



**Architecture
de
Sécurité**

INF 809

Architecture de sécurité

Notion de base

Cours 3

L'AE et SABSA

- Architecture d'entreprise
 - Simplification
 - Togaf
- Architecture de sécurité
 - Sabsa

Architecture d'entreprise

L'architecture d'entreprise est le processus qui consiste à transformer la stratégie d'entreprise ainsi que la vision de l'organisation en un portfolio de capacités technologiques, d'applications, d'information et de technologie qui permettront la réalisation de la stratégie et de la vision par la mise en place de feuilles de route précises.

- Assure l'alignement des stratégies d'entreprise et technologique en identifiant et permettant la réalisation des capacités d'affaire, garantissant que les investissements technologiques choisis soient alignés avec les objectifs de l'organisation
- Permet la création de feuille de route stratégique incluant les programmes clés pour soutenir l'atteinte des cibles d'affaire et des objectifs de l'organisation
- Permet la création d'une stratégie et d'une direction d'entreprise pour les technologies de l'information, grâce à une vigie structurée

Les principes sont des règles et des lignes directrices, destinés à être durables et rarement modifiés, qui informent et soutiennent la manière dont une organisation s'acquitte de sa mission. Selon l'organisation, les principes peuvent être établis à trois niveaux:

- **Entreprise:** Ces principes fournissent une base pour la prise de décision dans toute l'entreprise et informent comment l'organisation définit sa mission. Ces principes au niveau de l'entreprise se retrouvent couramment dans les organisations gouvernementales et à but non lucratif, mais également dans les organisations commerciales, en tant que moyen d'harmoniser la prise de décision dans l'organisation. Plus particulièrement, ils constituent un élément clé d'une stratégie de gouvernance d'architecture réussie.
- **Technologie de l'information (TI):** Ces principes fournissent des indications sur l'utilisation et le déploiement de toutes les ressources et actifs de l'entreprise. Ils sont conçus pour rendre l'environnement TI aussi productif et rentable que possible.
- **Architecture:** Ces principes sont un sous-ensemble des principes TI liés au travail d'architecture. Ils reflètent un niveau de consensus dans l'organisation et incarnent l'esprit et la pensée de l'AE. Les principes d'architecture peuvent être divisés principes qui gouvernent le processus d'architecture et/ou qui influencent le développement, la maintenance et l'utilisation de l'architecture d'entreprise.

Les différents principes d'architecture adoptés par l'organisation peuvent provenir de plusieurs sources différentes :

- ISO/IEC 27002:2013
- COBIT
- COSO
- Common Criteria
- ITIL
- FISMA
- ISF, ISM,
- NIST SP800's et NIST Cybersecurity Framework
- PCIDSS
- SABSA

Pour n'en nommer que quelques-uns. Pour développer une architecture solide, les principes doivent être définis clairement au niveau de l'entreprise, du domaine métier et au niveau des projets.

Architecture d'Entreprise

**Arch.
Affaire**

- Capacités
- Chaîne de valeur
- Information
- Organisation
- Parties prenantes
- Stratégies d'affaire
- Produits
- Actifs
- Initiatives
- Processus et règles d'affaire

**Arch.
Information**

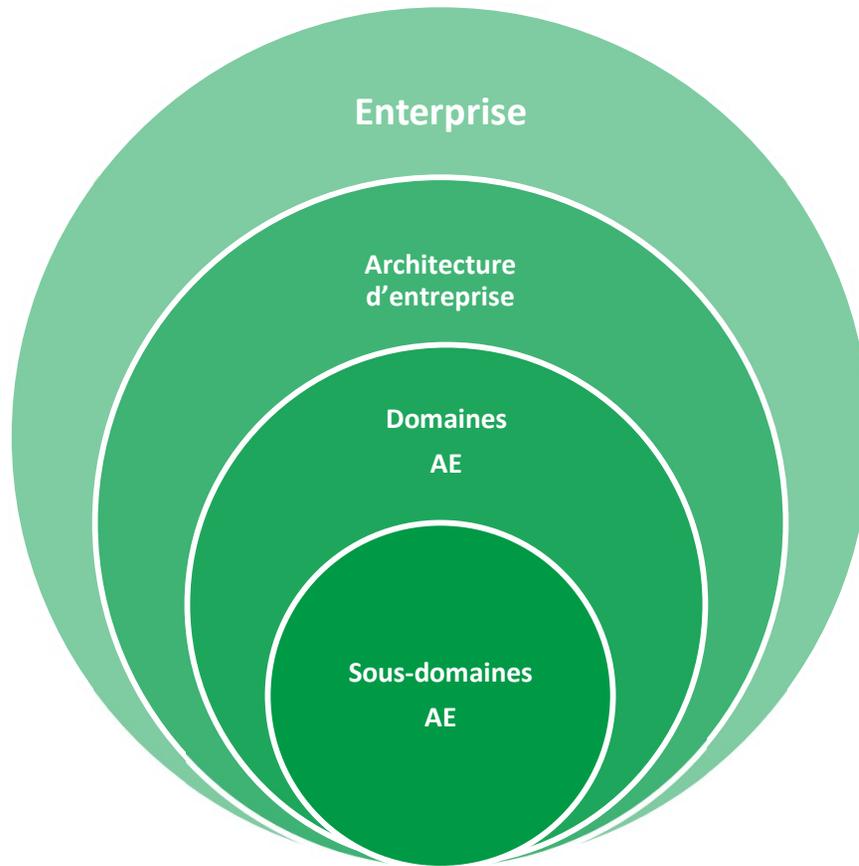
- Intégration des données
- Architecture des données
- MDM
- Tableau de bords et analytiques
- Intelligence d'affaire
- Modèles des données

**Arch.
Application**

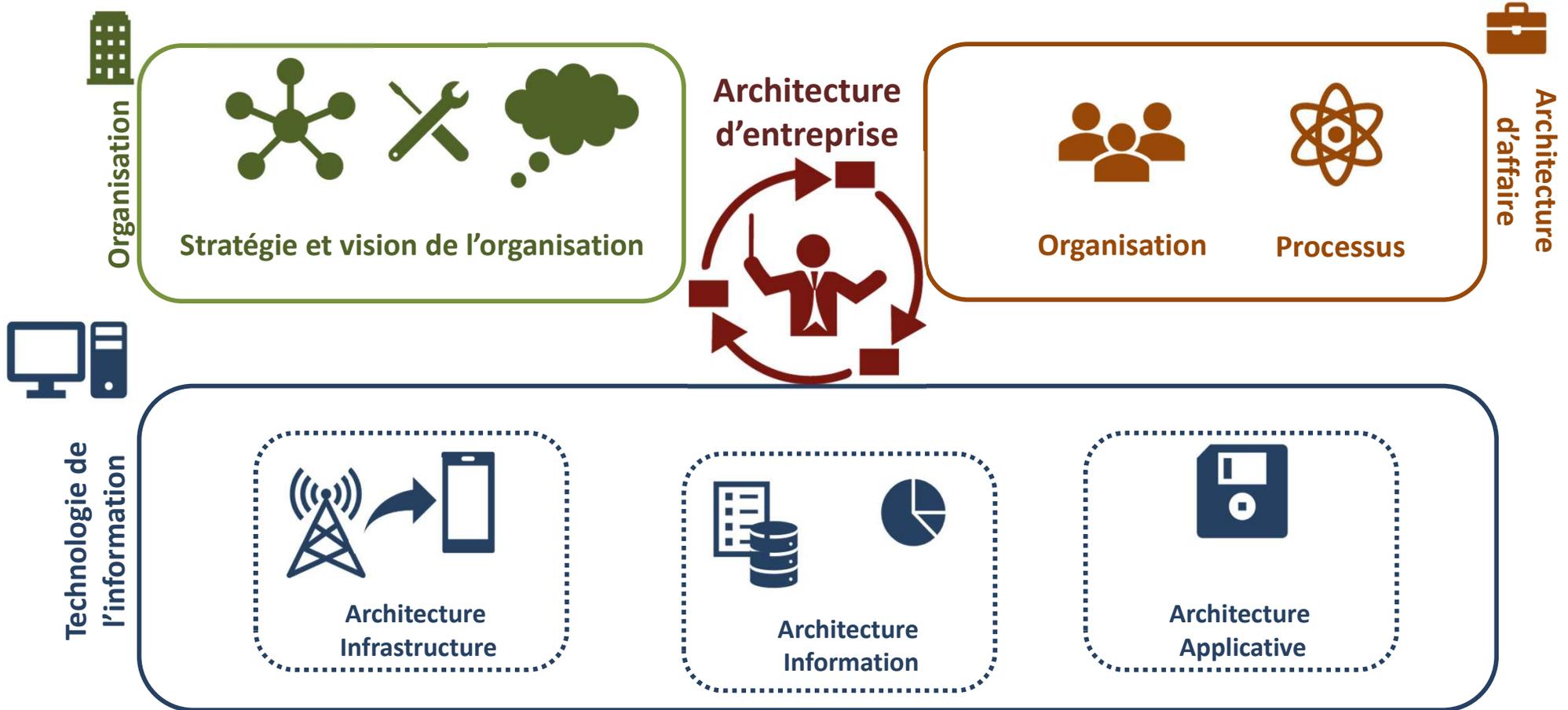
- Développement applicatif
- Définition des services
- Alignement des processus technologiques
- SOA
- MQ architecture
- Services

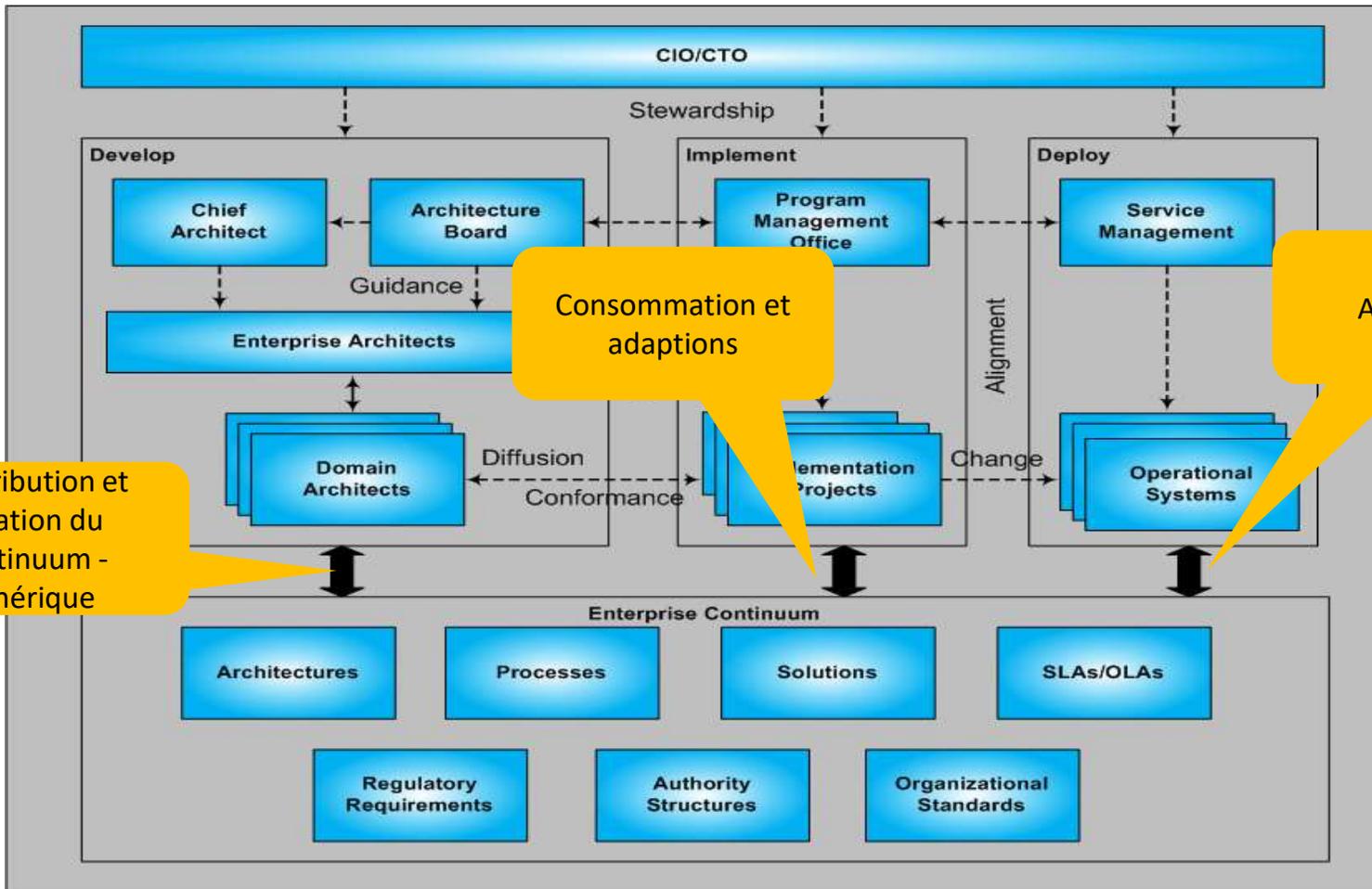
**Arch.
Infrastructure**

- Serveurs
- Réseau
- Télécommunication
- Systèmes d'exploitation
- Postes de travail
- Intergiciel
- SGBD
- Sécurité
- Stockage



L'approche des cercles concentriques permet une meilleure visualisation du rôle qu'exerce l'architecture d'entreprise face aux architectures métiers et à l'organisation





Contribution et création du continuum - générique

Consommation et adaptations

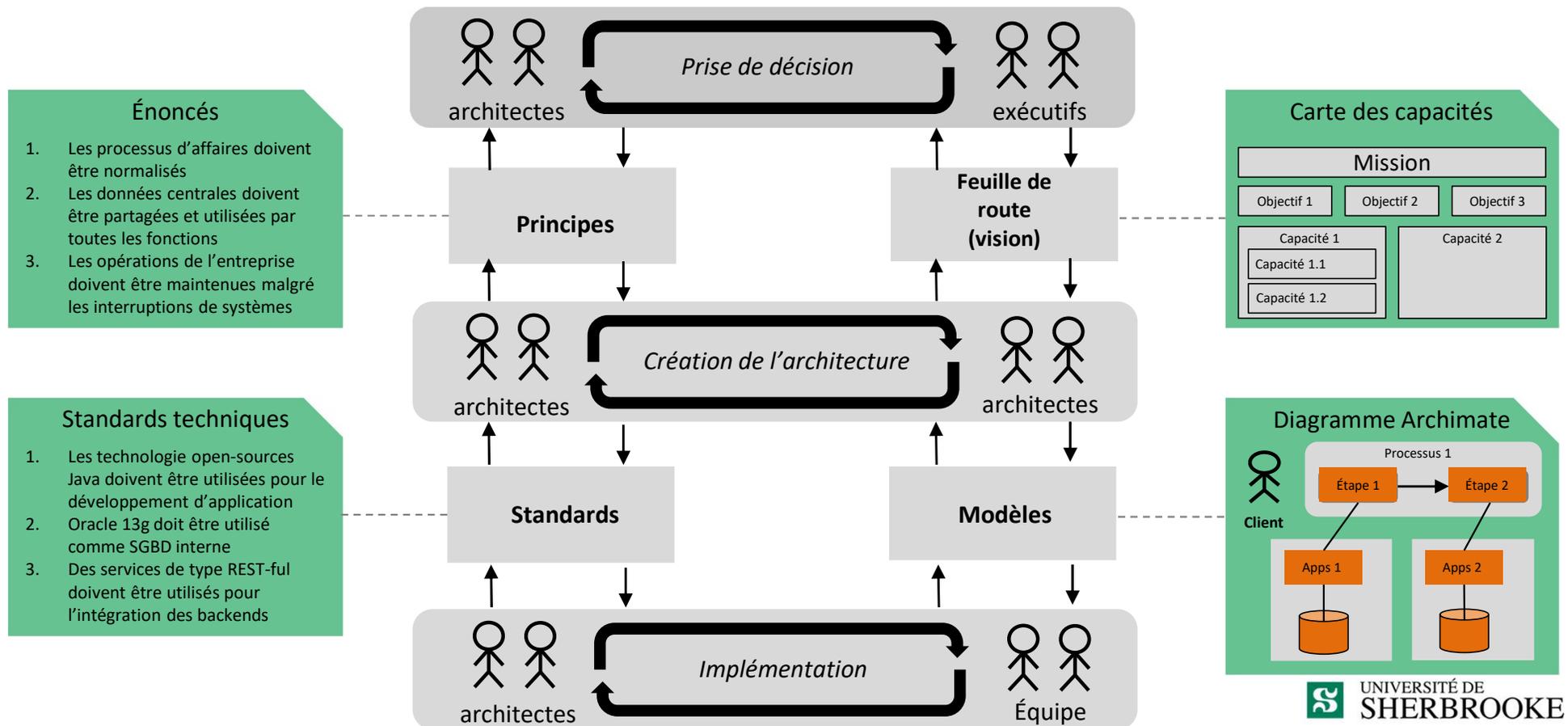
Alignement

- L'architecture d'entreprise est une pratique, pas un cadre de référence (e.g. Togaf, Zachman, Sabsa)
 - Il est important de comprendre que les cadres de référence disponible sur le marché ne reflète pas forcément ce qui est mis en place dans les organisation
 - Les cadres, si mis en place de manière intégrale, ne représente pas l'esprit d'agilité et d'efficacité que les organisations recherchent.
 - Lourdeur excessive
 - Complexité
 - Maintien de l'intégrité du cadre
- Généralement, l'AE se représente dans les organisations par 4 types fondamentaux de documents
 - La vision
 - Les différents principes directeurs
 - Les modèles (Building blocks, graph, etc)
 - Les standards

- Par contre, ces cadres représentent une excellente source de référence pour la mise en place d'une pratique efficace
 - Ils orientent ce que l'AE doit pouvoir accomplir pour une organisation

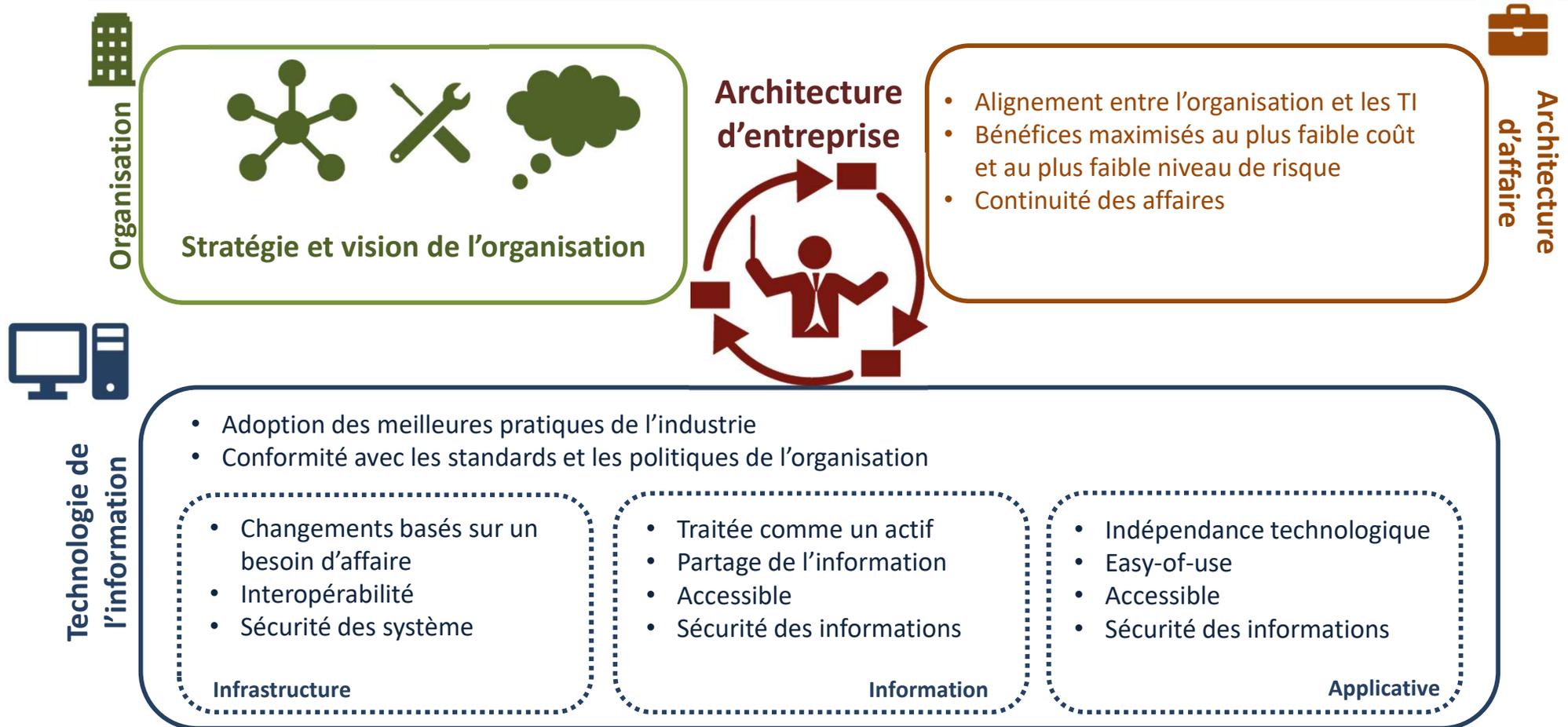
Par exemple* :

- Peu ou pas d'organisation vont suivre intégralement les étapes prescrites par la « architecture development method » ADM de TOGAF
- Les organisations n'ont aucun souhait à créer un modèle conceptuel décrivant leur organisation à la manière d'un immeuble, de manière très détaillée, tel que prescrit par Zachman et/ou SABSA



- Les principes peuvent être perçus comme des politiques de haut niveau
 - Aident à aligner le design des systèmes d'information à la philosophie de l'organisation
 - Aident à l'harmonie et l'homogénéité de l'écosystème TI
 - Permettent une meilleure gestion des investissements TI

Quelques exemples de principes d'AE...



