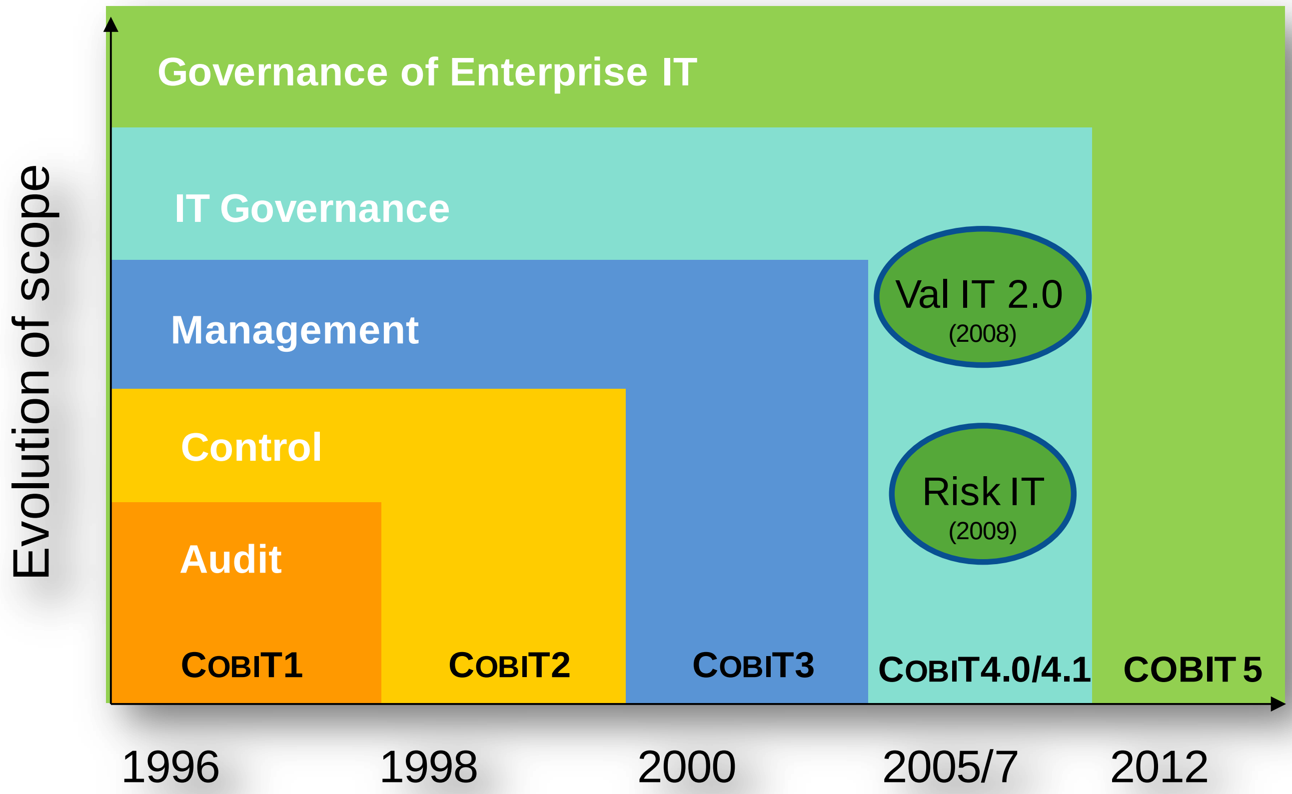
COBIT5

Présentation

2013

Pierre CALVANESE

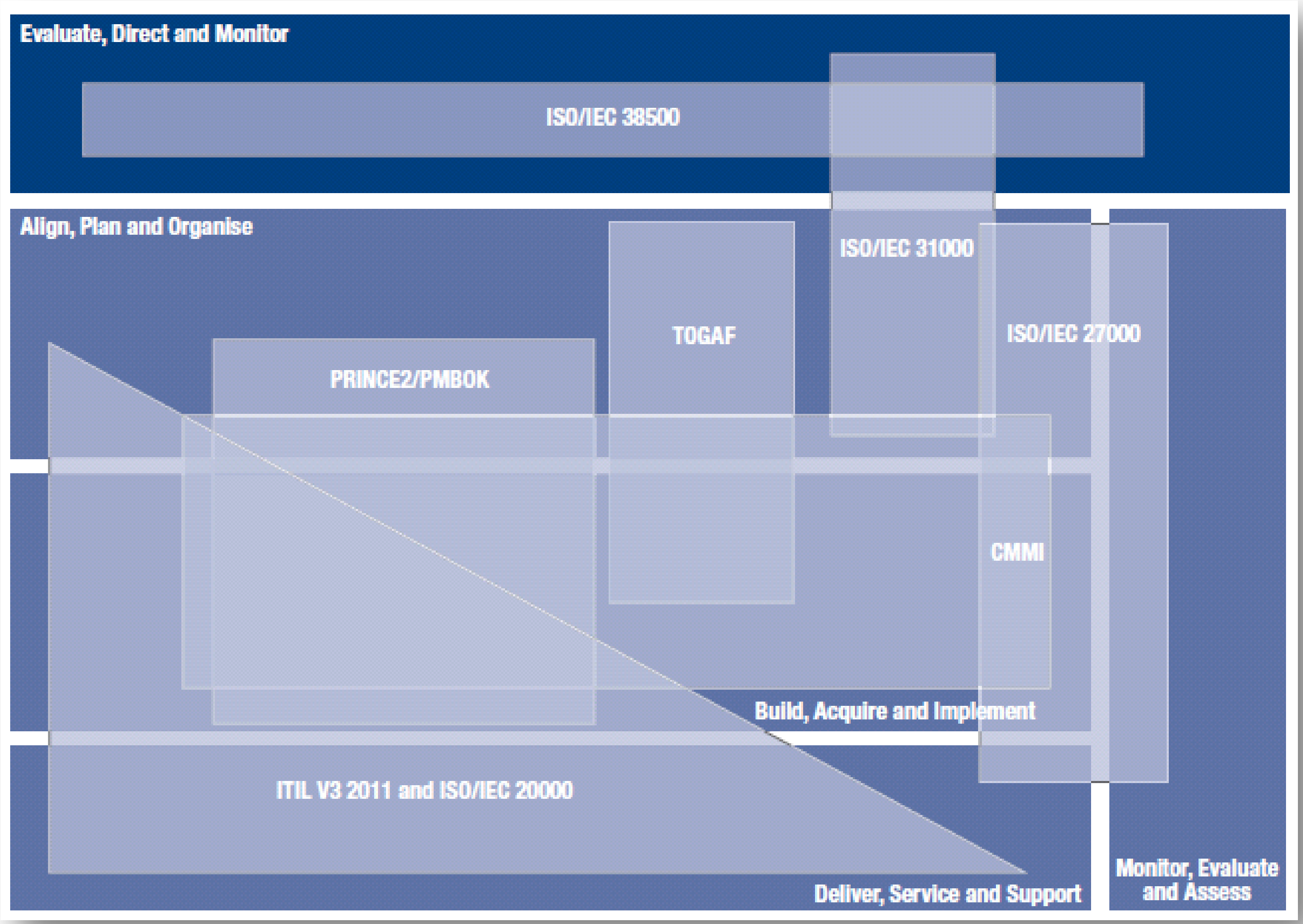
Un référentiel global d'entreprise



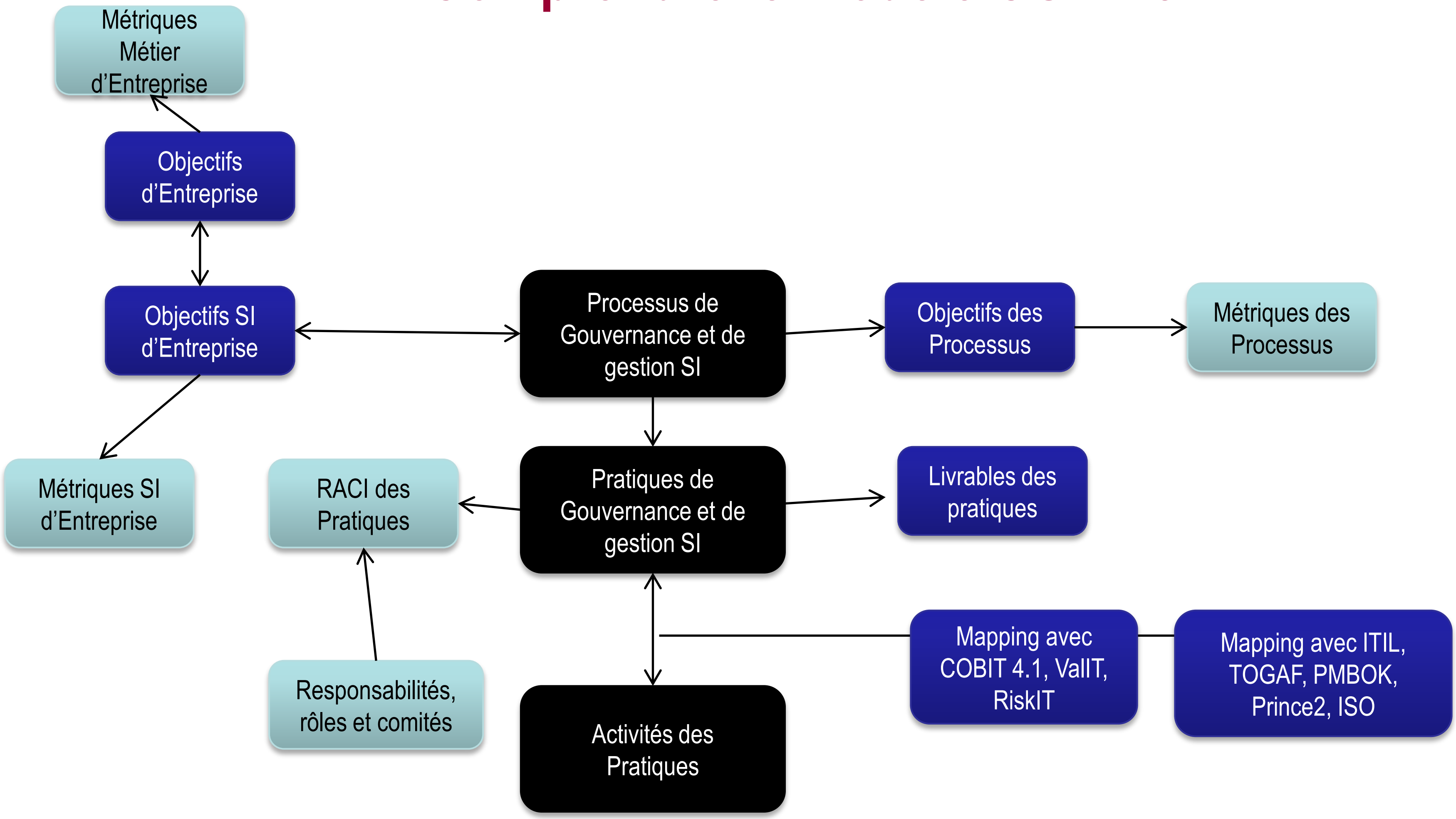
Source : ISACA

Les APPENDIX

E > Mapping COBIT5 entre les principaux standards et référentiels

