



IT Security in Hungarian public administration Models of Information Security Architecture in Practice

Bálint Molnár¹,

¹ *Loránd Eötvös University Of Sciences, Faculty
of Informatics, Information Systems Department*

E-mail: molnarba@inf.elte.hu



Tasks and issues

- There is a law on Information Security namely 2013. L. law, and its modification 2015. CXXX.
- Stakeholders : Central and local governments, and their offices, authorities, institutes, agencies etc.
- For Enterprises it is a proposal
- There is an obligation for stakeholders to categorize the information systems in operations
 - Assessment of information from the viewpoint of confidentiality, data protection, data privacy
 - Threats, vulnerabilities, risks either outside or inner



Tasks and issues

- Dealing with security issues during Stages within Life-cycle of Information Systems
 - Analysis
 - Design
 - Development
 - Operations
 - Maintenance
- The information security is wide spread
- It cannot be restricted only to some areas as
 - Network security
 - Virus protection
 - IP – Intrusion protection
 - Data, information protection and security
- A role is defined by the law : Custodian of Information Security
- The typical approach of Custodians to constrain their activities only on „security issues”



Holistic approach

- However, what is needed?
- An Enterprise Architecture approach
 - Applying of the analysis, design and descriptive methods
- What methods may be used
 - Zachman architecture/ontology
 - TOGAF (Open Group, <http://www.opengroup.org/subjectareas/enterprise/togaf>)
 - SABSA (Sherwood Applied Business Security Architecture, https://en.wikipedia.org/wiki/Sherwood_Applied_Business_Security_Architecture)
 - Software architecture (IEEE 1471-2000 (ISO/IEC 42010:2007)

Mit értünk architektúra alatt

IEEE 1471-2000 (ISO/IEC 42010:2007) (<http://www.iso-architecture.org/ieee-1471/ieee-1471-faq.html>)

Definition from ANSI/IEEE 1471-2000

“The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution”

– Boehm et al., 1995

A software system architecture comprises

A collection of software and system components, connections, and constraints.

A collection of system stakeholders' need statements.

A rationale which demonstrates that the components, connections, and constraints define a system that, if implemented, would satisfy the collection of system stakeholders' need statements.

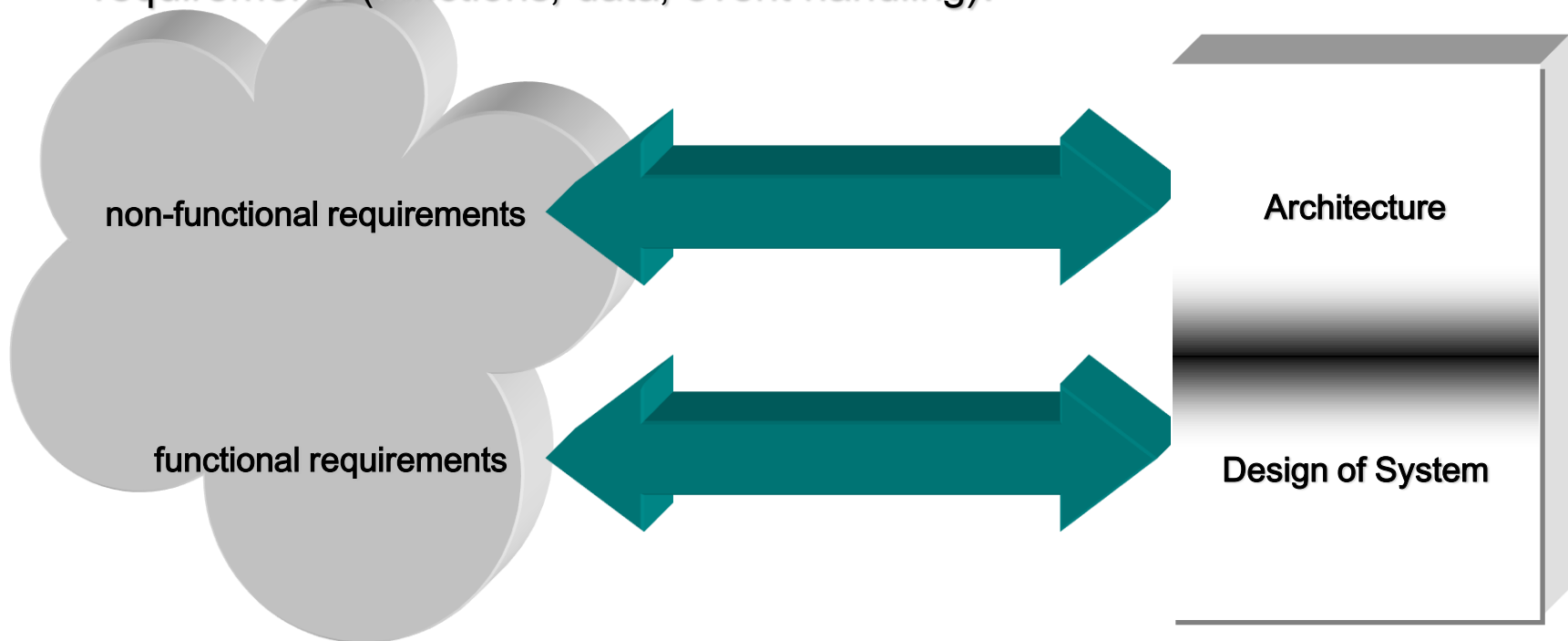


Architektúra tervezés kontra rendszertervezés



Architecture: The domain of decisions on non-functional requirements

Design of System: Successful implementation of functional requirements (functions, data, event handling).