Principle

Interoperability

Description

Software and hardware must follow established standards that promote data, application, and technology interoperability.

Rationale

Standards help ensure coherence, thus improving the ability to manage systems, raise user satisfaction, and protect current IT investments, thus maximizing return on investment and reducing costs.

Interoperability standards also help ensure support from several suppliers to their respective products, thus facilitating integration.

Implications

Interoperability and industry standards must be followed unless there is a mandatory business reason to implement a non-standard solution.

A process to establish standards, periodic revision, and exceptions must be established.

Current IT platforms must be identified and documented.

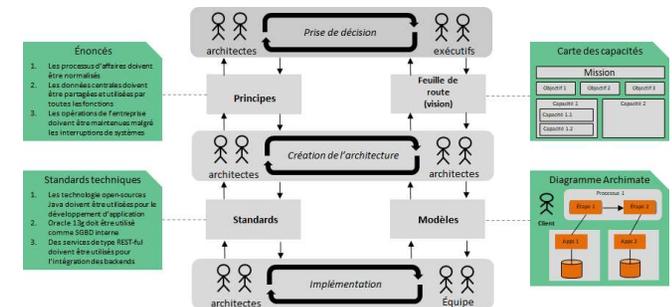
- Les feuilles de route (visions) sont des documents abstraits orientés sur les besoins d'affaire
 - Capability Mapping
 - Une capacité (*capability*) représente l'habilité d'une organisation effectuer une activité qui générera un extrant de valeur pour celle-ci
 - Les feuilles de route établies au niveau stratégique permettent d'avoir une vision de comment nous souhaitons faire évoluer les capacités technologiques et les architectures de ces capacités
 - Planification stratégique à long terme des aspirations TI en fonction des besoins d'affaire

Exemple : Migration vers SAP HANA (High performance Analytic Appliance)

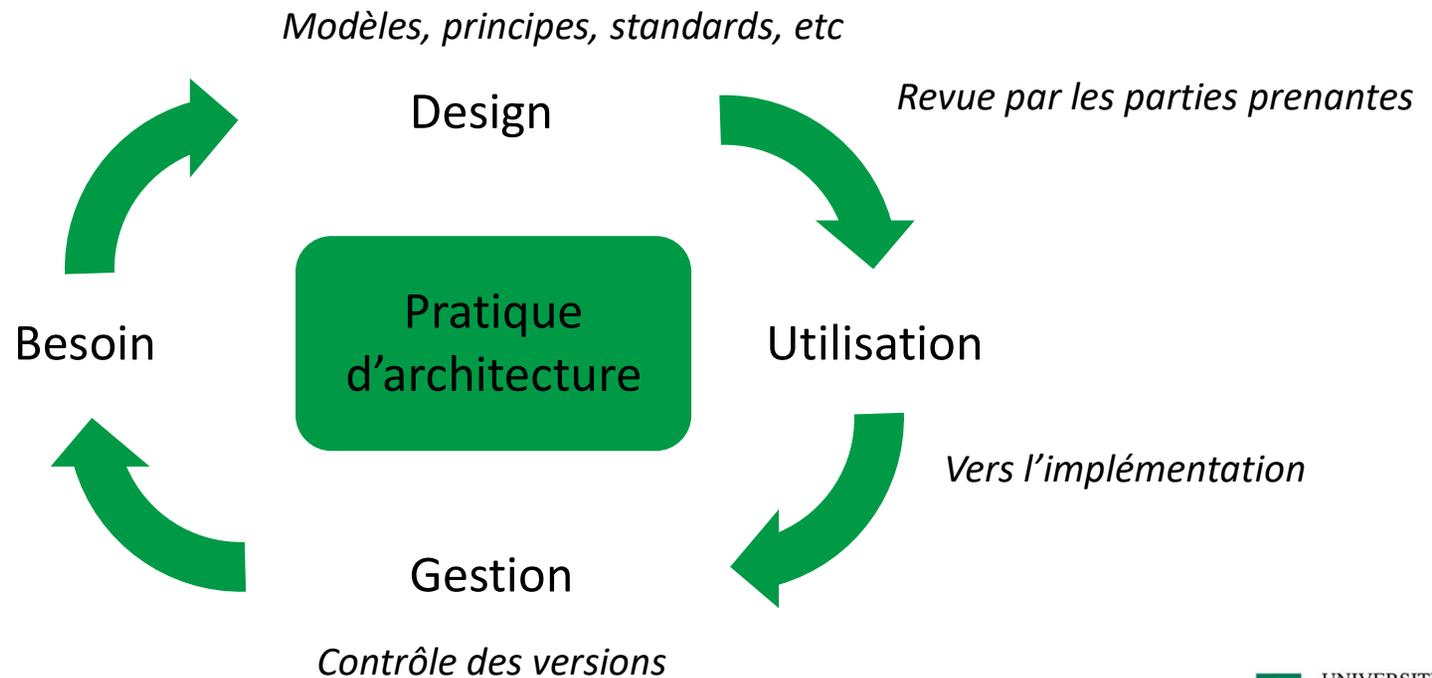
- Les standards technologiques sont des documents pour supporter la mise en place des technologies
 - Aident à limiter l'étendue des technologies qui devront être supportées
 - Favorisent l'uniformité de l'écosystème technologique
- Les modèles sont des diagrammes techniques détaillés
 - Permettent une meilleure sélection des options d'implémentation
 - Transmettent l'information pertinente dans un cadre tactique et/ou opérationnel

- Les *principes* et les *visions* sont des documents d'affaire
 - Simples et concis
 - Teneur stratégique pour l'organisation et les TI
 - Permettent aux gestionnaires des niveaux supérieurs de gérer l'environnement technologique efficacement
 - Interfaces entre l'organisation (sa conduite des affaires) et l'architecture
- Les standards et les modèles sont des documents TI
 - Purement technique
 - Orientations précises pour les spécialistes techniques
 - Interfaces entre les architectes d'entreprise, les architectes de solution et les équipes d'implémentation

- Les processus
 - Prise de décision
 - Le processus où les leaders et les architectes conviennent sur comment l'organisation doit fonctionner et où les investissements technologiques doivent être fait.
 - Les artéfacts de types Principes et Visions reflèteront les décisions qui ont été prises
 - Activités d'architecture
 - Le processus par lequel les architectes traduisent les décisions d'affaire en standards et en modèles afin de les rendre utilisable par les équipes d'implémentation
 - Implémentation
 - La réalisation et la mise en place de l'architecture

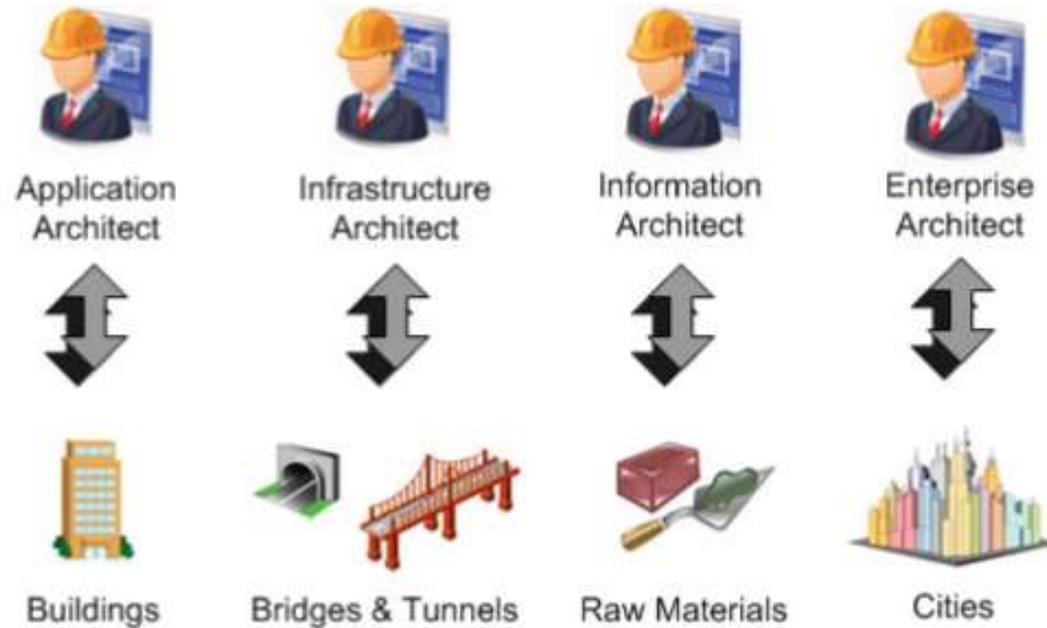


- AE n'est pas statique, elle est en constante évolution



- Imaginons que l'architecture d'entreprise est une ville. Alors son but serait de définir son infrastructure pour répondre aux besoins présents et futurs de sa population et d'assurer que celle-ci puisse s'adapter et évoluer selon les besoins des sa population.

Éléments d'architecture	Utilisation	Analogie - Ville
Feuille de route (Visions)	Stratégie TI à utiliser pour l'entreprise	Vision de la ville basée sur les besoins de ses résidents
Principes	Ligne directrice pour les investissements et le design	Zonage et code du bâtiment afin d'assurer la qualité et la constance
Building Blocks	Éléments standards HLD	Spécification des éléments préfabriqués des bâtiments
Modèle		Les plans de l'œuvre, selon différentes vues (coté, haut, bas, étage 1, étage 2)
Standards	Lignes directrices techniques à suivre	Code des bâtiments – Plomberie/Électricité/etc
Processus de gestion	Processus pour permettre les changements à l'arch.	Processus pour changer les plans de la ville ou soutenir les variances dans les T.Q.C.
Transition et planning	Priorisation des projets	Amélioration au plan de la ville



TOGAF

<http://pubs.opengroup.org/architecture/togaf91-doc/arch>

- ▶ TOGAF est un cadre d'architecture - The Open Group Architecture Framework (www.opengroup.org), ce n'est pas une pratique d'architecture ou une architecture
- ▶ TOGAF est un outil d'aide à l'intégration, à la production, à l'utilisation, et à la maintenance de l'architecture d'entreprise.
- ▶ La première version de TOGAF, développée en 1995, était basée sur le cadre d'architecture technique du ministère de la Défense des États-Unis pour Gestion de l'information (TAFIM – réf. Cours 1).
- ▶ La clé de TOGAF est sa méthodologie ADM (Architecture Development Method) pour développer une AE qui répond aux besoins de l'organisation.

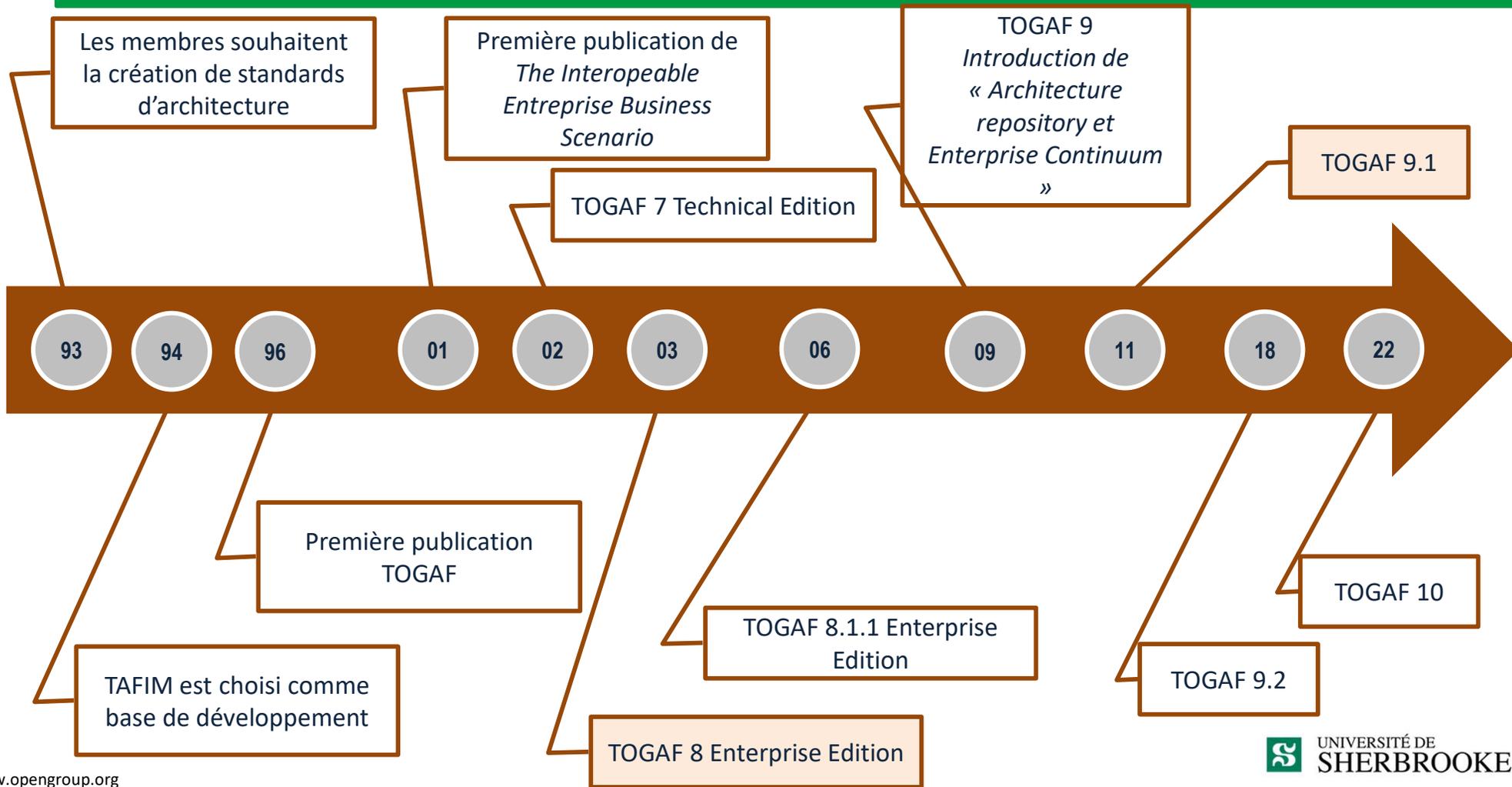
- ▶ Une méthodologie et un cadre d'architecture d'entreprise éprouvés utilisés par les principales organisations du monde pour améliorer l'efficacité de leurs activités
- ▶ La norme d'architecture d'entreprise la plus connue, assurant la cohérence des normes, des méthodes et des communications entre les professionnels de l'architecture d'entreprise
- ▶ Les professionnels de l'architecture d'entreprise maîtrisant les normes TOGAF jouissent d'une crédibilité, d'une efficacité d'emploi et de perspectives de carrière accrues.
- ▶ TOGAF aide les praticiens à éviter de s'enfermer dans des méthodes propriétaires, à utiliser les ressources de manière plus efficace et rentable et à obtenir un meilleur retour sur investissement.

Pour le cadre TOGAF, le terme «architecture» a deux significations en fonction du contexte:

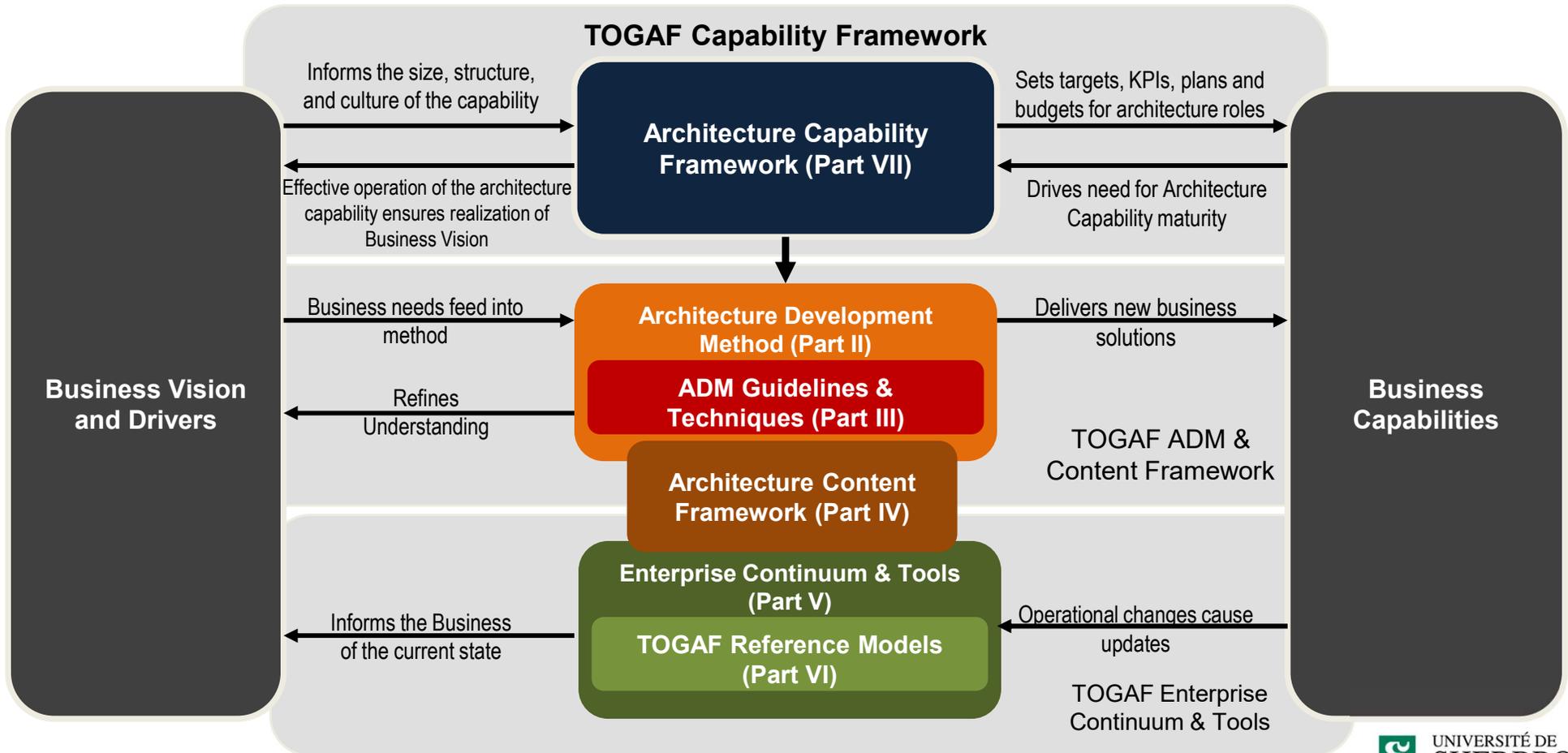
- ▶ Une description formelle d'un système ou un plan détaillé du système au niveau des composantes pour guider sa mise en œuvre.
- ▶ La structure des composants, leurs interrelations et les principes et directives régissant leur conception et leur évolution sur temps.