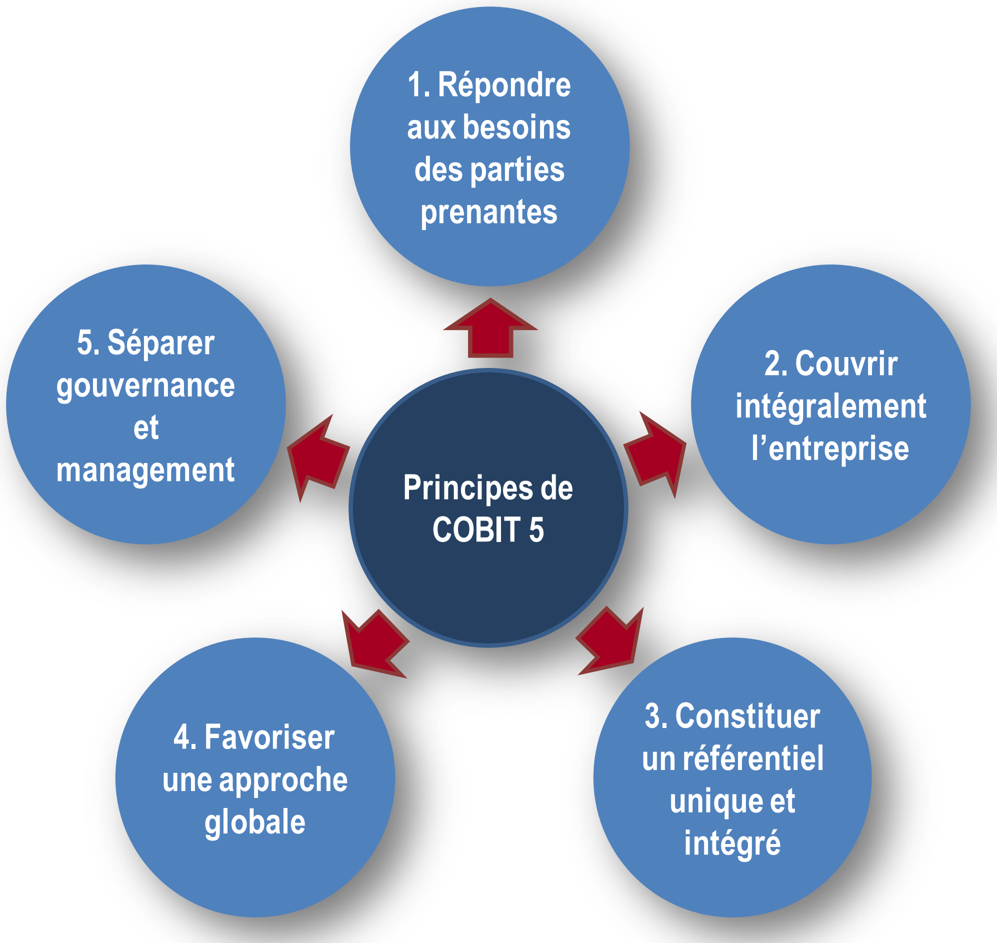


4. Comprendre le modèle COBIT5



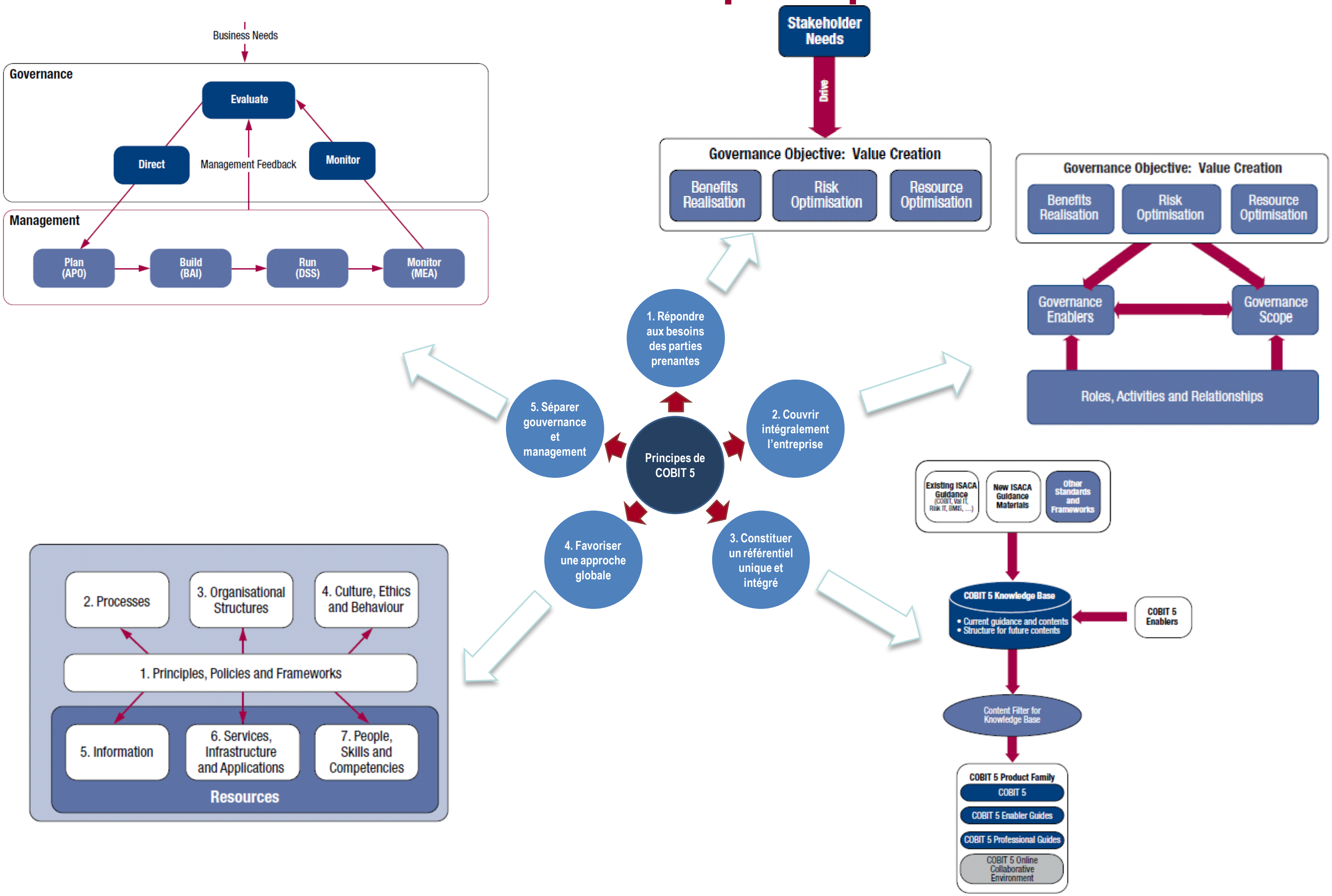
4. Nouveaux principes GEIT

Les principes de COBIT 5



Source: COBIT® 5, figure 2. © 2012 ISACA®

Détail des principes



Gouvernance et Management

