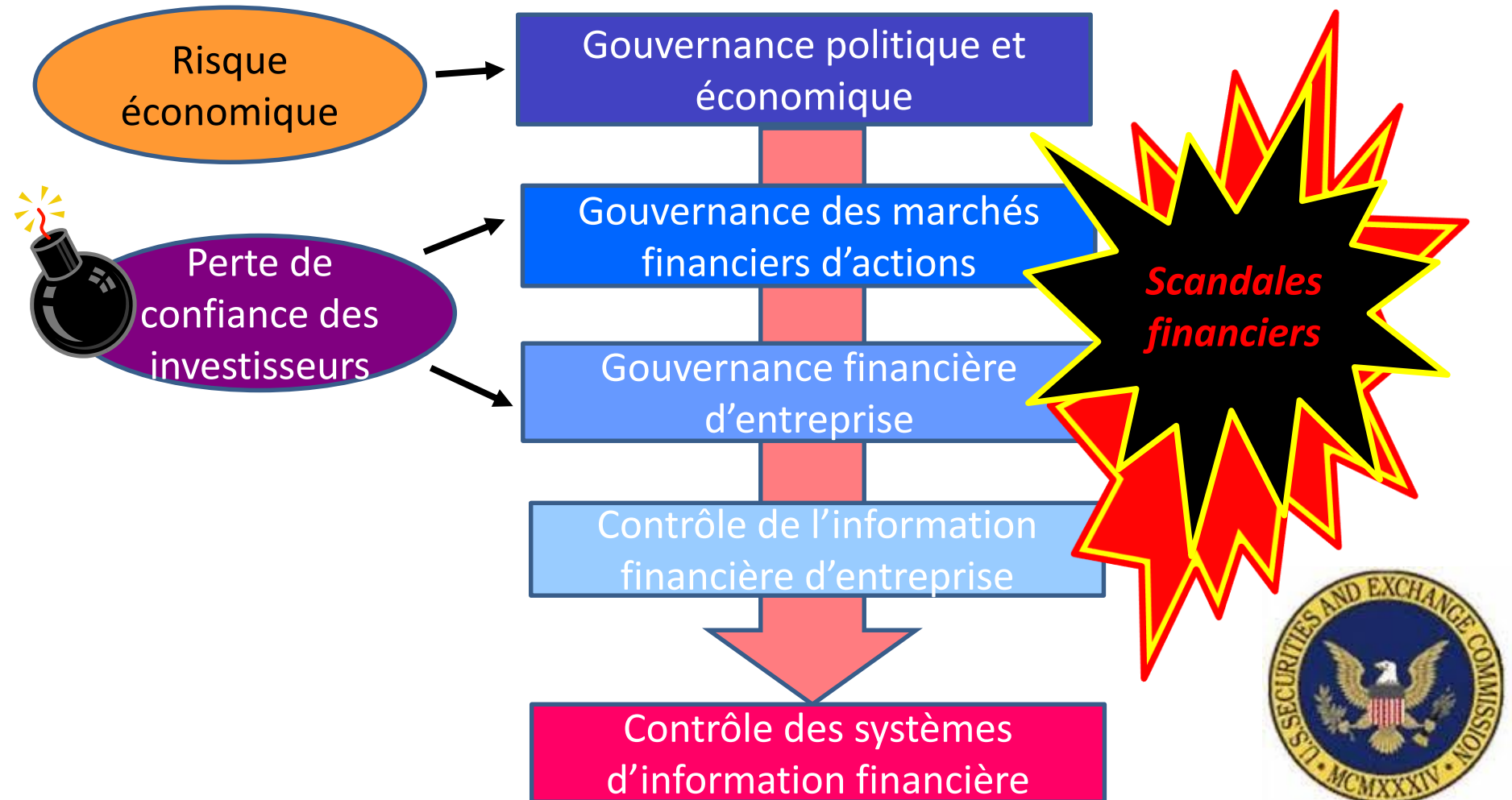
Point focal de la gouvernance du SI

❖ RAPPEL : La DSI gère plusieurs sortes d'actifs :