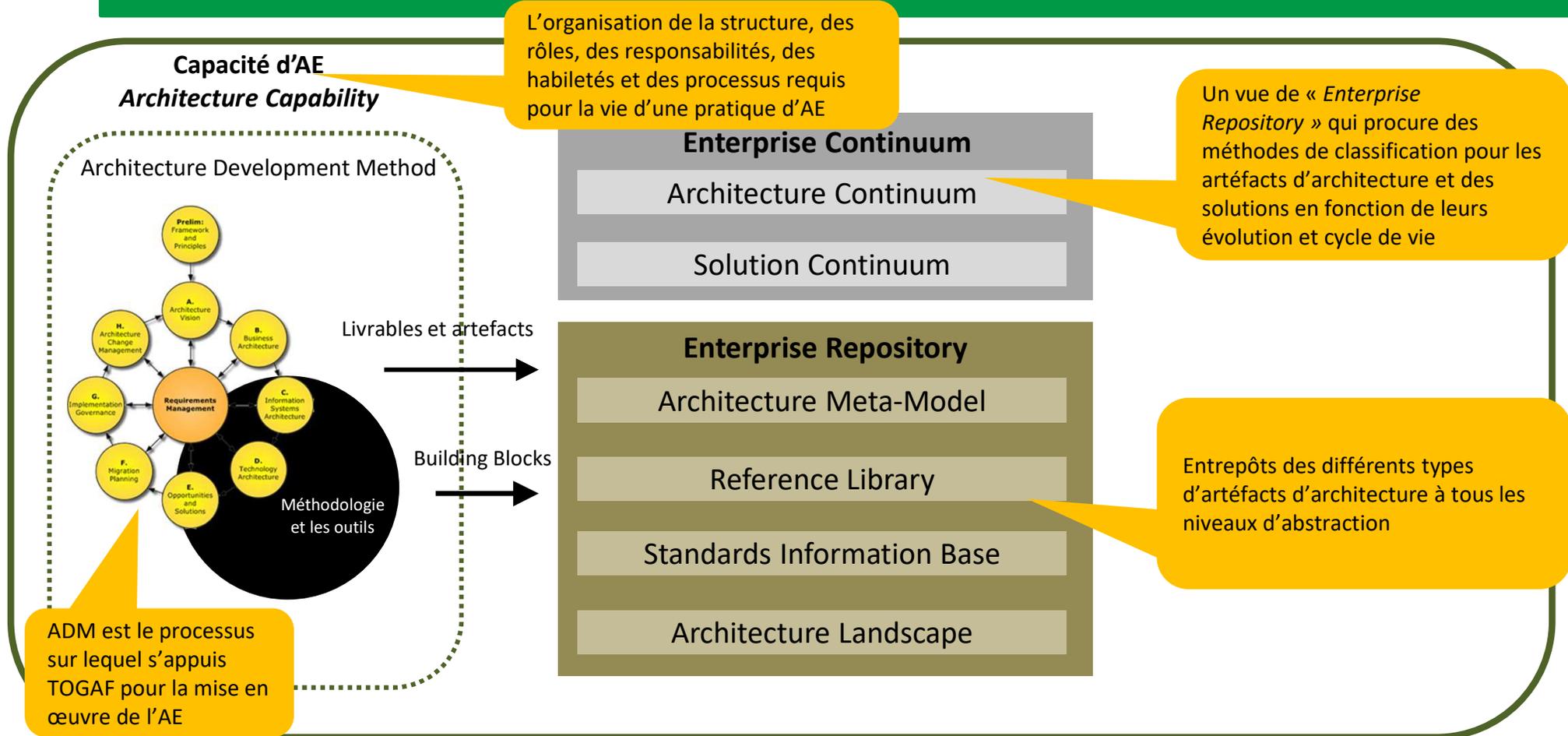
- **Activity:** A task or collection of tasks that support the functions of an organization; for example, a user entering data into an IT system or traveling to visit customers.
- **Application :**A deployed and operational IT system that supports business functions and services; for example, a payroll. Applications use data and are supported by multiple technology components but are distinct from the technology components that support the application.
- ★ - **Building Block :**Represents a (potentially re-usable) component of business, IT, or architectural capability that can be combined with other building blocks to deliver architectures and solutions.
- **Architecture Building Block (ABB) :**A constituent of the architecture model that describes a single aspect of the overall model.
- **Architecture Continuum :**A part of the Enterprise Continuum. A repository of architectural elements with increasing detail and specialization. This Continuum begins with foundational definitions such as reference models, core strategies, and basic building blocks. From there it spans to Industry Architectures and all the way to an organization's specific architecture.
- ★ - **Architecture Development Method (ADM) :**The core of TOGAF. A step-by-step approach to develop and use an enterprise architecture.
- **Architecture Domain :**The architectural area being considered. There are four architecture domains within TOGAF: Business, Data, Application, and Technology.
- **Architecture Framework :**A foundational structure, or set of structures, which can be used for developing a broad range of different architectures. It should contain a method for designing an information system in terms of a set of building blocks, and for showing how the building blocks fit together. It should contain a set of tools and provide a common vocabulary. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks.
- **Architecture View :** A *view* is a representation of a system from the perspective of a related set of concerns. A view is what you see (or what a stakeholder sees). Views are specific.

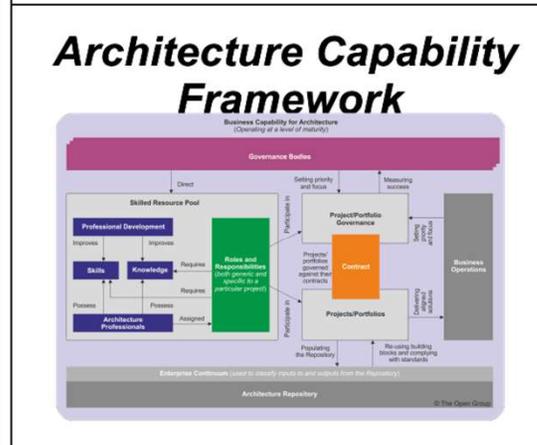
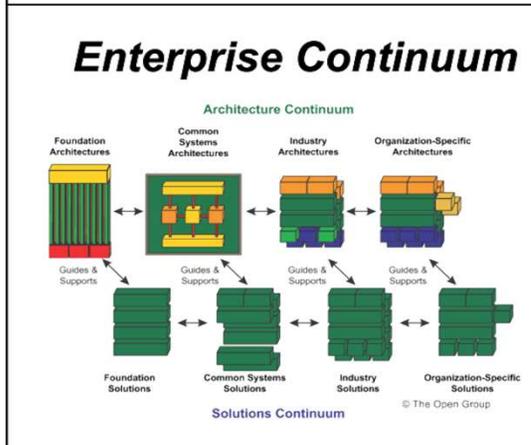
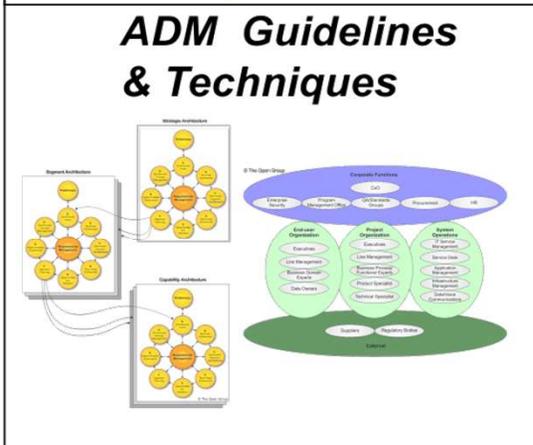
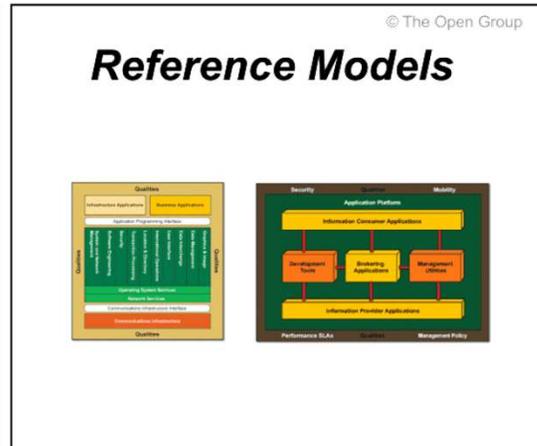
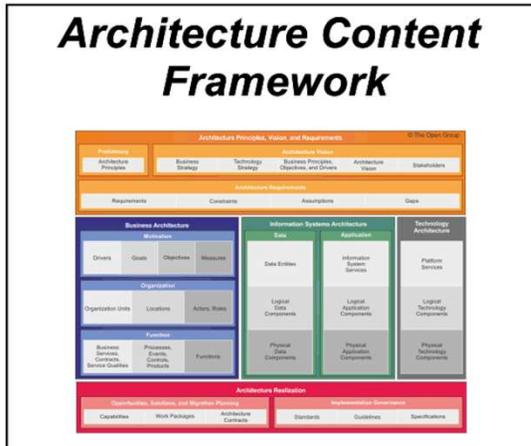
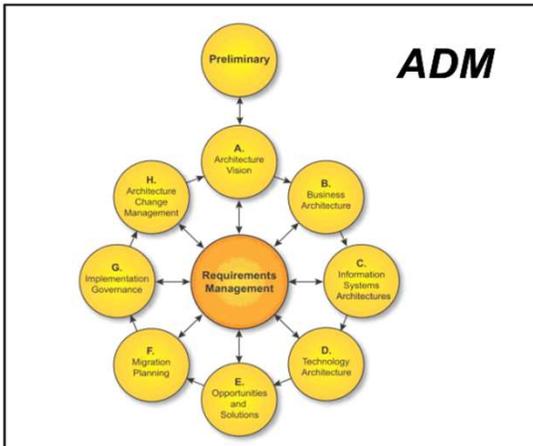
- **Architecture Viewpoint**: where you are looking from; the vantage point or perspective. Viewpoints are generic. A model (or description) of the information contained in a view.
- **Architecture Vision** : A high-level, aspirational view of the Target Architecture. A phase in the ADM which delivers understanding and definition of the Architecture Vision Level of granularity of work to be done.
- **Baseline** :A specification that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development or change and that can be changed only through formal change control procedures or a type of procedure such as configuration management.
- **Baseline Architecture** :The existing defined system architecture before entering a cycle of architecture review and redesign.
- **Business Governance** :Concerned with ensuring that the business processes and policies (and their operation) deliver the business outcomes and adhere to relevant business regulation.
- **Capability** :An ability that an organization, person, or system possesses. Capabilities are typically expressed in general and high-level terms and typically require a combination of organization, people, processes, and technology to achieve; or example, marketing, customer contact, or outbound telemarketing.
- **Concerns** :The key interests that are crucially important to the stakeholders in a system, and determine the acceptability of the system. Concerns may pertain to any aspect of the system's functioning, development, or operation, including considerations such as performance, reliability, security, distribution, and evolvability. Longer lasting than problem (eg. state of the economy), not a requirement, which is short term.
- **Enterprise** : The highest level (typically) of description of an organization and typically covers all missions and functions. An enterprise will often span multiple organizations.
- A "**pattern**" has been defined as: "an idea that has been useful in one practical context and will probably be useful in others" [*Analysis Patterns - Re-usable Object Models*].

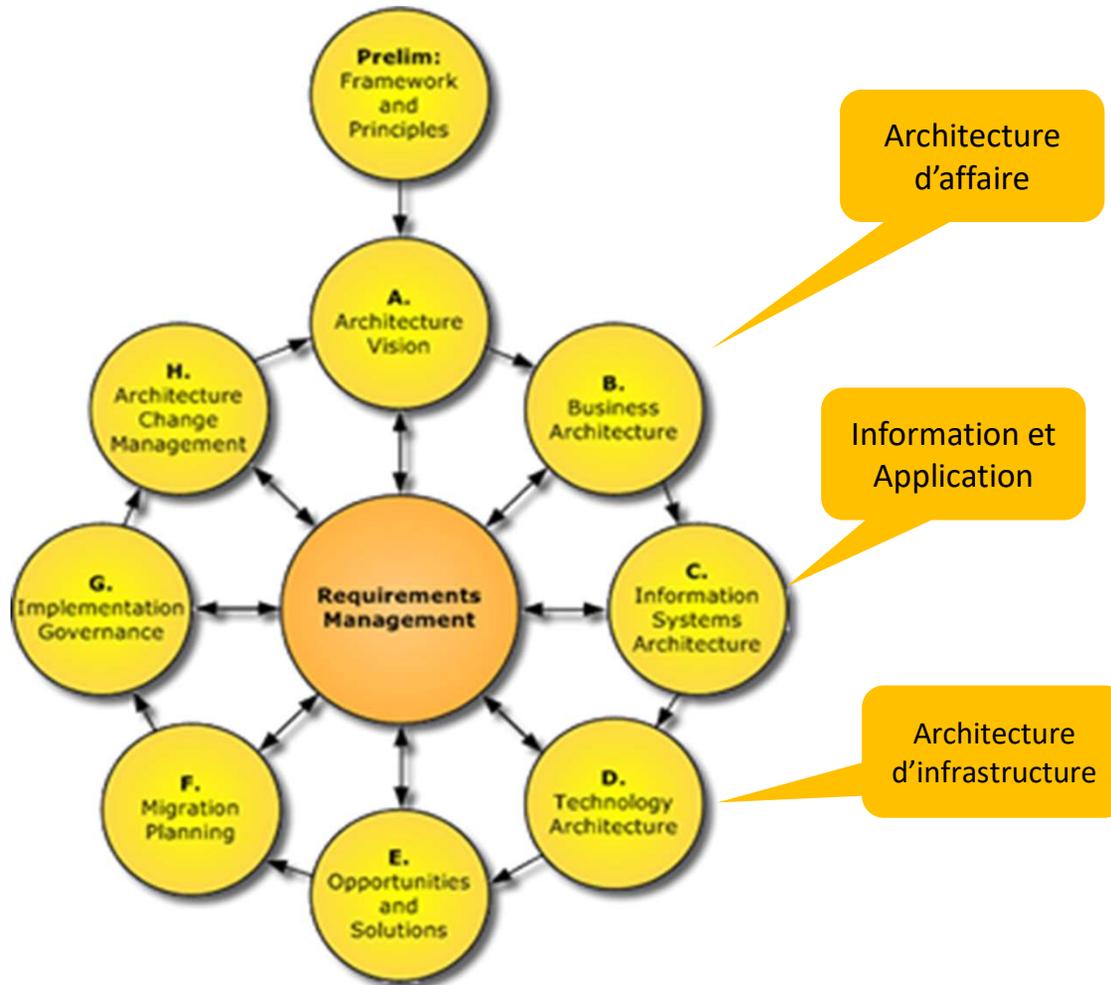


- ▶ TOGAF est un standard ouvert, qui n'est pas lié à un fournisseur, à une gamme d'outil ou à une technologie. Il est libre d'influence commerciale.
- ▶ Permet d'avoir à réinventer la roue pour développer une pratique d'AE
- ▶ Très orienté sur l'organisation et permet un alignement fort avec les TI
- ▶ Basé sur plus des meilleures pratique de l'industrie en AE
- ▶ Il est possible et simple de participer au développement du cadre
- ▶ C'est gratuit
- ▶ Adaptable pour répondre aux besoins de l'industrie
- ▶ Complémentaire à d'autres cadres de référence (e.g. SABSA)
- ▶ C'est compréhensible

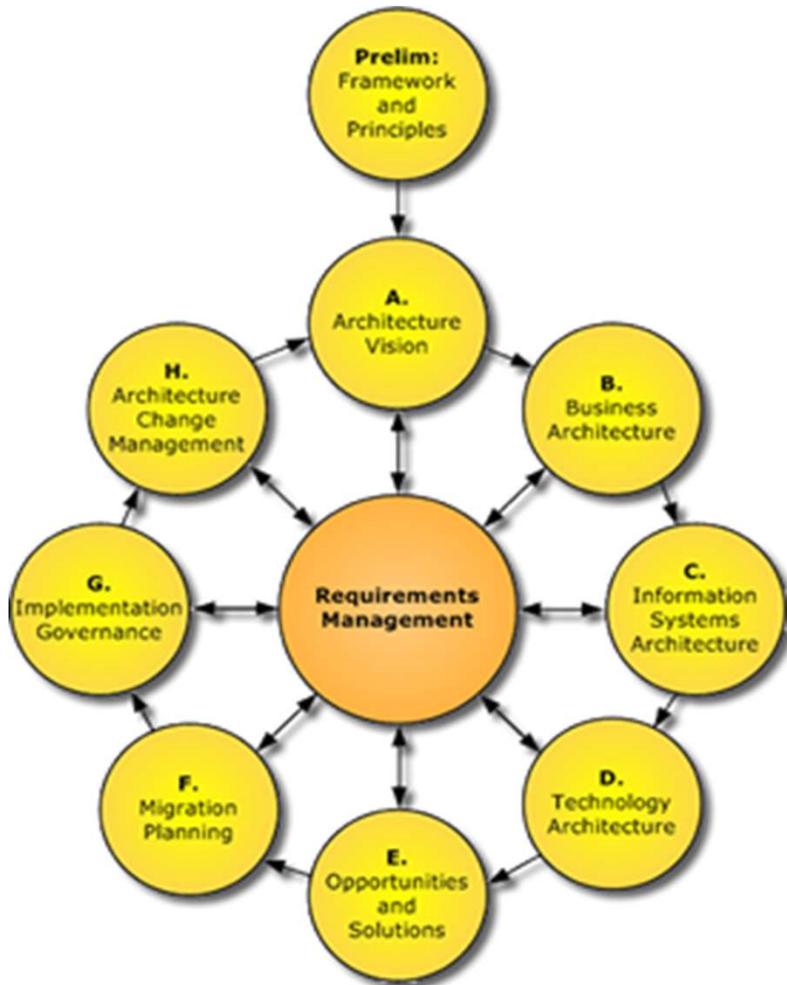








- L'ADM de TOGAF est considéré comme une méthodologie "framework-agnostic". Elle permet l'utilisation d'autres cadres possiblement déjà déployés dans les organisations tout en s'assurant d'offrir une structure et une cohérence à la pratique d'AE.
- Le cœur de TOGAF
- Une méthode éprouvée permettant de développer une pratique solide d'architecture
- Spécialement créée pour prendre en compte les requis d'affaire
- Une méthode itérative
- Un ensemble de vue d'architecture afin de s'assurer que les ensembles de requis complexes pourront être adressés



Il s'agit d'une méthode itérative, sur l'ensemble du processus (circulaire), entre chacune des phases et au sein de chacune des phases.

