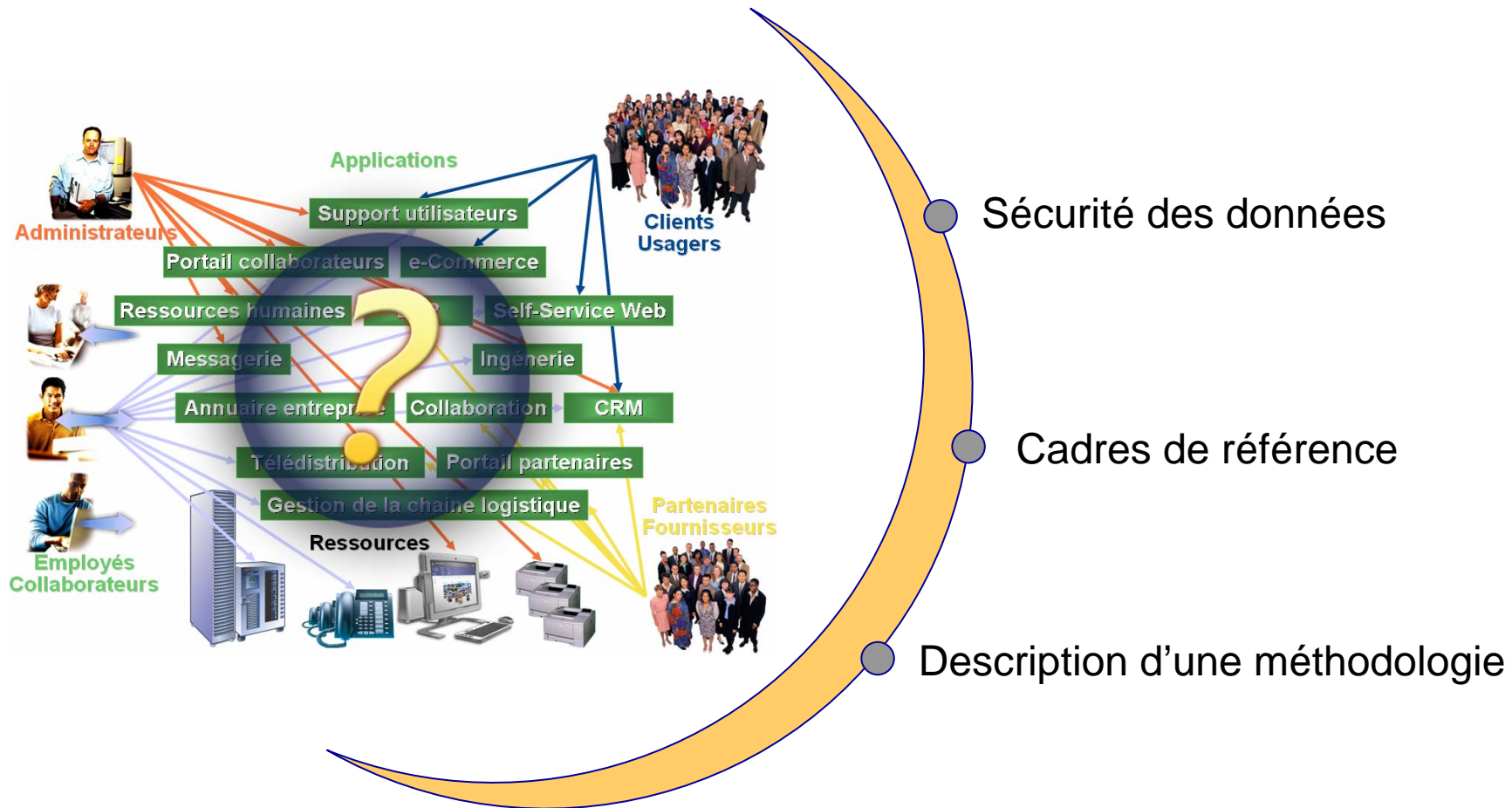




Architecture de référence pour la protection des données

Mercredi 21 Mars 2007

- Serge Richard – CISSP® / IBM France



Sécurité des données

Rappel sur les données informatiques

- Depuis le début de l'Histoire (apparition de l'écriture), l'homme manipule des informations, qui se traduisent par des données, plus en moins structurées. L'avènement de l'informatique depuis la fin des années 1940 aux États-Unis a introduit une forme numérique de données, enregistrées sur des supports électroniques. Cette évolution est comparable à l'avènement de l'imprimerie au XVe siècle dans les années 1450.
- À la base, le support des données est la mémoire de l'ordinateur, sur laquelle opèrent les instructions élémentaires des programmes informatiques. Il n'est pas possible de traiter la sécurité des données, sans rappeler cet aspect fondamental :
Les données sont traitées avec des matériels informatiques et des systèmes d'exploitation.
- Sur les différents types de matériels informatiques (avec leurs périphériques), on trouve toujours les différents types de support physique suivants : la Mémoire de l'ordinateur, les disques, armoires (périphériques), pour la sauvegarde et le stockage, les systèmes d'archivage...
- Les données peuvent circuler entre ces systèmes dans des réseaux physique de communication : réseaux de télécommunications, réseaux locaux, réseaux de télécommunications par satellites,...

- Les enjeux de la sécurité des données sont les suivants :
 - Libertés individuelles : protection de la vie privée (voir vie privée et informatique),
 - Bureautique : sécurité des données enregistrées sur le disque dur du micro-ordinateur (courriels, répertoires, fichiers documents, données des tableurs et des présentations,...),
 - Communication : ciblage des parties prenantes internes et externes en fonction de leurs intérêts, ne pas divulguer inutilement trop d'informations non structurées sur l'internet,
 - Hygiène et sécurité : identification des données nécessaires aux procédures de protection de la santé des employés,
 - Secret des affaires : protection du capital intellectuel de l'entreprise
 - Marketing : identification des marchés sensibles, veille concurrentielle,
 - Recherche et développement : alignement du processus de R&D sur les besoins du marché, identifiés et validés par le marketing : sécurisation des données issues de la veille en entreprise, de la veille technologique, et développement du capital intellectuel de l'entreprise.
 - Exemple dans la chimie : fiche de données de sécurité, pour les substances chimiques pour l'industrie du pneumatique, de l'automobile,...
 - Traçabilité des documents et responsabilité du fait des produits défectueux : pouvoir donner la preuve de la qualité d'un produit.
 - Achats : demandes d'achat (dans l'aéronautique, l'automobile,... par exemple), critères utilisés pour le choix des fournisseurs.
- La sécurité des données implique certaines façons de structurer les données.