- ❑ Matériels et Logiciels (actifs corporels et incorporels)
 - *financement avec engagements à moyen terme enregistrés dans les comptes de l'entreprise en tant que coût (dépenses, immobilisations)*
- ❑ 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*
 - *Cette valeur peut être approchée par la valeur portée par les données (volume financier des commandes, factures, etc., mais aussi valeur des plafonds d'indemnisation prévus par les assurances Tous risques informatiques **côté clients ou** Responsabilité Civile Professionnelle **côté fournisseurs**)*

La sécurité du Système d'Information

Rappel SOX : Pourquoi le SI est-il concerné ?



La sécurité du Système d'Information

Contrôle de l'information, contrôle des systèmes

❖ PRINCIPE : Données et traitements sont une implantation automatisée des activités des métiers et services



La gouvernance dissocie les contenus et les contenants

- Le service SI résultant est une coproduction des métiers et de l'IT
- Un propriétaire unique amène des défauts techniques ou/et fonctionnels
- Couplage infrastructures-applications reste fort, surtout en termes de sécurité
- Le besoin d'administration technique des systèmes est du coup un facteur de risque parce qu'il peut conduire à cumuler tous les privilèges (tous les droits)















La sécurité du Système d'Information

Les principaux risques liés à la sécurité du SI

RISQUES

FACTEURS DE RISQUE

-  Systèmes non disponibles ou non accessibles
-  Traitements non-conformes ou non fiables
-  Données incorrectes ou corrompues
-  Malversations, escroqueries
-  Vol de données
-  Vol autres composants

-  Obsolescence ou inadéquation des matériels, logiciels, documentation
-  Politique de sécurité inadaptée
-  Absence de processus de validation (plan de test, tests, corrections)
-  Modifications hors de contrôle des processus validés, notamment les applications testées et validées
-  Non respect des séparations de pouvoirs au sein des applications
-  Intrusions ou/et usurpation d'identités, déni de service