À chaque itération, de nouvelles décisions peuvent être prise:

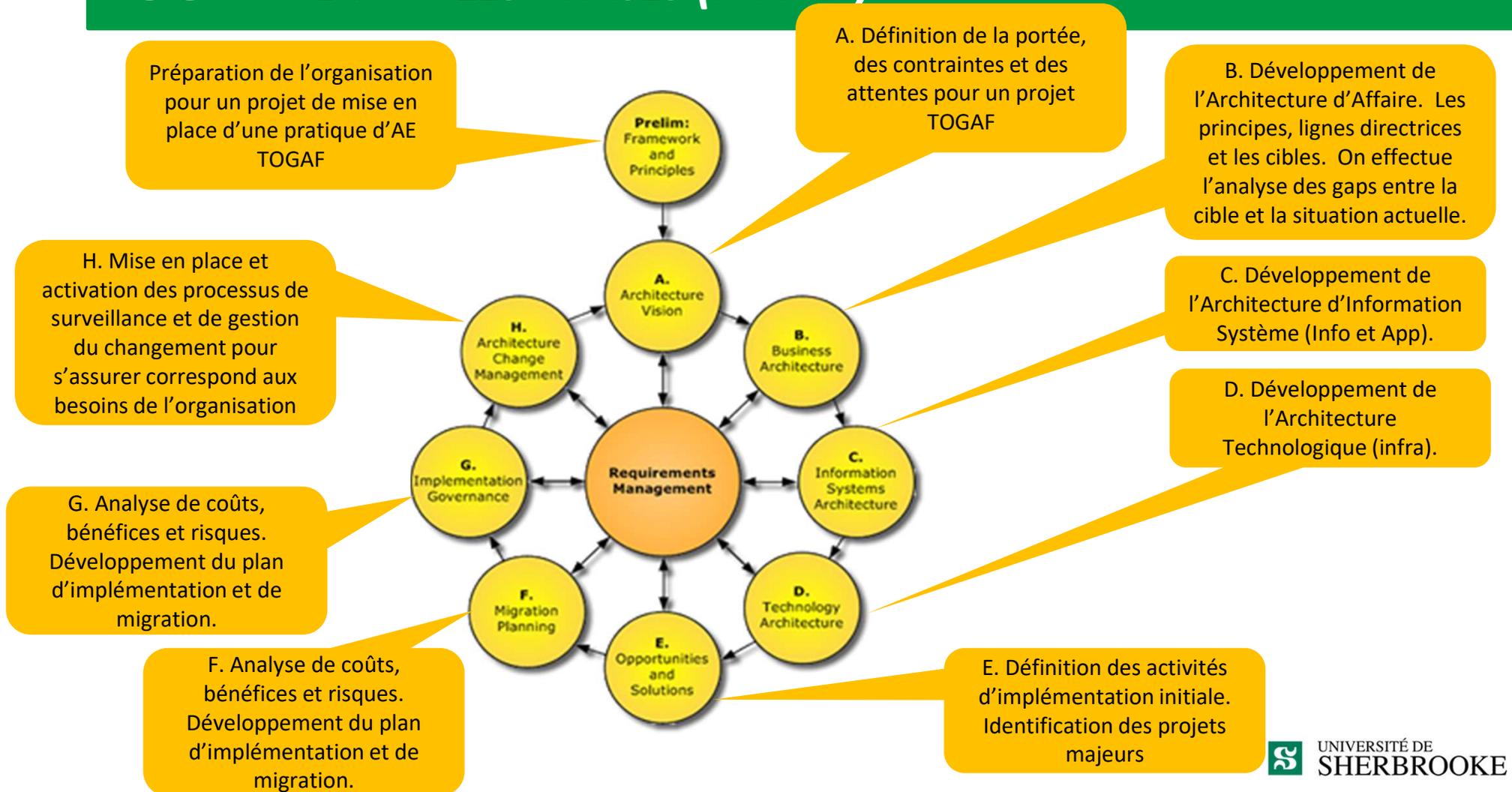
- Couverture d'entreprise
- Niveau de détail
- Horizon temporel

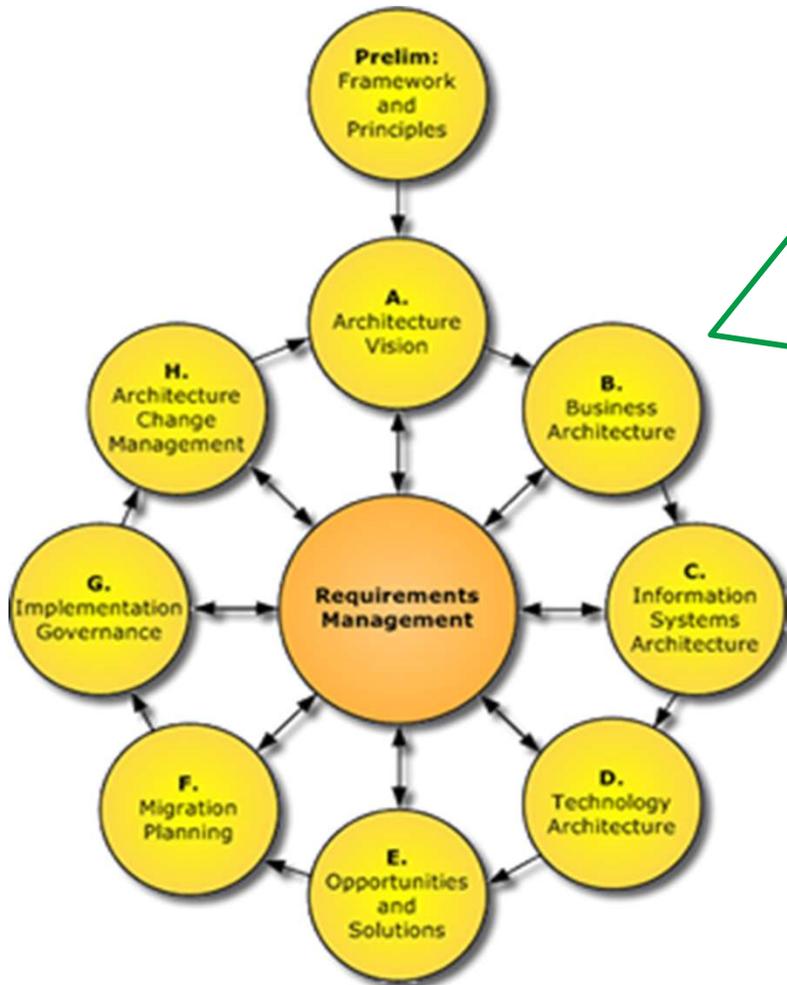
La méthodologie favorise la réutilisation naturelle des actifs d'architecture:

- Itérations précédentes d'ADM
- Autres cadres, modèles de système, modèles industriels, etc.

Les considérations décisionnelles sont

- Compétence
- Disponibilité des ressources
- Valeur revenant à l'entreprise



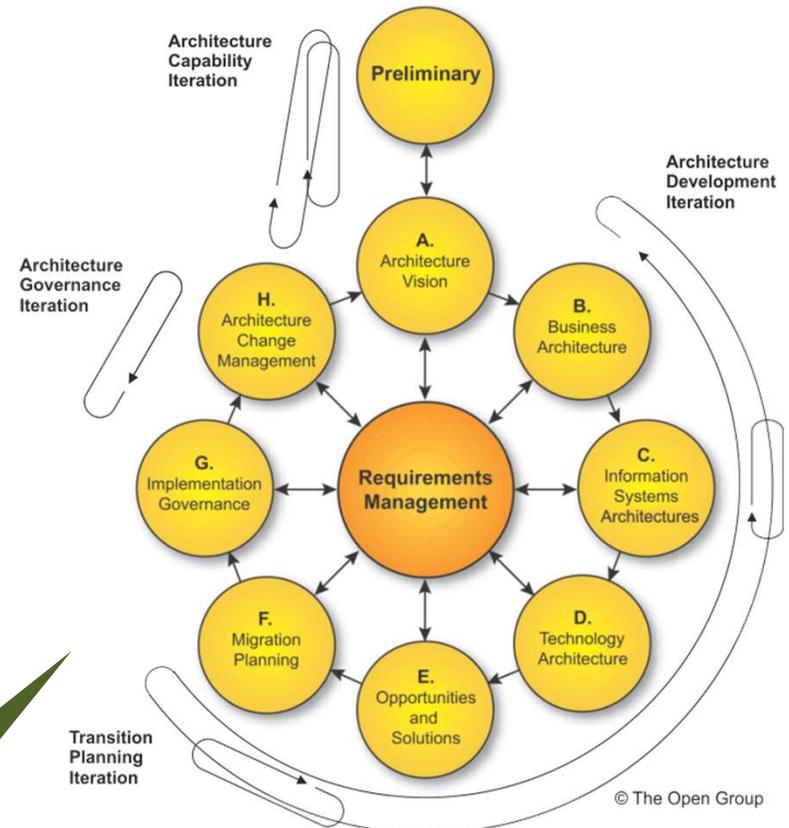


9. Création du document décrivant la pratique d'architecture métier
9. Création...
8. Finalisation
7. Revue des partis prenantes
6. Résoudre les impacts du changement
5. Définir des candidats au roadmap
4. Analyse de gap
3. Créer la cible
2. Développer la description de l'architecture actuelle
1. Choisir les modèles de référence, les outils et les vues.

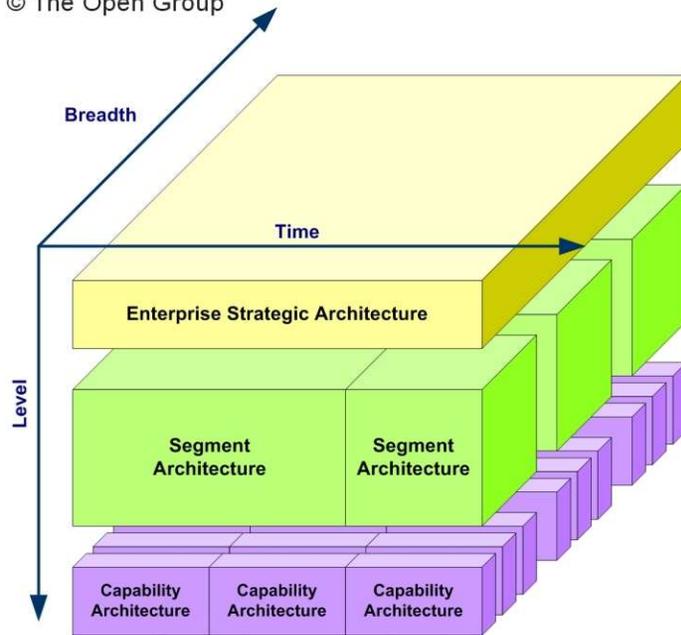
- ▶ Un ensemble de directives (*guidelines*) et de techniques pour soutenir l'application du ADM
- ▶ Les directives aident à adapter le processus ADM à différents scénarios, y compris différents styles de processus (par exemple, l'utilisation de *plusieurs itérations*) et des exigences spécifiques (par exemple, la sécurité).
- ▶ Les techniques proposées prennent en charge des tâches spécifiques au sein du processus ADM (par exemple, la définition de principes, de scénarios d'entreprise, l'analyse des écarts, la planification de la migration, la gestion des risques, etc.).

- L'ADM soutient le concept d'itération de trois (3) manières:
 - Itération circulaire: l'ADM est présenté de manière circulaire. La fin d'une étape d'architecture alimente l'étape subséquente.
 - Itération entre les phases: TOGAF décrit le concept d'itération à travers différentes phases (e.g. le retour à l'architecture d'affaire une fois le cycle d'architecture technologique terminée).
 - Cycle d'une seule phase: TOGAF prend en charge l'exécution répétée d'une activités au sein d'une même phase ADM en tant que technique d'élaboration de contenu.

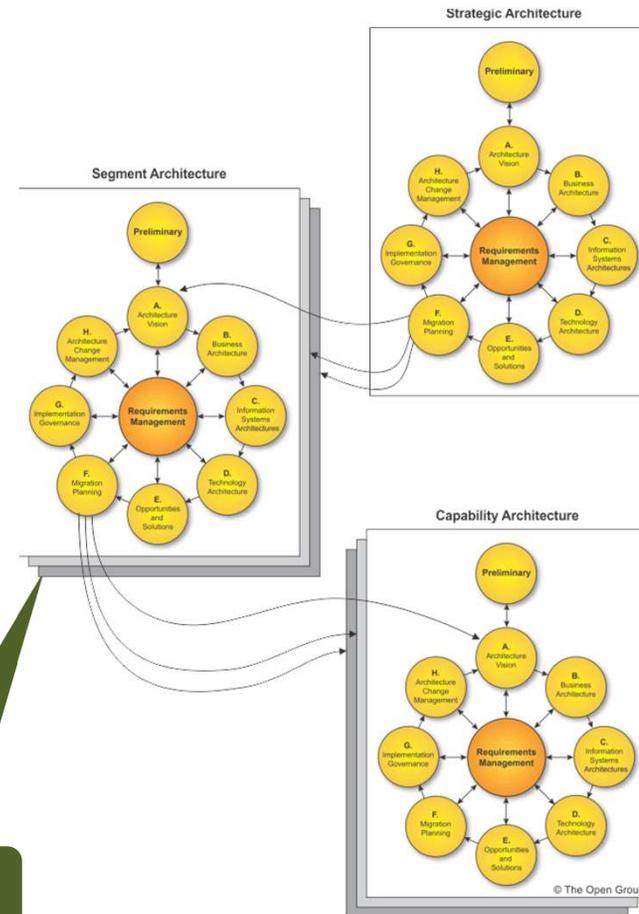
Exemple de guideline

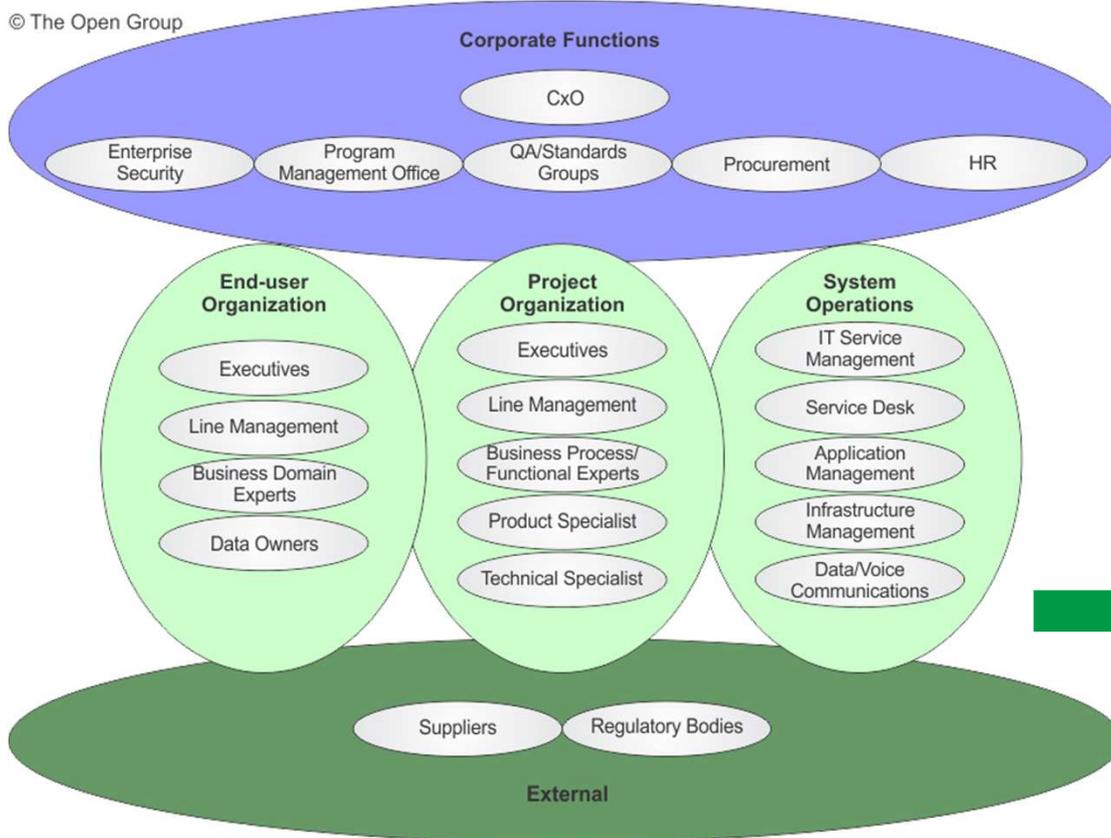


© The Open Group



Exemple de guideline





- Technique utilisé pour s'assurer le support des parties prenantes
- Devrait être fait à la phase A

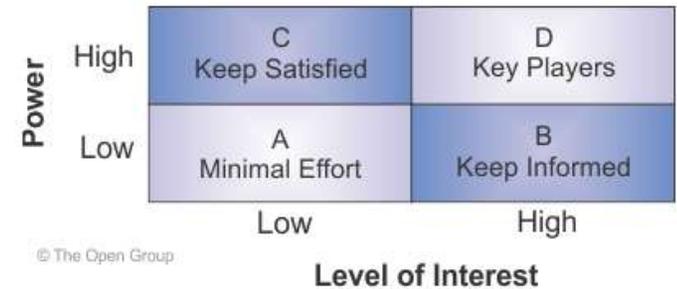
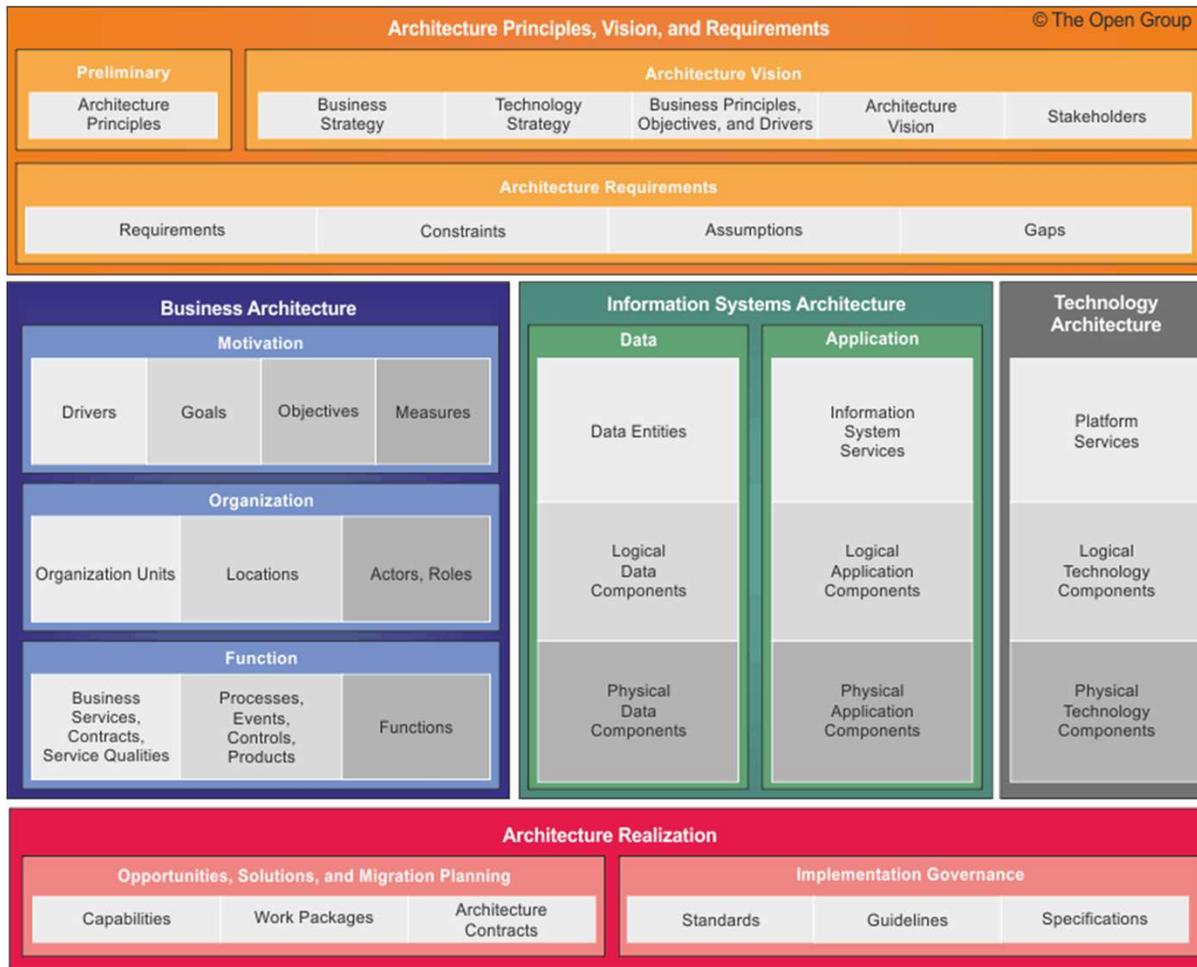


Figure 24-2: Stakeholder Power Grid

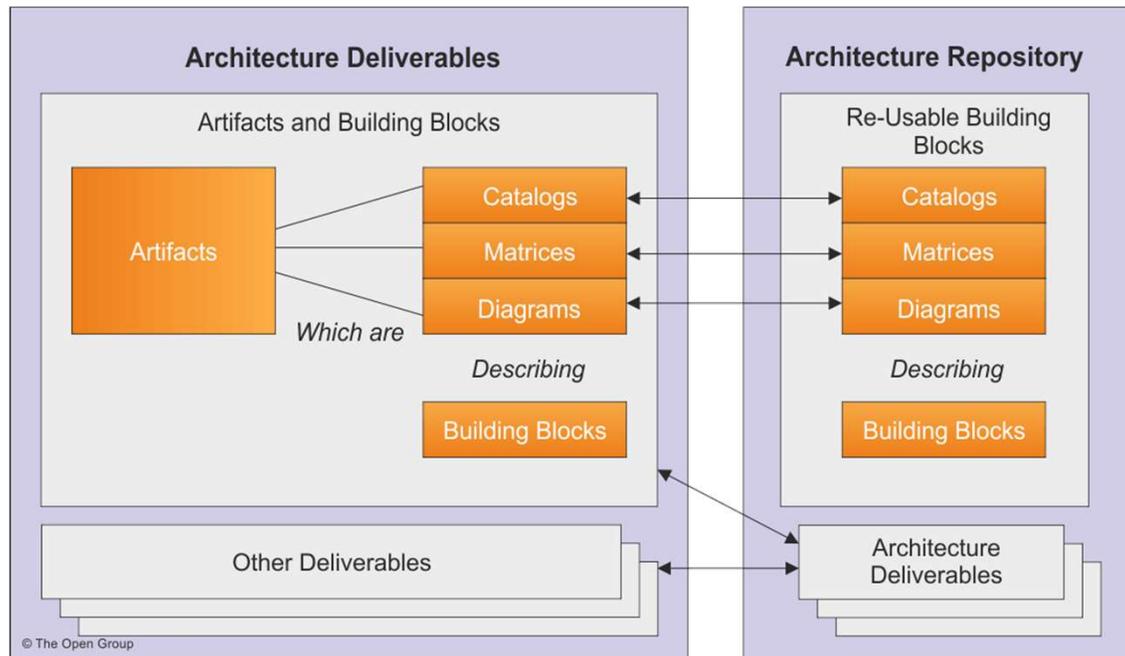


Fournit un modèle détaillé des extraits d'architecture, notamment :

- les livrables (*deliverables*)
- les artefacts contenus dans les produits livrables
- Les blocs de construction d'architecture (ABB) que les livrables représentent.

