DAUPHINE
UNIVERSITÉ PARIS

Capitalisation

ITIL / CoBIt: Mise en oeuvre

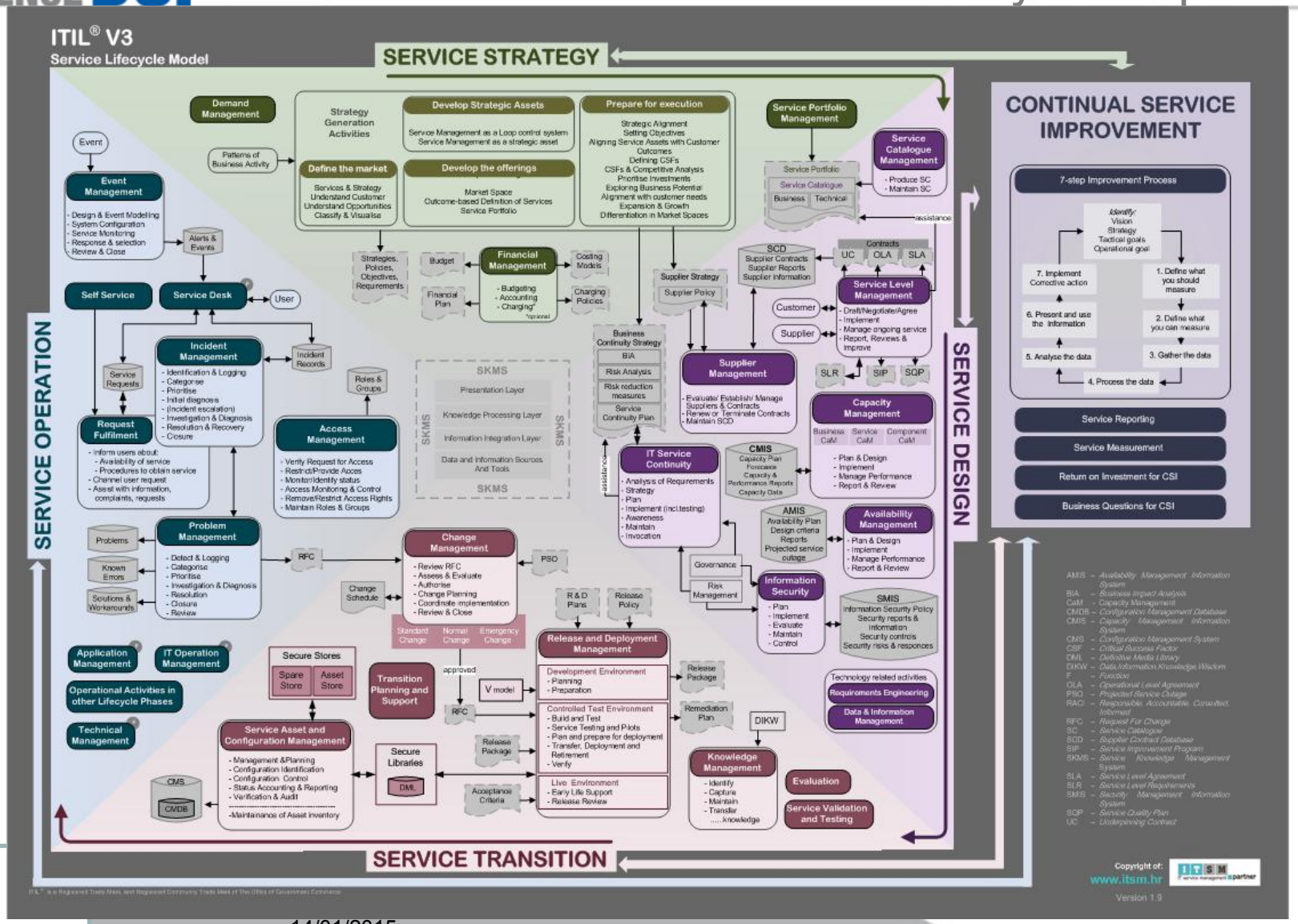
RÉFÉRENCE DSI

Le contenu d'ITIL

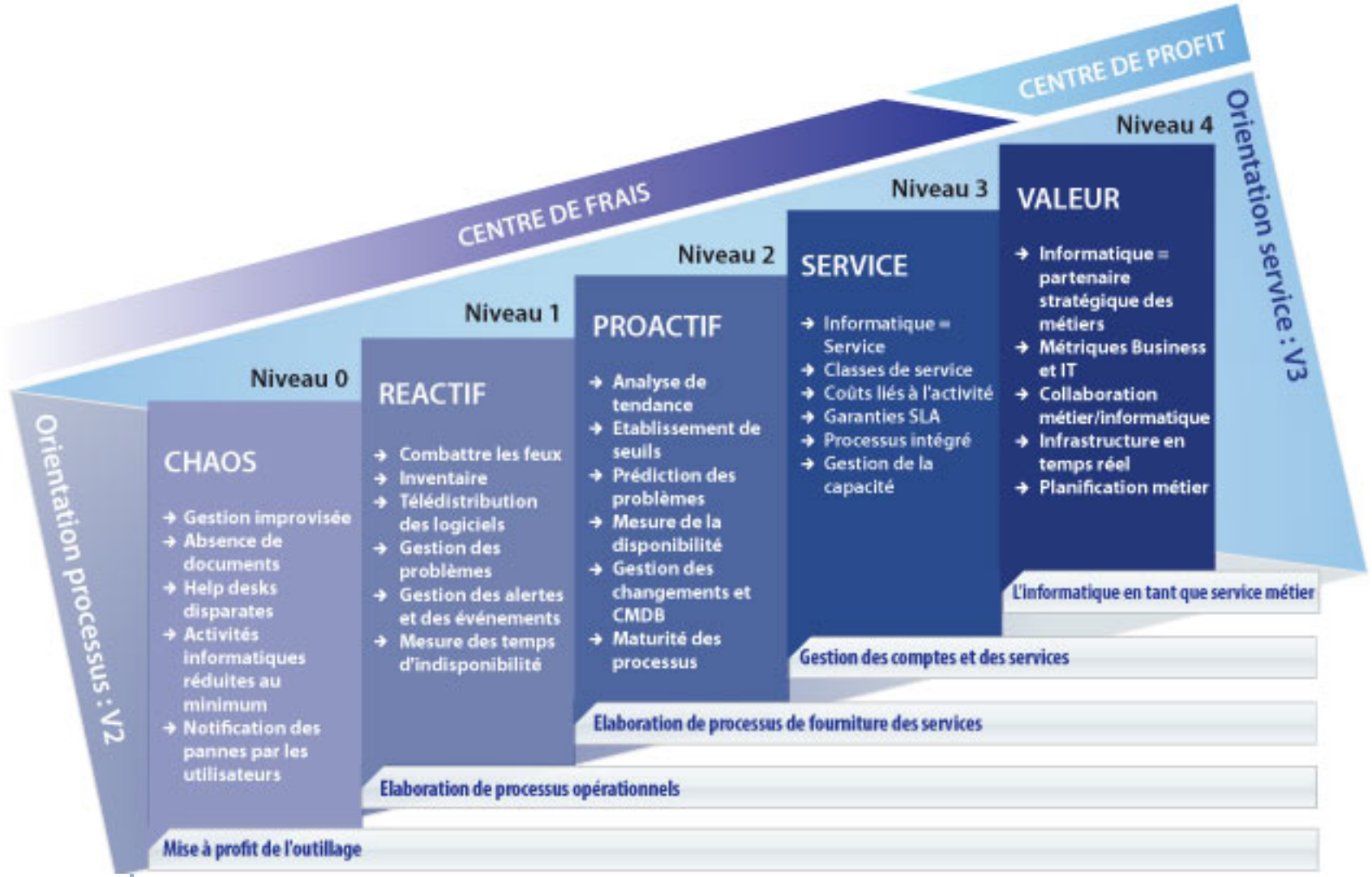
- ITIL est actuellement organisée autour du cycle de vie d'un service:
  - Service Strategy:
    - Mettre en place les règles du jeu.
    - Gérer la relation avec le Client.
    - Gérer un catalogue et un portefeuille de services.
    - Gérer le Budget.
  - Service Design:
    - Concevoir le service et les niveaux de service attendus.
    - Gérer les moyens et conditions nécessaires à la mise à disposition du service.
  - Service transition:
    - Gérer l'éco système dans lequel s'inscrit le service.
    - Gérer la mise en production/ l'évolution.
  - Service operation:
    - Gérer les événements/ les incidents/ les problèmes/ les accès.
  - Continual Service improvement:
    - Mettre en place un processus d'amélioration continue.

RÉFÉRENCE DSI

Une vue synthétique d'ITIL

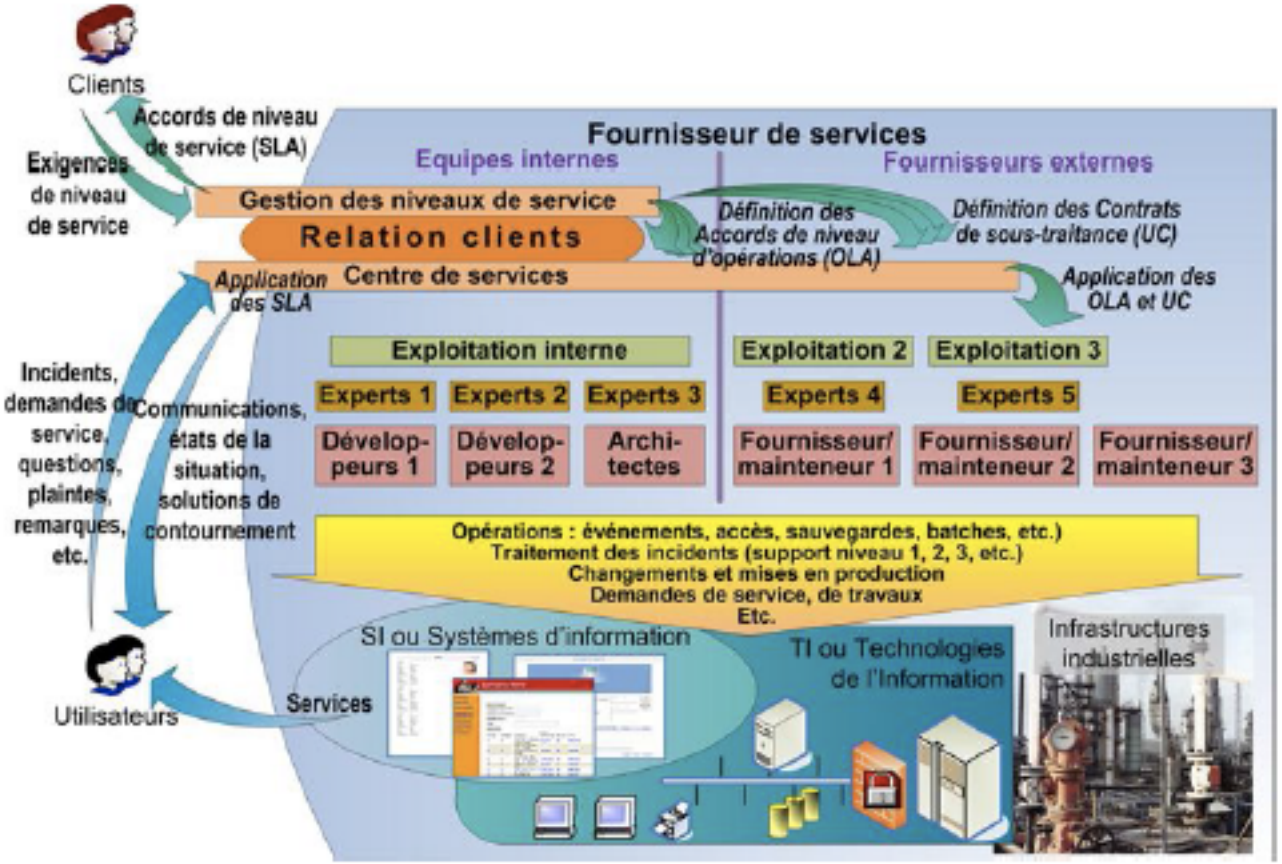


Modèle de maturité

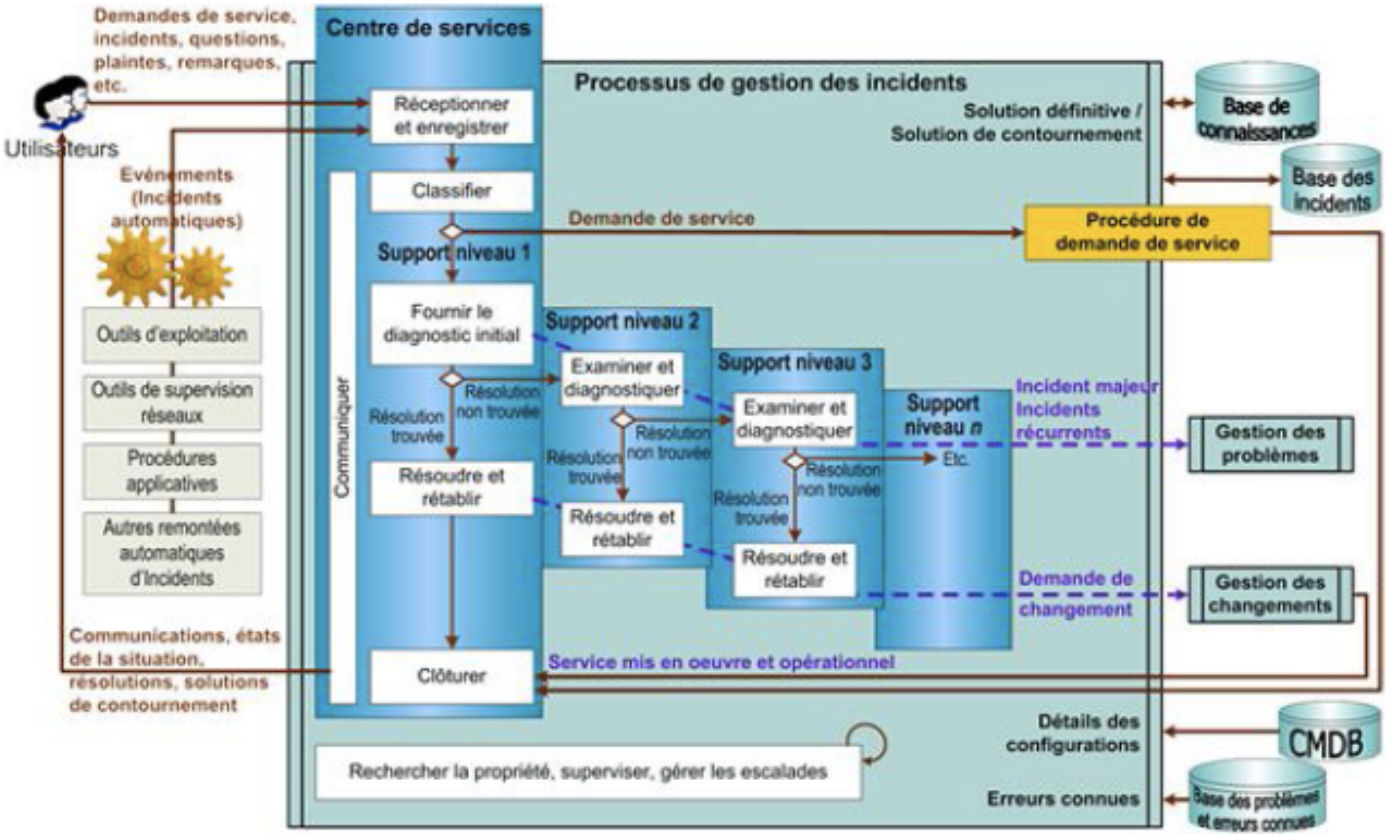


- Un exemple: La mise en place du centre de service.
  - LA GESTION DES INCIDENTS
  - LA GESTION DES PROBLEMES