La sécurité du Système d'Information

Trois niveaux de préoccupations

CTRL DES FACTEURS DE RISQUE

*REACTION AU
RISQUE REALISE*

ACCESSIBILITE

Physique

Logique

INTEGRITE

Composants

Données

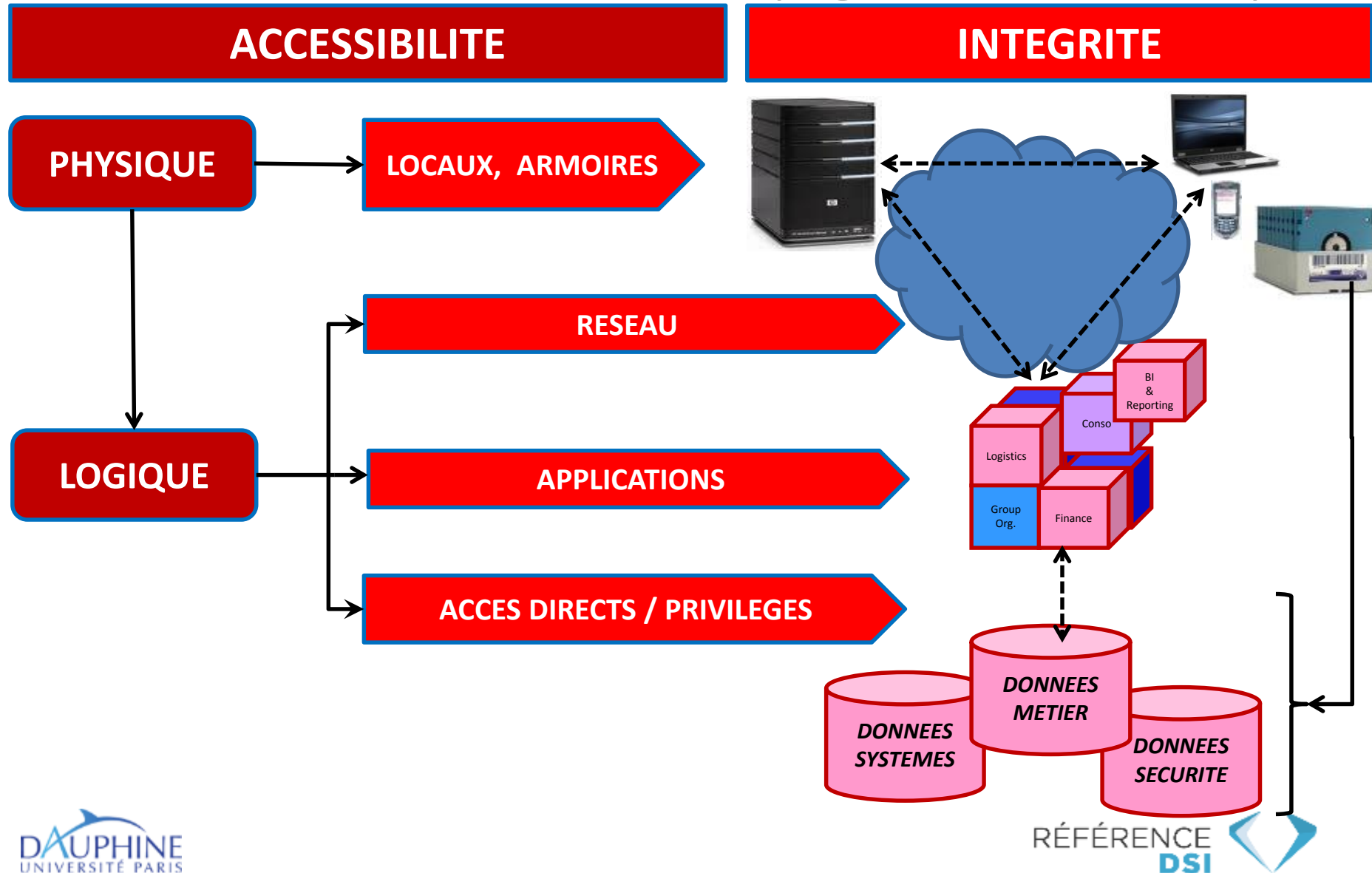
PERENNITE

Backup
& Recovery

Disaster
Recovery Plan
(PRA/PCA)