De plus, le CT :

- Il favorise une plus grande cohérence dans les résultats TOGAF produit.
- Il fournit une liste complète des extraits d'architecture.
- Il favorise une meilleure intégration des produits de travail
- Il fournit un standard ouvert détaillé sur la manière dont les architectures doivent être décrites
- Il comprend un métamodèle détaillé



Le *Architecture Content Framework* utilise 3 catégories pour décrire les extraits d'architecture, selon le contexte en cause

Deliverables (Bien livrables)

Produits formels

Selon l'entente contractuelle

Extraits de projets

Il peut contenir plusieurs artéfact

Artefacts

Produit précis qui décrit une architecture d'un point de vue spécifique

Par exemple: spécification de use-case, requis d'architecture, diagram réseau, etc

Classé selon :

Catalogs (liste de trucs),

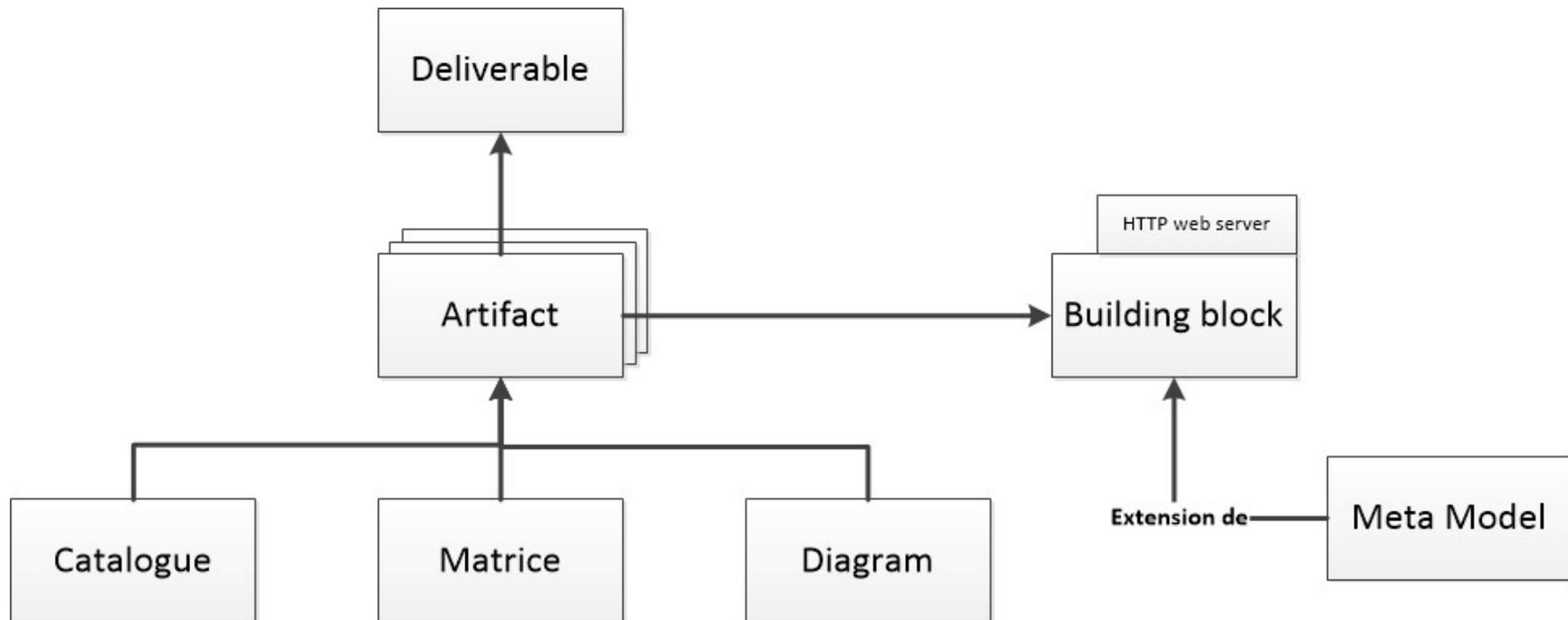
Matrices (représentation des relations entre les trucs) or

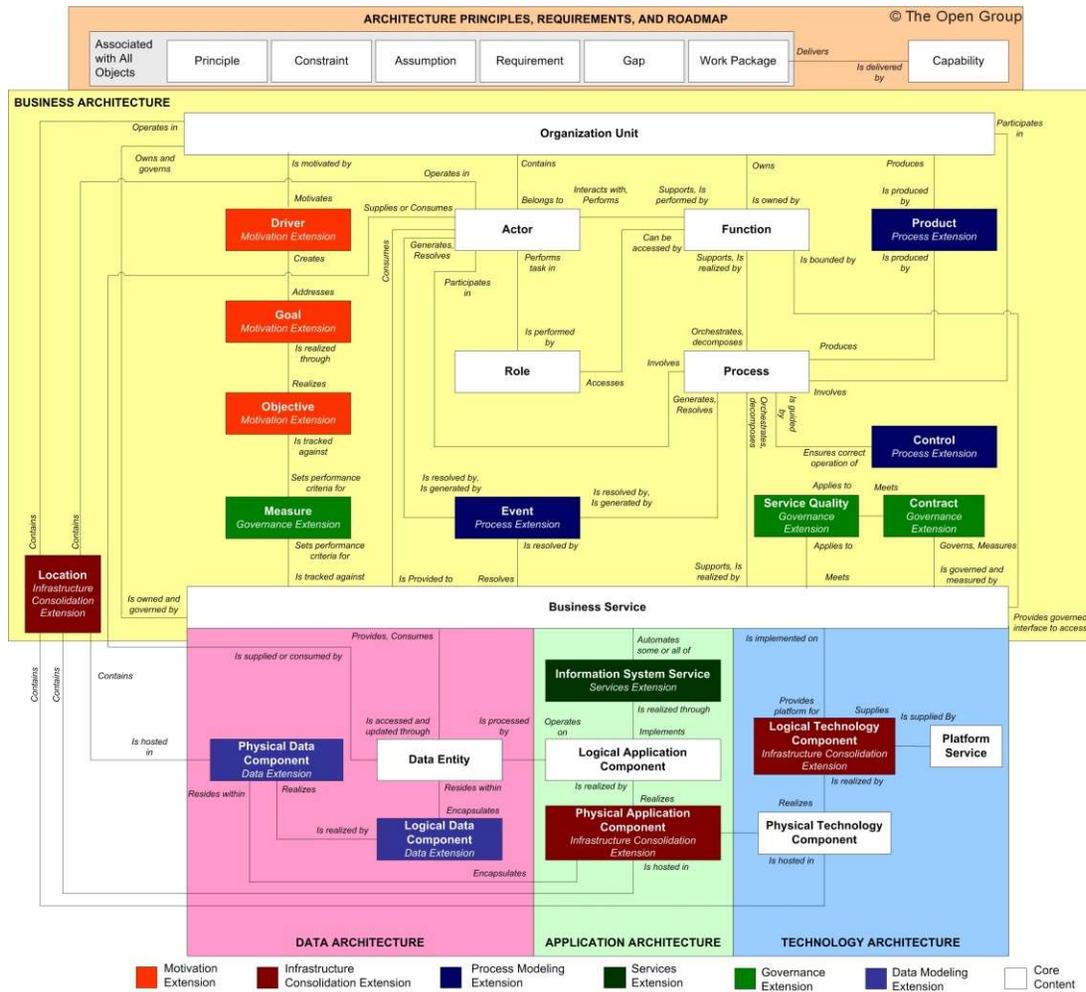
diagrams (dessins de trucs).

Les artefacts forment le contenu du *Architecture Repository*

Building blocks

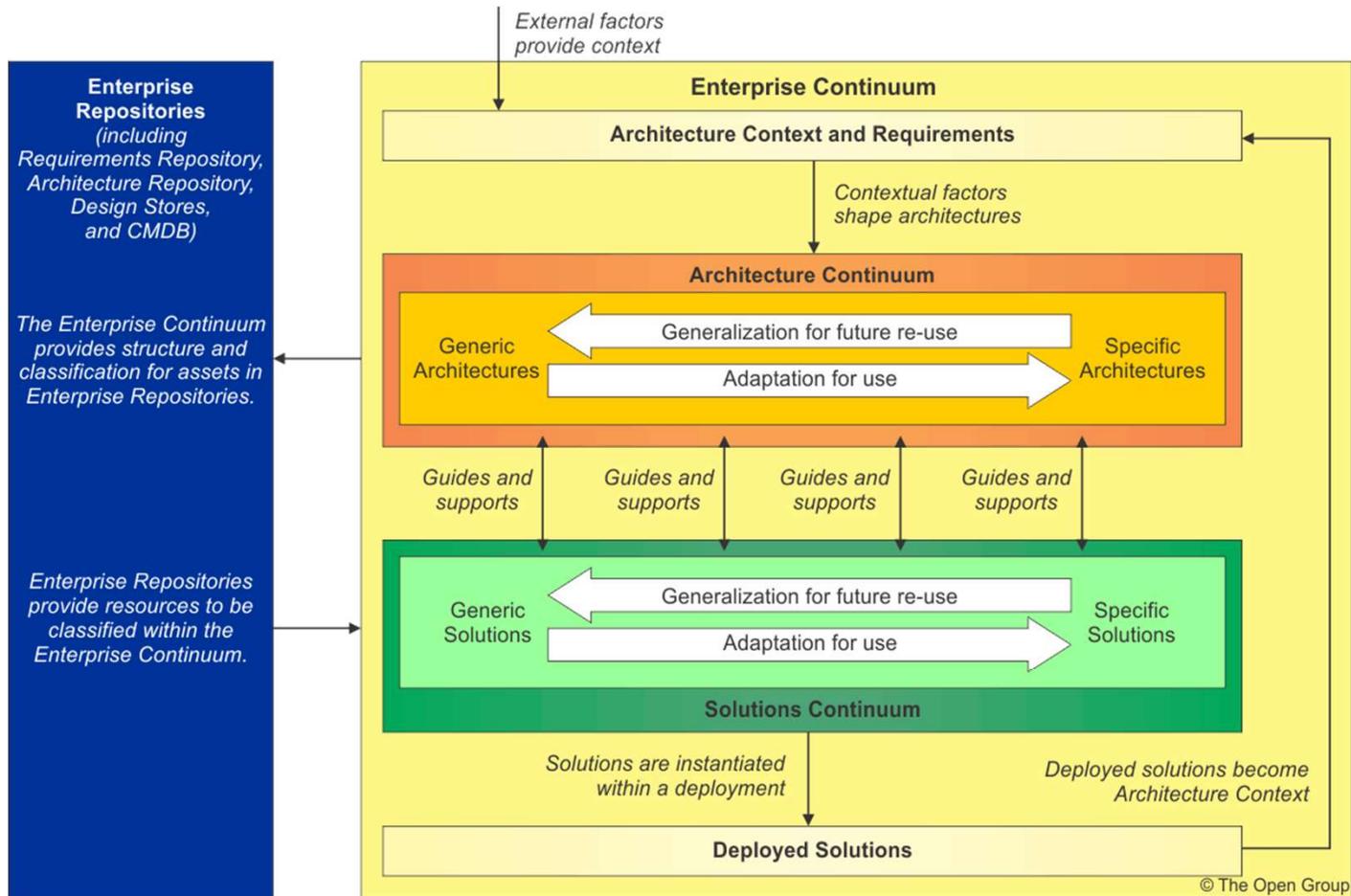
Éléments abstraits et réutilisables qui peuvent être combinés avec d'autres BB pour livrer des architectures et des solutions



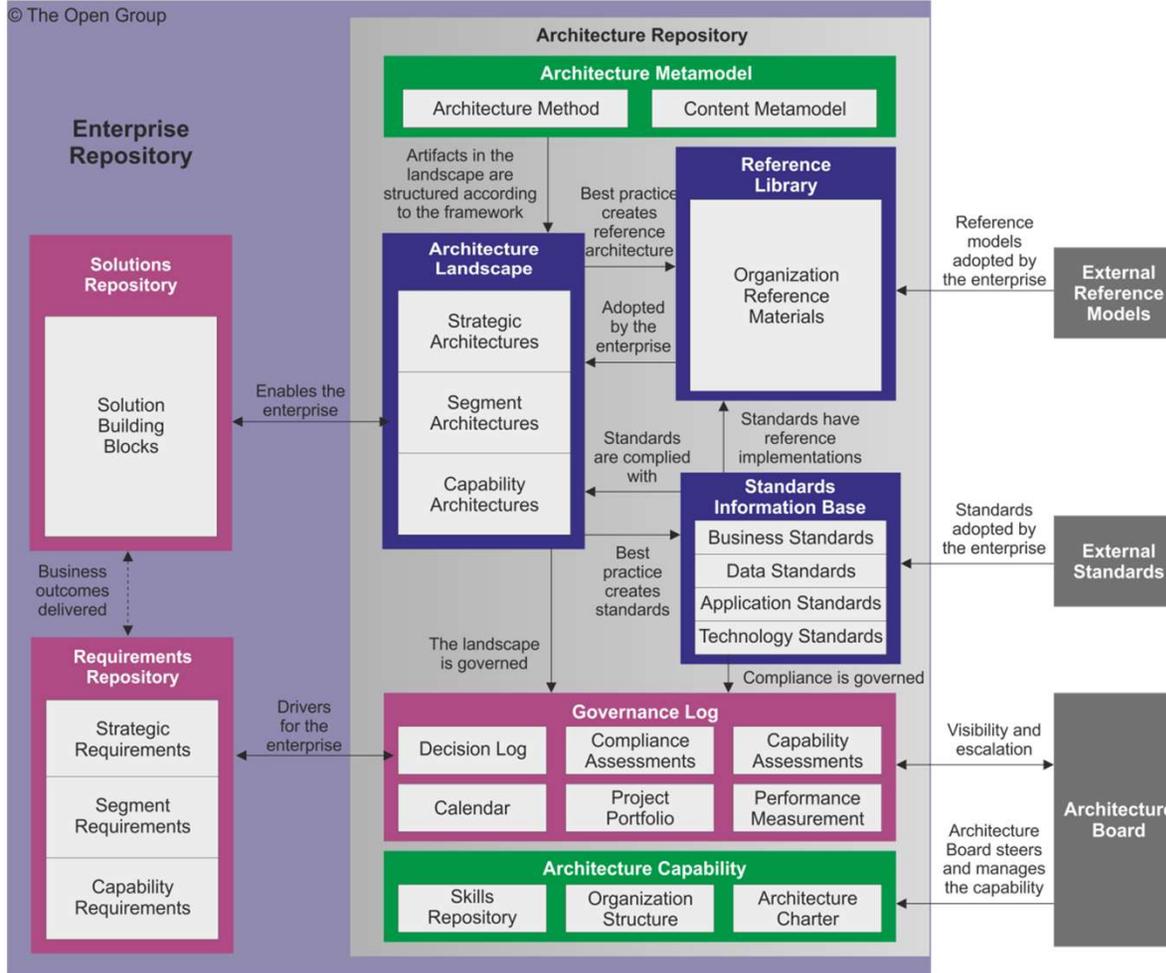


Représentation détaillée du Metamodel TOGAF

Le METAMODEL est une description structurée de comment et avec quoi l'architecture d'entreprise doit être décrite.



Foundation Architectures	Common Architectures	Industry Architectures	Organization-specific Architectures
TOGAF TRM including OS and DBMS, BDNA, Open Infrastructure Architecture repository OIAr	TOGAF III-RM, IT4IT, ERP-Architecture	BIAN Capability Map, ERP-Architecture for Automotive	Capability Map Company XY, ERP Architecture Company XY
Linux, SAP Hana, MS SQL, Kafka	SAP ERP	SAP ERP Automotive	SAP ERP of Company XY

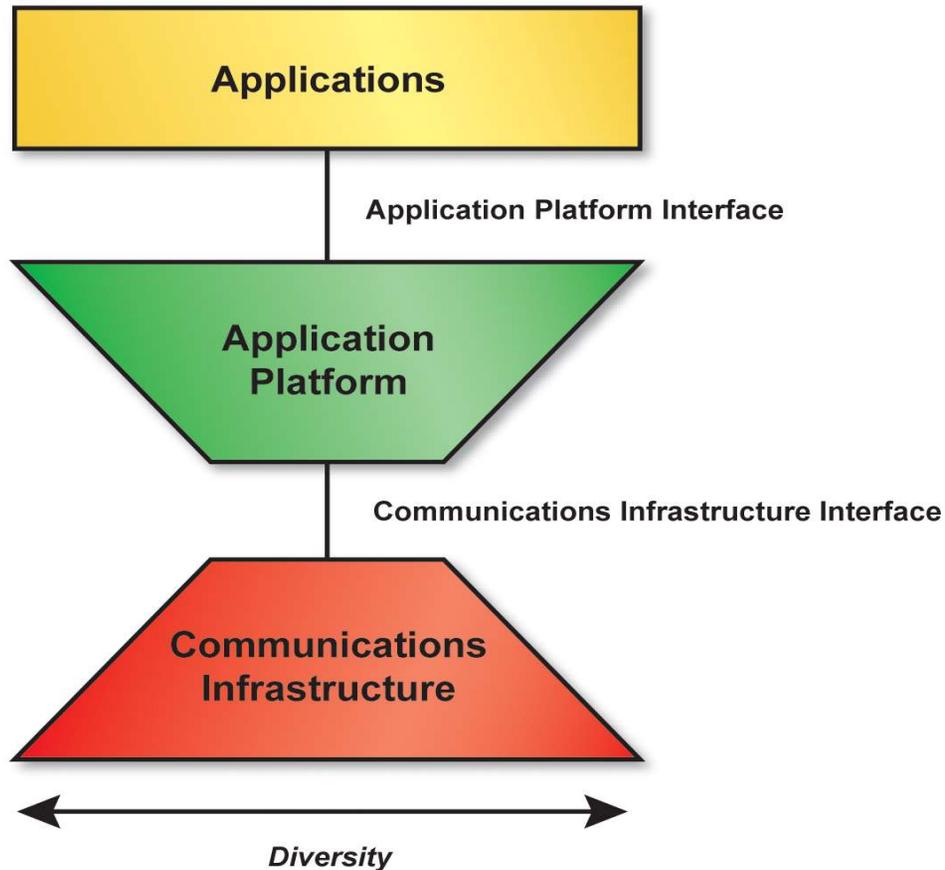


Afin de supporter le Continuum, TOGAF propose un concept de référentiel qui est utilisé pour déposer les différentes classes d'architecture, à différents niveaux d'abstraction, qui ont été créées par ADM.