That is generic scheme – The real world is much more complex.



The quality feature of Systems

Efficiency

Time behaviour

Resource utilization

Efficiency compliance

Security

Usability

Maintainability

Portability

Reliability

Testability

Viewpoint of
End-user

Time to market

Cost / benefit

Estimated life cycle

Market niche

Interoperability to legacy
systems

Backup













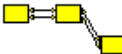























Developer's view

Business
view

ISO/IEC 9126-2001 Information Technology – Software Product Quality
(http://en.wikipedia.org/wiki/ISO_9126)

Zachman Framework



	Data	Function	Network	People	Time	Motive
Planner's View	Business Things  Entity = Class of Business Thing	Processes Performed  Function = Class of Business Process	Business Locations  Node = Major Business Locations	Organizations  People = Major Organizations	Significant Events  Time = Major Business Event	Goals and Strategy  Ends/Means = Major Business Goals
Owner's View	Semantic Model  Ent = Business Entity Rel = Relationship	Process Model  Proc = Process I/O = Resources	Logistics System  Node = Location Link = Linkage	Work Flow Model  People = Organization Work = Work Product	Master Schedule  Time = Business Event Cycle = Business Cycle	Business Plan  End = Objective Means = Strategy
Designer's View	Logical Data Model  Ent = Data Entity Rel = Relationship	Application Architecture  Proc = Function I/O = User Views	System Architecture  Node = IS Function Link = Line Properties	Interface Architecture  People = Role Work = Deliverable	Processing Structure  Time = System Event Cycle = Processing	Business Rule Model  End = Structure Means = Action
Builder's View	Physical Data Model  Ent = Segment/Table Rel = Pointer/Key	System Design  Proc = Function I/O = Data Elements	Technology Architecture  Node = Hardware/Software Link = Line Specs	Screen Architecture  People = User Work = Screen Format	Control Structure  Time = Execute Cycle = Component	Rule Design  End = Condition Means = Action
Integrator's View	Data Definition  Ent = Field Rel = Address	Program  Proc = Statement I/O = Control Block	Network Architecture  Node = Addresses Link = Protocols	Security Architecture  People = Identity Work = Job	Timing Definition  Time = Interrupt Cycle = Machine Cycle	Rule Design  End = Sub-Condition Means = Step
User's View	Data  Ent = Rel =	Function  Proc = I/O =	Network  Node = Link =	Organization  People = Work =	Schedule  Time = Cycle =	Strategy  End = Means =

A complex model – Big Picture

Why we need it?



Carte Figurative des pertes successives en hommes de l'Armée Française dans la campagne de Russie 1812-1813.
 Dressée par M. Minard, Inspecteur Général des Ponts et Chaussées en retraite. Paris, le 20 Novembre 1869.

Les nombres d'hommes présents sont représentés par les largeurs des zones colorées à raison d'un millimètre pour dix mille hommes; ils sont de plus écrits en travers des zones. Le rouge désigne les hommes qui entrent en Russie, le noir ceux qui en sortent. — Les renseignements qui ont servi à dresser la carte ont été puisés dans les ouvrages de M. M. Chiers, de Légar, de Fezensac, de Chambray et le journal inédit de Jacob, pharmacien de l'Armée depuis le 28 Octobre. Pour mieux faire juger à l'œil la diminution de l'armée, j'ai supposé que les corps du Prince Nicôme et du Maréchal Davout qui avaient été détachés sur Minsk et Mohilow et ont rejoint vers Orscha et Witebsk, avaient toujours marché avec l'armée.

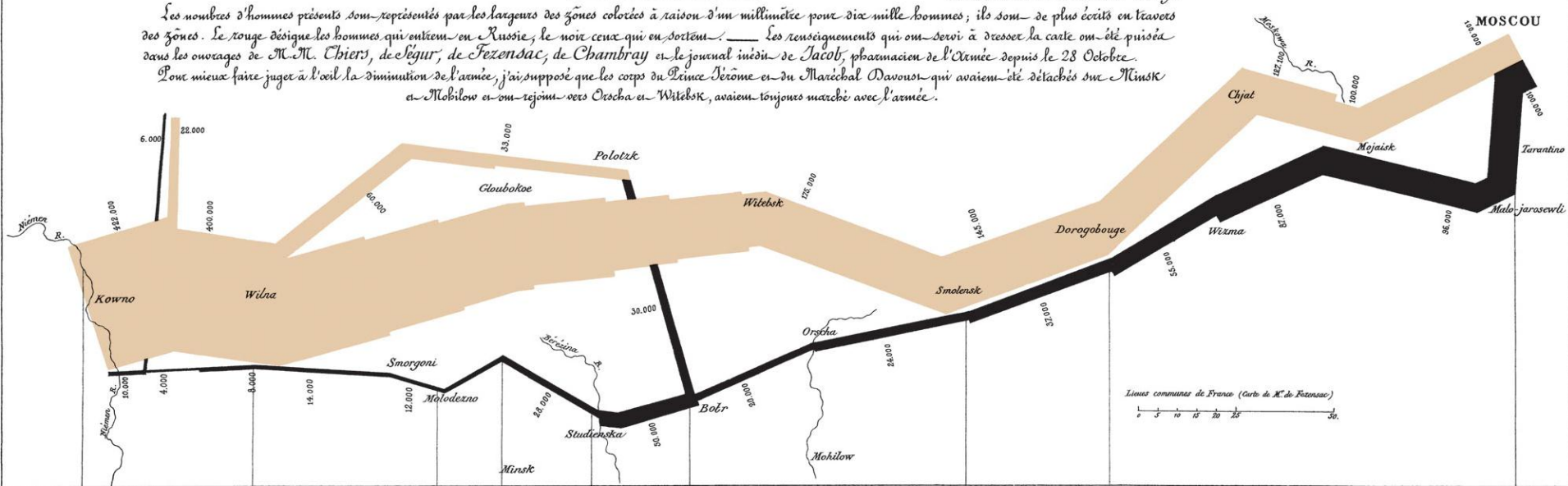
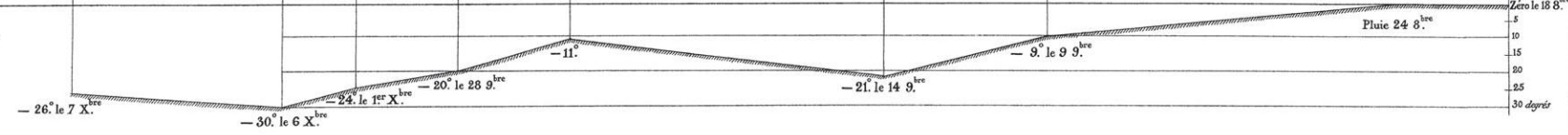