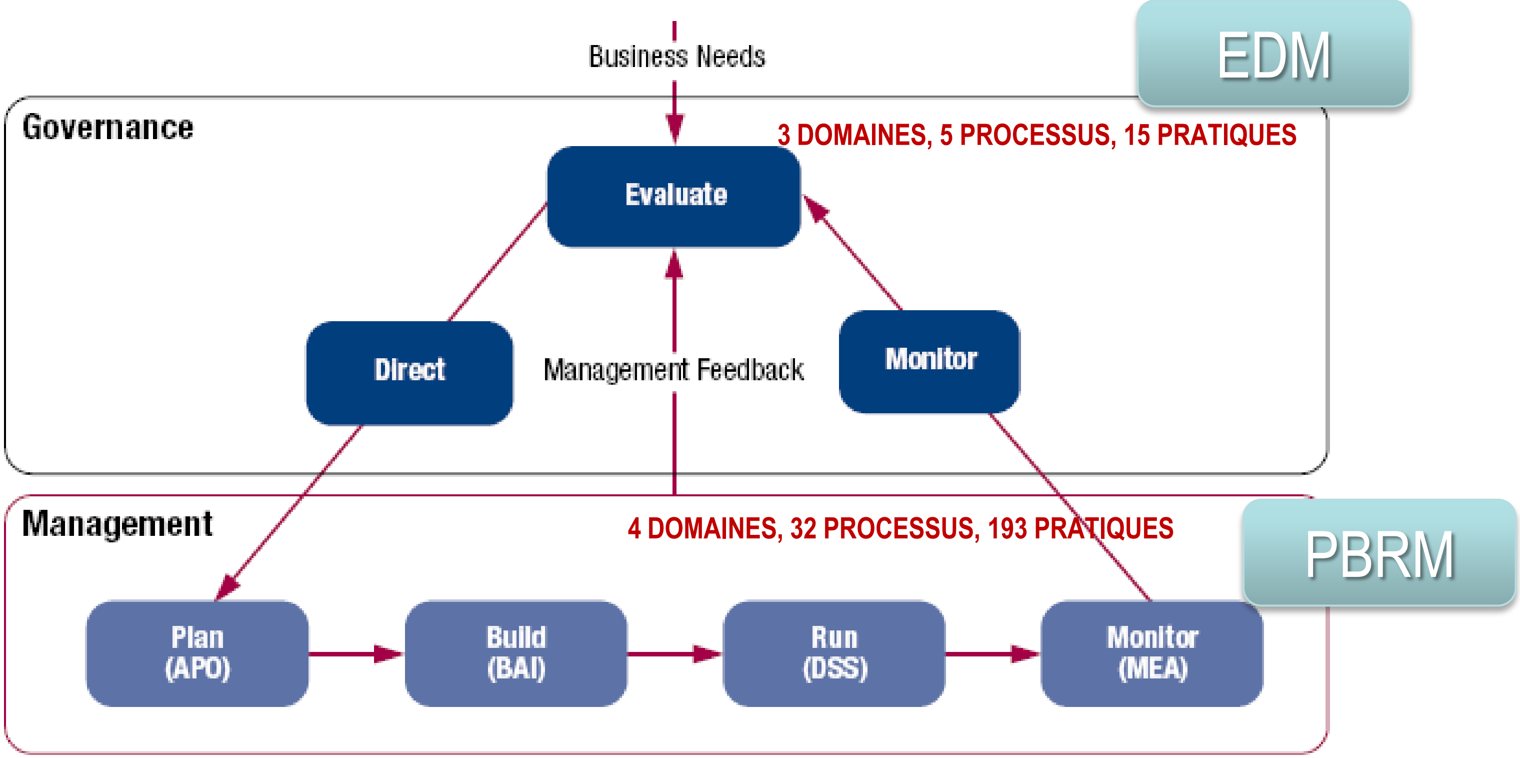
- La gouvernance s'assure que les besoins, les conditions et les options des parties prenantes sont **évalués** afin de déterminer des objectifs à atteindre équilibrés et sur lesquels l'entreprise est d'accord. Elle **donne le cap** en fixant les priorités et en prenant