C'est l'approche de TOGAF pour faciliter la coopération entre les parties prenantes et les différentes pratiques d'architecture.

TOGAF offre 2 modèles de référence

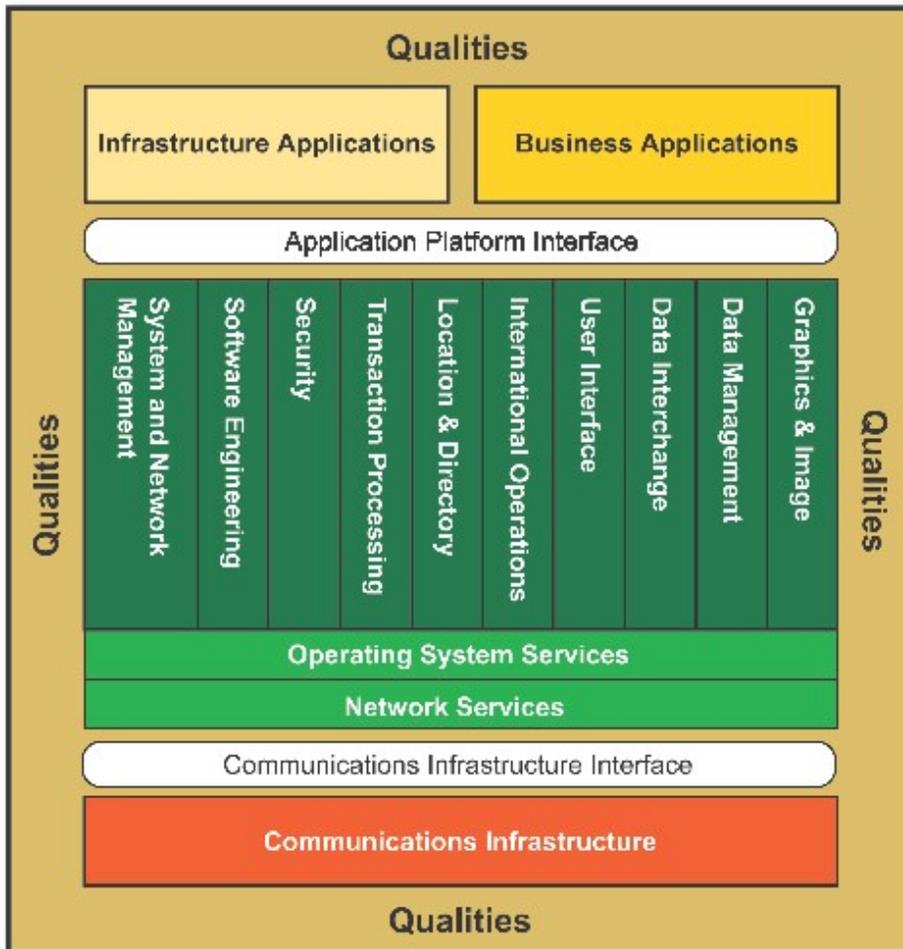
- Le TOGAF Technical Reference Model (TRM)
 - Une architecture de fondation
 - Un modèle et une taxonomie générique pour les plateformes de services
- Le Integrated Information Infrastructure Model (III-RM)
 - Un modèle pour les application d'affaire et l'infrastructure applicative
 - Spécialement conçu pour supporter la vision du *Boundaryless Information Flow*



TOGAF offre un modèle graphique et une taxonomie complète qui peuvent être utilisés comme référence pour faire la modélisation de plusieurs artefacts du modèle de référence

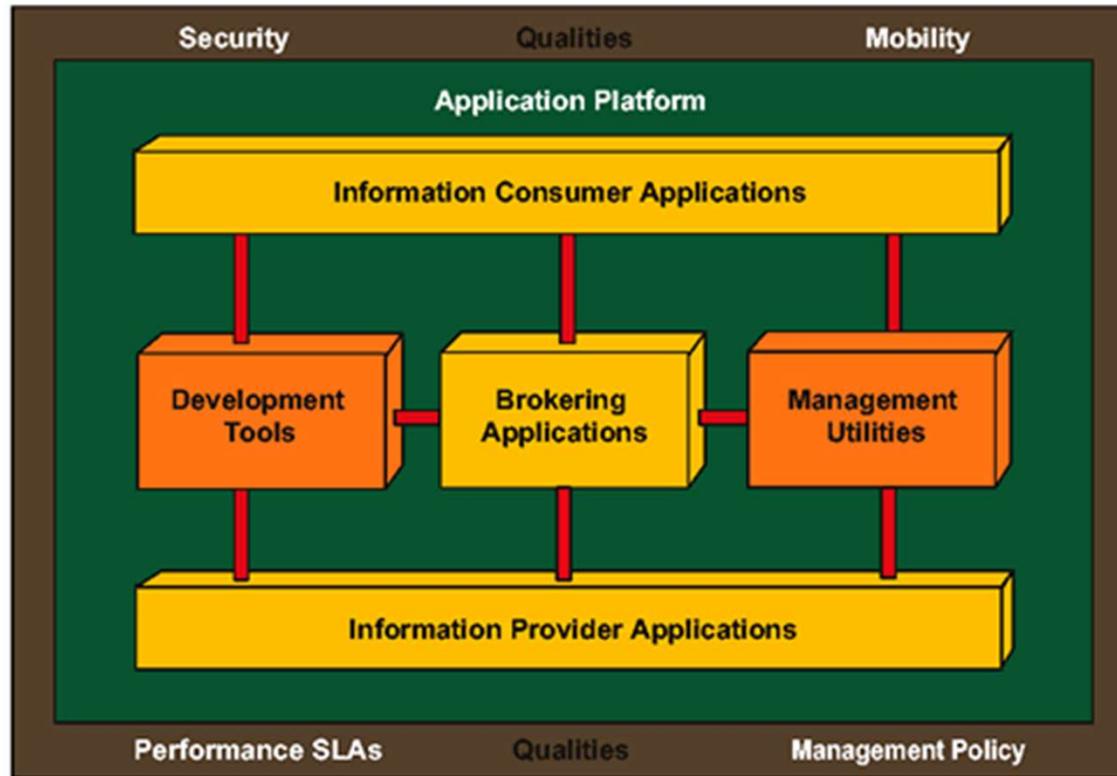
Selon la nomenclature TOGAF, il s'agit d'une « Foundation Architecture ». Donc, une architecture de BB et de standards qui supporte l'ensemble des « Common System »

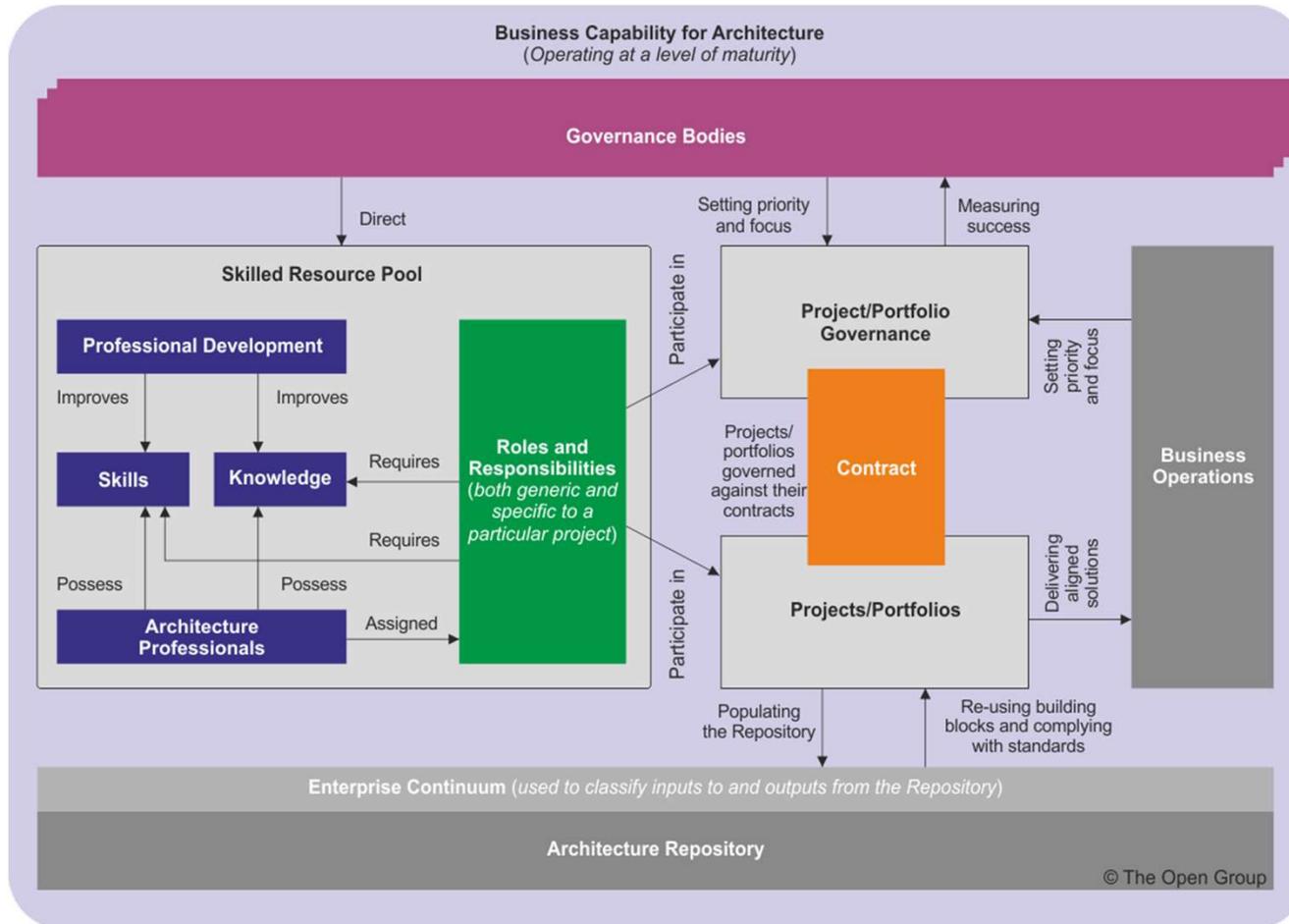
Le TRM décrit une architecture fondamentale sur laquelle les autres architectures, plus spécifiques, pourront se baser



Le TRM met en évidence 2 éléments :

- Une taxonomie qui définit les différents termes et qui procure une description cohérente des éléments conceptuels et des composantes d'un IS
- Un modèle, qui représente graphiquement la taxonomie (*ce graphique*)





Une définition structurée des habiletés, des rôles et des responsabilités de l'organisation pour mettre en place et conduire une pratique d'architecture d'entreprise. Ce qui inclus :

- Référence pour un comité d'architecture
- Orientation pour effectuer l'évaluation de la performance des contrats d'architecture
- Processus et structures organisationnelles requises pour effectuer une saine gouvernance de la pratique
- Techniques pour faire l'évaluation de la maturité de la pratique d'architecture
- Une description des habiletés et des connaissances requises par les architectes

TOGAF, c'est :

- Un cadre efficace et normalisé reconnu par l'industrie pour l'architecture d'entreprise
- TOGAF est un complément aux autres cadres ou pratiques déjà en place. Il n'est pas en compétition avec ceux-ci
- Un répertoire/référenciel des meilleurs pratiques
- Sans biais envers les outils, les technologies ou les fournisseurs
- Permet de cibler l'atteinte du « Boundaryless Information Flow »

Architecture de sécurité

- Une méthodologie
 - pour développer une architecture de sécurité orientée sur les risques et les opportunités d'affaire
 - Orientée sur la livraison de solution de sécurité qui supporte les besoins de l'entreprise*

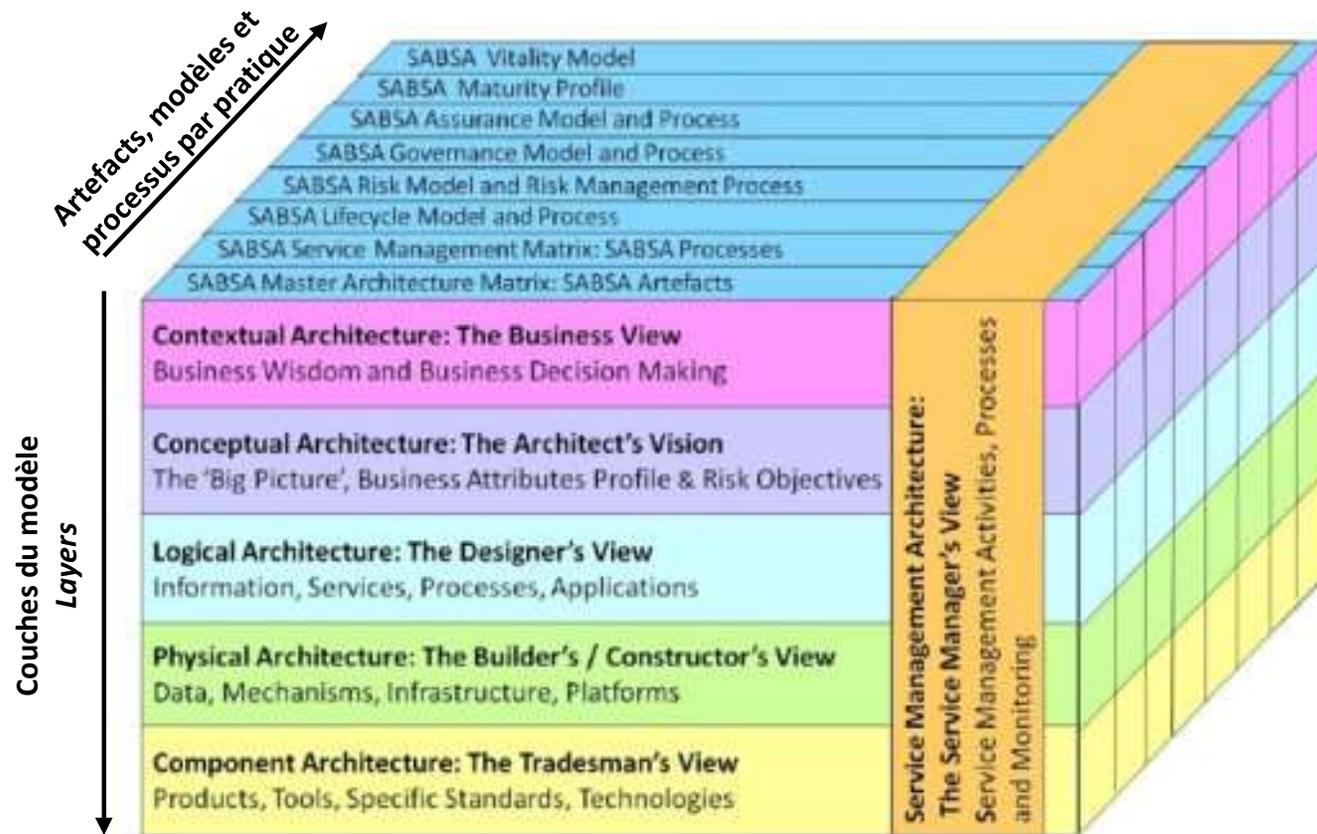
- Sherwood Applied Business Security Architecture (SABSA)
 - Créé par John Sherwood, David Lynas et Adrew Clark
 - Débute en 1996*
 - À cette époque, aucun cadre n'existe pour supporter correctement l'AS
 - De nos jours, c'est le cadre utilisé « de facto » globalement dans plusieurs marchés et secteurs de l'économie, incluant les gouvernement et les secteurs de la défenses**
 - Développé à partir des éléments qui étaient absents des autres cadres d'AE ou de livraisons
 - Aucune préférence sur les choix technologique (technologie agnostique)
 - Open source & gardé par le « SABSA Institute »**

*cours 1

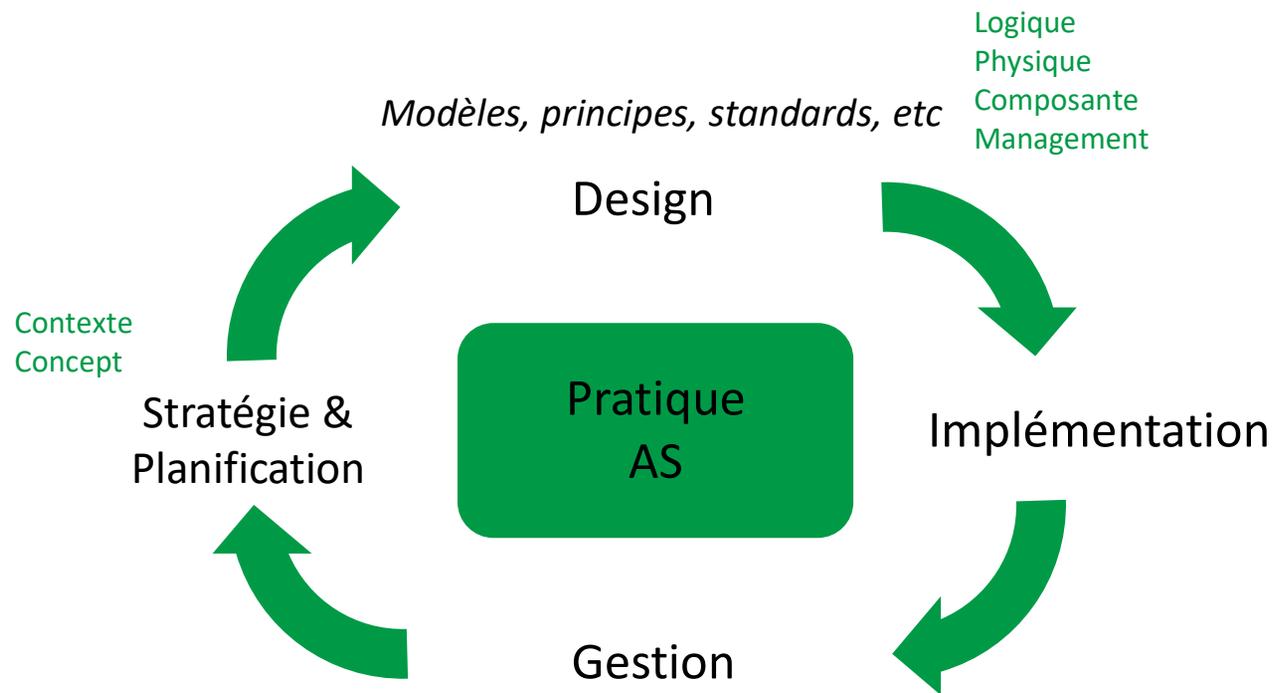
** www.sabsa.org

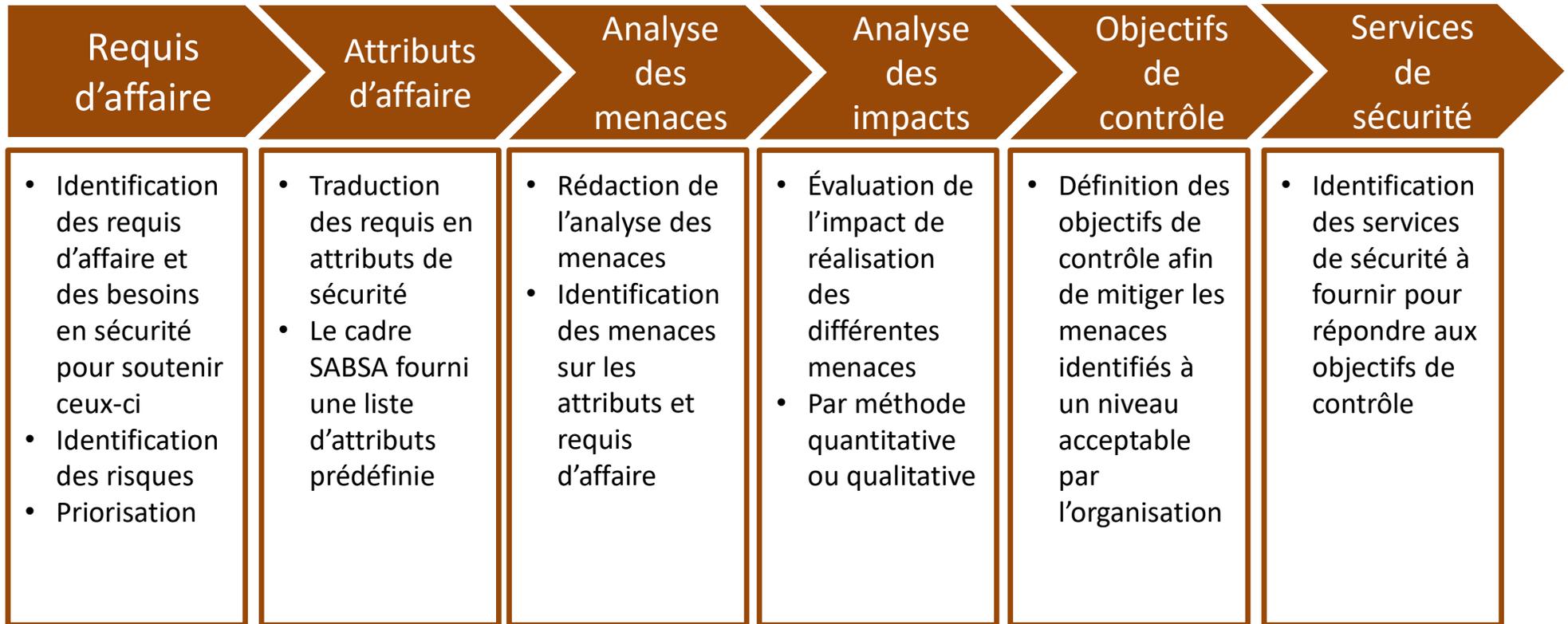
- SABSA Institute

- Créé en 2012/13 afin de protéger et d'assurer les développement futur du cadre SABSA
- A pour but d'assurer une évolution et une maturité cohérente et aligné sur les besoins du marché
- Aussi... gère et chapeaute la certification d'architecture SABSA