L'exemple du centre de services

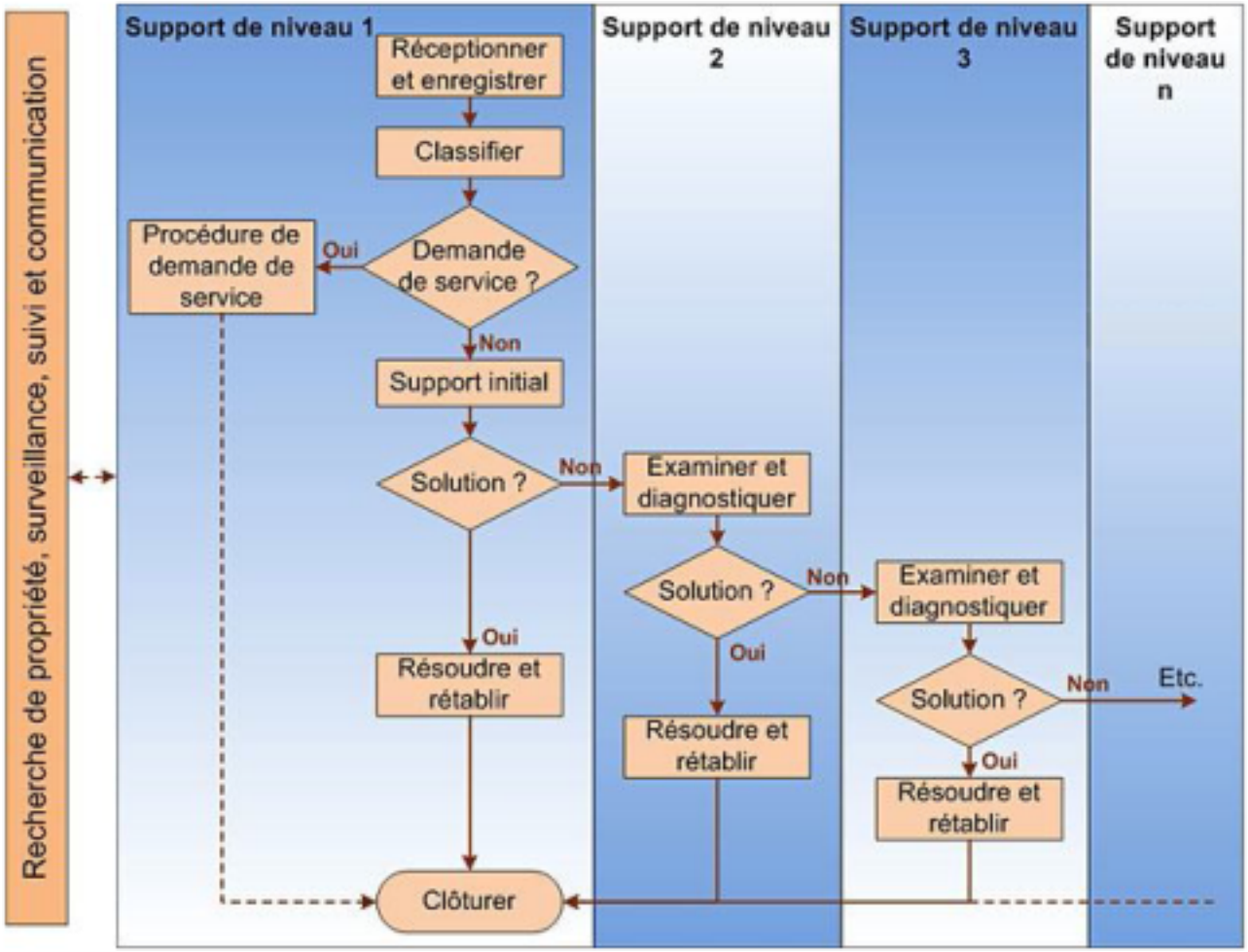


L'exemple du Centre de Services

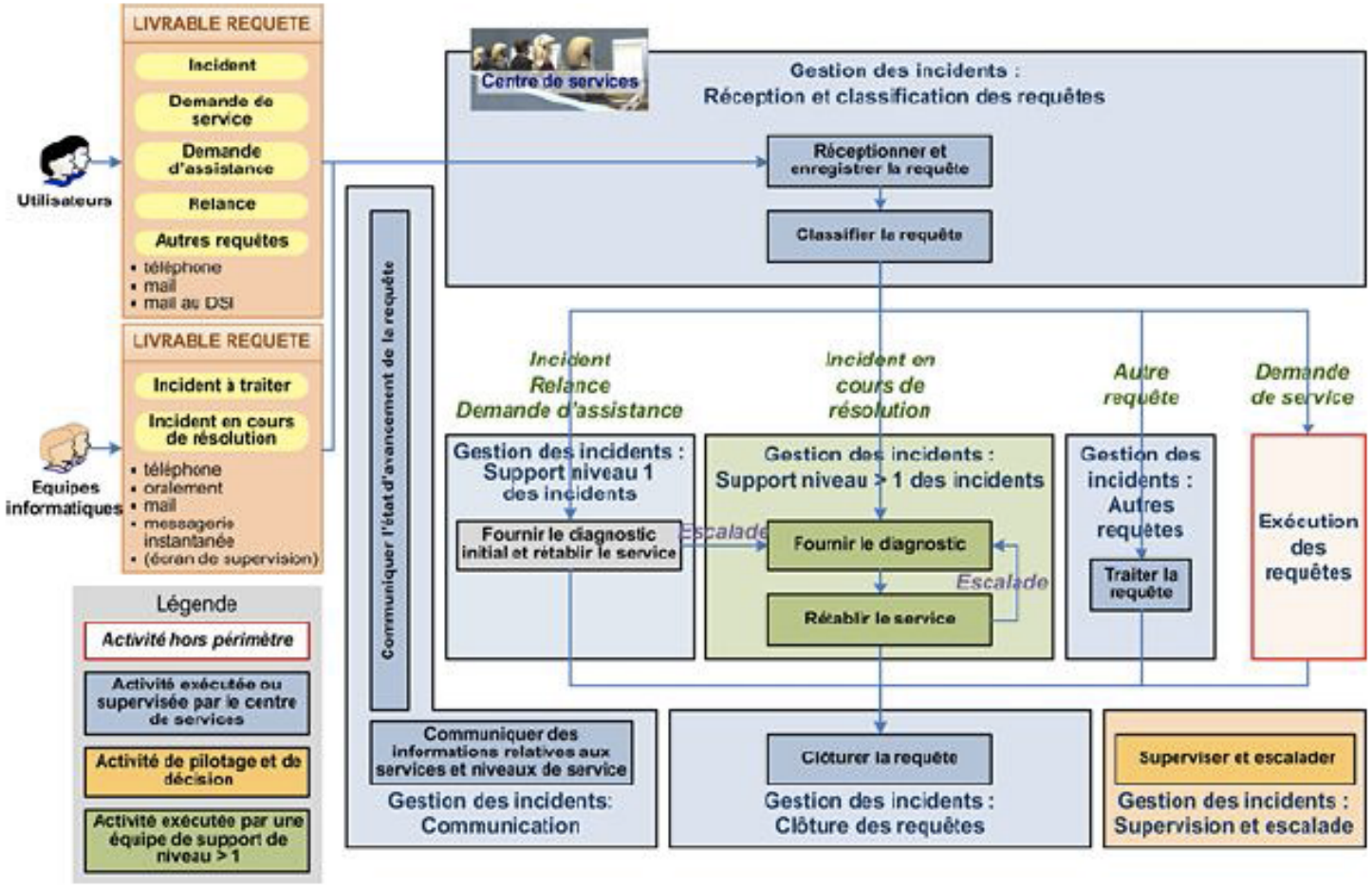


RÉFÉRENCE DSI

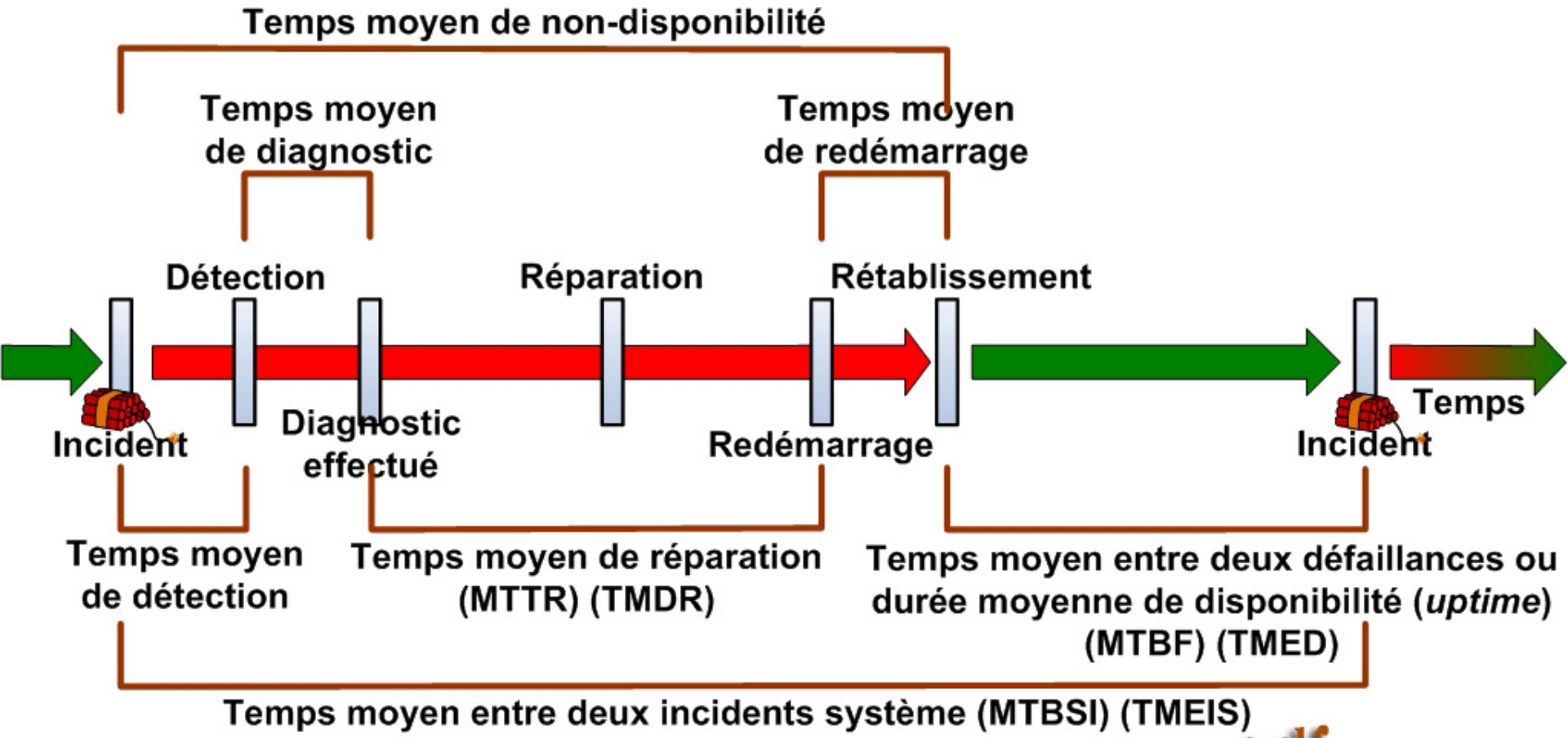
Gestion des incidents: Notion de Niveau de support



La Gestion des Incidents

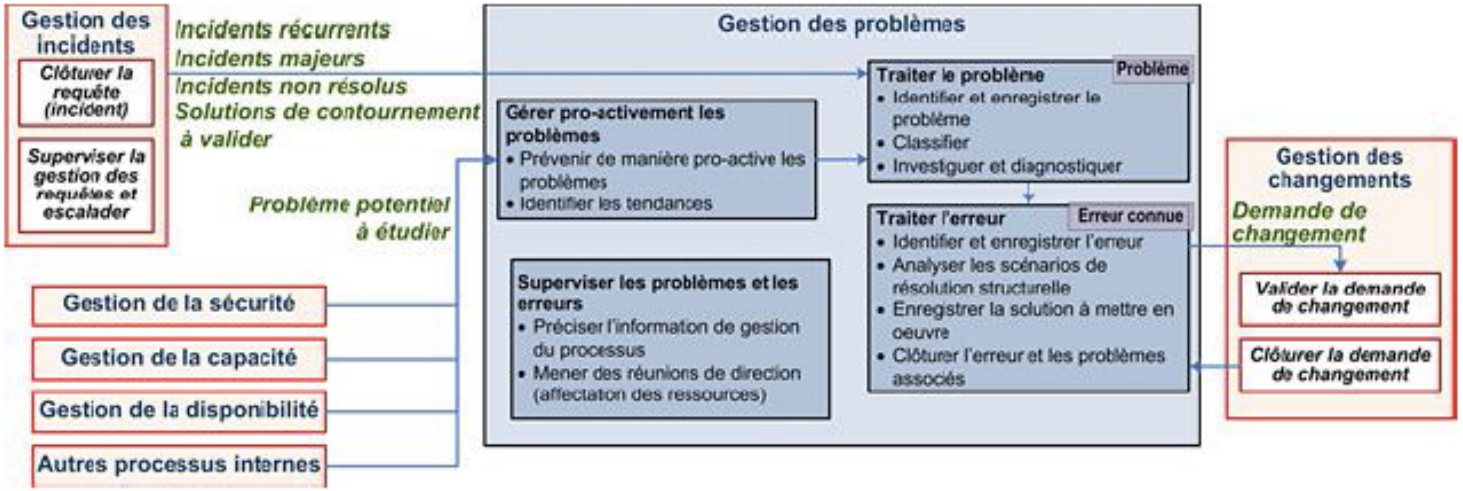


Mesurer l'efficacité de la gestion des incidents…

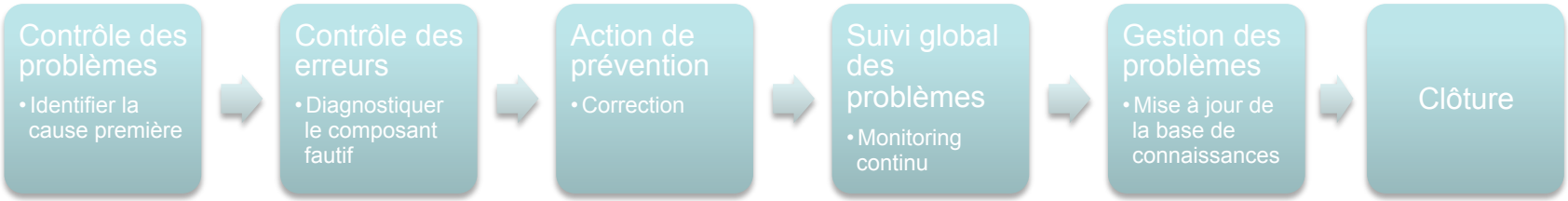


- Un exemple: La mise en place du centre de service.
  - LA GESTION DES INCIDENTS
  - LA GESTION DES PROBLEMES