les décisions. Elle **surveille** la performance et la conformité par rapport aux orientations et aux objectifs convenus.

- Le **management planifie, réalise, fait fonctionner et surveille** les activités pour les aligner sur les orientations fixées par l'organe de gouvernance afin d'atteindre les objectifs de l'entreprise.

5. Séparer gouvernance et management

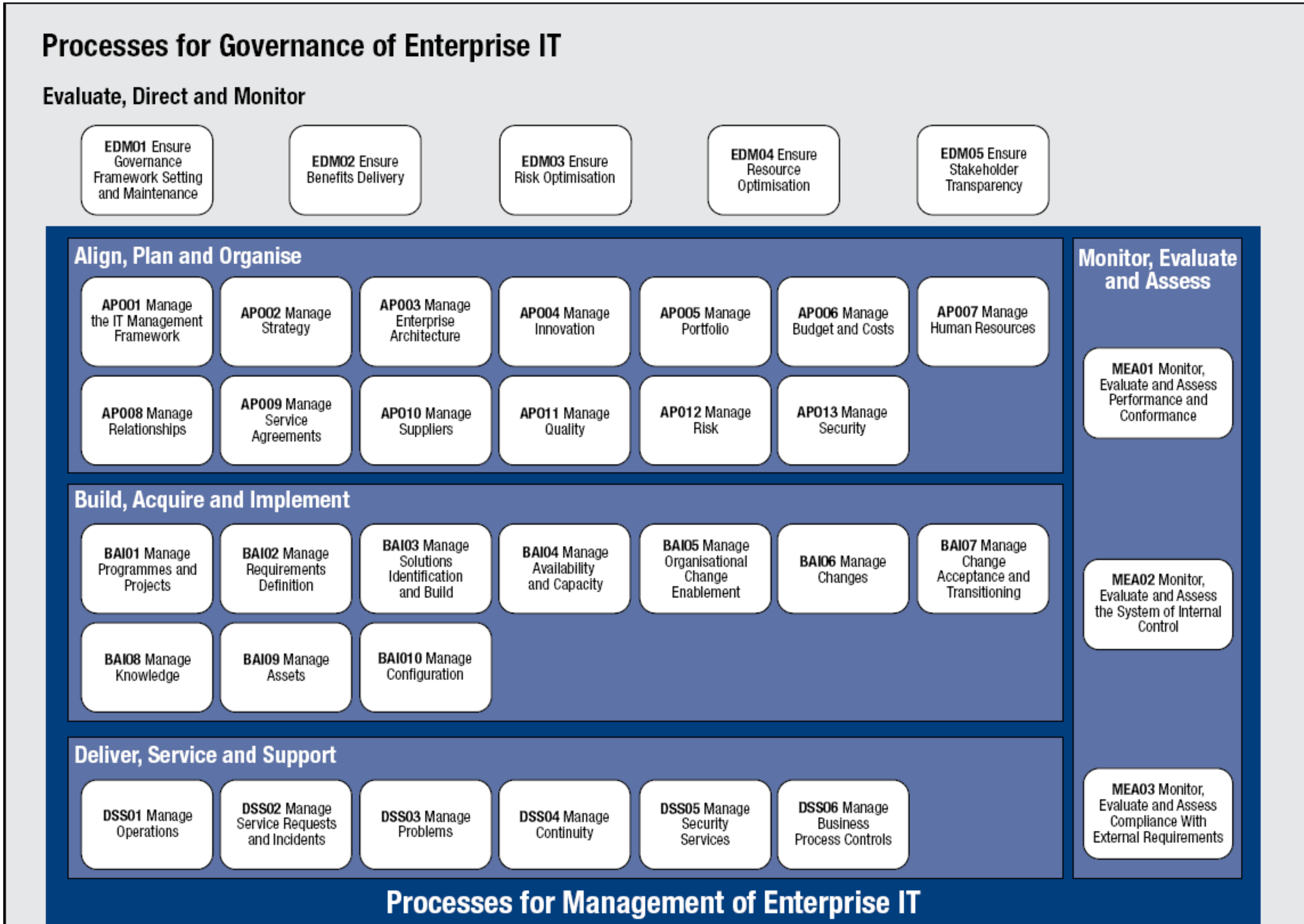
COBIT 5 ne se veut pas normatif mais préconise que les organisations mettent en œuvre des processus de gouvernance et de management de façon à couvrir les domaines clés comme indiqué.