TABLEAU GRAPHIQUE de la température en degrés du thermomètre de Réaumur au dessous de zéro.

Les Cosaques passent au galop le Niemen gelé.



Autog. par Regnier, 8. Par. S^{te} Marie St O^{de} à Paris.

Imp. Lith. Regnier et Doussot.

Zachman Framework

Row 1 – Scope

External Requirements and Drivers
Business Function Modeling

■ Row 2 – Enterprise Model

Business Process Models

■ Row 3 – System Model

Logical Models
Requirements Definition

■ Row 4 – Technology Model

Physical Models
Solution Definition and Development

■ Row 5 – As Built

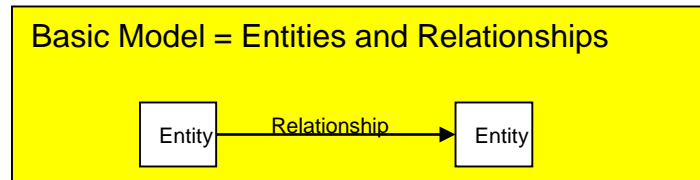
As Built
Deployment

■ Row 6 – Functioning Enterprise

Functioning Enterprise
Evaluation

		Mit	Hogyan	Hol	Ki	Mikor	Miért	
1	Környezet							Környezet
2	Fogalmi							Fogalmi
3	Logikai							Logikai
4	Fizikai							Fizikai
5	Megvalósított							Megvalósított
6	Működő							Működő
		Mit	Hogyan	Hol	Ki	Mikor	Miért	

Basic Rules of the Framework



Rule 1:

Columns have no order

■ Rule 2:

Each column has a simple, basic model

■ Rule 3:

Basic model of each column is unique

■ Rule 4:

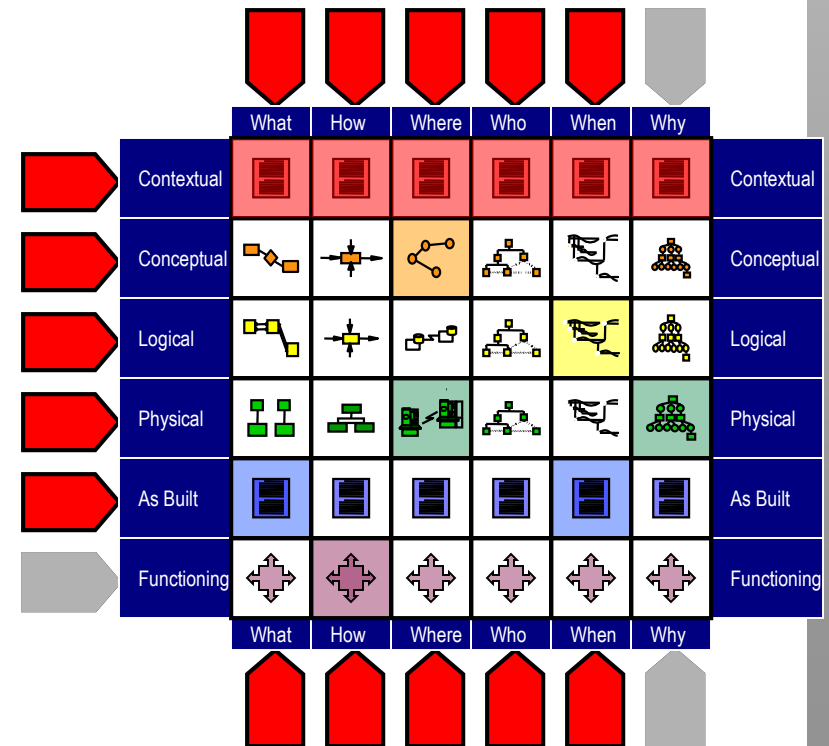
Each row represents a distinct view








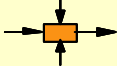

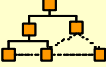



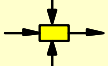

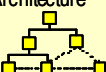




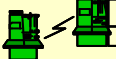
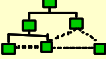