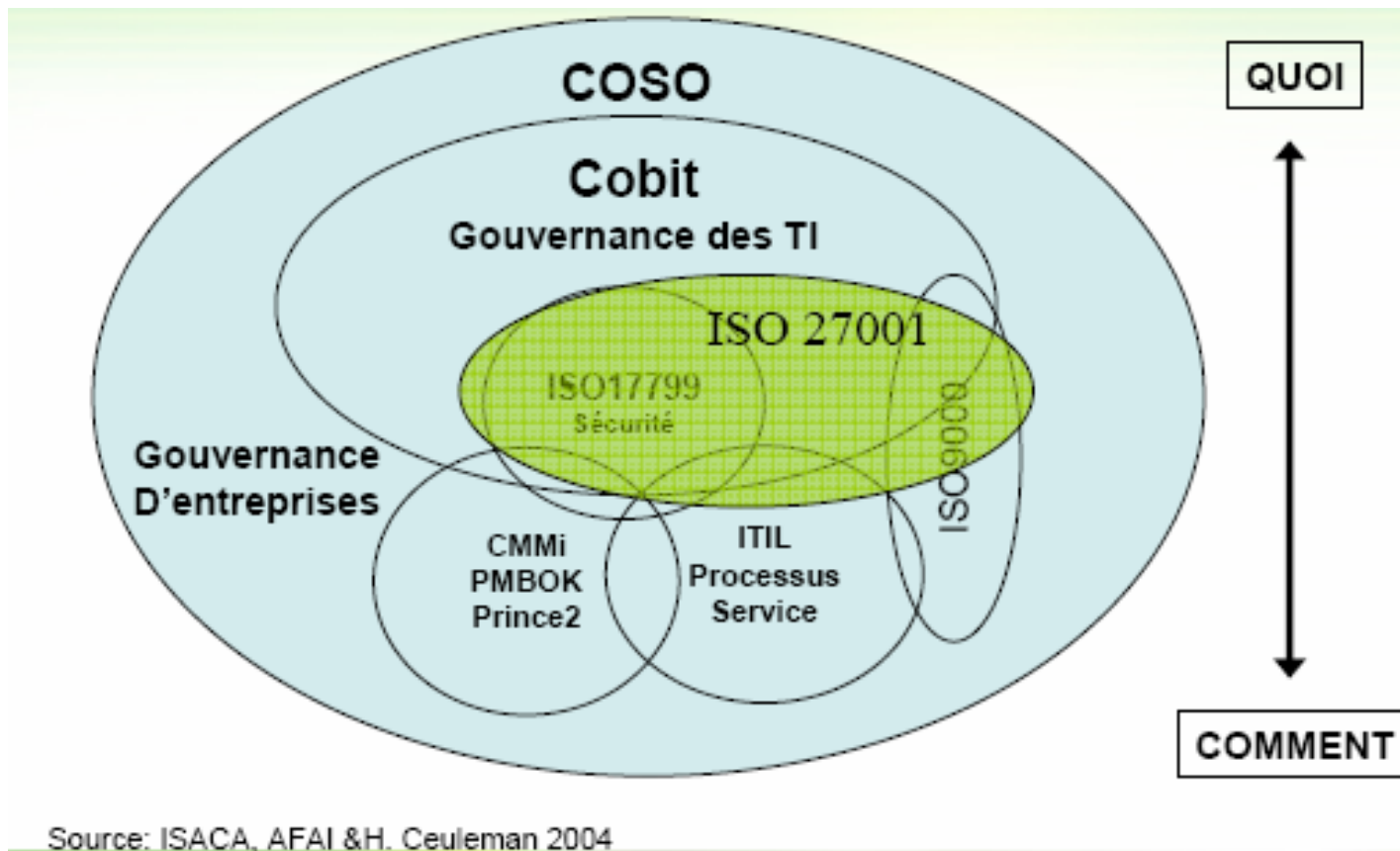
- On distingue en sécurité de l'information plusieurs aspects, qui sont liés aux données :
 - La confidentialité : C'est le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé
 - L'intégrité : Cela désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.
 - La disponibilité : Cela désigne la capacité à un système de garder des données accessibles.
- On trouve aussi (norme ISO 13335) :
 - L'authentification : C'est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...).
 - La non répudiation : Cela signifie la possibilité de vérifier que l'expéditeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message
 - La gestion de la preuve : Cela a pour objectif d'organiser de manière efficace et systématique tous les documents ou données dont une entreprise peut avoir besoin pour justifier de son activité

- Pour sécuriser les données sensibles, il faut tout d'abord avoir conscience des actifs de l'entreprise à protéger, et de leur valeur. Différentes classifications des actifs existent, sans qu'il y ait de normalisation de tous les types d'actifs. Voici une courte liste proposée par la norme ISO 13335 (concepts et modèles de sécurité informatique) :
 - Personnes ,
 - Capacité à fournir un produit, un service,
 - Actifs physiques,
 - Informations / données (structurées ou non),
 - Actifs intangibles.

- Les méthodes d'audit d'intelligence économique et d'ingénierie des connaissances proposent également des questionnaires types permettant de répertorier les éléments de la mémoire d'entreprise, de les évaluer et de les structurer en processus métier, en parallèle aux processus de gestion administrative.