7 DOMAINES, 37 PROCESSUS, 208 PRATIQUES



Source : ISACA

4. Nouveau modèle de référence Processus



Source: COBIT® 5, figure 16.

COBIT® 5
AN ISACA® FRAMEWORK

4. Nouveau modèle de référence 37 Processus, 208 Pratiques

Les Processus de Gouvernance SI

Evaluer, Diriger, et Monitorer (EDM) 5 Processus, 15 Pratiques

- **EDM1** Etablir et maintenir le cadre de Gouvernance
- **EDM2** Assurer l'optimisation de la Valeur
- **EDM3** Assurer l'optimisation du Risque
- **EDM4** Assurer l'optimisation des Ressources
- **EDM5** Assurer la Transparence pour les Parties prenantes

Les Processus de Management SI

Aligner, planifier et organiser (APO) 13 Processus, 70 Pratiques

- **APO01** Définir le cadre de Gestion IT
- **APO02** Définir la Stratégie
- **APO03** Gérer l'Architecture d'Entreprise
- **APO04** Gérer l'Innovation
- **APO05** Gérer le Portefeuille
- **APO06** Gérer le budget et les coûts
- **APO07** Gérer les Ressources Humaines
- **APO08** Gérer les Relations
- **APO09** Gérer les accords de Services
- **APO10** Gérer les fournisseurs
- **APO11** Gérer la Qualité
- **APO12** Gérer les Risques
- **APO13** Gérer la Sécurité

Bâtir, acquérir et implémenter (BAI) 10 Processus, 57 Pratiques

- **BAI01** Gérer les Programmes et les Projets
- **BAI02** Définir les Exigences
- **BAI03** Identifier et construire les solutions
- **BAI04** Gérer la disponibilité et la capacité
- **BAI05** Gérer le changement organisationnel
- **BAI06** Gérer les changements
- **BAI07** Accepter et mettre en œuvre les changements
- **BAI08** Gérer la connaissance
- **BAI09** Gérer les actifs
- **BAI10** Gérer les configurations

Délivrer, servir et supporter (DSS) 6 Processus, 49 Pratiques

- **DSS01** Gérer les opérations
- **DSS02** Gérer les requêtes de services et incidents
- **DSS03** Gérer les problèmes
- **DSS04** Gérer la Continuité
- **DSS05** Gérer la sécurité des services
- **DSS06** Gérer les contrôles des Processus Métiers

Monitorer, évaluer et apprécier (MEA) 3 Processus, 17 Pratiques

- **MEA01** Surveiller, évaluer et estimer la Performance et la Conformité
- **MEA02** Surveiller, évaluer et estimer le système de Contrôle Interne
- **MEA03** Surveiller, évaluer et estimer la conformité avec les exigences externes

VAL IT RISK IT Nouveaux Processus

Détail des 37 Processus du référentiel

Un Processus

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

- •Description du Processus
- •Déclaration de la finalité du Processus
- •Les buts de l'IT et ses métriques
- •Les buts du Processus et ses métriques