■ Rule 5:

Each cell is unique

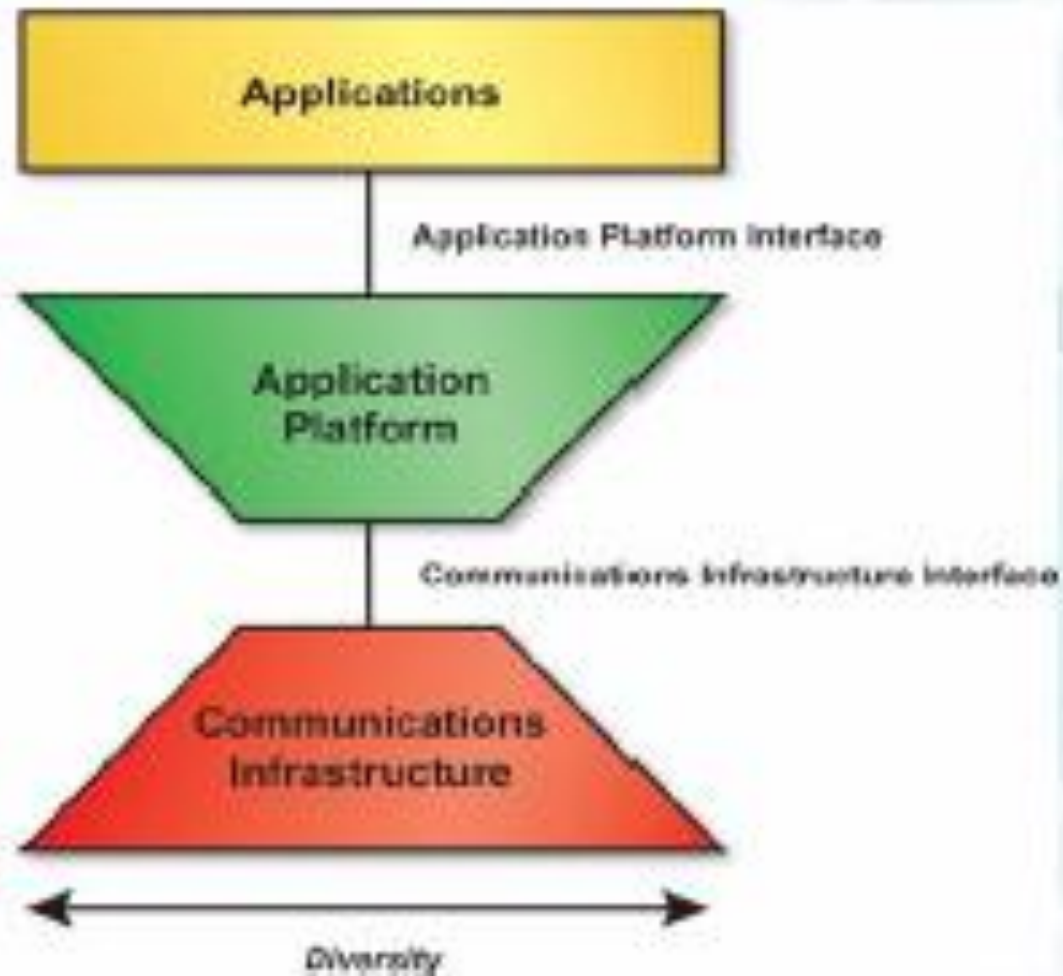
■ Rule 6:

Combining the cells in one row forms a complete description from that view



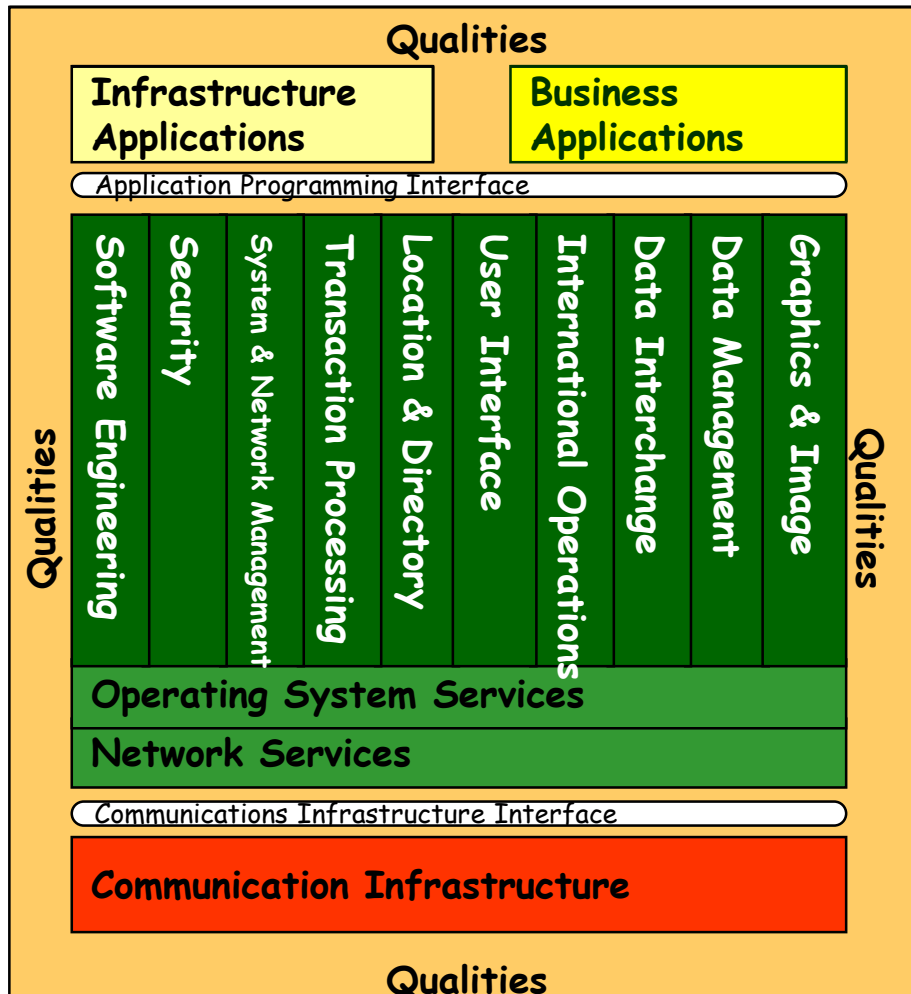
VA Enterprise Architecture	DATA <i>What</i>	FUNCTION <i>How</i>	NETWORK <i>Where</i>	PEOPLE <i>Who</i>	TIME <i>When</i>	MOTIVATION <i>Why</i>	Based on work by John A. Zachman
SCOPE (CONTEXTUAL) <i>Planner</i>	Things Important to the Business  Entity = Class of Business Thing	Processes Performed  Function = Class of Business Process	Business locations  Node = Major Business Locations	Important Organizations  People = Major Organizations	Events Significant to the Business  Time = Major Business Event	Business Goals and Strategy  Ends/Mean = Major Business Goals	SCOPE (CONTEXTUAL) <i>Planner</i>
ENTERPRISE MODEL (CONCEPTUAL) <i>Owner</i>	Semantic Model  Ent = Business Entity Rel = Business Relationship	Business Process Model  Proc = Business Process I/O = Business Resources	Business Logistics System  Node = Business Location Link = Business Linkage	Work Flow Model  People = Organization Unit Work = Work Product	Master Schedule  Time = Business Event Cycle = Business Cycle	Business Plan  End = Business Objective Means = Business Strategy	ENTERPRISE MODEL (CONCEPTUAL) <i>Owner</i>
SYSTEM MODEL (LOGICAL) <i>Designer</i>	Logical Data Model  Ent = Data Entity Rel = Data Relationship	Application Architecture  Proc = Application Function I/O = User Views	Distributed System Architecture  Node = IS Function Link = Line Characteristics	Human Interface Architecture  People = Role Work = Deliverable	Processing Structure  Time = System Event Cycle = Processing Cycle	Business Rule Model  End = Structural Assertion Means = Action Assertion	SYSTEM MODEL (LOGICAL) <i>Designer</i>
TECHNOLOGY MODEL (PHYSICAL) <i>Builder</i>	Physical Data Model  Ent = Segment/Table Rel = Pointer/Key	System Design  Proc = Computer Function I/O = Data Elements/Sets	Technology Architecture  Node = Hardware/Software Link = Line Specifications	Presentation Architecture  People = User Work = Screen Format	Control Structure  Time = Execute Cycle = Component Cycle	Rule Design  End = Condition Means = Action	TECHNOLOGY MODEL (PHYSICAL) <i>Builder</i>
DETAILED REPRESENTATIONS (OUT-OF-CONTEXT) <i>Sub-Contractor</i>	Data Definition  Ent = Field Rel = Address	Program  Proc = Language Statement I/O = Control Block	Network Architecture  Node = Addresses Link = Protocols	Security Architecture  People = Identity Work = Job	Timing Definition  Time = Interrupt Cycle = Machine Cycle	Rule Design  End = Sub-Condition Means = Step	DETAILED REPRESENTATIONS (OUT-OF-CONTEXT) <i>Sub-Contractor</i>
FUNCTIONING ENTERPRISE	Data Ent = Rel =	Function Proc = I/O =	Network Node = Link =	Organization People = Work =	Schedule Time = Cycle =	Strategy End = Means =	FUNCTIONING ENTERPRISE
	DATA <i>What</i>	FUNCTION <i>How</i>	NETWORK <i>Where</i>	PEOPLE <i>Who</i>	TIME <i>When</i>	MOTIVATION <i>Why</i>	