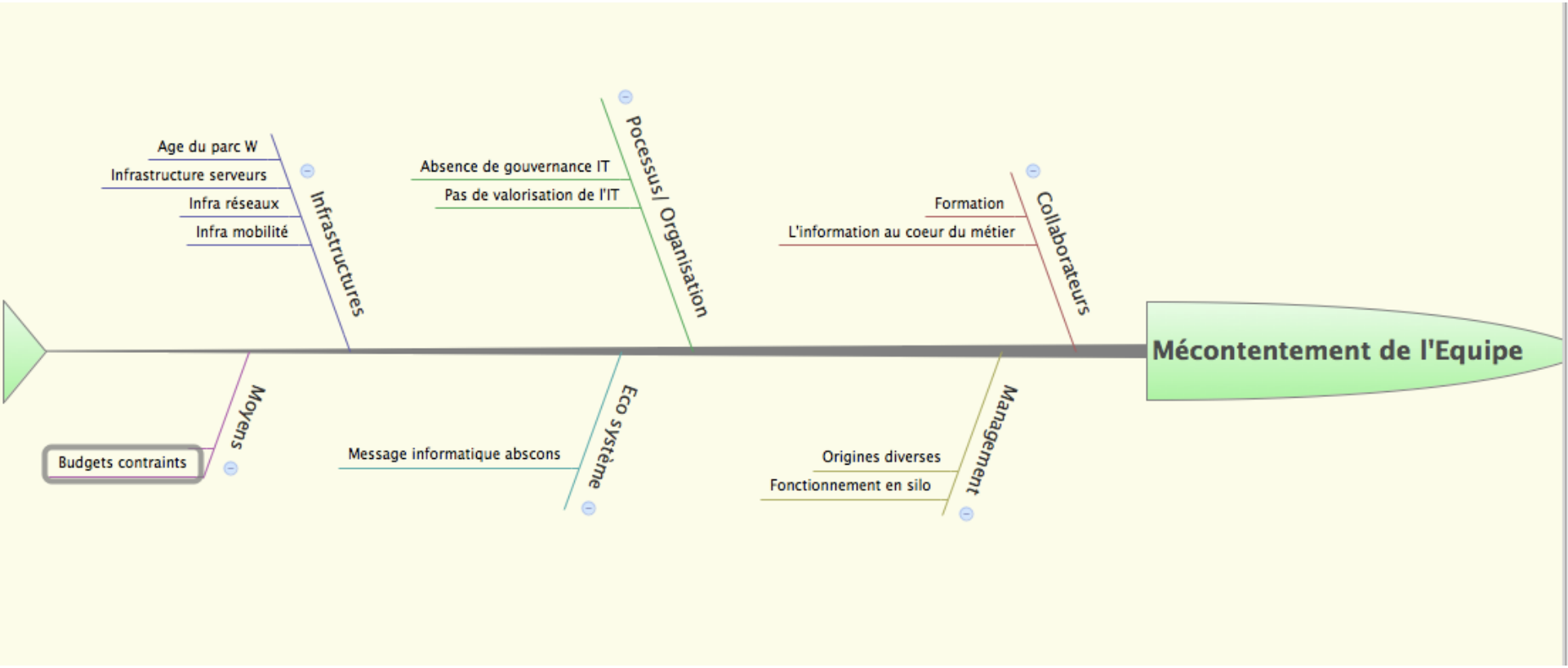
La Gestion des Problèmes



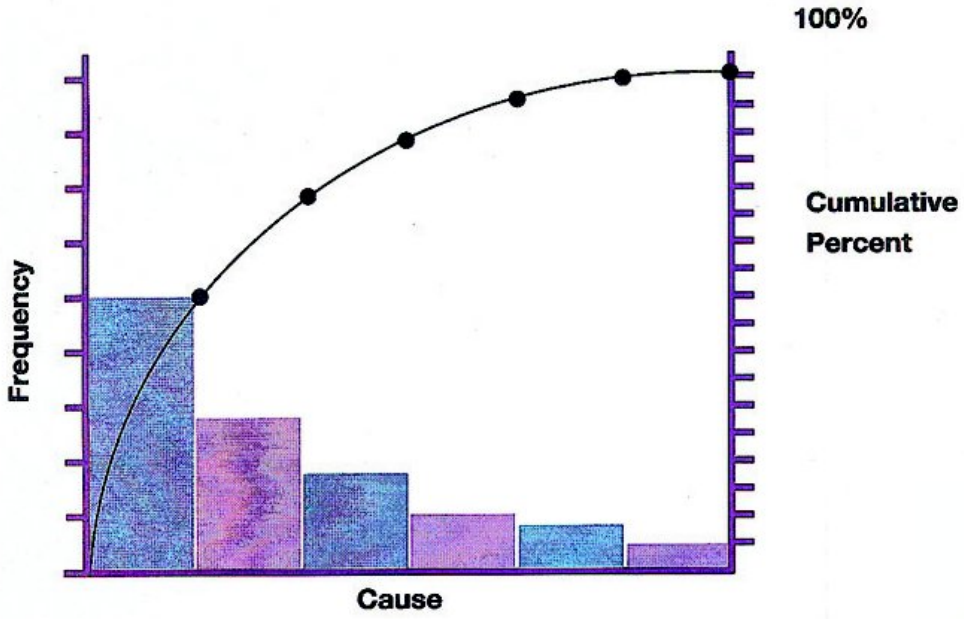
Cycle de vie d'un problème

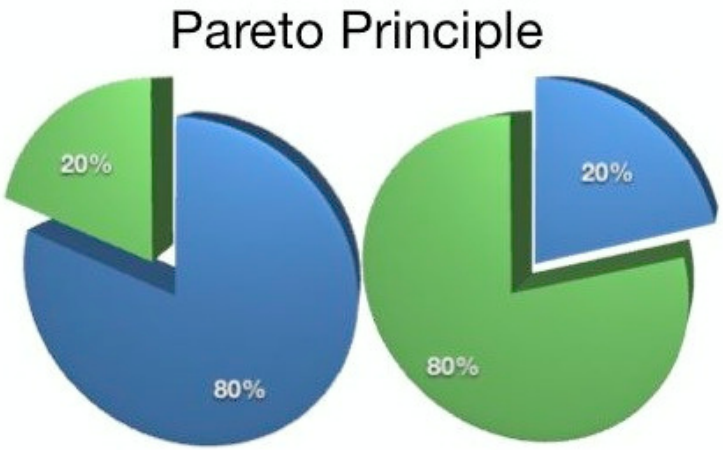


Résolution de problèmes: Diag Ishikawa Causes/ Effets



Résolution de problèmes: Pareto





20% of the input (time, resources, effort)
accounts for 80% of the output (results, rewards)

Résolution de problèmes

- Résoudre un problème, c'est répondre de manière systématique aux questions suivantes:
  - Que fait on, et pourquoi?
  - Qui le fait, et pourquoi cette personne?
  - Ou le fait on, et pourquoi là?`
  - Quand le fait on et pourquoi à ce moment là?
  - Comment le fait on et pourquoi ainsi?
  - Pourquoi avons nous ce problème?
- Résoudre un problème, c'est:
  - travailler en commun.
  - Objectiver et documenter
  - Analyser les données
  - Décider ensemble.
  - Mettre en œuvre un plan d'actions.

- Un exemple: La mise en place d'un catalogue de services
  - DEFINIR UN SERVICE
  - DEFINIR UN NIVEAU DE SERVICE
  - PILOTER

Définir un service.

- C'est mettre en œuvre quatre types de ressources:
  - Une infrastructure
  - Des applications
  - Des informations
  - Des Ressources Humaines

Composantes d'un service

- Composantes d'un service:
  - Processus Métier
  - Description du service
  - Engagement de niveau de service
    - SLR/ SLA
  - Infrastructure
    - Liste des équipements nécessaires
  - Environnement
    - Conditions nécessaires au bon fonctionnement
  - Données
    - Données en entrée et en sortie
  - Applicatifs
    - Liste des applicatifs mis en jeu.
  - Support de service
    - Liste des services liés
  - Operational Service Agreement
    - Liste de tous les services opérationnels sous jacents
  - Support:
    - Liste des équipes de support interne nécessaires.
  - Fournisseur:
    - Liste de tous les fournisseurs nécessaires.

Une Fiche Service

Utilité du service

Décrire les principales fonctions de l'application.

Organisation métier :	Toutes
Propriétaire métier :	Mr Dupont, Directeur
Contacts métiers :	Mme Durand, Mr Dubois

Garantie du service

Décrire les différents niveaux de services standards proposés avec ce service (pas de recommandations sur leur nombre sauf à ne pas dépasser un nombre raisonnable au-delà duquel cela devient difficile à comprendre).

Ce service est proposé avec deux niveaux de garantie :

Garantie "BASE"

INCIDENTS
Impact : de 1 à 3
Urgence : de 2 à 4
Priorité = formule(Impact, Urgence)
Délai de résolution : au mieux

DISPONIBILITE
Une interruption ou dégradation de service ne dépassera pas 4 heures.
Le total des indisponibilités dans le mois ne dépassera pas 16 heures.

Ne préciser dans chaque niveau de service que les thèmes pour lesquels la direction informatique peut s'engager.

Garantie "OR"

INCIDENTS
Impact : de 1 à 3
Urgence : de 2 à 4
Priorité = maximum(Impact, Urgence)
Délai de résolution : 2 heures maximum

DISPONIBILITE
Une interruption ou dégradation de service ne dépassera pas 2 heures.
Le total des indisponbilités dans le mois ne dépassera pas 4 heures.

SECURITE
Garanties de sécurité

CAPACITE
Garanties de capacité

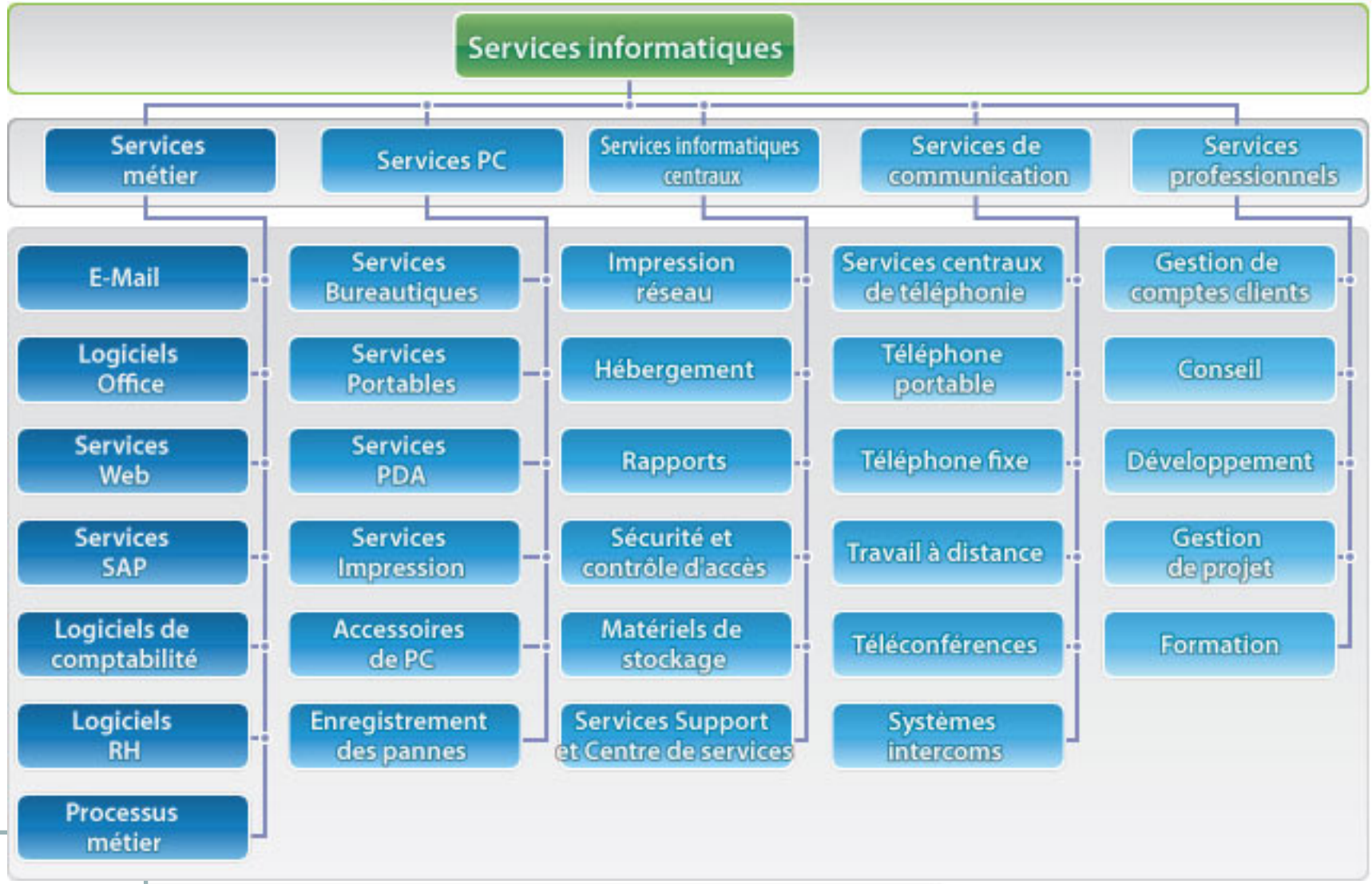
CONTINUITE
Garanties de continuité

Demandes de service

Les demandes de service suivantes peuvent être effectuées auprès du centre de services informatiques :