Un RACI

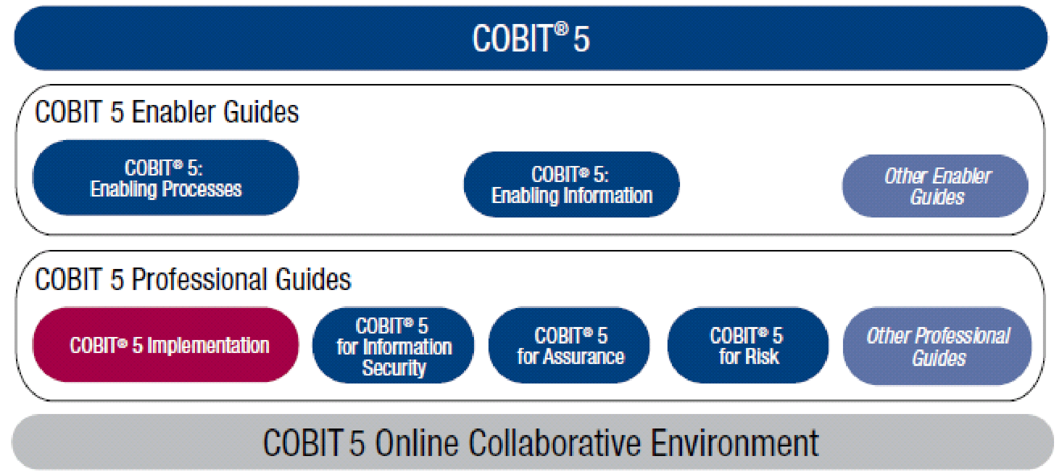
Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information 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

Les Input/out et Activités

EDM01 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
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.	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.				
Governance Practice	**Inputs**		**Outputs**	
	From	**Description**	**Description**	**To**
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.			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.				

Liens avec les autres référentiels

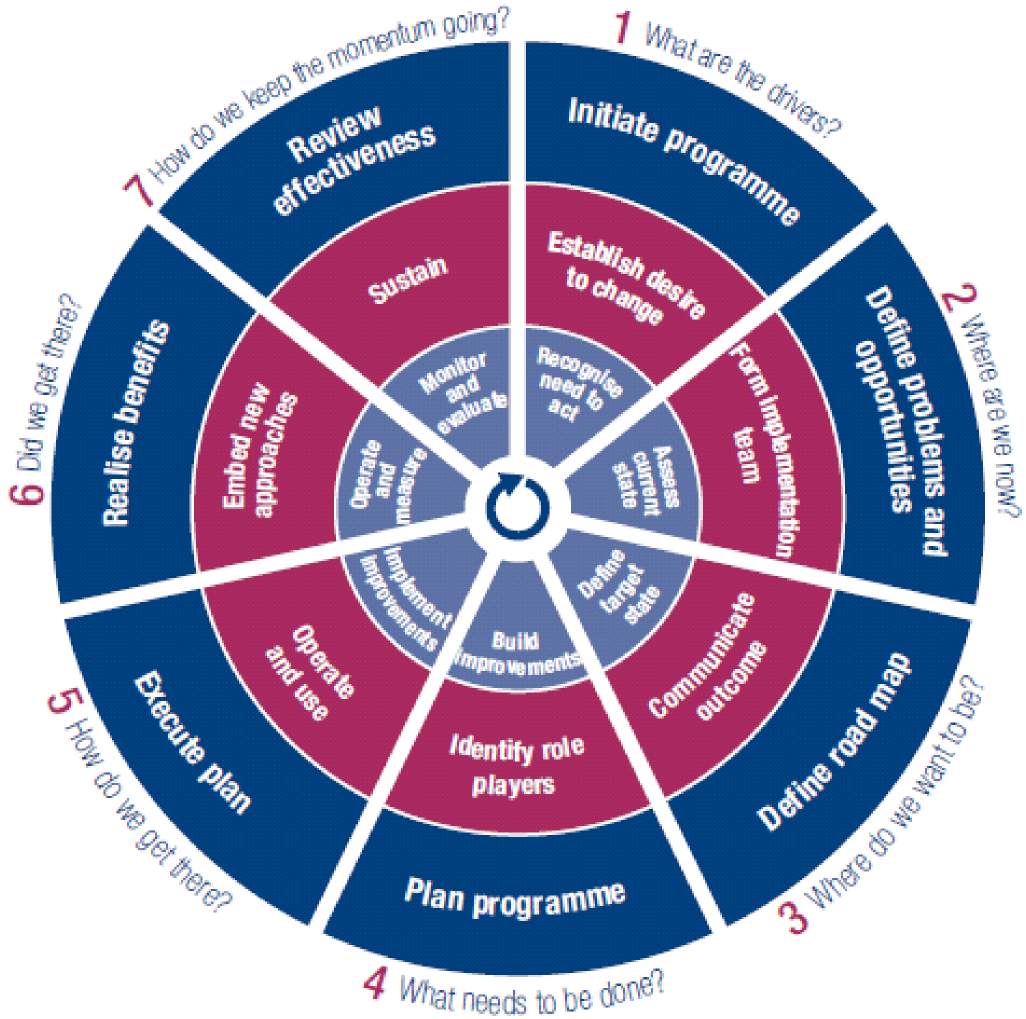
Related Standard	Detailed Reference
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	
ISO/IEC 38500	
King III	• 5.1. The board should be responsible for information technology (IT) governance. • 5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework.
Organisation for Economic Co-operation and Development (OECD)	Corporate Governance Principles