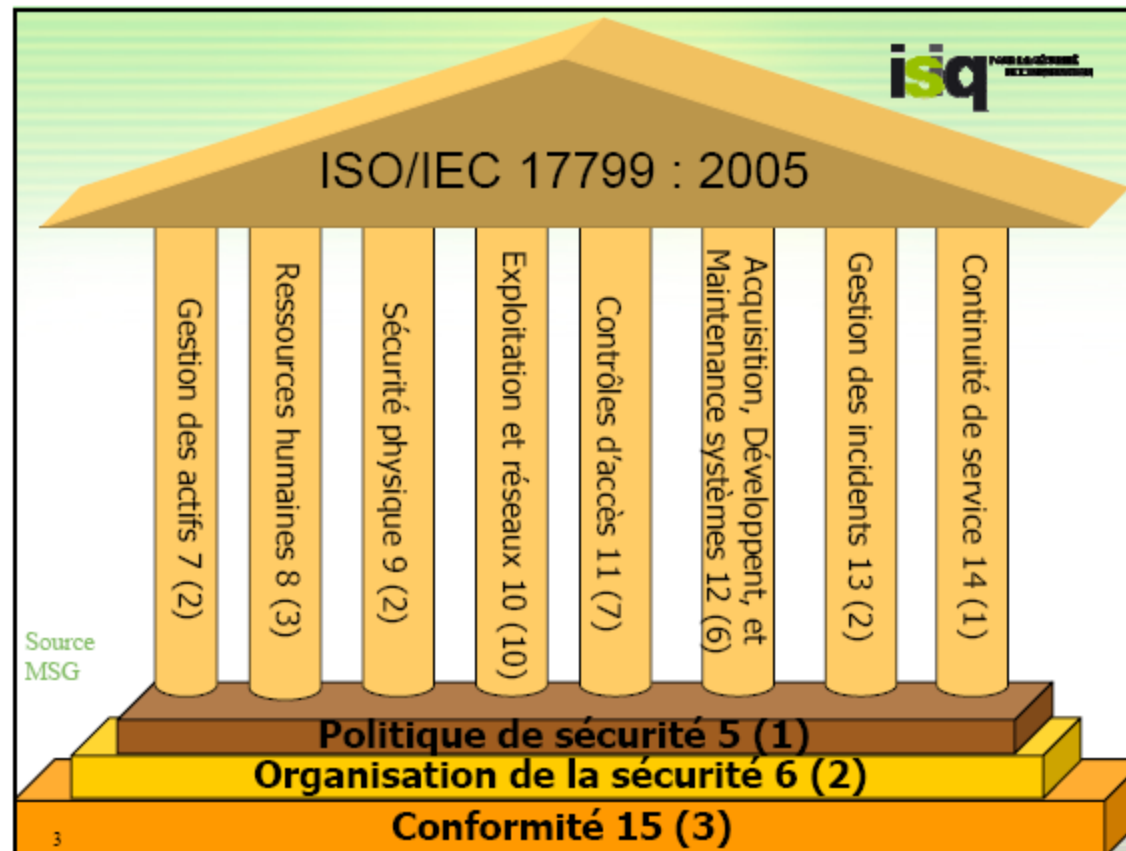
Cadres de référence













Positionnement des cadres de références



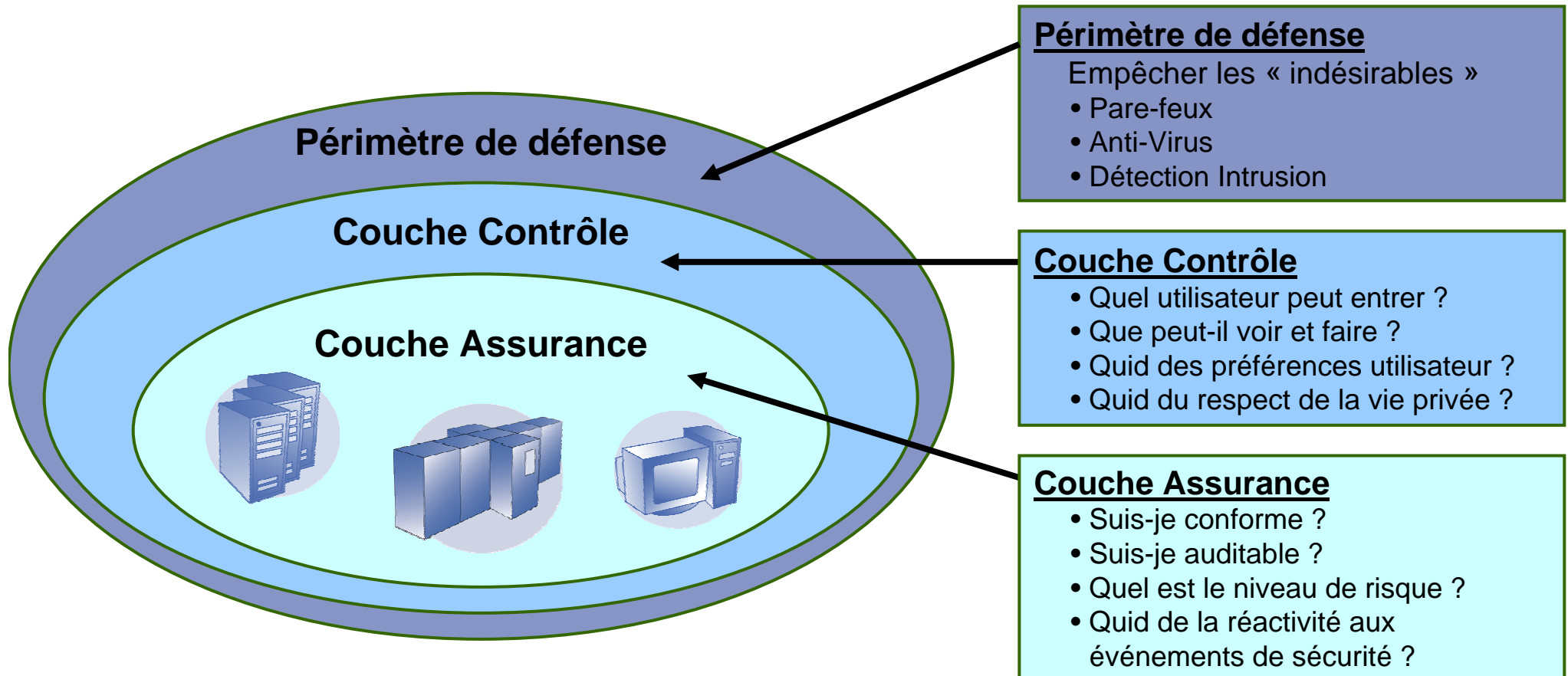
Source: ISACA, AFAI & H. Ceuleman 2004

Le référentiel ISO/IEC 17799 : 2005



		WHAT	HOW	WHERE	WHO	WHEN	WHY
		DATA	FUNCTION	NETWORK	PEOPLE	TIME	MOTIVATION
SCOPE (contextual)		List of Things Important to the Business  Entity = Class of	List of Processes the Business Performs  Process = Class of	List of Locations in Which the Business Operates  Node = Major Business	List of Organizations Important to the Business  People = Major	List of Events/Cycles Significant to the Business  Time = Major Business	Lists of Business Goals/Strategies  End/Means = Major
Planner		WHY	HOW	WHAT	WHO	WHERE	WHEN
BUSI (concept)	Business Architecture	Enterprise Missions	Enterprise Activities	Enterprise Information	Enterprise Organizations	Enterprise Locations	Enterprise Workload
Owner	Application Architecture	Applications/ Missions	Common Mission Applications	Knowledge & Property Applications	People & Organization Applications	Collaboration Applications	Budget & Financing Applications
SYST (logical)	Data Architecture	Information/ Missions	Common Mission Information	Knowledge & Property Data	People & Organization Data	Location Data	Budget & Financing Data
Designer	Security Architecture	Security Policy	Application Security	Information Security	Identification Security	Network security	Financial Security
TECH (physical)	Technology Architecture	Application Technologies	Integration Technologies	Data Technologies	Security Technologies	Network Technologies	Platform Technologies
Builder							