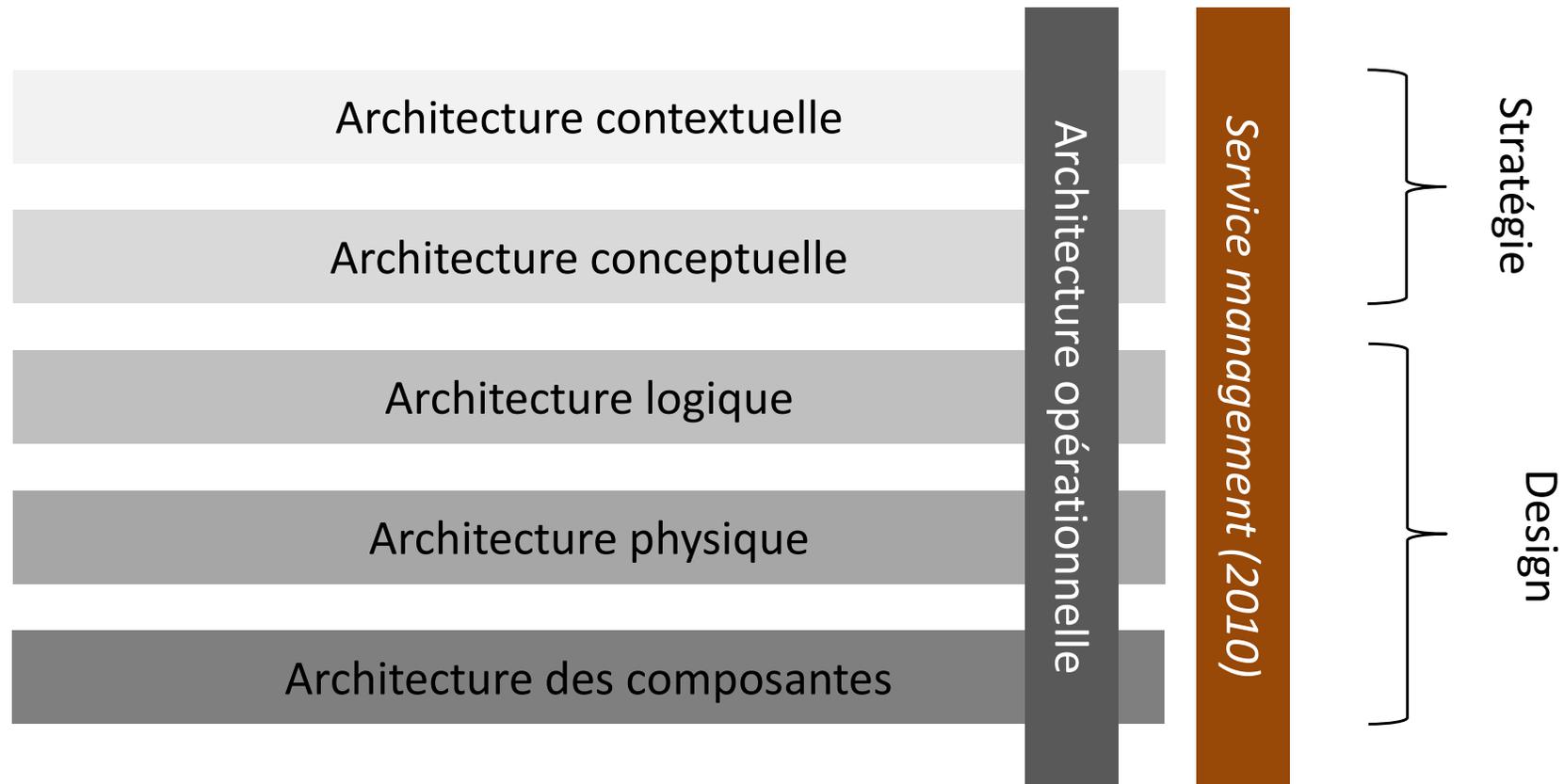
- Tel que l'AE, l'AS n'est pas statique, elle est en constante évolution

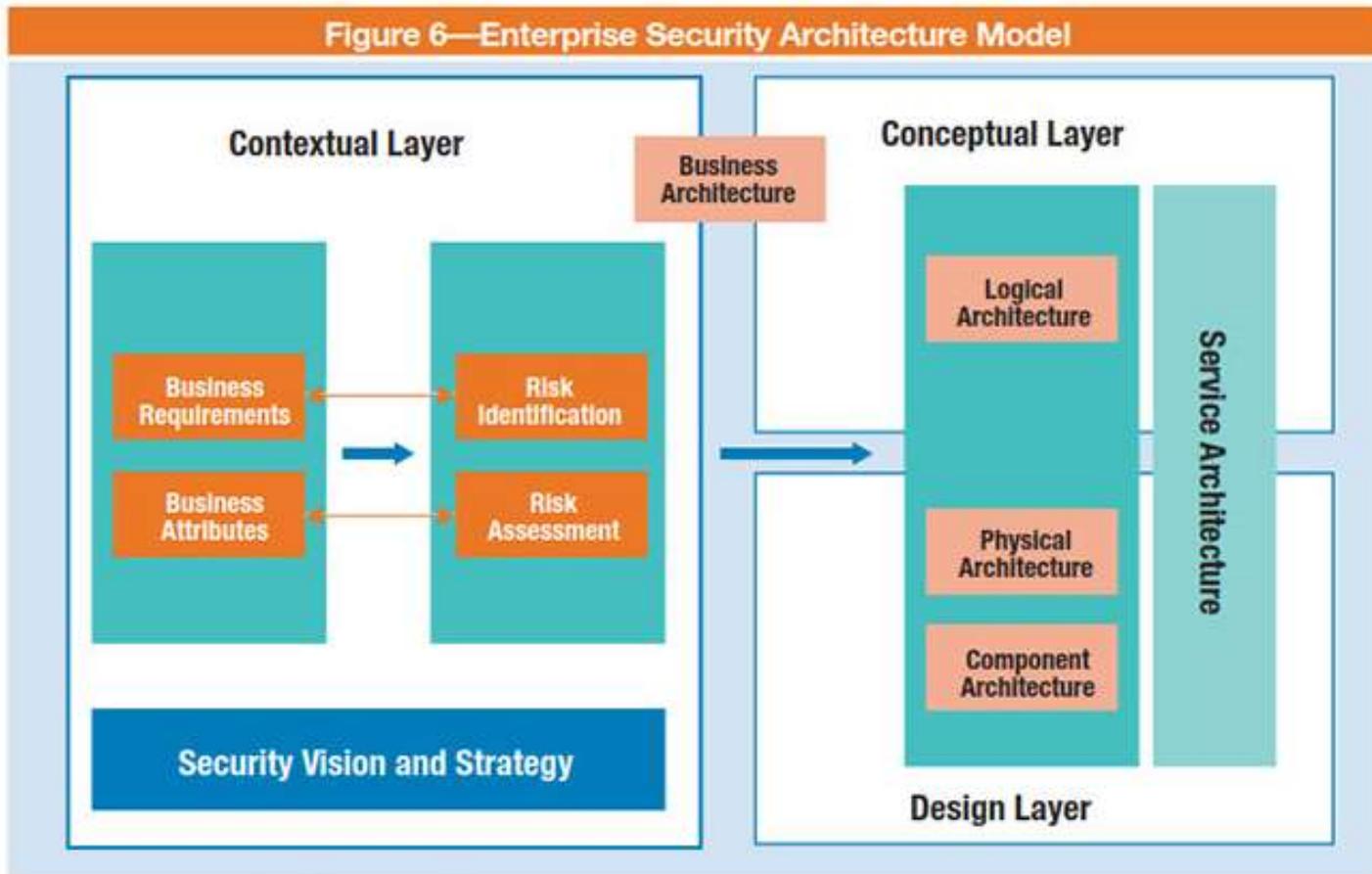




- Les 6 vues et les 6 couches du cadre SABSA

Vues	Couches
The business view	Contextuelle
The architect's view	Conceptuelle
The designer's view	Logique
The builder's view	Physique
The tradesman's view	Composante
The facilities manager's view	Opérationnelle





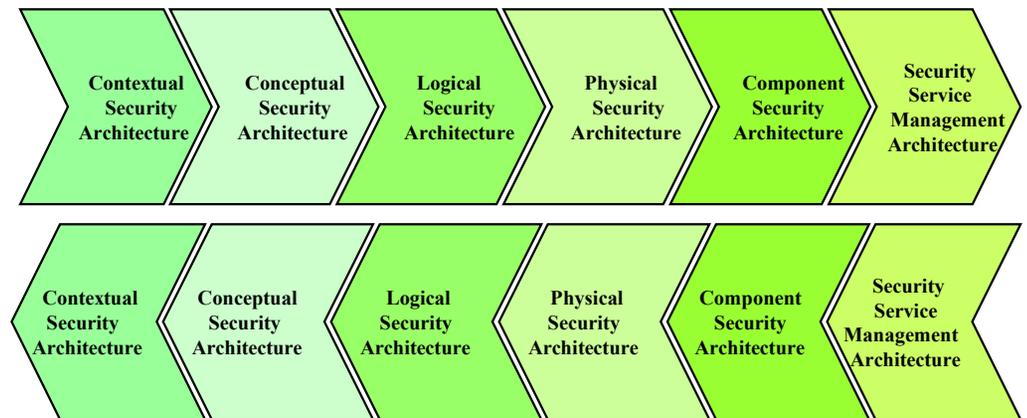
- Pour soutenir l'analyse détaillée de chacune des couches du modèle, celui-ci utilise les mêmes 6 questions fondamentales que Zachman
 - Quoi ? (*What ?*)
 - *Les actifs*
 - Pourquoi ? (*Why ?*)
 - *Les motivations*
 - Comment ? (*How ?*)
 - *Les processus*
 - Qui ? (*Who ?*)
 - *Les individus*
 - Où ? (*Where ?*)
 - *Endroits*
 - Quand ? (*When ?*)
 - *Moments*

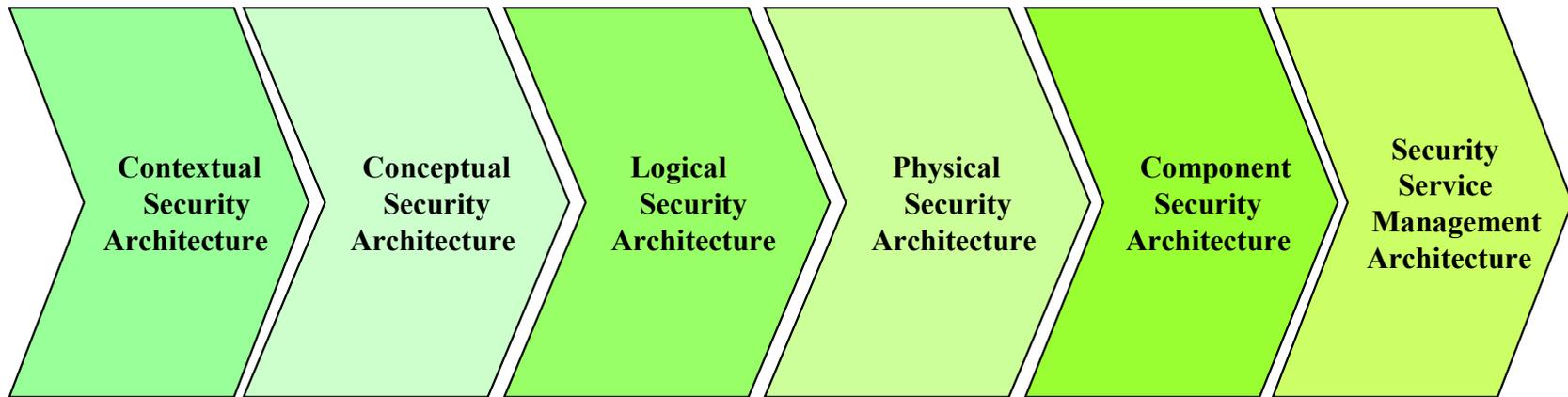
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

- Plusieurs modèles disponible pour une utilisation immédiate, ou pour être adaptés selon les besoin :

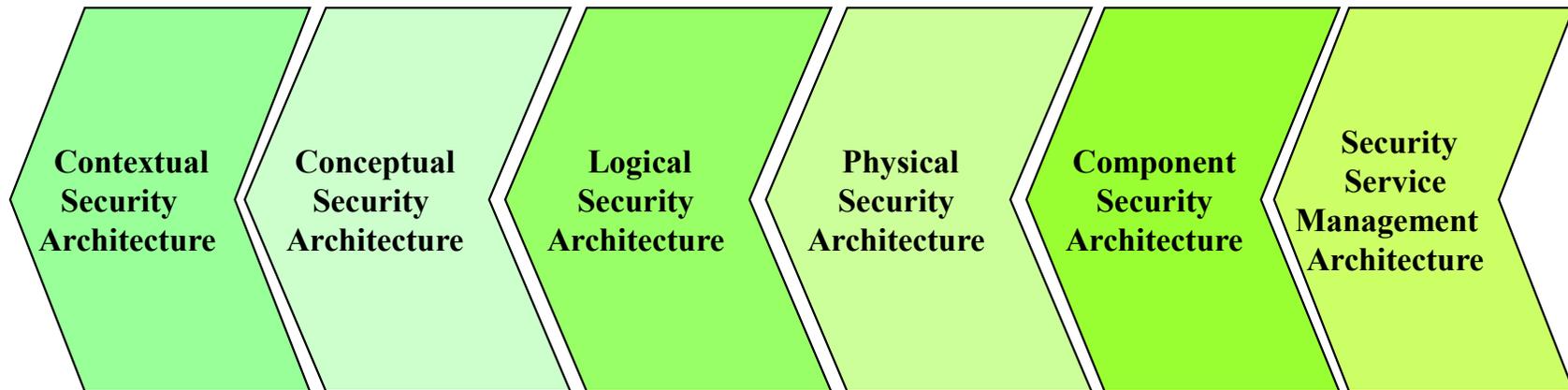
- *Attribute profiling*
- *Risk & Opportunity Model*
- *Multi-Tiered Control Strategy*
- *Assurance Framework*
- *Maturity Model*
- *Governance Model*
- *Vitality Model*
- *Domain & Trust Model*
- *Policy Model*
- *Lifecycle Model*
- *etc*

- Probablement l'outil le plus puissants de SABSA
- Abstraction conceptuelle des véritables besoins de l'organisation
- Standardisés et réutilisables
- Procure une traçabilité bi-directionnelle du requis à la composante
- Permet de définir
 - La surveillance
 - Le reporting

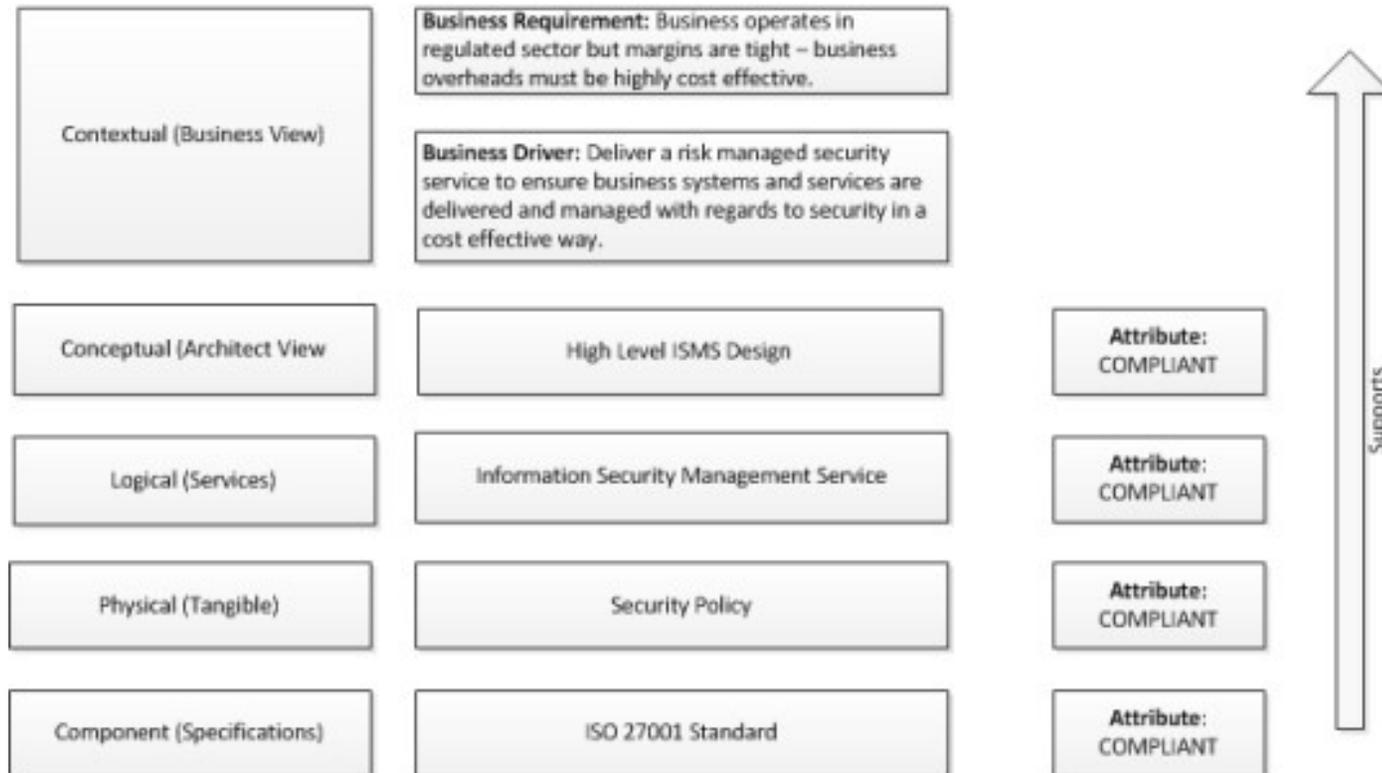




- Chaque requis d'affaire pour la sécurité est répondu et le risque résiduel est acceptable pour l'organisation



- Chaque éléments opérationnels ou technologiques de sécurité peut être justifié par une référence à un risque touchant un requis d'affaire.