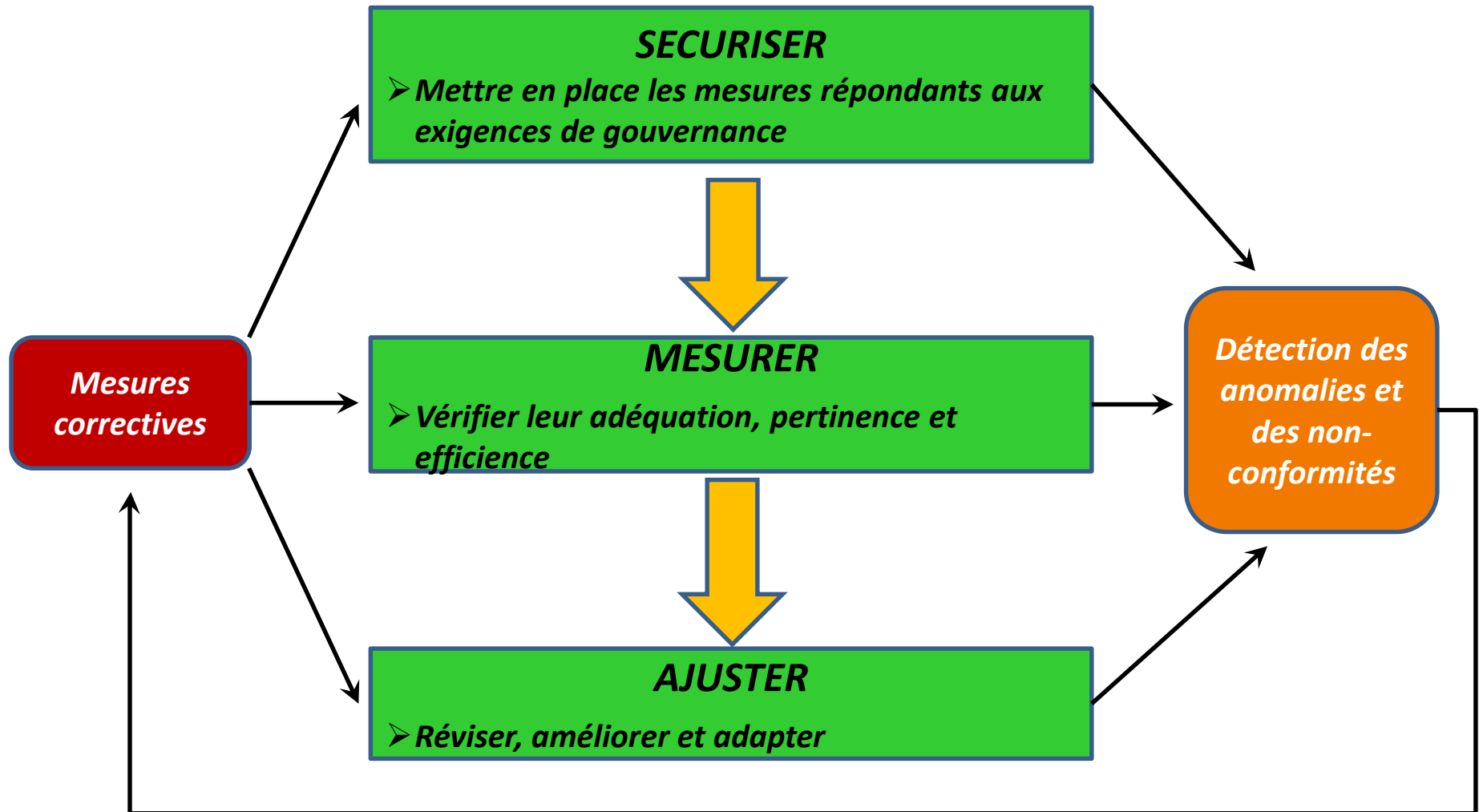
La sécurité du Système d'Information

Illustration du couplage des facteurs de risques



La sécurité du Système d'Information

Manager la sécurité du SI



La sécurité du Système d'Information

Implanter

ACCESSIBILITE

IMPLANTATION

PHYSIQUE

LOCAUX, ARMOIRES

- Badges, clés, contrôle d'accès
- Alimentation courants forts/faibles
- Température, humidité

LOGIQUE

RESEAU

- Identification, droits sur ressources
- Firewalls, antivirus
- Sauvegarde des configurations

APPLICATIONS

- Identification, droits applicatifs
- Sauvegarde des données
- Sauvegarde des traitements

**ACCES DIRECTS /
PRIVILEGES**

- Identification, type de privilège
- Sauvegarde données de sécurité

La sécurité du Système d'Information

Contrôler

ACCESSIBILITE

CONTROLE

PHYSIQUE

LOCAUX, ARMOIRES

- Audit et test des accès et moyens d'accès
- Audit conditions physiques

RESEAU

- Revue et test des identités et des droits
- Ctrl des sauvegardes
- Test de restauration

LOGIQUE

APPLICATIONS

- Revue et test des identités et des droits
- Ctrl des sauvegardes
- Test de restauration

ACCES DIRECTS / PRIVILEGES

- Revue et test des identités et des droits
- Ctrl des sauvegardes
- Test de restauration



La sécurité du Système d'Information

Zoom sur certains contrôles remarquables

ACCESSIBILITE

CONTROLE

PHYSIQUE

LOCAUX, ARMOIRES

- Système de contrôle d'accès et fourniture des fluides (courants forts/faibles, climatisation, ...) souvent géré par Services Généraux

- Environnements multiples avec droits adaptés selon population
- Maîtrise des flux inter-environnement (mise en test, mise en production)
- Programmes et outils adoptants
- Habilitations et monitoring des actions sur les données à l'aide de tels outils
- Monitoring et revue des actions d'administration