DETAILED REPRESENTATIONS (out-of-context)		e.g., Data Definition  Entity = Field Relationship = Address	e.g., Program  Process = Language Statement I/O = Control Block	e.g., Network Architecture  Node = Address Link = Protocol	e.g., Security Architecture  People = Identity Work = Job	e.g., Timing Definition  Time = Interrupt Cycle = Machine Cycle	e.g., Rule Specification  End = Sub-condition Means = Step
Subcontractor							
FUNCTIONING ENTERPRISE		e.g.: DATA	e.g.: FUNCTION	e.g.: NETWORK	e.g.: ORGANIZATION	e.g.: SCHEDULE	e.g.: STRATEGY

Architecture Sécurisée : il faut plus qu'une simple défense « périmétrique »



Description d'une méthodologie

- Les projets de système d'information et le chantier d'urbanisation du système d'information, doivent intégrer les données correspondant à la sécurité de l'information

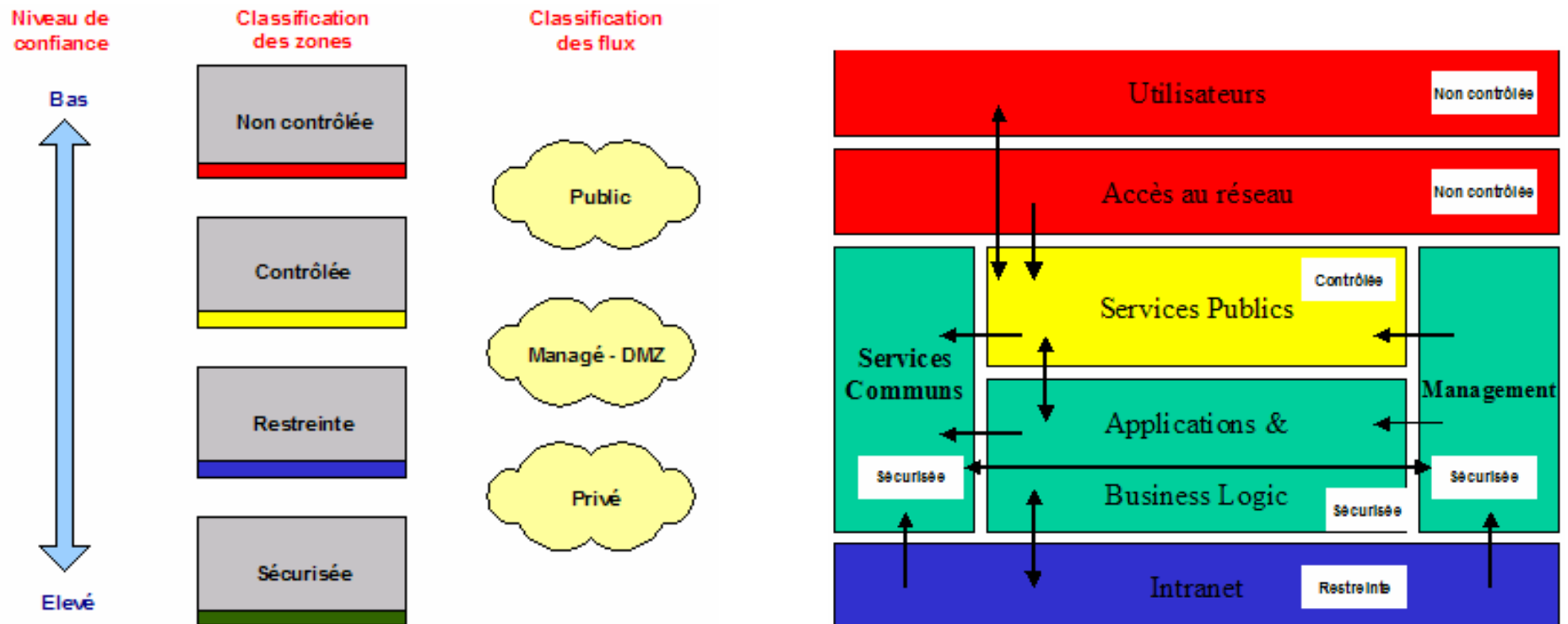
- L'urbanisation consiste à découper le SI en modules autonomes, dans le découpage d'un SI on distingue habituellement différents types de zones :
 - Les zones des échanges avec l'extérieur du SI : acquisition/émission de/vers les partenaires, clients, fournisseurs, etc. ;
 - Les zones des activités opérationnelles : gestion des opérations bancaires, gestion des opérations commerciales, gestion des opérations logistiques internes, etc. ;
 - Les zones de gestion des données de référence communes à l'ensemble du SI : les référentiels de données structurées (données clients, catalogue de produits et services, etc.) ;
 - Les zones de gestion des gisements de données : ensemble des informations produites quotidiennement, communes à l'ensemble du SI (données de production, etc.) ;
 - Les zones des activités de support : comptabilité, ressources humaines, etc. ;
 - Les zones des traitements pour l'aide à la décision et le pilotage : informatique décisionnelle.