- **Demande d'un nouveau poste bureautique** : Demande de poste bureautique à

Etablir un catalogue de services

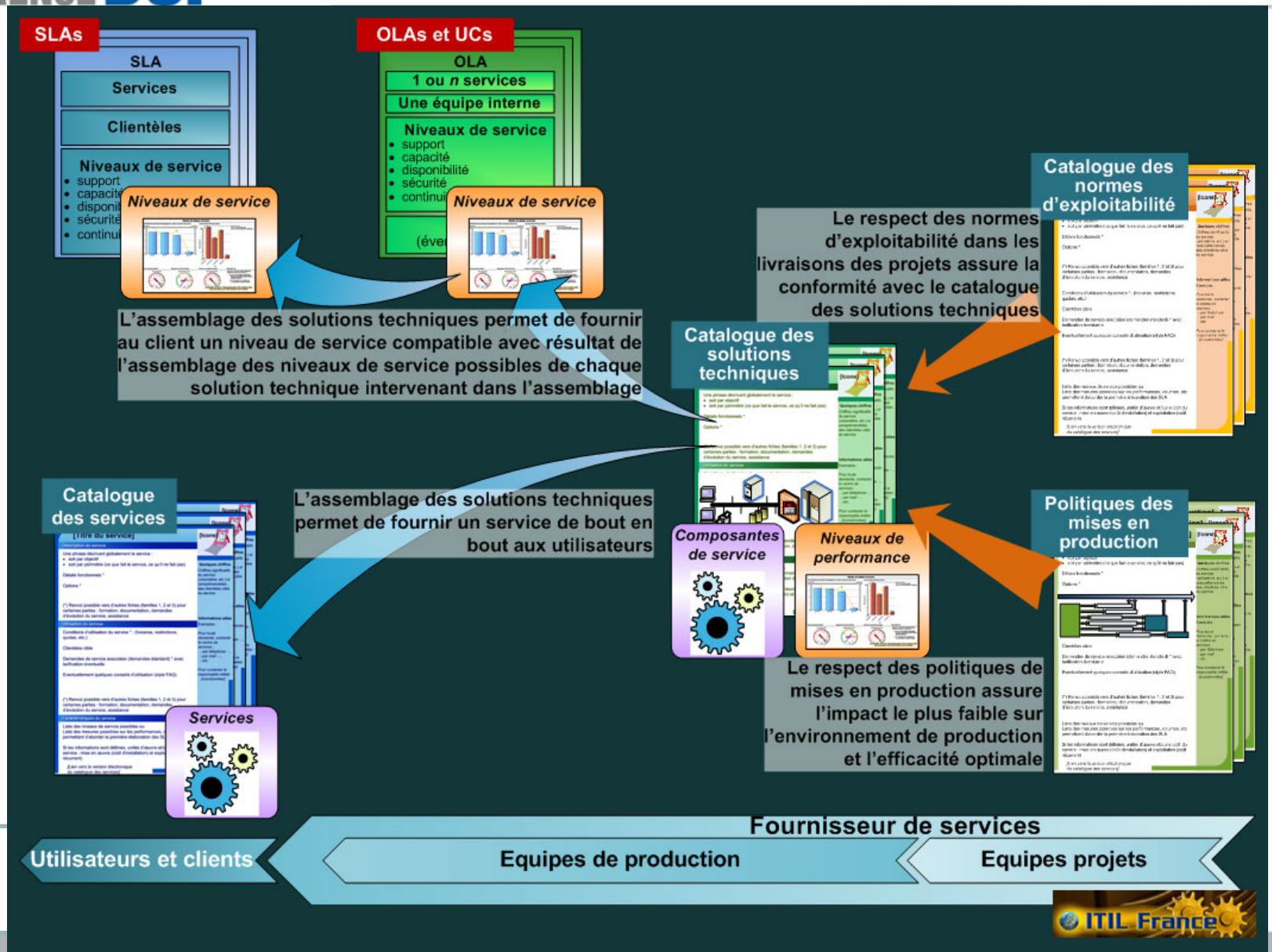


Catalogue de services

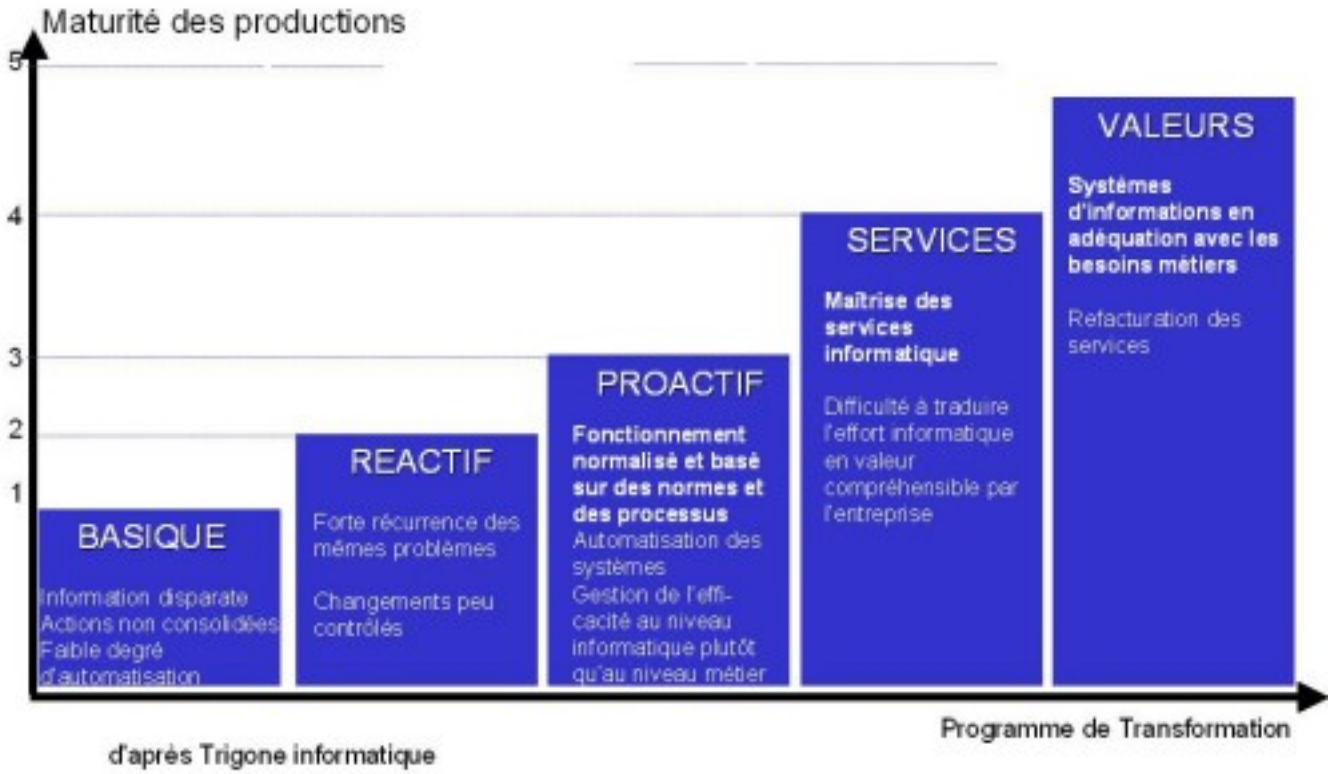
- Les services sont répertoriés suivant les attributs suivants:
  - Nom.
  - Description.
  - Type de service:
    - Métier, Infras, Réseaux, Applicatif.
  - Services dépendants
  - Propriétaire.
  - Utilisateur.
  - Impact métier.
  - Priorité.
  - SLA.
  - Planification.
  - Contacts.
  - Rapports
  - Sécurité

- Un exemple: La mise en place d'un catalogue de services
  - DEFINIR UN SERVICE
  - DEFINIR UN NIVEAU DE SERVICE
  - PILOTER

Gérer un niveau de service



Courbe de maturité des productions



d'après Trigone informatique

Relations entre SLR, SLA et OLA.

Contenu d'un SLA

- Description de l'Accord
  - Périmètre, formalisation de l'accord.
- Description des services inclus
  - Prenant compte des services dépendants.
- Planification
  - Horaires, fréquences, cycles…
- Disponibilité
  - En pourcentage des heures d'opération du client.
- Fiabilité
  - MTBF, MTBSI
- Support
  - Heures d'ouverture du support, temps de réponse maximal admissible.
- Débits temps de réponse
  - Rapidité, nombre d'accès simultanés
- Continuité du service
  - Référence au PCA

Le contenu d'ITIL

- Un exemple: La mise en place d'un catalogue de services
  - DEFINIR UN SERVICE
  - DEFINIR UN NIVEAU DE SERVICE
  - PILOTER

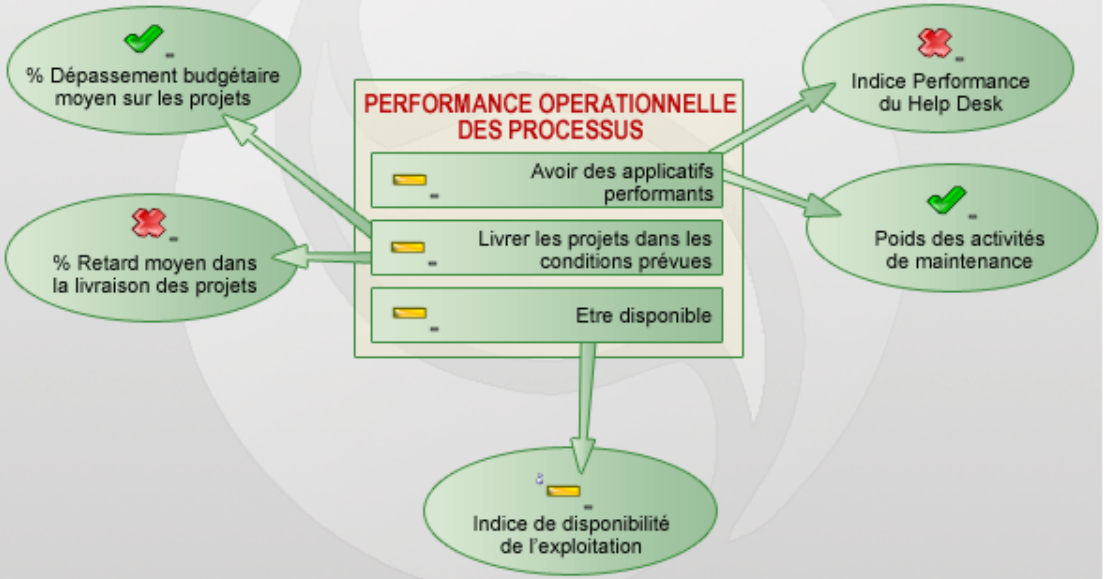
Tableaux de bord | Types d'i
Sommaire des indicateurs
Responsabilités
Liste de surveillance
Indicateurs Elémentaire
IT ScoreCard
Branches d'activités
Domaines d'Etudes
Commercial/Decisi
Industrie
R&D
SUPPORT

IT ScoreCard

Indicateurs | Image | Détails

Tendance	Valeur cible	Valeur réelle	Écart	Nom

Carte Stratégique IT



COGNOS Metrics Manager

Connexion : Administrator | Déconnexion | Préférences | 2003 Août (PAJ) | Administration

Tableaux de bord | Types d'i

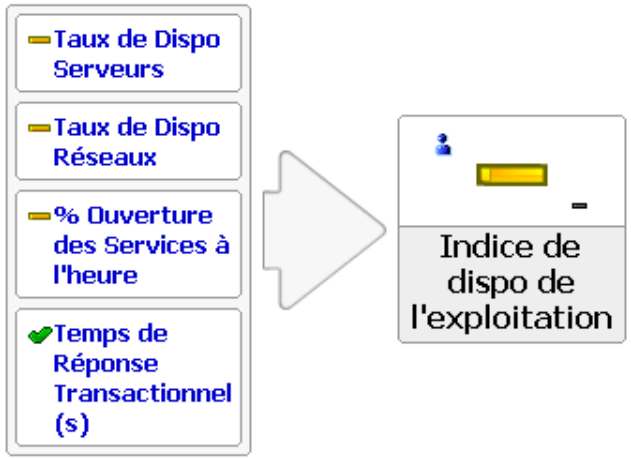
- Sommaire des indicateurs
  - Responsabilités
  - Liste de surveillance
  - Indicateurs Elémentaire
- IT ScoreCard
  - Branches d'activités
    -
    -
    -
    -
  - Domaines d'Etudes
    - Commercial/Decisi
    - Industrie
    - R&D
    - SUPPORT

Sommaire des indicateurs > IT ScoreCard > Indice de dispo de l'exploitation

Indice de dispo de l'exploitation

Historique | Rapports | Image | Détails

État	Tendance		Valeur réelle	Valeur cible	Écart	Propriétaire	Dernière modification
–	–		4/5	5/5	-1/5	Administrator	1 oct. 03



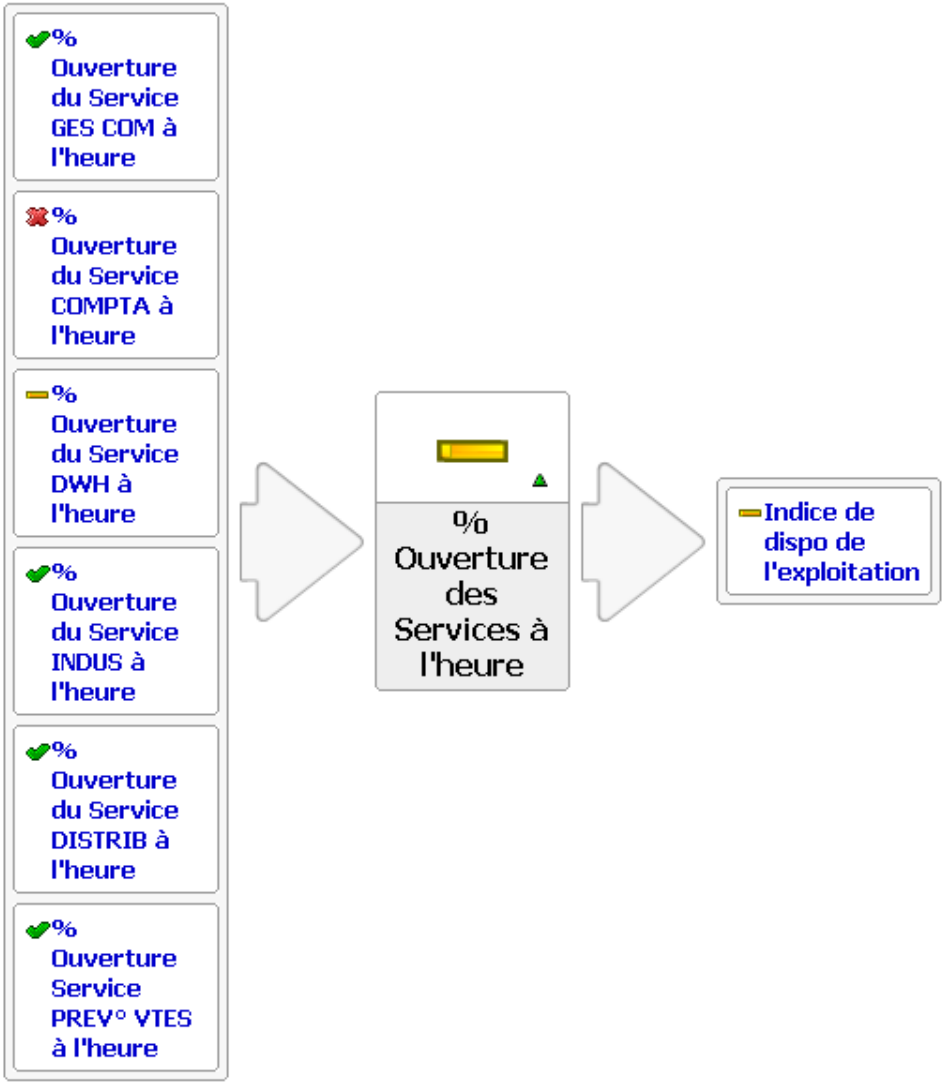
Tableaux de bord | Types d'i

- Sommaire des indicateurs
  - Responsabilités
  - Liste de surveillance
  - Indicateurs Elémentaire
- IT ScoreCard
  - Branches d'activités
    -
    -
    -
    -
  - Domaines d'Etudes
    - Commercial/Decisi
    - Industrie
    - R&D
    - SUPPORT

% Ouverture des Services à l'heure

Historique | Rapports | Image | Détails

État	Tendance		Valeur réelle	Valeur cible	Écart	Propriétaire	Dernière modification
—	▲		99,13%	100,00%	-0,87%	Administrator	1 oct. 03



Tableaux de bord | Types d'i

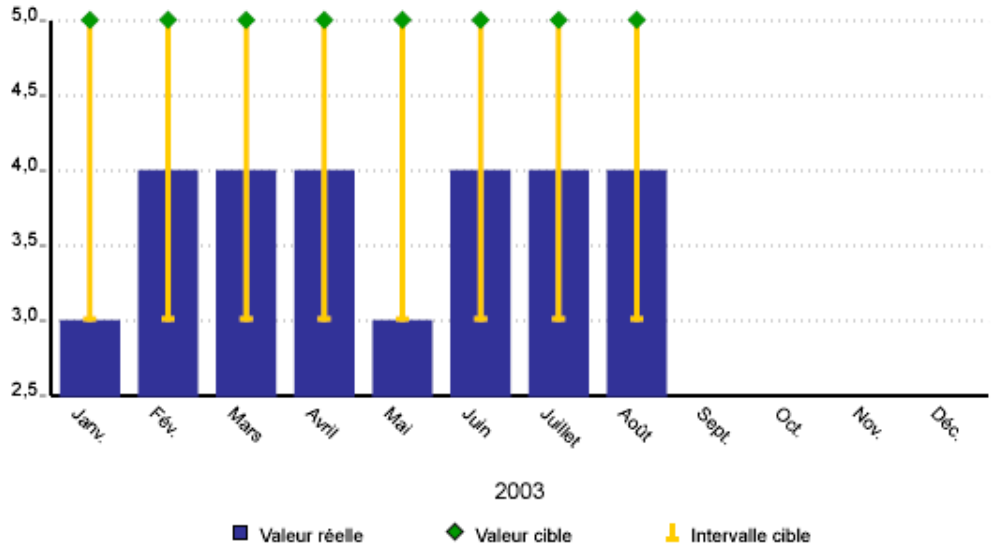
- Sommaire des indicateurs
  - Responsabilités
  - Liste de surveillance
  - Indicateurs Elémentaire
- IT ScoreCard
  - Branches d'activités
  - Domaines d'Etudes
    - Commercial/Decisi
    - Industrie
    - R&D
    - SUPPORT

Indice de dispo de l'exploitation

Historique | Rapports | Image | Détails

État	Tendance		Valeur réelle	Valeur cible	Écart	Propriétaire	Dernière modification
—	–		4/5	5/5	-1/5	Administrator	1 oct. 03