High-level technical reference model





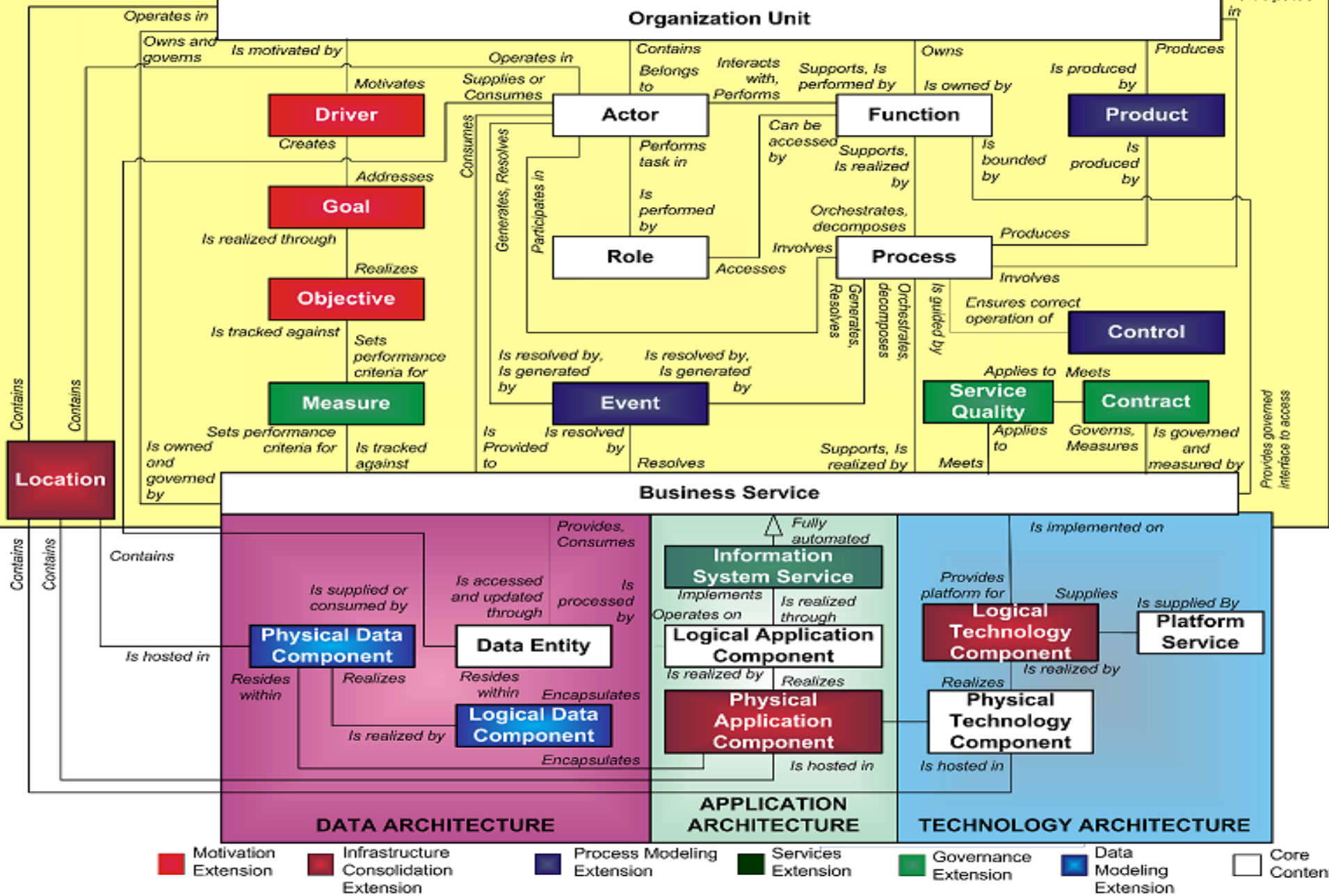
Foundation Architecture: Technical Reference Model (TRM)



Associated with detailed taxonomy of **services** defines scope of each service category

Identifies system-wide capabilities (“**qualities**”), e.g.:

- Internationalization
- Security
- Management



Cross reference tables, matrices, catalogs and diagrams

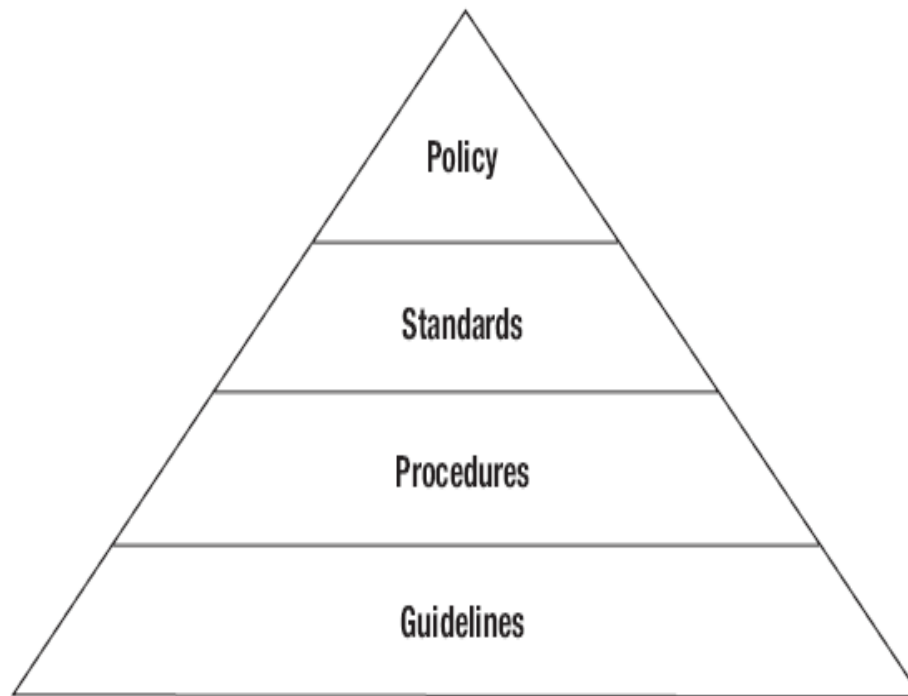


<p>Preliminary Phase</p> <ul style="list-style-type: none"> Principles catalog 	<p>Phase B, Business Architecture</p> <ul style="list-style-type: none"> Organization/Actor catalog Driver/Goal/Objective catalog Role catalog Business Service/Function catalog Location catalog Process/Event/Control/Product catalog Contract/Measure catalog Business Interaction matrix Actor/Role matrix Business Footprint diagram Business Service/Information diagram Functional Decomposition diagram Product Lifecycle diagram Goal/Objective/Service diagram Use-Case diagram Organization Decomposition diagram Process Flow diagram Event diagram 	<p>Phase C, Data Architecture</p> <ul style="list-style-type: none"> Data Entity/Data Component catalog Data Entity/Business Function matrix System/Data matrix Class diagram Data Dissemination diagram Data Security diagram Class Hierarchy diagram Data Migration diagram Data Lifecycle diagram 	<p>Phase C, Application Architecture</p> <ul style="list-style-type: none"> Application Portfolio catalog Interface catalog System/Organization matrix Role/System matrix System/Function matrix Application Interaction matrix Application Communication diagram Application and User Location diagram System Use-Case diagram Enterprise Manageability diagram Process/System Realization diagram Software Engineering diagram Application Migration diagram Software Distribution diagram
<p>Phase A, Architecture Vision</p> <ul style="list-style-type: none"> Stakeholder Map matrix Value Chain diagram Solution Concept diagram 	<p>Phase D, Technology Architecture</p> <ul style="list-style-type: none"> Technology Standards catalog Technology Portfolio catalog System/Technology matrix Environments and Locations diagram Platform Decomposition diagram Processing diagram Networked Computing/Hardware diagram Communications Engineering diagram 	<p>Phase E, Opportunities & Solutions</p> <ul style="list-style-type: none"> Project Context diagram Benefits diagram 	<p>Requirements Management</p> <ul style="list-style-type: none"> Requirements catalog

Documentation for Information Security



policies, standards, procedures and guidelines.





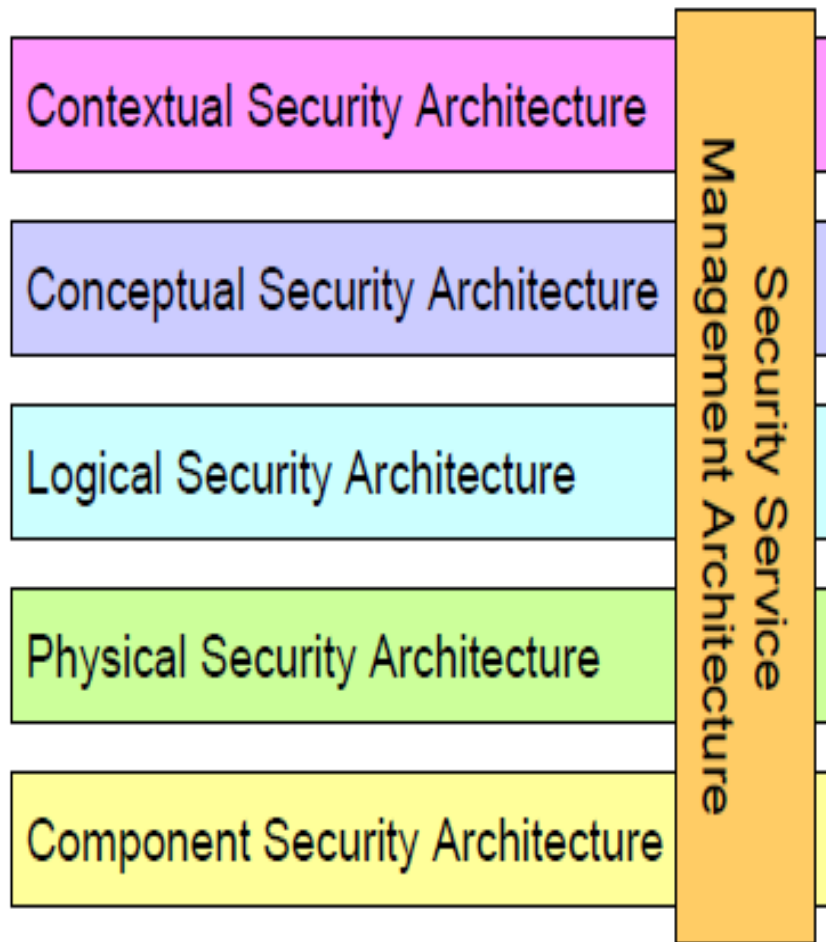
Options for Implementation

Open frameworks

Directed implementation

Level of Policies COBIT: ingyenes NIST: ingyenes ISO 27000/...: \$...	SABSA
Szabvány szint ISO 15408: \$.....	
Level of Procedures	Development is required on their own

SABSA Model for Information Security





Layers of Security Architecture

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture



Information
Systems in
Operation
IT
Infrastructure

SABSA matrix



	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	Processing 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 & Performance 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