Présentation de la méthodologie MASS d'IBM

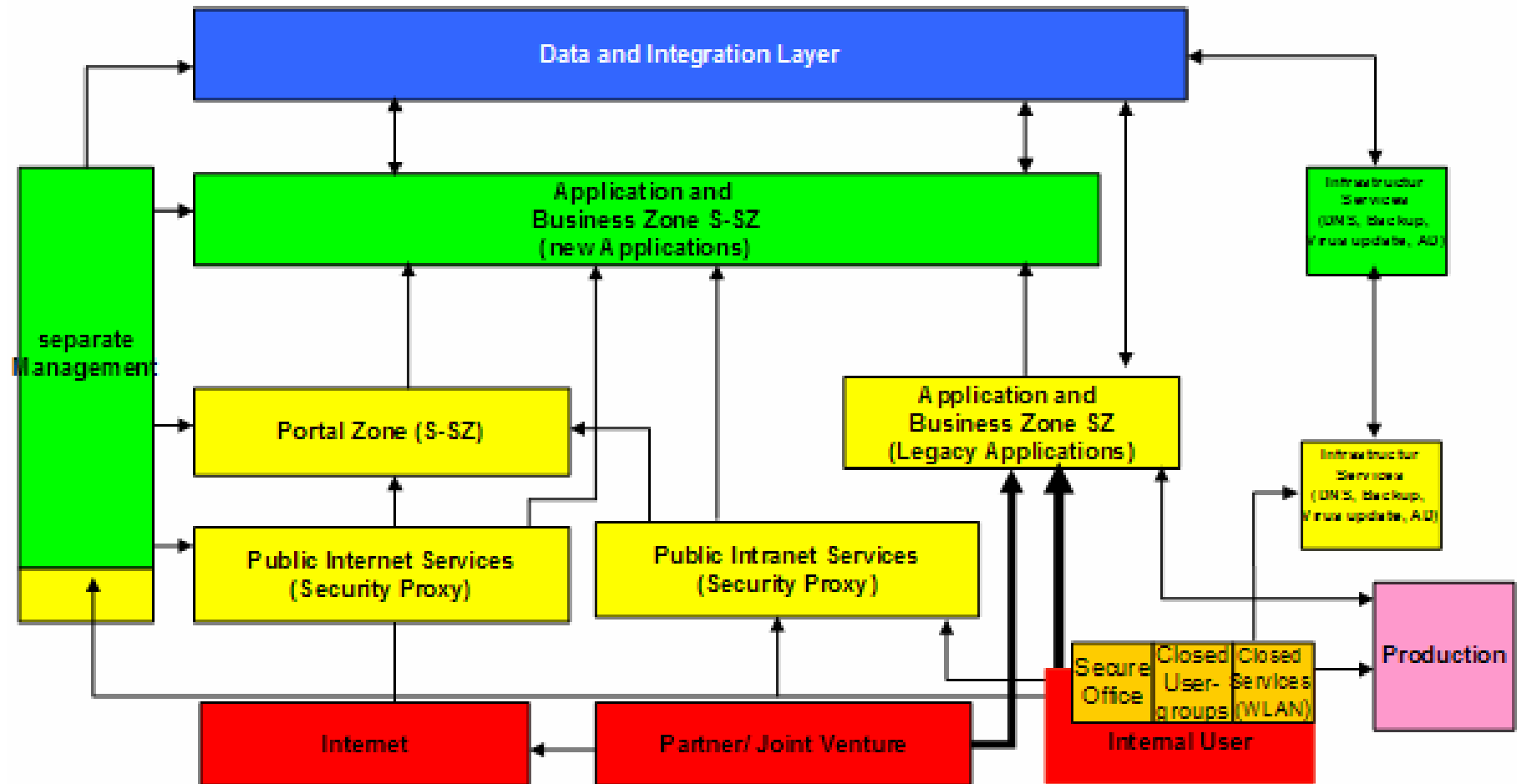
- La méthodologie MASS (Method for Architecting Secure Solutions) d'IBM s'appuie sur les principes de l'urbanisation du système d'information ainsi que sur les critères communs (CC).
- Les avantages de cette méthode, c'est quelle permet de bien définir les besoins en sécurité du système d'information ou d'une partie du système d'information. Elle permet de valider un niveau de sécurité EAL4.

Common Criteria	Definition	US TCSEC	European ITSEC
EAL0		D: minimal protection	E0
EAL1	functionally tested		
EAL2	structurally tested	C1: Discretionary security protection	E1
EAL3	methodically tested and checked	C2: Controlled access protection	E2
EAL4	methodically designed, tested and reviewed	B1: Labeled security protection	E3
EAL5	semiformally designed and tested	B2: Structured protection	E4
EAL6	semiformally verified design and tested	B3: Security domains	E5
EAL7	formally verified design and tested	A1: Verified design	E6

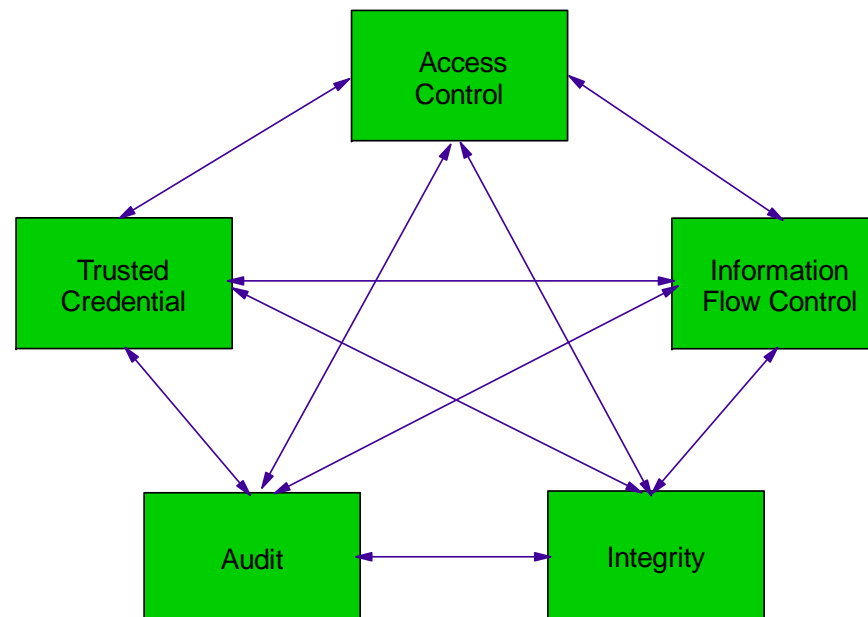
■ Définition des zones de contrôle de l'infrastructure