Indice de dispo de l'exploitation



Comparaison : Aucune — Suivant

Commentaires et état des opérations :2003 Août

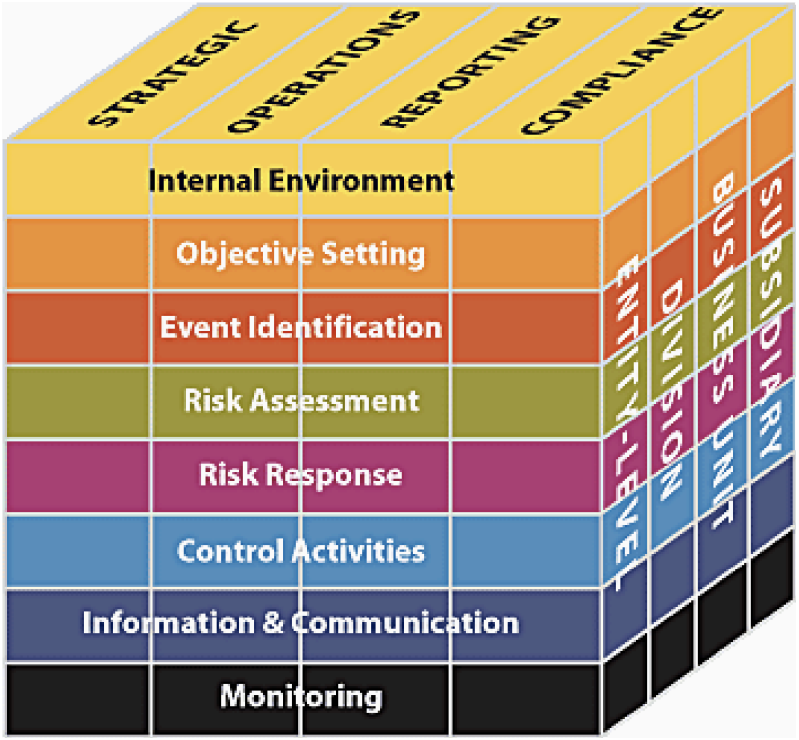
Suivi : Administrator — Modification

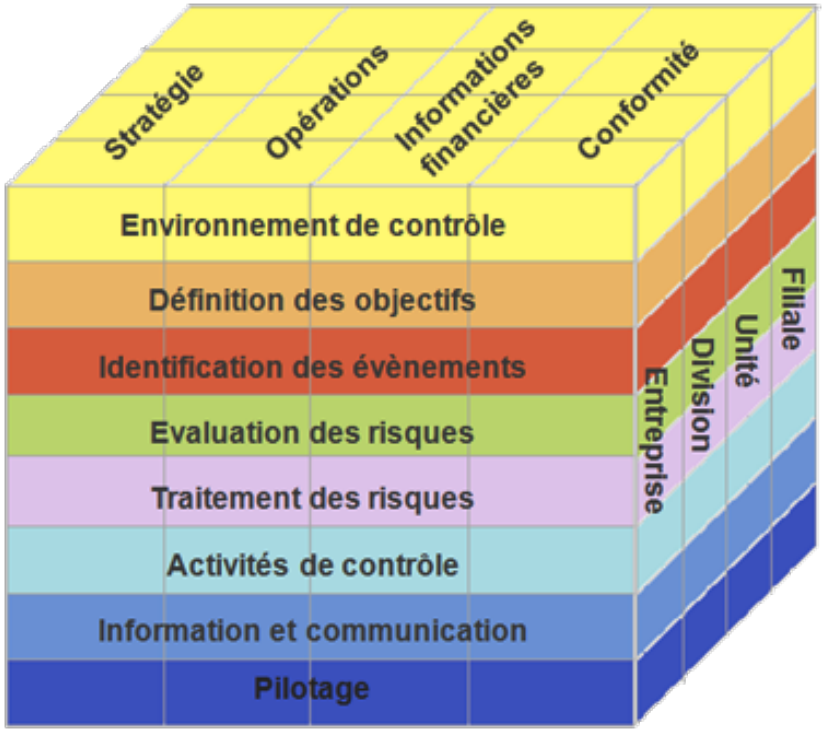
COSO/ CoBiT

COSO based audits

1	Eléments concernant COSO
2	Overview COBIT
3	Mapping COSO/COBIT
4	Exemple de matrice d'analyse: EDM 01

COSO Framework





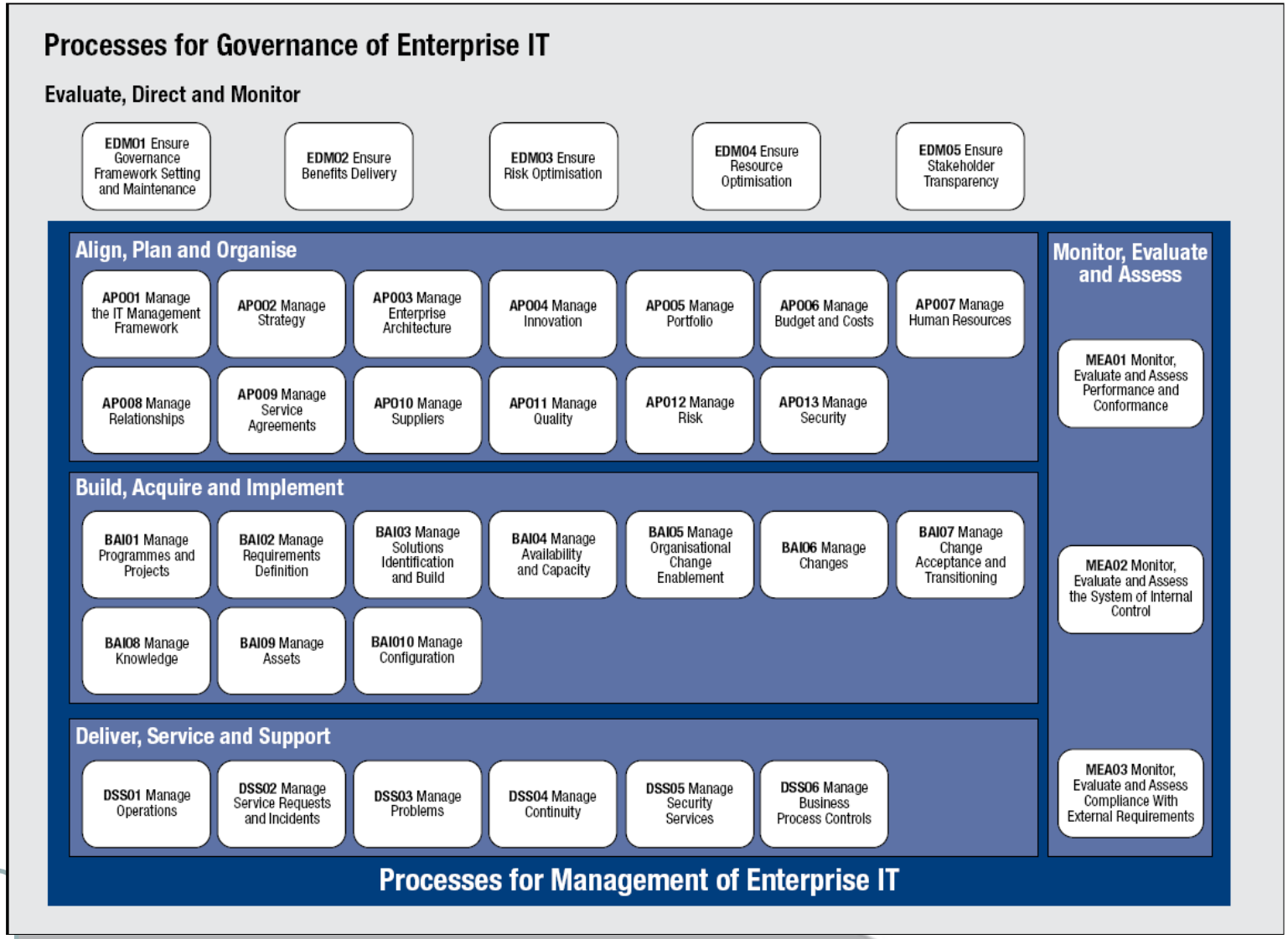
COSO based audits

RATING CRITERIA FOR COSO-BASED AUDITS

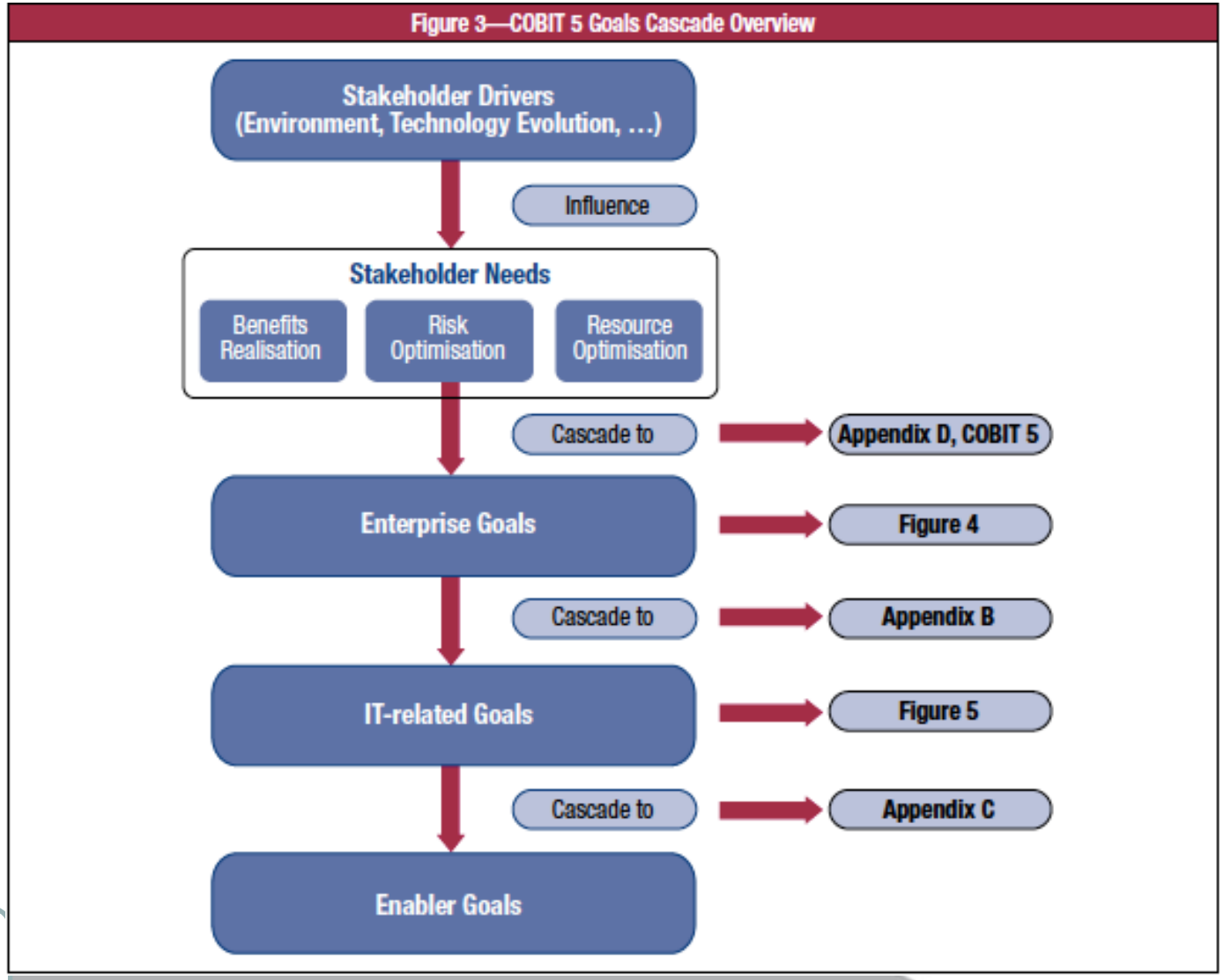
Control Component	CRITERIA FOR UNSATISFACTORY RATING
Control Environment	"Hard controls" are missing or inadequate. There are verified instances of breakdowns of "soft controls."
Risk Assessment	Management has not predefined relevant objectives. Such objectives are incompatible with broader objectives. Management has not identified relevant risks to achieving its objectives. Management does not have a basis for determining which risks are most critical. Management has not ensured mitigation of critical operating risks. Audit tests detect key risks not previously contemplated by management.
Control Activities	Key control activities are not functioning as intended. Management's risk mitigation strategy is not adequately reflected within control activities.
Information & Communication	Key metrics are not identified, collected, and communicated. Employees do not understand their control responsibilities, and this is pervasive. Customer or supplier complaints and disputes are not resolved, or remedial action is not undertaken in a timely manner.
Monitoring	Management has not established a means of determining the quality of the internal control system over time, either through independent evaluations or ongoing, structured, and independent process checks.
Overall	The ratings of all components should be considered to determine whether controls provide reasonable assurance that management objectives will be achieved. A strength in the internal controls of one component may compensate for a control weakness in another.

1	Eléments concernant COSO
2	Overview COBIT
3	Mapping COSO/COBIT
4	Exemple de matrice d'analyse: EDM 01

COBIT 5 Process reference model



COBIT 5 Cascade d'objectifs



BSC et objectifs d'entreprise

Figure 4—COBIT 5 Enterprise Goals				
BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

BSC et objectifs IT

Figure 5—IT-related Goals		
IT BSC Dimension	**Information and Related Technology Goal**	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

Métriques / Objectifs d'entreprise

Figure 6—Enterprise Goal Sample Metrics		
BSC Dimension	**Enterprise Goal**	**Metric**
Financial	1. Stakeholder value of business investments	• Percent of investments where value delivered meets stakeholder expectations • Percent of products and services where expected benefits are realised • Percent of investments where claimed benefits are met or exceeded
	2. Portfolio of competitive products and services	• Percent of products and services that meet or exceed targets in revenues and/or market share • Ratio of products and services per life cycle phase • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage
	3. Managed business risk (safeguarding of assets)	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Frequency of update of risk profile
	4. Compliance with external laws and regulations	• Cost of regulatory non-compliance, including settlements and fines • Number of regulatory non-compliance issues causing public comment or negative publicity • Number of regulatory non-compliance issues relating to contractual agreements with business partners
	5. Financial transparency	• Percent of investment business cases with clearly defined and approved expected costs and benefits • Percent of products and services with defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information • Percent of service cost that can be allocated to users

Métriques. Objectifs d'entreprise

Figure 6—Enterprise Goal Sample Metrics *(cont.)*		
BSC Dimension	**Enterprise Goal**	**Metric**
Customer	6. Customer-oriented service culture	• Number of customer service disruptions due to IT service-related incidents (reliability) • Percent of business stakeholders satisfied that customer service delivery meets agreed-on levels • Number of customer complaints • Trend of customer satisfaction survey results
	7. Business service continuity and availability	• Number of customer service interruptions causing significant incidents • Business cost of incidents • Number of business processing hours lost due to unplanned service interruptions • Percent of complaints as a function of committed service availability targets
	8. Agile responses to a changing business environment	• Level of board satisfaction with enterprise responsiveness to new requirements • Number of critical products and services supported by up-to-date business processes • Average time to turn strategic enterprise objectives into an agreed-on and approved initiative
	9. Information-based strategic decision making	• Degree of board and executive management satisfaction with decision making • Number of incidents caused by incorrect business decisions based on inaccurate information • Time to provide supporting information to enable effective business decisions
	10. Optimisation of service delivery costs	• Frequency of service delivery cost optimisation assessments • Trend of cost assessment vs. service level results • Satisfaction levels of board and executive management with service delivery costs
Internal	11. Optimisation of business process functionality	• Frequency of business process capability maturity assessments • Trend of assessment results • Satisfaction levels of board and executives with business process capabilities
	12. Optimisation of business process costs	• Frequency of business process cost optimisation assessments • Trend of cost assessment vs. service level results • Satisfaction levels of board and executive management with business processing costs
	13. Managed business change programmes	• Number of programmes on time and within budget • Percent of stakeholders satisfied with programme delivery • Level of awareness of business change induced by IT-enabled business initiatives
	14. Operational and staff productivity	• Number of programmes/projects on time and within budget • Cost and staffing levels compared to benchmarks
	15. Compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices
Learning and Growth	16. Skilled and motivated people	• Level of stakeholder satisfaction with staff expertise and skills • Percent of staff whose skills are insufficient for the competency required for their role • Percent of satisfied staff
	17. Product and business innovation culture	• Level of awareness and understanding of business innovation opportunities • Stakeholder satisfaction with levels of product and innovation expertise and ideas • Number of approved product and service initiatives resulting from innovative ideas