LOGIQUE

RESEAU

APPLICATIONS

**ACCES DIRECTS /
PRIVILEGES**



La sécurité du Système d'Information

Suivi opérationnel : monitoring et traçabilité

ACCESSIBILITE

- Unicité des comptes utilisateurs par ressource
- Structure et péremption des mots de passe, limitation du nombre de tentatives d'identification
- Succès/échecs d'authentification à tous niveaux : physiques, réseau, applications
- Affectation des droits et revue périodique par le management des habilitations, droits et privilèges
- Inactivation des comptes par défaut
- Inactivation des comptes non utilisés depuis une période donnée
- Suppression immédiate des comptes au départ des collaborateurs de la société

INTEGRITE

- Existence et diffusion d'une charte d'utilisation des moyens informatiques
- Application régulière et contrôlée des correctifs logiciels
- Sauvegardes régulières et contrôlées
- Traitements automatiques et leurs conditions d'exécution validés par les parties prenantes
- Etapes clés du cycle de développement des systèmes et applications : livrables, tests, ...
- Etapes clés du cycle d'exploitation : incidents, demandes, maintenance, changements, ...

La sécurité du Système d'Information

Suivi opérationnel, audit et plan de progrès

- Le monitoring et la traçabilité des décisions et actions sont les conditions de base du plan de progrès en matière de sécurité du SI
- Les incidents et anomalies suivent le cycle standard de traitement des incidents d'exploitation (revue, diagnostic et correction des incidents, ou gestion en tant que problème si récurrent ou potentiellement récurrent)
- Ce suivi est complété par un audit périodique (annuel ou bi-annuel) de forme et de fond :
 - Forme : existence des procédures applicables aux différents thèmes de sécurité du SI : gestion des comptes et des droits, privilèges, cycle de vie, mise en production, etc.
 - Fond : application effective desdites procédures, preuves de leur application

La sécurité du Système d'Information

Suivi opérationnel, audit et plan de progrès

- L'audit relève les exceptions constituant les non-conformités
- Il se base généralement sur un questionnaire d'enquête (audit de forme) accompagné de tests très ciblés (audit de fond).
 - Par exemple, confronter les comptes actifs avec la liste du personnel et ses entrées/sorties, vérifier les conditions de création et suppression des comptes
- Le plan de progrès concerne :
 - Les défauts de forme : procédures absentes, inadaptées ou non applicables
 - Les défauts d'application des procédures : les exceptions dues à un défaut de contrôle, à une difficulté technique (outil inadapté, données incorrectes), à un défaut dans la chaîne de décision (hors délai, contributeur défaillant), etc.
- Le plan de progrès prévoit des échéances de correction échelonnées:
 - Immédiate pour les actions correctives du passé (exemple : suppression des comptes non utilisés ou des personnes parties)
 - Différée pour les actions nécessitant une élaboration (outil, procédure, ...)

La sécurité du Système d'Information

Ne perdez pas de vue que ...

- Les opérations visant à nuire aux entreprises par le « piratage » des Systèmes d'Information reposent sur des actions techniques informatiques qui exploitent des failles de l'organisation cible.
 - Les failles techniques des logiciels sont généralement traitées par les correctifs publiés par les éditeurs, mais en temps différé.
- Les attaques utilisent le réseau pour atteindre les points névralgiques
 - La connaissance de la topologie et l'organisation du réseau est nécessaire; il faut donc l'explorer ou obtenir par d'autres biais les informations qui permettent d'en identifier les points névralgiques
- 💣 ***Une attaque «qui marche», c'est 80% de social et 20% de technique***
- 💣 ***La majorité des sinistres ont une origine interne à l'entreprise***
 - Organisation rigoureuse de la sécurité (chacun ne voit que ce dont il a besoin , privilèges limités à un nombre restreint de personnes et révisés régulièrement, portes dérobées neutralisées, correctifs appliqués)
 - Education des utilisateurs à la confidentialité des aspects IT