Exemple de définition des zones

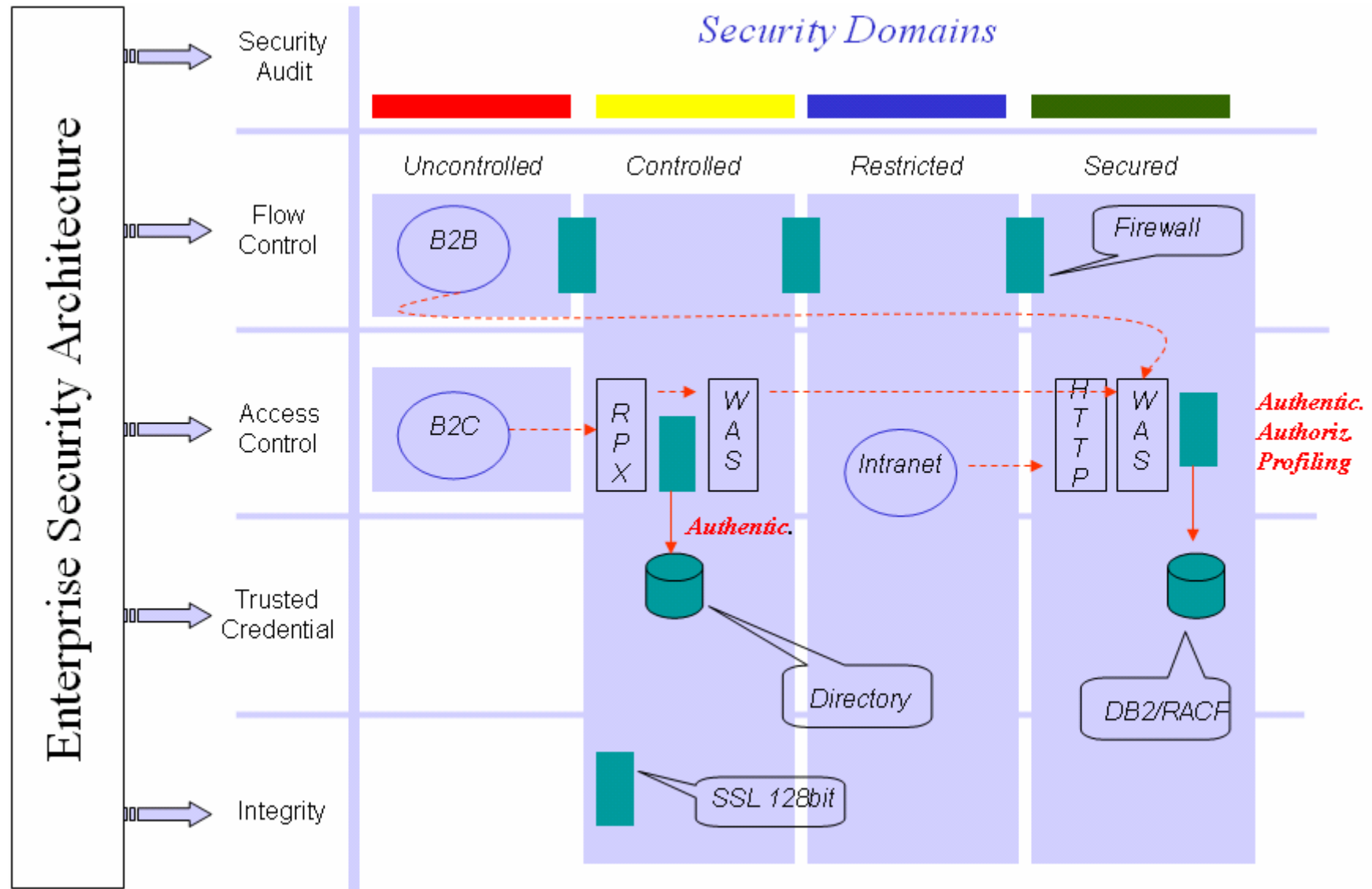


- Confronter les flux et les zones aux cinq critères communs que sont l'Audit, l'Intégrité, Flux d'information, Contrôle d'accès, Identification/permission.