>Les publications

3. Mise en œuvre de COBIT5

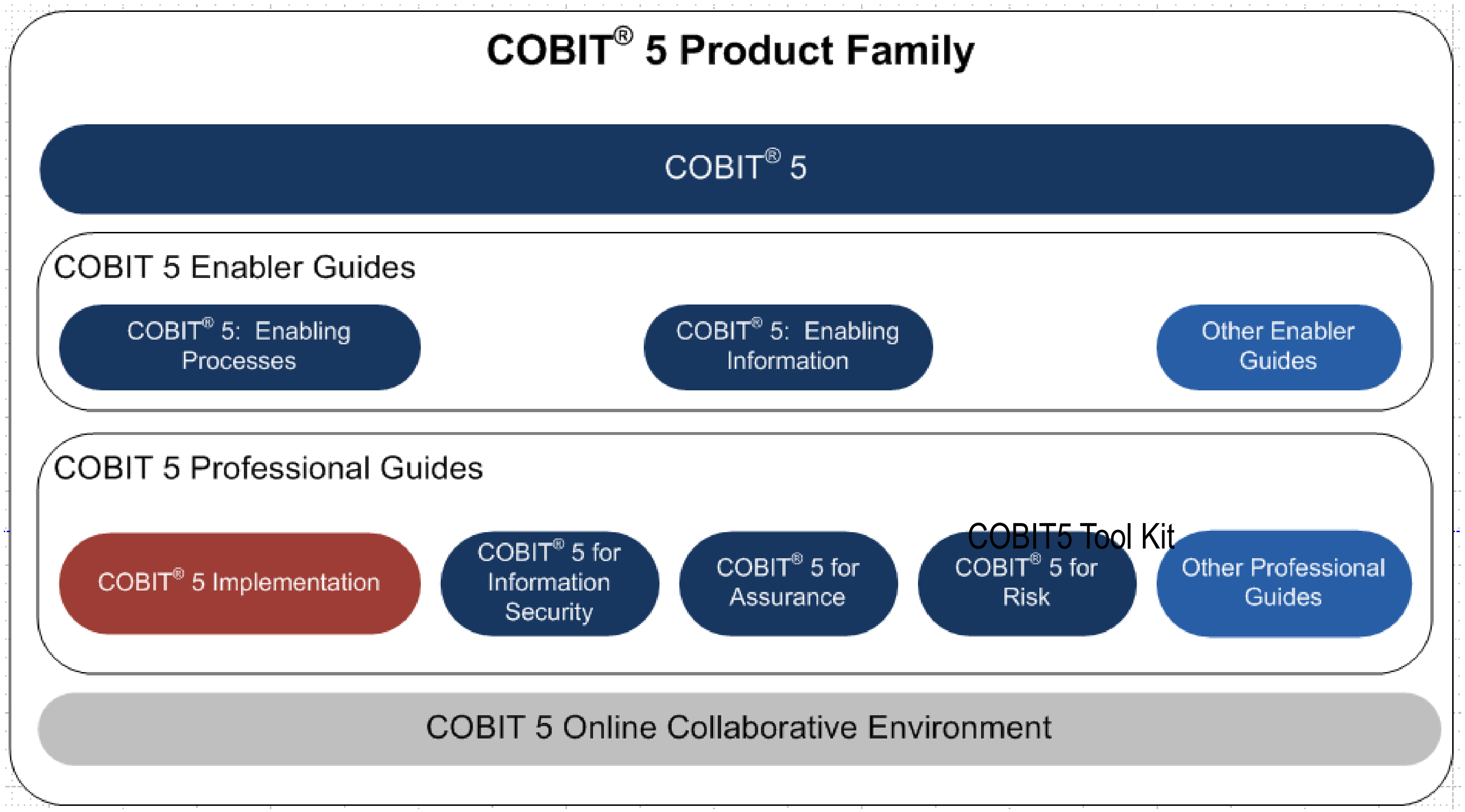
Implementation
L'approche du Cycle de Vie en 7 phases



- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

COBIT 5

Une famille de produits



Source : ISACA

4. Buts et métriques

- COBIT 5 suit le même concept d’objectifs et de métriques que COBIT 4.1, Val IT et Risk IT, mais sont renommés objectifs d’entreprise, objectifs IT et objectifs de processus reflétant ainsi les différents niveaux de vue de l’entreprise.

- COBIT 5 propose des objectifs en cascade basés sur les objectifs d’entreprise conduisant aux objectifs IT et supportés par des processus critiques.

- COBIT 5 fournit aussi des exemples d’objectifs et de métriques au niveau des pratiques de l’entreprise, des processus et du management. Ceci est un changement au regard de COBIT4.1, Val IT et Risk qui proposait cette démarche un niveau en dessous.

COBIT®5
AN ISACA® FRAMEWORK

Principe 1 : L'approche BSC et objectifs

Figure 5—COBIT 5 Enterprise Goals				
		Relation to Governance Objectives		
BSC Dimension	Enterprise Goal	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 environ			
	9. Information-based strategic decision making			
	10. Optimisation of service delivery costs			
Internal	11. Optimisation of business process functionality			
	12. Optimisation of business process costs			
	13. Managed business change programmes			
	14. Operational and staff productivity			
	15. Compliance with internal policies			
Learning and Growth	16. Skilled and motivated people			
	17. Product and business innovation culture			

Figure 6—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