Le modèle SABSA

- À partir des réponses reçues de l'analyse détaillées (6 questions clés de la matrices), nous devrions être en mesure d'obtenir une compréhension adéquate des requis de l'organisation pour la mise en place d'une architecture de sécurité et/ou d'un système sécuritaire
- Nous devrions être en mesure de synthétiser l'architecture du système et l'architecture de sécurité requise pour répondre au requis d'affaire

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Frameworks	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schemas; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times; Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man/ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identifiers; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetables

- L'architecture contextuelle se soucie de :
 - *What ? L'organisation et ses actifs à protéger (marque, réputation, relations d'affaires, etc) et ses besoins en terme de sécurité (Revenue, e-biz, continuité des affaires, conformité aux lois, etc)*
 - *Why ? Les risques d'entreprise exprimés sous forme de ce que sont les actifs critiques, les objectifs, les facteurs de succès ainsi que les menaces et les vulnérabilités qui mettent ceux-ci à risque. Comment ceci justifie-t-il les besoins de sécurité (protection de la marque, contre les fraudes, assurances, continuité des affaires, etc) --> Modèle et scénario de risques*
 - *How ? Les processus d'affaire qui ont besoin d'être sécurisés (Approvisionnement, distribution, vente, communication, etc)*
 - *Who ? L'aspect organisationnel de la sécurité (structure de gestion, approvisionnement, externalisation, partenariat)*
 - *Where ? Le contexte géographique (les sites, le campus, travail à distance, etc)*
 - *When ? Les dépendances temporelles liées aux affaires (transactions, opérations, mise en marché, etc)*

- C'est la présentation du concept général qui permettra à l'AS de répondre aux besoins de sécurité de l'organisation
- Cette couche définit les principes et les concepts fondamentaux qui seront utilisés dans la sélection et l'organisation des couches logique et physique, qui sont les sous-couche d'abstraction avant de toucher aux composantes proprement dites.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Frameworks	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schemas; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times; Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identifiers; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

- L'architecture conceptuelle se soucie de :
 - *What ? Qu'est-ce qu'on veut protéger (SABSA utilise un modèle d'attribut abstraits, voir ch.6)*
 - *Why ? En quoi la sécurité sera importante, quels seront les objectifs des contrôles que nous mettrons en place ?*
 - *How ? Comment allons-nous atteindre notre but ? C'est ici qu'on décrit la stratégie de sécurité à adopter. La stratégie devient la colle des différentes technologies de sécurité*
 - *Who ? On identifie qui seront les responsables des différents aspects de la sécurité et les différents niveau de confiance entre elles*
 - *Where ? Quels domaines de sécurité visons nous ?*
 - *When ? On s'intéresse aux différents moment où la sécurité devient importante.*

- Comprendre l'organisation et ses risques

Consolider et analyser les requis d'affaire

- Stratégie d'affaire
- Processus et fonctions d'affaire
- Structure organisationnelle (le personnel, la géographie, les partenaires)
- Budgets, contraintes technique, humaines et temporelles

Décrire les requis d'affaire

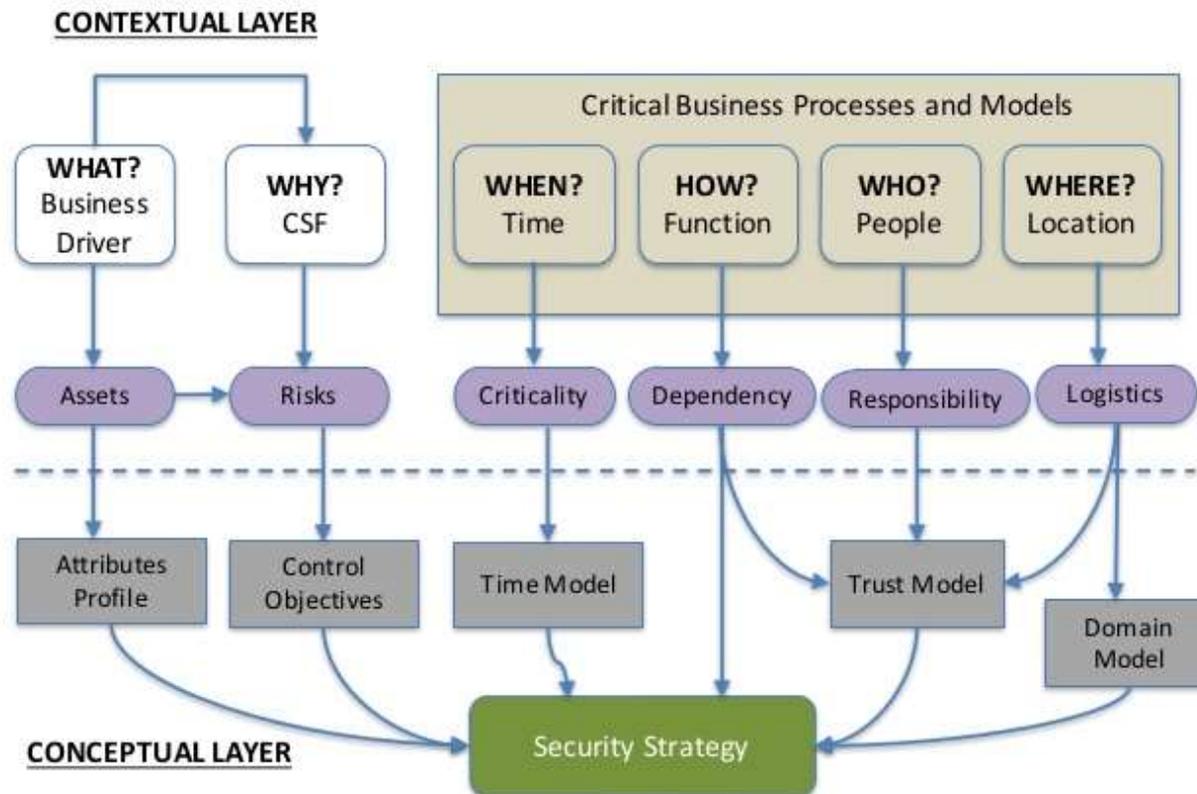
- En utilisant les attributs, décrire l'organisation en terme de stratégie, ses actifs, ses buts et ses objectifs → C'est ce qui donne le profile d'attribut

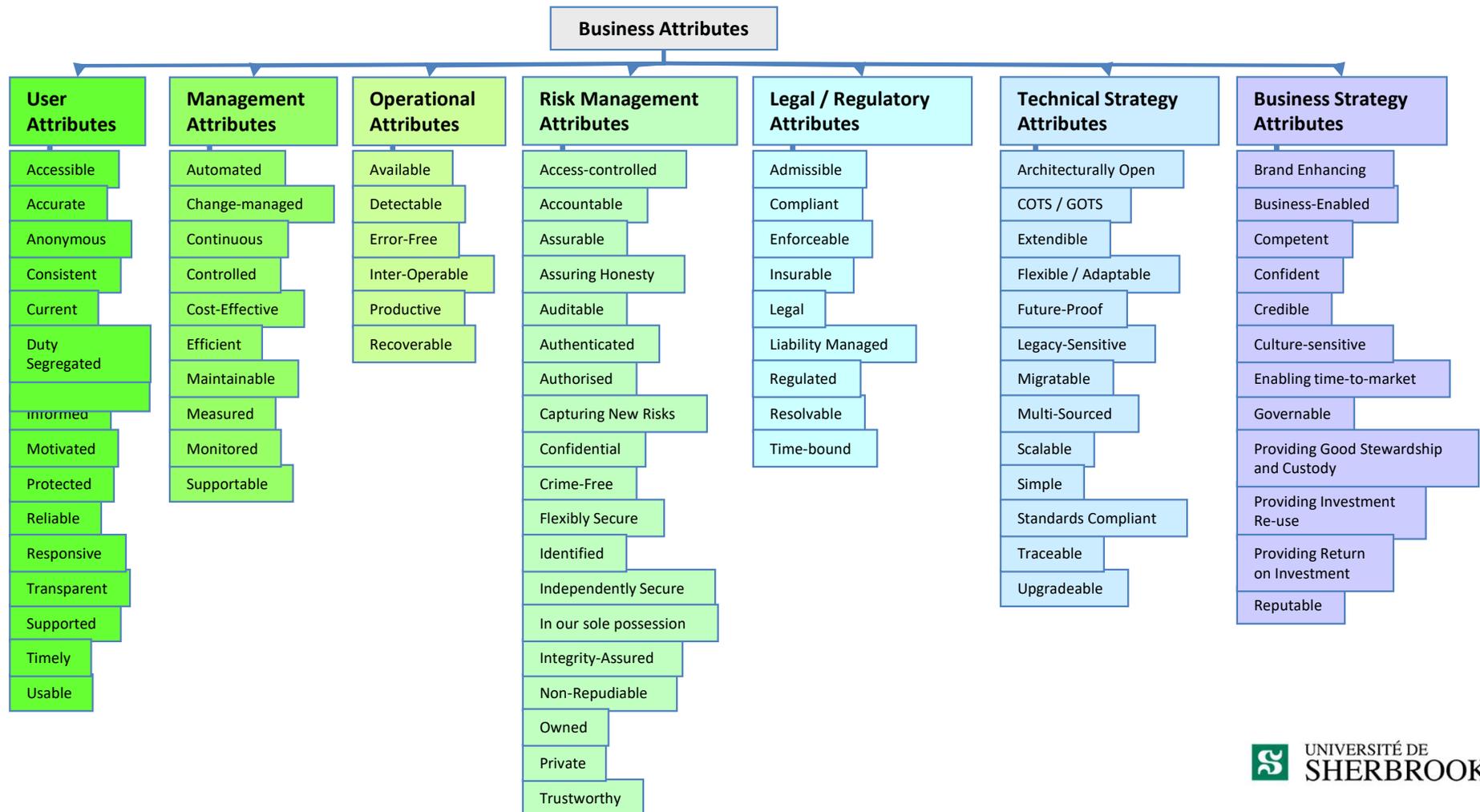
Analyse des risques d'affaire

- Faire l'analyse des menaces par rapport aux actifs, aux buts et aux objectifs
- Définir les impacts de la réalisation de ce menaces
- Identifier les vulnérabilités procédurales et techniques → Objectifs de contrôles

- La stratégie*

Comment le contexte et le concept forme la stratégie

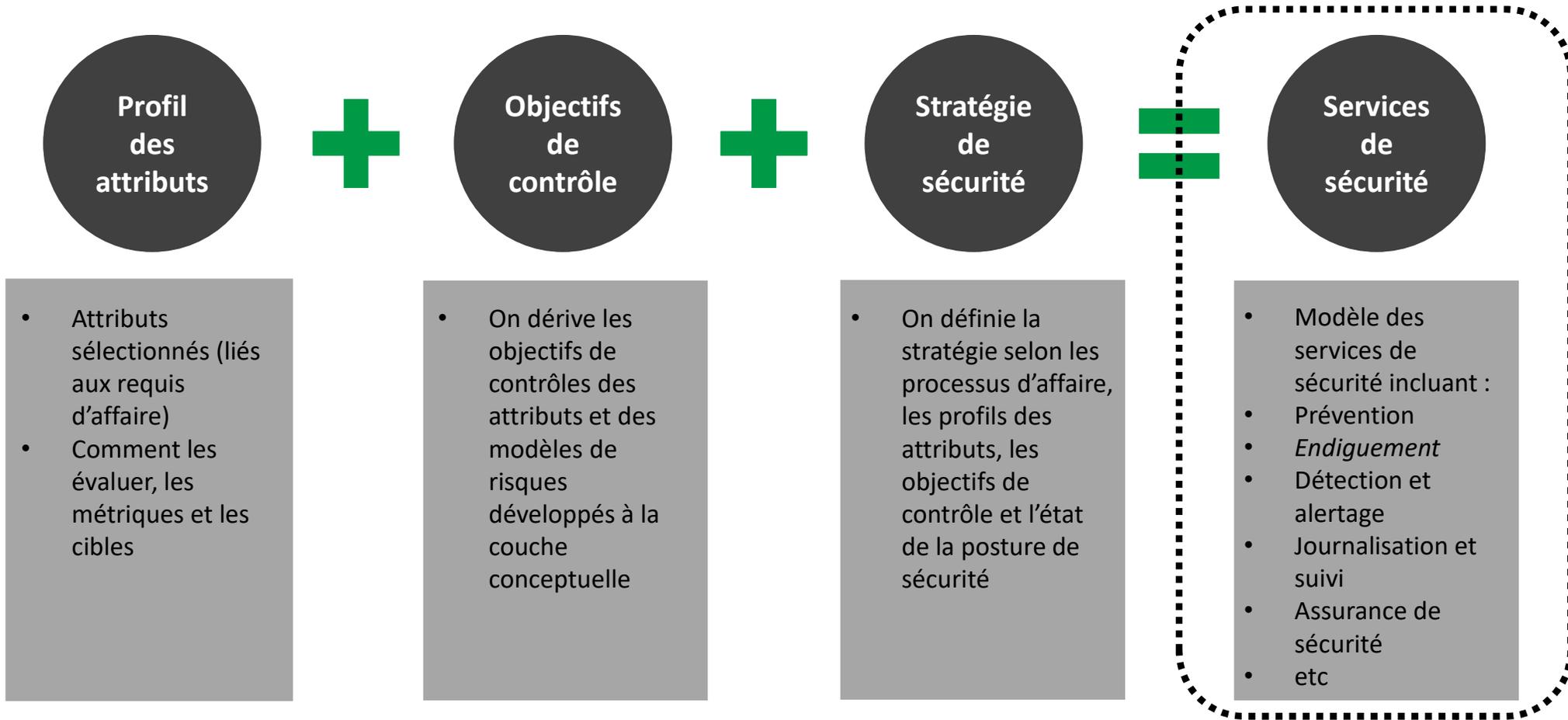




- Souvent appeler l'ingénierie du système (*system ingeniering*)
- C'est à ce niveau qu'on modélise le système en fonction des requis d'affaire et de sécurité
 - La majorité des services de sécurité sont représentés sous forme d'éléments logiques
 - Les flux logiques sont illustrés ainsi que les relations entre les éléments
- Niveau d'abstraction logique – on décrit ce qu'on veut construire

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architectures	Entity Schemas; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man/ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetables

- L'architecture logique se soucie de :
 - *What ? L'information qui doit être sécurisée*
 - *Why ? Les politiques de sécurité (générales, certification, env. physique, env. logique, etc)*
 - *How ? Les services de sécurité logiques qui seront requis (Services DICA) et comment ils travailleront ensemble*
 - *Who ? La définition des différentes entités (utilisateur, auditeur, admin, etc), leurs attributs, le profil de leurs rôles et leurs privilèges*
 - *Where ? On s'intéresse aux domaines de sécurité touchés et leurs différentes relations*
 - *When ? On spécifie les différents cycles liés à l'exécution des services de la sécurité (enregistrement, certification, login, gestion des sessions, etc)*



- Les modèles de sécurité de l'architecture physique qui décrivent les modèles technologiques et qui décrivent les requis fonctionnels des différentes composantes du systèmes
 - Plateforme
 - HW
 - Réseau
 - OS, DB, Fichiers
- Les mécanismes et le HW qui sera utilisé pour offrir les services

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives, Policy Architecture	Process Mapping Framework, Architectural Strategies for ICT	Owners, Custodians and Users, Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

- L'architecture physique se soucie de :
 - *What ? Les modèles de données*
 - *Why ? Les différentes règles qui régissent les décisions des systèmes (conditions, procédures, pratiques et les actions)*
 - *How ? Les mécanismes de sécurité qui seront mis en place (encryption, gestion de l'accès, antivirus, URL filtering, antispam, etc)*
 - *Who ? Qui sont les utilisateurs et les applications qu'ils utilisent et quelles seront leurs limitations de sécurité*
 - *Where ? L'infrastructure technologique de sécurité (l'installation physique du HW, SW et du réseau)*
 - *When ? Dépendances temporelles sur l'exécution des tâches (séquences, évènements, durée de vie, etc)*

- Assemblage des produits provenant de fournisseurs spécialisés
- Intégration de ces différentes technologies
 - HW, SW, SOA
 - Standards de sécurité (e.g., US National Institute of Standards and Technology [NIST], ISO)
 - Outils et produits de sécurité (e.g., antivirus [AV], virtual private network [VPN], firewall, wireless security, vulnerability scanner)
 - Service de sécurité Web (e.g., HTTP/HTTPS protocol, application program interface [API], web application firewall [WAF])

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Frameworks	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schemas; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times; Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Services
COMPONENT MANAGEMENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Procedures	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identifiers; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Notes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetables

- L'architecture des composante se soucie de :
 - *What ? Les données, les champs, les adresses et tout autres structures de données pertinentes*
 - *Why ? Standards de sécurité*
 - *How ? Produits spécialisés sous toutes leurs formes (HW, SW)*
 - *Who ? Identité des utilisateurs, les privilèges, les fonctions, les ACL*
 - *Where ? Processus système, node, protocoles, etc*
 - *When ? Étape de sécurité prédéfinie*

- Ce qu'on obtient généralement...

Architecture contextuelle

- Requis d'affaire
- Priorisation et importance
- Scénarios de menace
- Analyse d'impact

Architecture conceptuelle

- Profil d'attributs
- Modèle de risque
- Modèle des domaines de sécurité

Architecture Logique

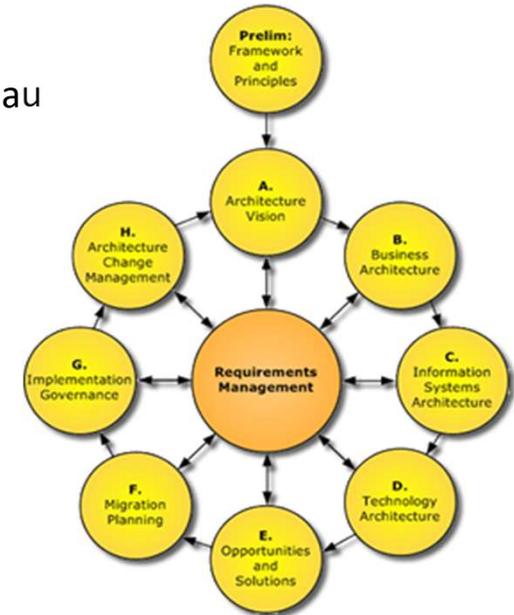
- Associations des domaines de sécurité
- Cadre des services de sécurité

Architecture physique et les composants

- Design détaillé de l'infrastructure et des composants
- Lien entre les contrôles et les objectifs de contrôle

Utilisation du cadre TOGAF pour developper une architecture de Sécurité d'entreprise

- Ce que TOGAF et SABSA nous disent :
- Il est impératif d'utiliser une approche TOP-DOWN
 - Il s'agit de l'hypothèse de base de toutes les architectures de niveau entreprise
- Définir les cibles
 - Les moteurs d'affaires
 - Les objectifs de l'organisation
 - La vision pour le modèle de capacité d'architecture de sécurité
- Définir les attributs d'affaire requis pour atteindre les cibles
- Identifier les risques associés aux attributs qui peuvent avoir un impact sur l'atteinte des cibles
- Identifier les contrôles requis
- Définir un programme pour faire le design et l'implantation des contrôles



Question ?