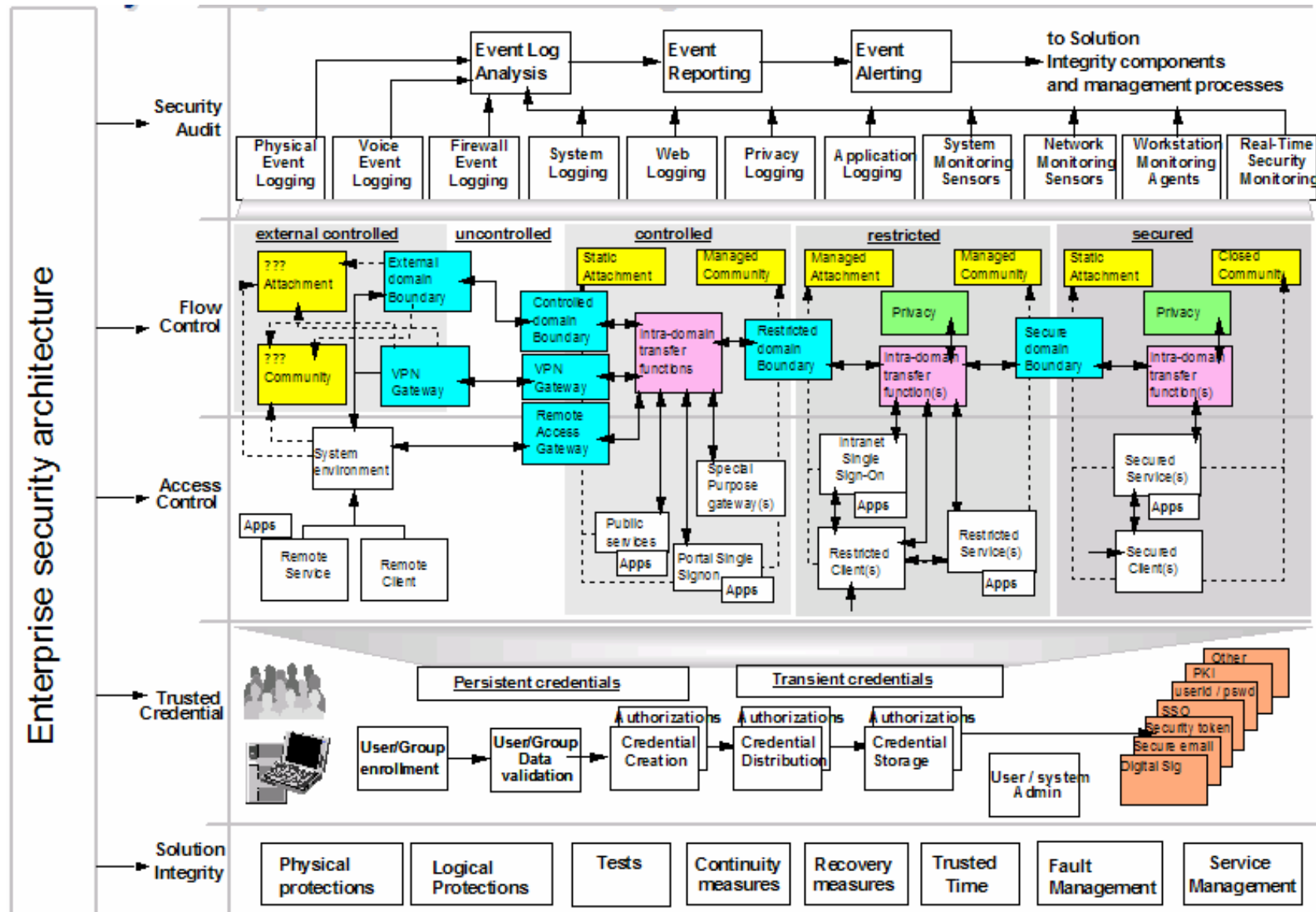


IT Security subsystems

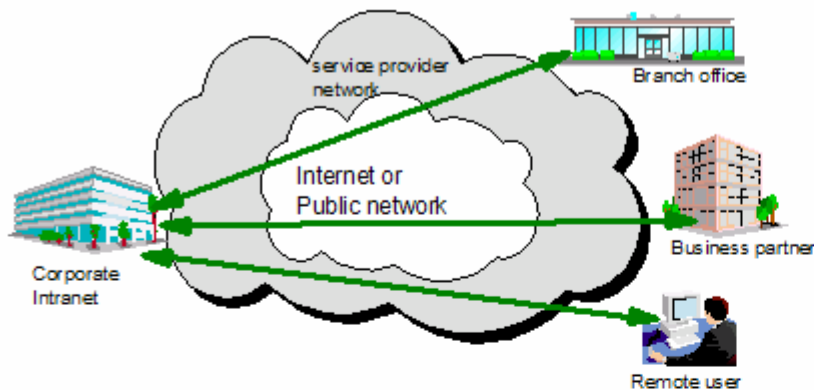
Exemple des Critères Communs de la sécurité



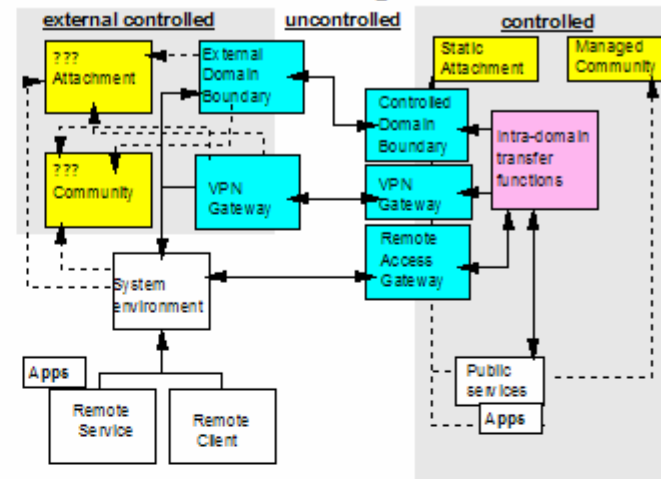
Vue générale avec les Critères Communs de la sécurité