Métriques/ Objectifs IT

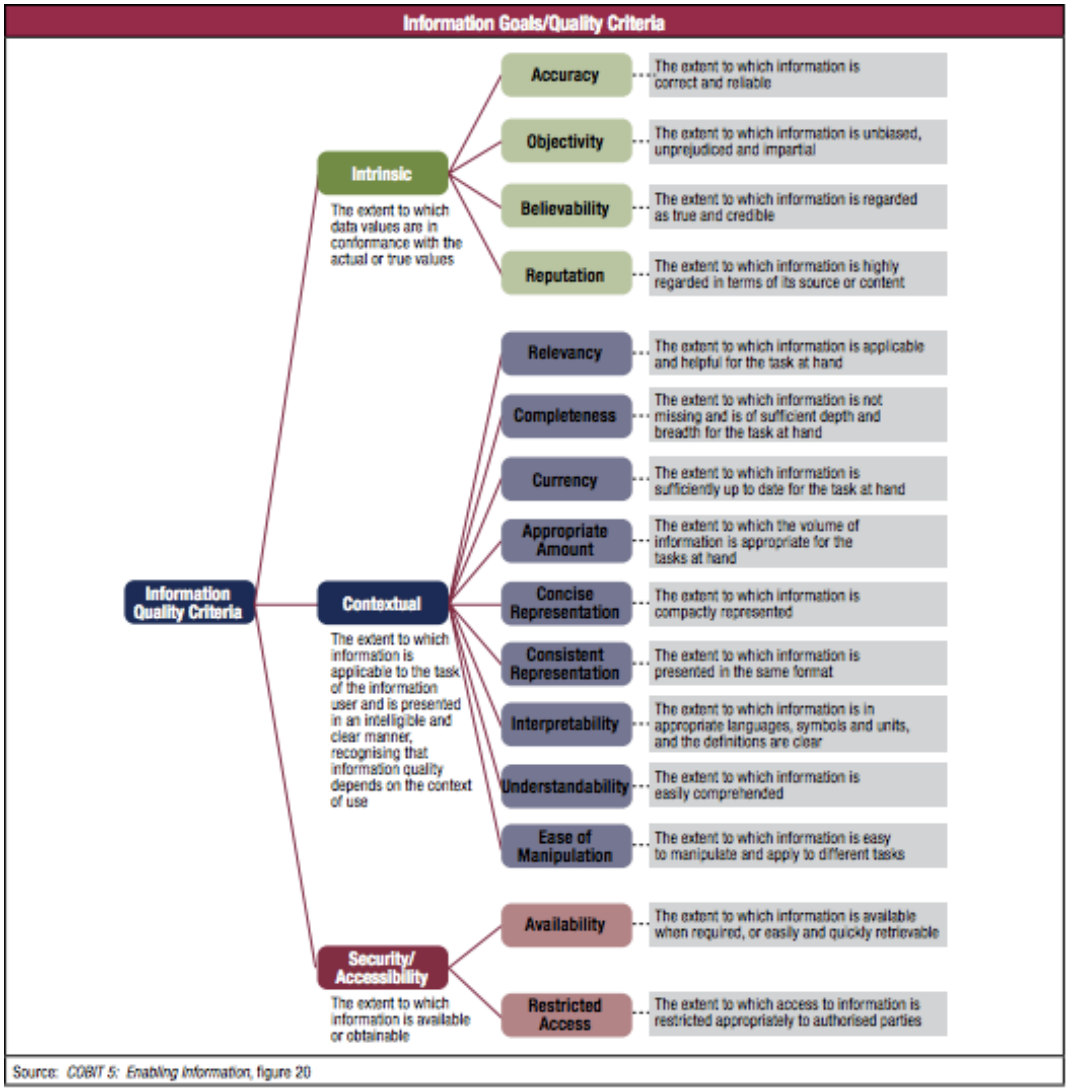
Figure 7—IT-related Goal Sample Metrics		
BSC Dimension	**IT-related Goal**	**Metric**
Financial	01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
	02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
	03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions

RÉFÉRENCE DSI

Figure 7—IT-related Goal Sample Metrics (cont.)

BSC Dimension	IT-related Goal	Metric
Financial (cont.)	04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
	05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
	06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information
Customer	07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery
	08 Adequate use of applications, information and technology solutions	• Percent of business process owners satisfied with supporting IT products and services • Level of business user understanding of how technology solutions support their processes • Satisfaction level of business users with training and user manuals • Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions
Internal	09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
	10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines
	11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
	12 Enablement and support of business processes by integrating applications and technology into business processes	• Number of business processing incidents caused by technology integration errors • Number of business process changes that need to be delayed or reworked because of technology integration issues • Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues • Number of applications or critical infrastructures operating in silos and not integrated
	13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost
	14 Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
	15 IT compliance with internal policies	• Number of incidents related to non-compliance to policy • Percent of stakeholders who understand policies • Percent of policies supported by effective standards and working practices • Frequency of policies review and update
Learning and Growth	16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
	17 Knowledge, expertise and initiatives for business innovation	• Level of business executive awareness and understanding of IT innovation possibilities • Level of stakeholder satisfaction with levels of IT innovation expertise and ideas • Number of approved initiatives resulting from innovative IT ideas

COBIT 5 Information quality goals

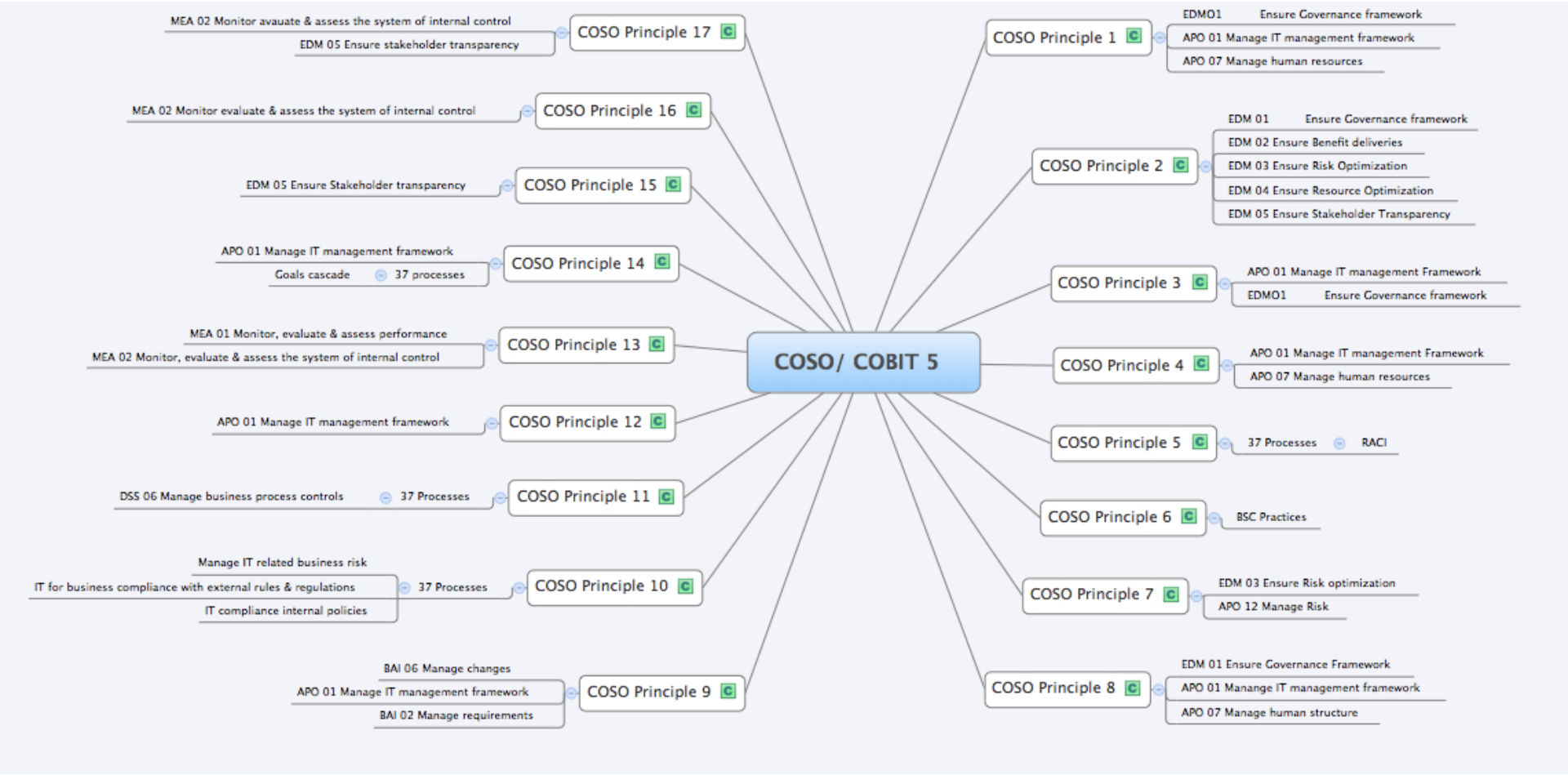


Source: *COBIT 5: Enabling Information*, figure 20

COSO based audits

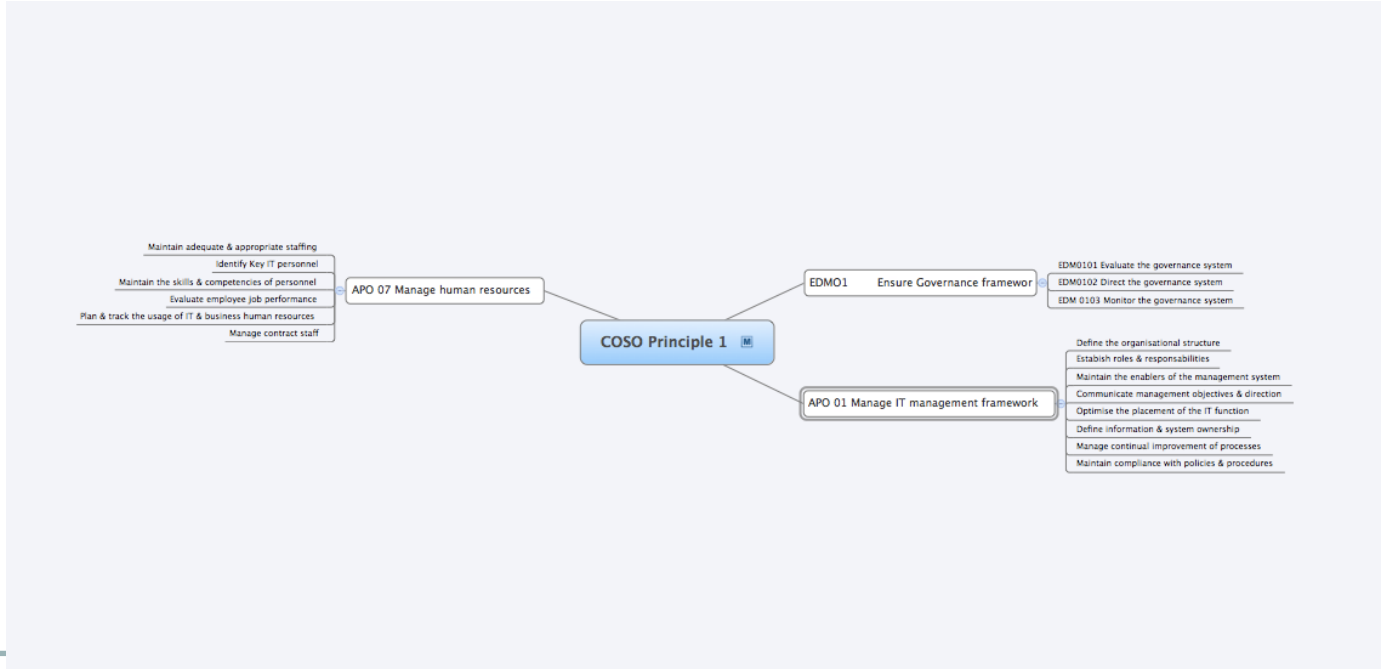
1	Eléments concernant COSO
2	Overview COBIT
3	**Mapping COSO/COBIT**
4	Exemple de matrice d'analyse: EDM 01

COSO principles vs COBIT framework



COSO principles vs COBIT framework

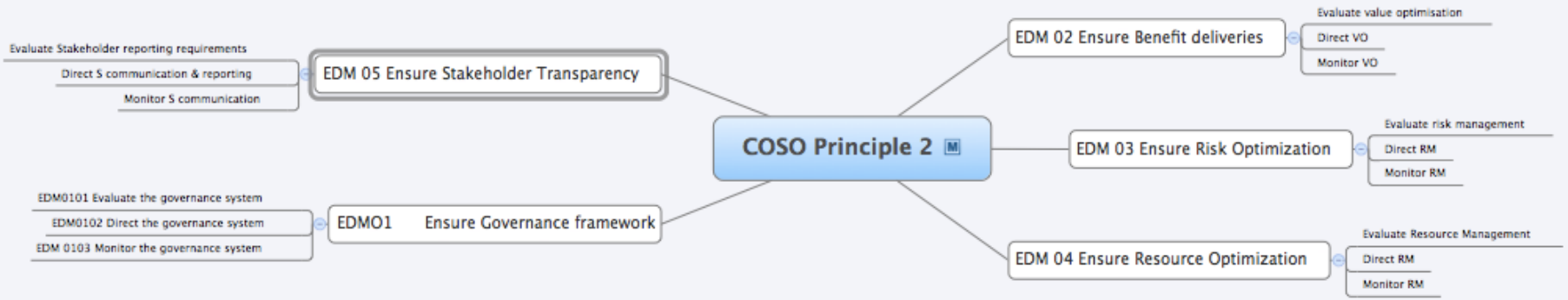
"1. The organization demonstrates a commitment to integrity and ethical values."	The COBIT 5 Culture, Ethics and Behaviour enabler addresses enterprise ethics and individual ethics and behaviors, including risk taking, by following policy and addressing negative outcomes. The COBIT 5 processes EDM01 *Ensure governance framework setting and maintenance* and APO01 *Manage the IT management framework* include activities to embed enterprise integrity and ethical value aspects within the governance and management framework. The COBIT 5 process APO07 *Manage human resources* includes activities to address integrity and ethical value aspects from a human resources perspective.



COSO principles vs COBIT framework

"2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control."

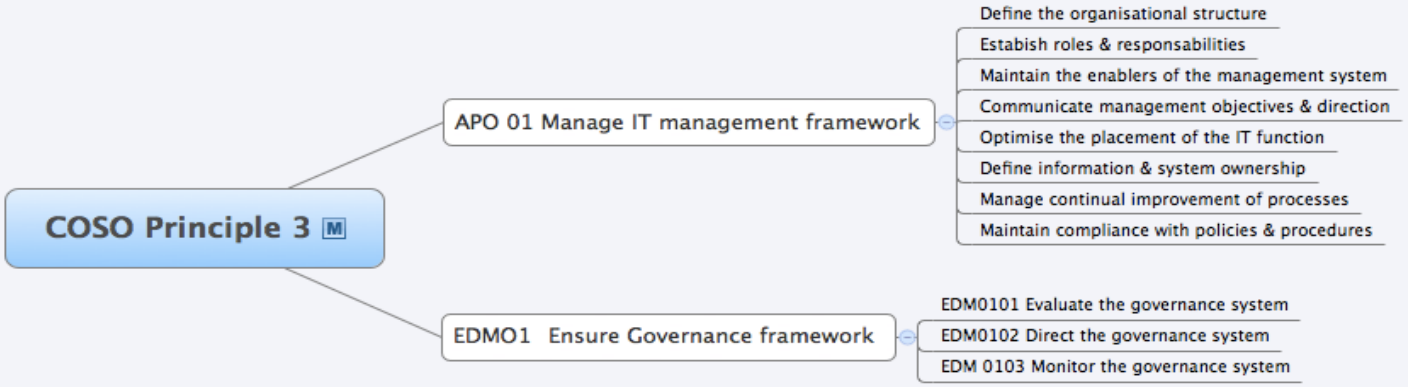
The COBIT 5 principle Separating Governance from Management supports the second COSO principle by differentiating governance and management disciplines and making independence easier to establish and maintain. In addition, all five COBIT 5 governance processes (EDM01 through EDM05) reinforce this separation in their RACI chart guidance.



COSO principles vs COBIT framework

"3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives."

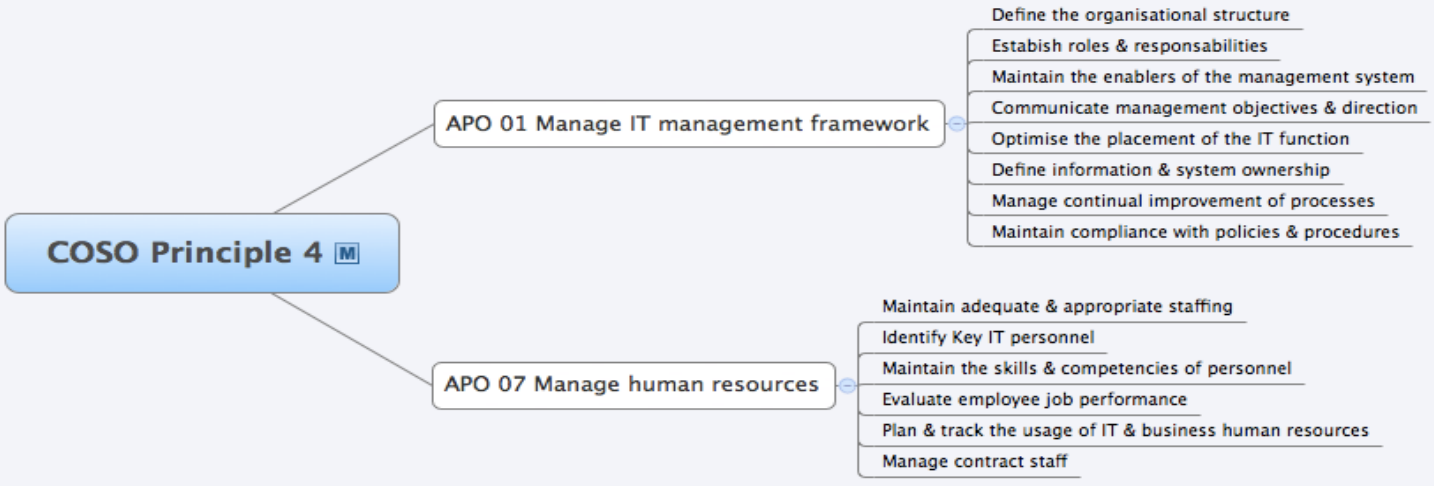
The COBIT 5 Organisational Structure enabler addresses practices, such as operating principles, span of control (scope) definition, level of authority, delegation of authority powers and escalation paths, to support the establishment of effective organizational structures within enterprises. COBIT 5 process APO01 *Manage the IT management framework* includes activities to address the required definition of an organizational structure for the enterprise. APO01 takes direction from COBIT 5 process EDM01 *Ensure governance framework setting and maintenance* in respect to enterprise governance requirements.



COSO principles vs COBIT framework

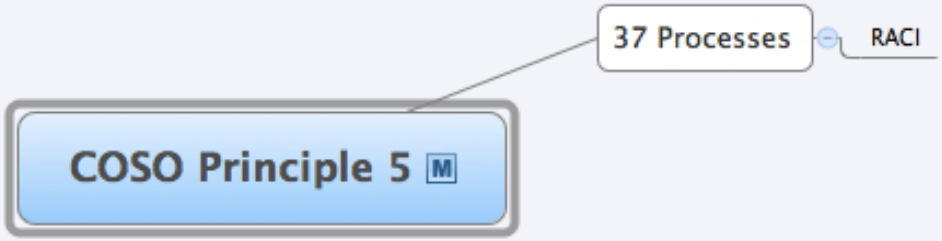
"4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives."

The COBIT 5 People, Skills and Competencies enabler addresses the life cycle aspects that are related to people—knowing the current skills base; the skills that need to be retained, developed or acquired to meet enterprise goals; and the skills that can be disposed of when no longer needed. COBIT 5 process APO01 *Manage the IT management framework* includes activities to establish roles and responsibilities to support achievement of enterprise objectives. COBIT 5 process APO07 *Manage human resources* includes activities to address the attraction, development and retention of competent people.



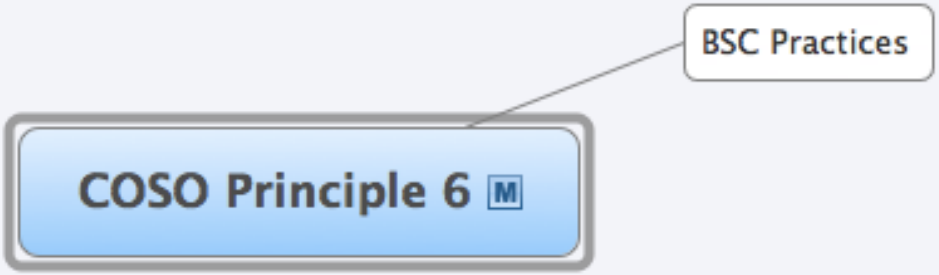
COSO principles vs COBIT framework

"5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives."	The COBIT 5 Processes enabler and the RACI charts that support the 37 processes are particularly relevant in the context of individual accountability. The enabler and charts strongly advocate the assignment of responsibilities and accountabilities and provide examples of roles and responsibilities for the individual and group roles for all key GEIT-related processes and activities.



COSO principles vs COBIT framework

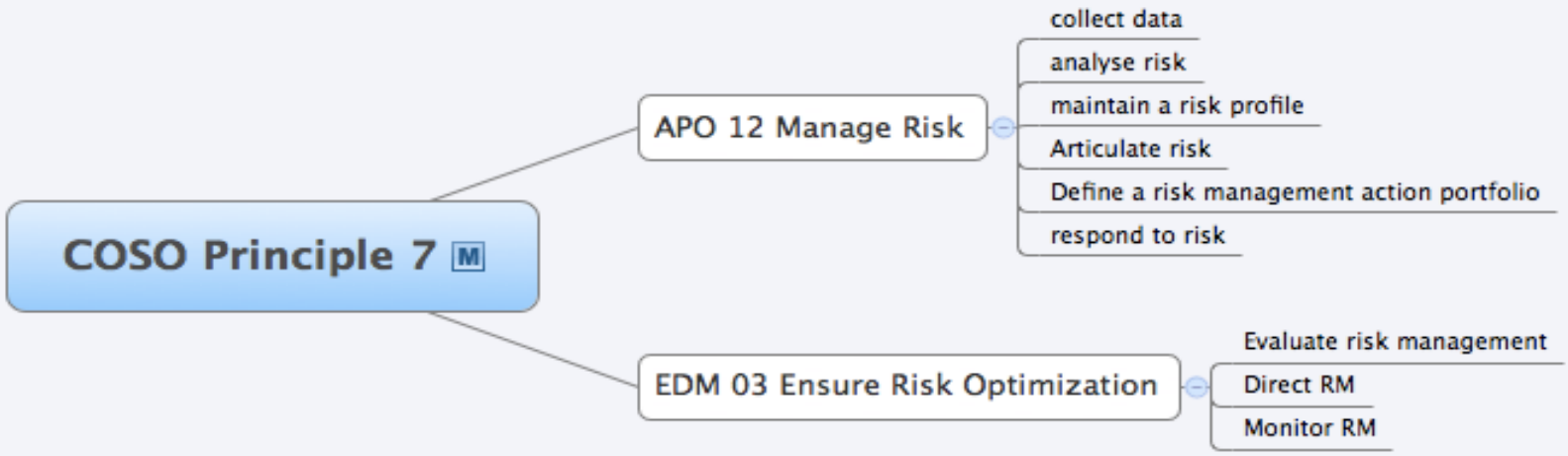
"6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives."	The COBIT 5 framework focuses on enterprise objectives through the use of the goals cascade model, which is based on BSC theory. This model supports the enterprise by clearly defining its business objectives in a way that enables the identification and assessment of risk that relates to meeting objectives. The guidance for each of the 37 COBIT processes includes process goals (objectives).



COSO principles vs COBIT framework

"7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed."

The COBIT 5 Processes enabler guidance specifically addresses risk governance (process EDM03 *Ensure risk optimisation*) and management (process APO12 *Manage risk*). These processes include the practices and activities required to govern and manage risk effectively—including the identification, analysis and management of the risk. These processes drive other areas, e.g., information security and business continuity, which are addressed by other specific COBIT 5 processes.



COSO principles vs COBIT framework

"8. The organization considers the potential for fraud in assessing risks to the achievement of objectives."

The COBIT 5 framework does not focus on fraud as a specific business risk, although the guidance supports the establishment of a sound governance and management environment, within which practices and supporting activities can be established and performed to support effective fraud prevention activities. The specific inclusion of the COBIT 5 Culture, Ethics and Behaviour enabler helps to ensure that a culture that is fraud-risk-aware is established and that the consequences of engaging in such behavior are clearly communicated where appropriate. COBIT 5 processes EDM01, APO01 and APO07 support culture, ethics and behaviour objectives, including an enterprise's approach to fraud. COBIT process MEA03 *Monitor, evaluate and assess compliance with external requirements* should also be considered, because fraud prevention (bribery, privacy, etc.) is often part of an enterprise's external compliance requirements.

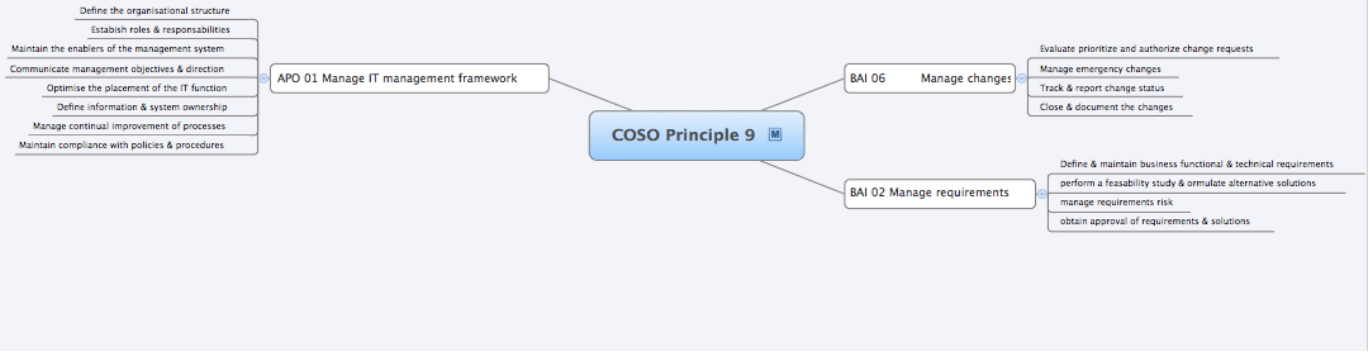
COSO principles vs COBIT framework

"9. The organization identifies and assesses changes that could significantly impact the system of internal control."

The COBIT 5 Processes enabler guidance specifically addresses changes in COBIT 5 process BAI06 *Manage changes*, which is directly linked to the IT-related goal "Managed IT-related business risk." This process, like the COSO principle, recognizes that changes within an enterprise can introduce risk and, therefore, need to be a focus from this perspective.

Further, as changes occur in all areas of control activity (information, applications and general control activities over technology), these changes are addressed by various COBIT 5 processes. COBIT 5 process APO01 *Manage the IT management framework* addresses the management framework and manages changes to general controls. COBIT 5 process BAI06 *Manage changes* and, for programs and projects, COBIT 5 process BAI02 *Manage requirements definition* manage the changes to business processes, applications and infrastructure.

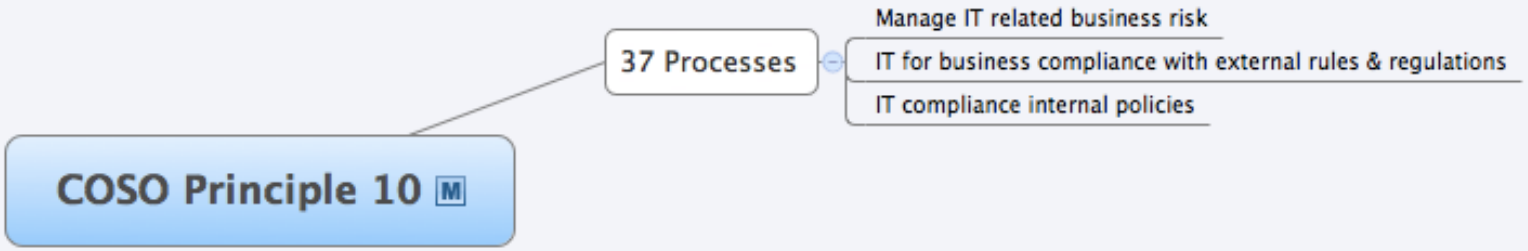
All changes need to be tested and approved by following the COBIT 5 process BAI07 *Manage change acceptance and transitioning*. Impacts to business processes are handled according to COBIT 5 process BAI05 *Manage organisational change enablement*.



COSO principles vs COBIT framework

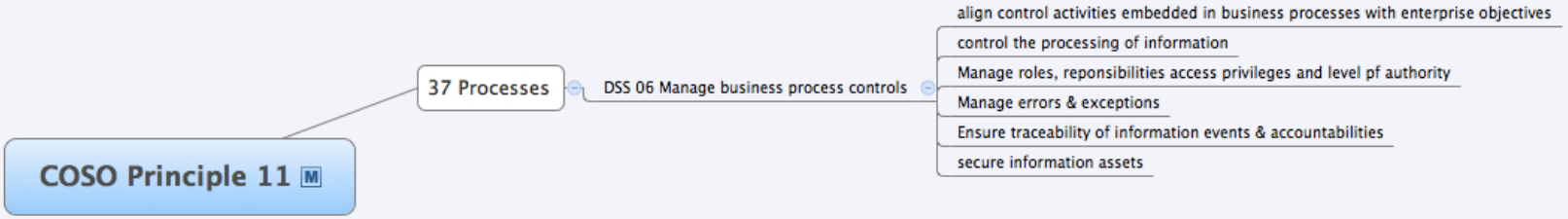
"10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels."

The COBIT 5 Processes enabler guidance for the 37 COBIT 5 processes supports enterprises in their selection and development of control activities and other arrangements (e.g., structural segregation of duties), particularly with the practices and activities to consider for IT-related enterprise processes. This guidance includes how the IT-related enterprise process practices and activities support the IT-related goals of "Managed IT-related business risk," "IT compliance and support for business compliance with external laws and regulations" and "IT compliance with internal policies."