Solution environment



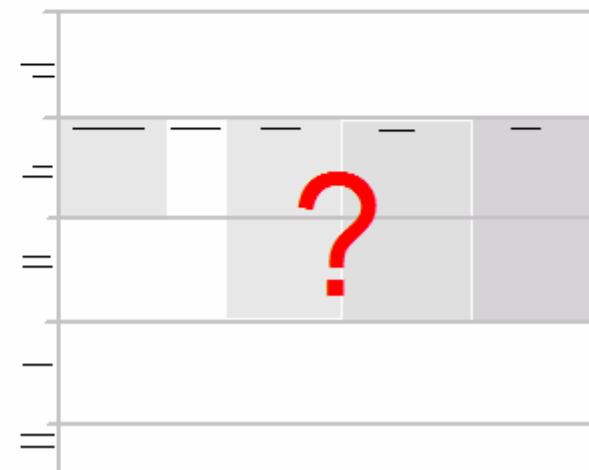
Functional design model



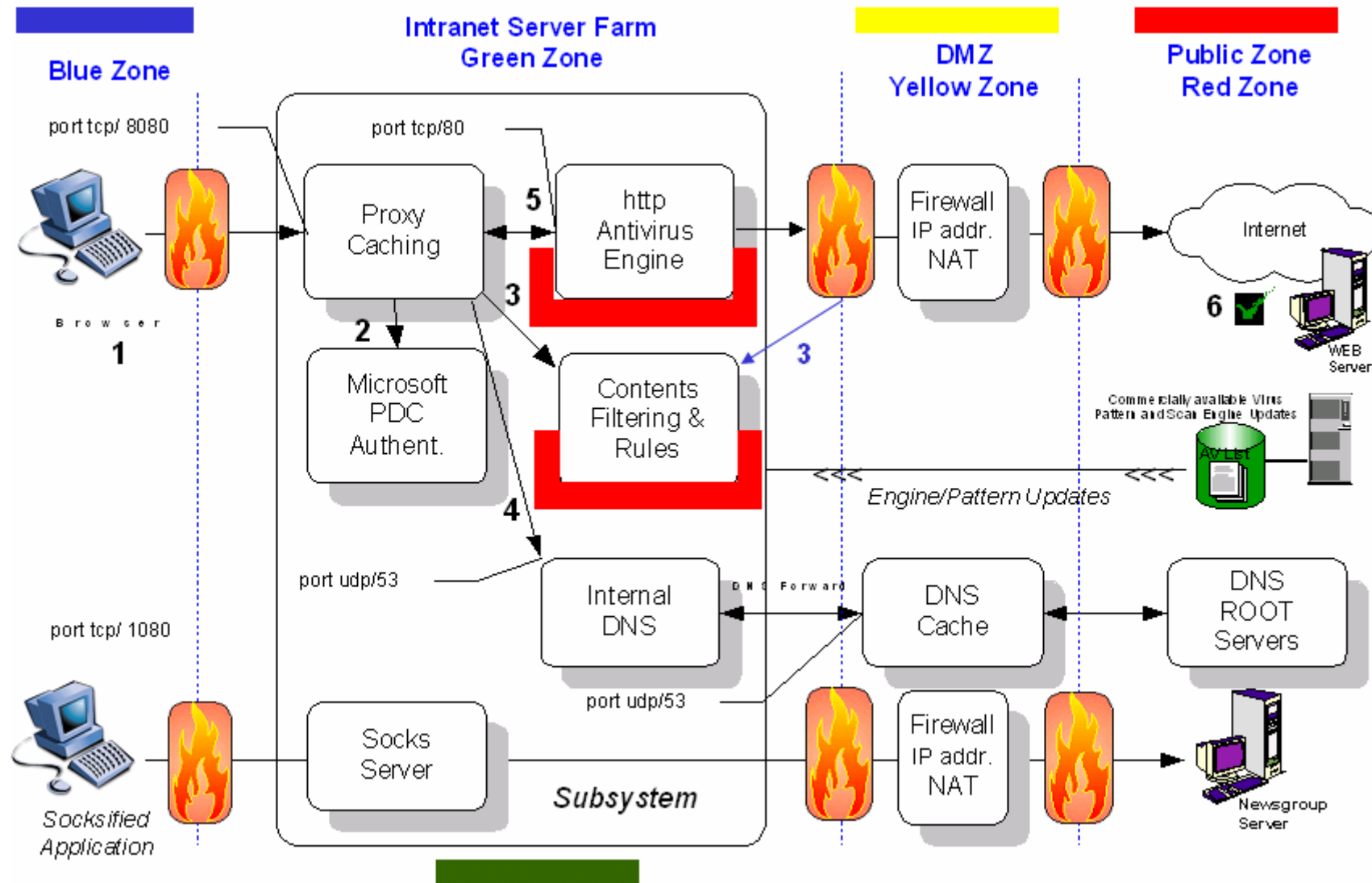
Security Design Objectives

1. Control access to, and use of, systems and processes consistent with roles and responsibilities
2. Control access to information consistent with roles, responsibilities and privacy policies
3. Control the flow of information consistent with information classification, and privacy policies
4. Manage the reliability and integrity of components in support of compliance requirements
5. Prevent or mitigate attacks
6. Deploy and manage trusted identity to ensure accountability
7. Prevent or mitigate fraud

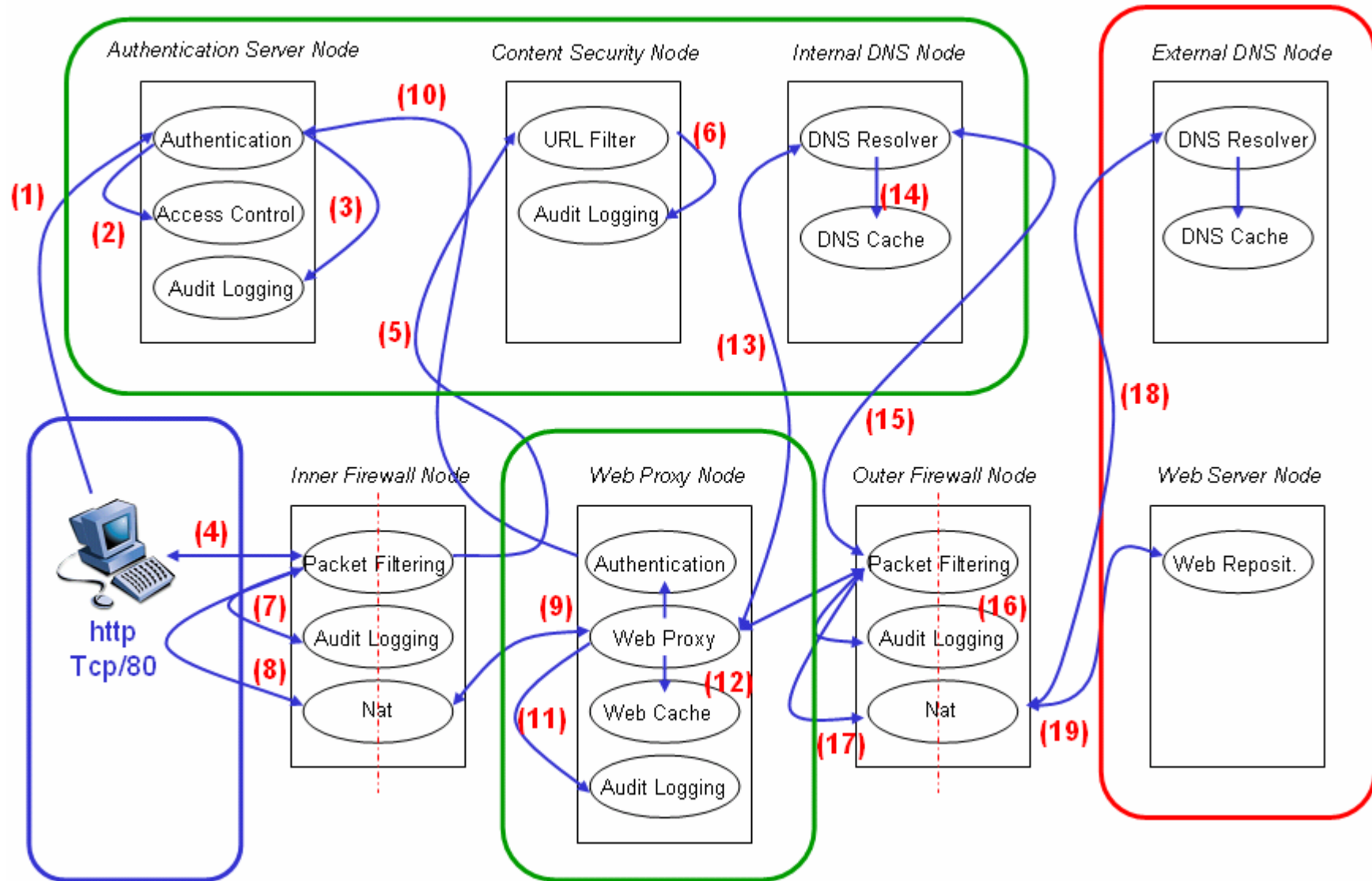
Solution design model



Exemple d'une infrastructure d'accès internet (1/2)



Exemple d'une infrastructure d'accès internet (2/2)



- Enterprise Security Architecture (ESA):
 - ESA se rapporte **à la conception cohésive** des services de sécurité.
 - ESA doit assurer les services de confidentialité, d'intégrité, et de disponibilité dans toute l'entreprise et doit s'aligner avec les objectifs business.
 - "Elements of an Enterprise Security Architecture: Policy , Security Domains, Trust Levels, Tiered Networks"

- Infrastructure Security Architecture (ISA):
 - ISA se rapporte aux éléments **de support** requis pour les mécanismes de sécurité.
 - ISA doit assurer la performance, la disponibilité, la fiabilité des mécanismes en place et cela dans le respect des besoins fonctionnels. ISA est un sous-ensemble d'ESA.
 - "Elements of an Infrastructure Security Architecture: Intrusion Detection Systems, Firewalls, & Host-based Protection"