COSO principles vs COBIT framework

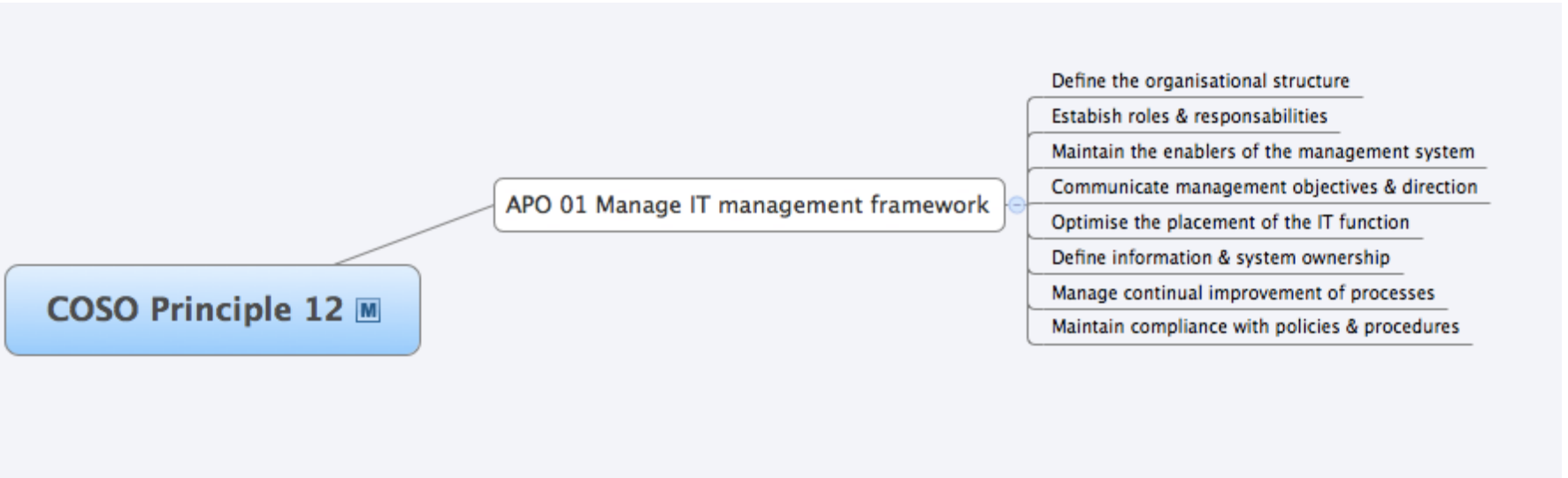
"11. The organization selects and develops general control activities over technology to support the achievement of objectives."	The COBIT 5 principles and enablers can be applied to the governance and management of any type of enterprise activity as described in the previous paragraph (COSO principle 10). Detailed COBIT 5 guidance relates generically to the governance and management of information and information technology assets. As such, the detailed guidance in COBIT 5 is directly supportive of COSO principle 11, "selects and develops general control activities over technology."[16] Control activities can be process activities within all of the 37 COBIT processes or relate to other enabler types. In particular, COBIT 5 process DSS06 *Manage business process controls* ensures that control activities that are embedded in business processes (automated controls or application controls) are adequately managed.



COSO principles vs COBIT framework

"12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action."

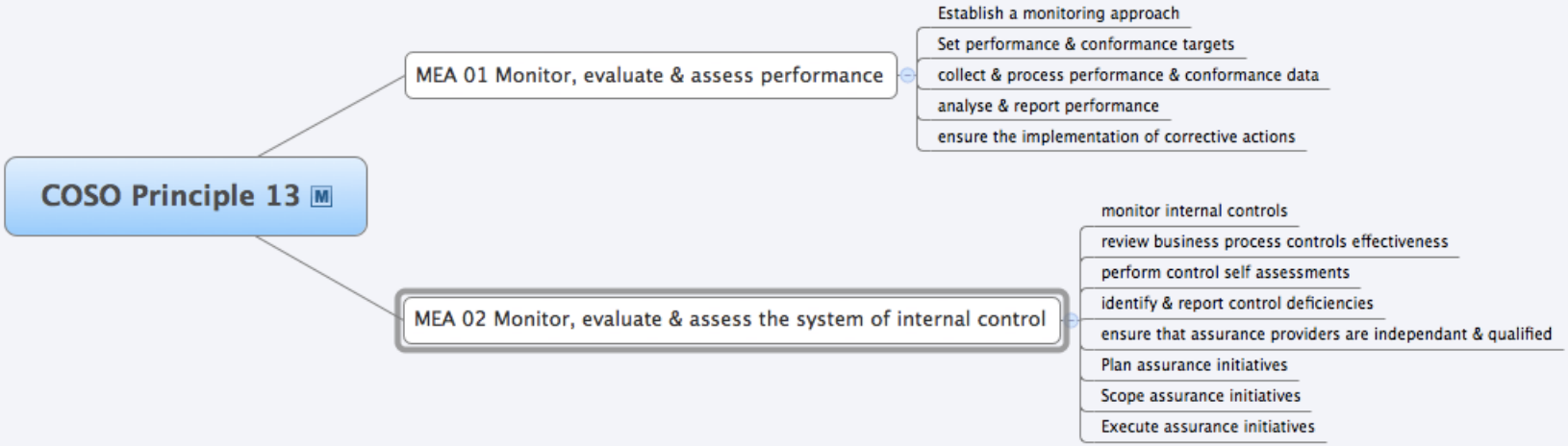
The COBIT 5 Principles, Policies and Frameworks enabler is central to effective enterprise IT governance and management. Enterprise policies are central to COBIT 5 support of achievement of enterprise goals, including mitigation of risk through the use of appropriate activities. COBIT 5 process APO01 *Manage the IT management framework* includes activities that address the implementation of enterprise policies.



COSO principles vs COBIT framework

"13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control."

The COBIT 5 Information enabler model describes 15 Information quality goals, which are categorized into intrinsic, contextual and security/accessibility quality dimensions. Considering each quality goal helps enterprises to ensure that the information used supports enterprise business goals, including control objectives. The guidance for the 37 COBIT 5 processes includes inputs and outputs that are the communication of information across, and to and from, the enterprise. In particular, COBIT 5 process MEA01 *Monitor, evaluate and assess performance and conformance* addresses performance and conformance data, and COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control* addresses control effectiveness reviews.

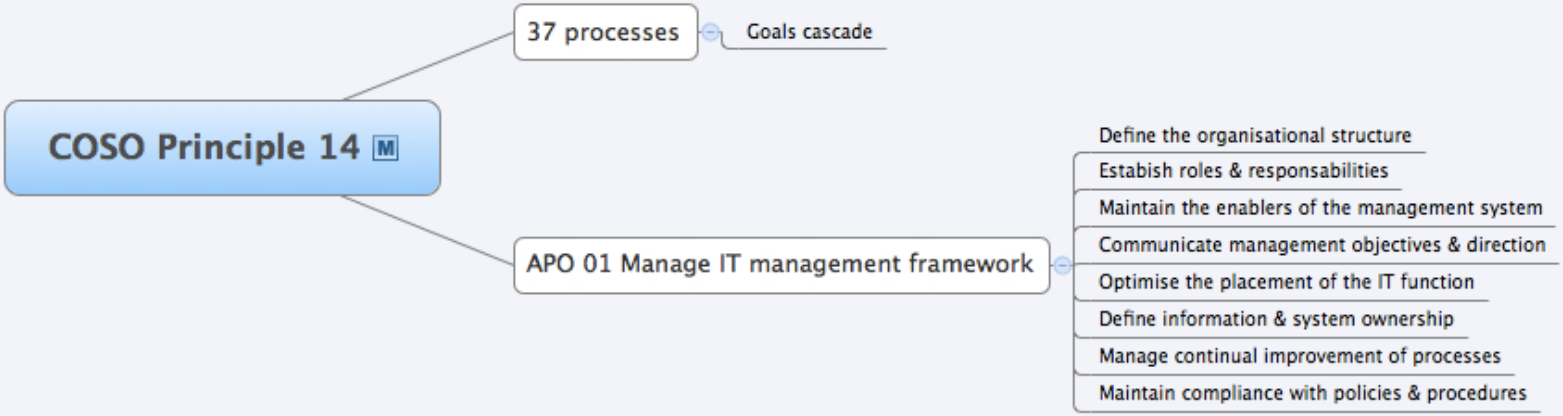


COSO principles vs COBIT framework

"14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control."

The COBIT 5 framework provides sound, structured and comprehensive guidance that facilitates effective internal communication of GEIT aspects and issues between the multiple internal stakeholders. This includes the communication of clear objectives that result from the goals cascade, including Processes enabler goals (objectives), which are provided for all 37 COBIT 5 processes. The need to communicate information with stakeholders as part of enterprise process design and execution, to support the achievement of process and related business goals, is addressed in the RACI charts, with the responsibilities of "consult" and "inform," and the input and output suggestions that support the process guidance for the 37 COBIT 5 processes.

This communication is implemented and managed following COBIT 5 process APO01 *Manage the IT management framework*. In addition, a comprehensive guide, *COBIT 5 Implementation*, is available.



COSO principles vs COBIT framework

"15. The organization communicates with external parties regarding matters affecting the functioning of internal control."	The COBIT 5 framework also provides a sound basis for effective communication of GEIT aspects and issues to external stakeholders when appropriate. In particular, the COBIT 5 process EDM05 *Ensure stakeholder transparency* requires that the communication to stakeholders is effective and timely and that a reliable, consistent basis for reporting is established.

COSO principles vs COBIT framework

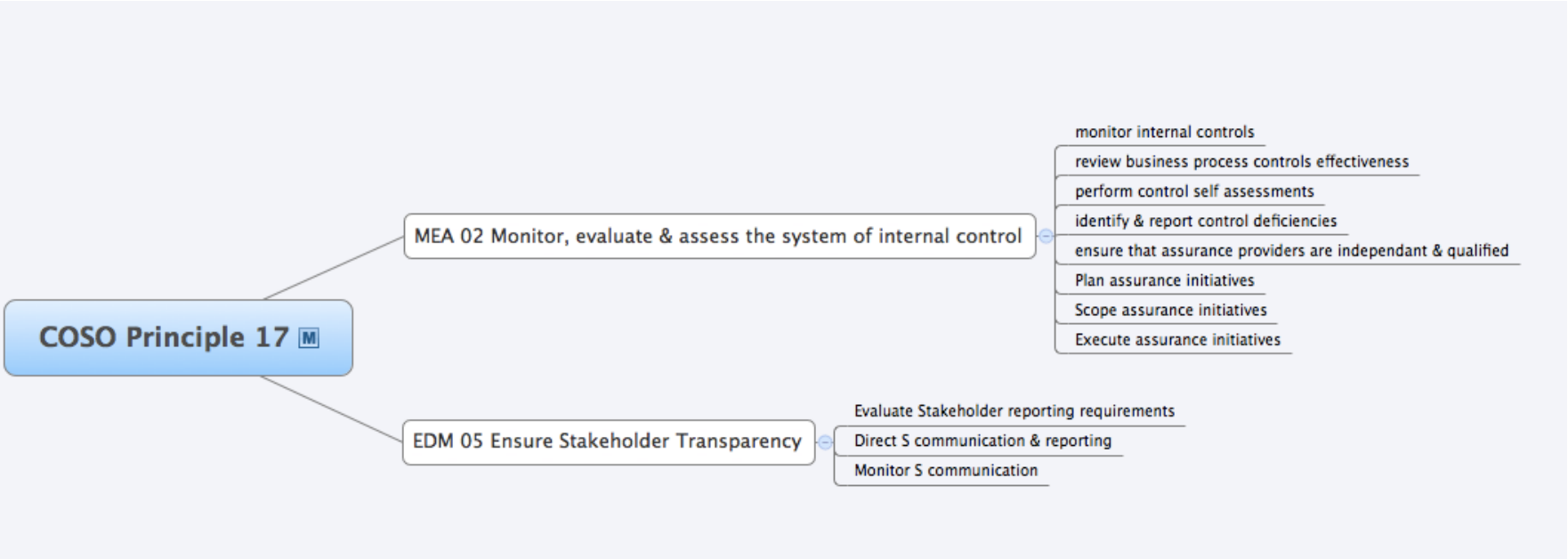
"16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning."

The COBIT 5 Processes enabler guidance specifically addresses monitoring, evaluation and assessment of internal control adequacy (COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control)*. This process includes the practices and activities that are required to monitor internal controls; review business process controls effectiveness; perform control self-assessments; identify and report control deficiencies; ensure that assurance providers are independent and qualified; and plan, scope and execute assurance activities.

COSO principles vs COBIT framework

"17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate."

As noted in the previous paragraph, COBIT 5 process MEA02 *Monitor, evaluate and assess the system of internal control* includes the practices and activities that are required to identify control deficiencies; analyze and identify their underlying root cause; escalate control deficiencies; and report to stakeholders as appropriate. In addition, COBIT 5 process EDM05 *Ensure stakeholder transparency* includes practices and activities to evaluate, direct and monitor stakeholder reporting and communication requirements, including those that are related to control deficiencies, to senior management and the board, as appropriate.



1	Eléments concernant COSO
2	Overview COBIT
3	Mapping COSO/COBIT
4	Exemple de matrice d'analyse: EDM 01

RÉFÉRENCE

EDM01 Ensure Governance Framework Setting and Maintenance	Area: Governance Domain: Evaluate, Direct and Monitor

Process Description
Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Process Purpose Statement
Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.

The process supports the achievement of a set of primary IT-related goals:

IT-related Goal	Related Metrics
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions
07 Delivery of IT services in line with business requirements	• Number of business disruptions due to IT service incidents • Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT service delivery

Process Goals and Metrics

Process Goal	Related Metrics
1. Strategic decision-making model for IT is effective and aligned with the enterprise's internal and external environment and stakeholder requirements.	• Actual vs. target cycle time for key decisions • Level of stakeholder satisfaction (measured through surveys)
2. The governance system for IT is embedded in the enterprise.	• Number of roles, responsibilities and authorities that are defined, assigned and accepted by appropriate business and IT management • Degree by which agreed-on governance principles for IT are evidenced in processes and practices (percentage of processes and practices with clear traceability to principles) • Number of instances of non-compliance with ethical and professional behaviour guidelines
3. Assurance is obtained that the governance system for IT is operating effectively.	• Frequency of independent reviews of governance of IT • Frequency of governance of IT reporting to the executive committee and board • Number of governance of IT issues reported

EDM 01 Process. RACI

EDM01 RACI Chart																										
Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM01.01 Evaluate the governance system.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Direct the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Monitor the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

EDM 01.01 Activities

RÉFÉRENCE DSI

EDM01 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
EDM01.01 Evaluate the governance system. Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make a judgement on the current and future design of governance of enterprise IT.	**From**	**Description**	**Description**	**To**
	MEA03.02	Communications of changed compliance requirements	Enterprise governance guiding principles	All EDM AP001.01 AP001.03
	Outside COBIT	• Business environment trends • Regulations • Governance/decision-making model • Constitution/bylaws/ statutes of organisation	Decision-making model	All EDM AP001.01
			Authority levels	All EDM AP001.02
Activities				
1. Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.				
2. Determine the significance of IT and its role with respect to the business.				
3. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT.				
4. Align the ethical use and processing of information and its impact on society, natural environment, and internal and external stakeholder interests with the enterprise's direction, goals and objectives.				
5. Determine the implications of the overall enterprise control environment with regard to IT.				
6. Articulate principles that will guide the design of governance and decision making of IT.				
7. Understand the enterprise's decision-making culture and determine the optimal decision-making model for IT.				
8. Determine the appropriate levels of authority delegation, including threshold rules, for IT decisions.				

EDM 01.02 Activities

Governance Practice	Inputs		Outputs	
EDM01.02 Direct the governance system. Inform leaders and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed-on governance design principles, decision-making models and authority levels. Define the information required for informed decision making.	**From**	**Description**	**Description**	**To**
			Enterprise governance communications	All EDM AP001.04
			Reward system approach	AP007.03 AP007.04
Activities				
1. Communicate governance of IT principles and agree with executive management on the way to establish informed and committed leadership.				
2. Establish or delegate the establishment of governance structures, processes and practices in line with agreed-on design principles.				
3. Allocate responsibility, authority and accountability in line with agreed-on governance design principles, decision-making models and delegation.				
4. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision-making with appropriate information.				
5. Direct that staff follow relevant guidelines for ethical and professional behaviour and ensure that consequences of non-compliance are known and enforced.				
6. Direct the establishment of a reward system to promote desirable cultural change.				

EDM 01.03 Activities

EDM01 Process Practices, Inputs/Outputs and Activities *(cont.)*				
Governance Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
EDM01.03 Monitor the governance system. Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.	MEA01.04	Performance reports	Feedback on governance effectiveness and performance	All EDM APO01.07
	MEA01.05	Status and results of actions		
	MEA02.01	• Results of benchmarking and other evaluations • Results of internal control monitoring and reviews		
	MEA02.03	Results of reviews of self-assessments		
	MEA02.06	Assurance plans		
	MEA03.03	Compliance confirmations		
	MEA03.04	• Reports of non-compliance issues and root causes • Compliance assurance reports		
	Outside COBIT	• Obligations • Audit reports		
Activities				
1. Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise IT.				
2. Periodically assess whether agreed-on governance of IT mechanisms (structures, principles, processes, etc.) are established and operating effectively.				
3. Assess the effectiveness of the governance design and identify actions to rectify any deviations found.				
4. Maintain oversight of the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.				
5. Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control.				
6. Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.				