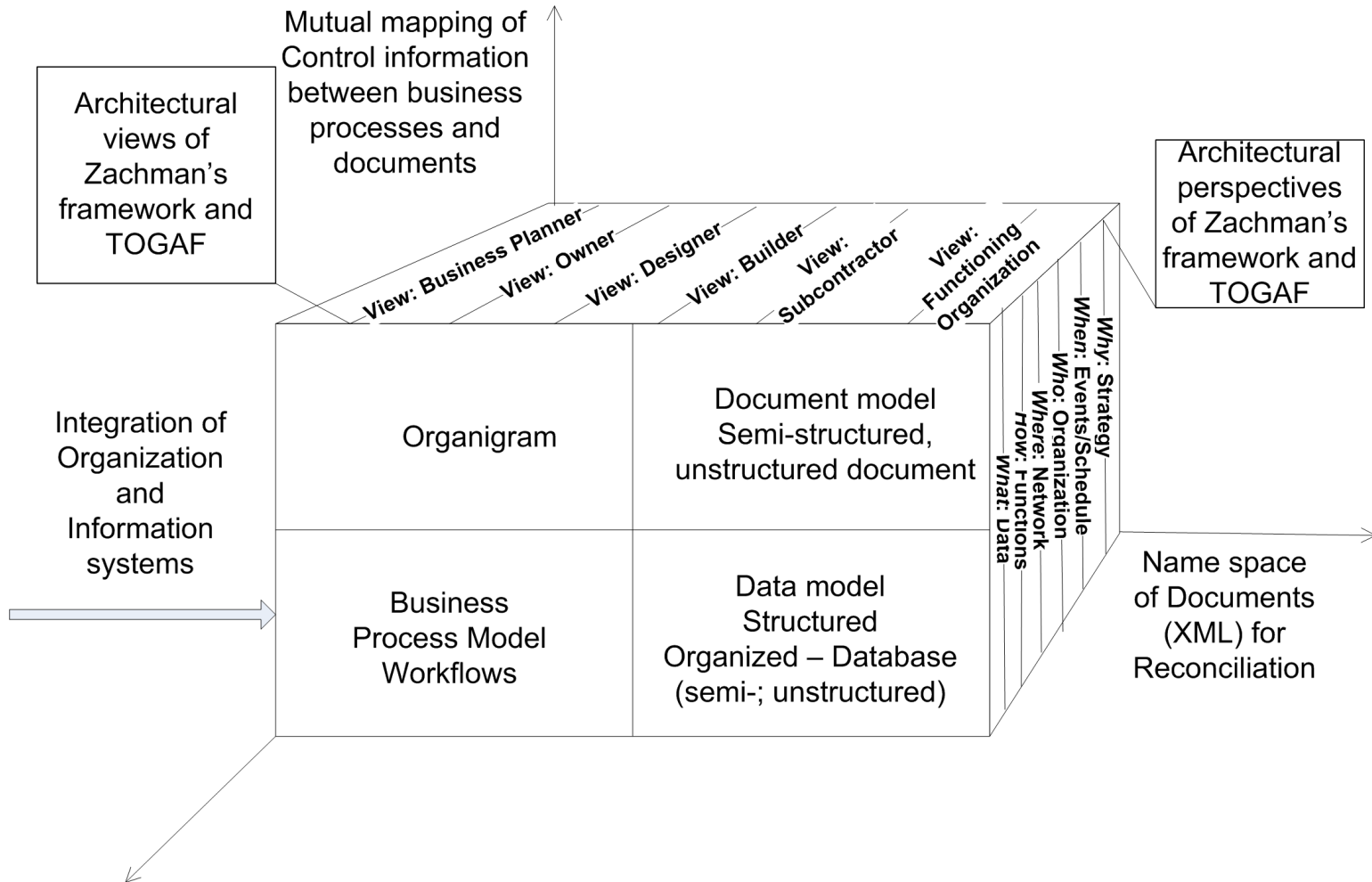
SABSA matrix and ITIL v3



TABLE 7. SABSA SERVICE MANAGEMENT MATRIX (aligned with ITIL v3)

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
CONTEXTUAL ARCHITECTURE	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities for Providing Value to Customers	Managing Service Providers & Service Customers; Contract Man'ment	Demand Man'ment; Service Supply, Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing ORM Objectives	Service Delivery Planning	Service Management Roles	Service Portfolio	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Risk Analysis on Business Attributes Proxy Assets	SLA Planning; BCP; Financial Planning & ROI; Transition Planning	Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Service Catalogue	Managing Service Performance Criteria and Targets
LOGICAL ARCHITECTURE	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management; Test & Validation Management	Policy Development; Policy Compliance Auditing	SLA Management; Supplier Management; BCM; Cost Management; Transition Management	Access Management; User Privileges, Account Administration & Provisioning	Configuration Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Asset Security & Protection	Operational Risk Data Collection	Operations Management	User Support	Service Resources Protection	Service Performance Data Collection
	Change Management; Software & Data Integrity Protection	Operational Risk Management Architecture	Job Scheduling; Incident & Event Management; Disaster Recovery	Service Desk; Problem Man'ment; Request Man'ment	Physical & Environmental Security Management	Systems and Service Monitoring Architecture
COMPONENT ARCHITECTURE	Tool Protection	ORM Tools	Tool Deployment	Personnel Deployment	Security Management Tools	Service Monitoring Tools
	Product & Tool Security & Integrity; Product & Tool Maintenance	ORM Analysis, Monitoring and Reporting Tools & Display Systems	Product & Tool Selection and Procurement; Project Management	Recruitment Process Disciplinary Process Training & Awareness Tools	Products & Tools for Managing Physical & Logical Security of Installations	Service Analysis, Monitoring and Reporting Tools & Display Systems

Enterprise architecture and document centric approaches



Conclusion



- Creating and maintaining information security requires:
 - Methods for systematic description and design for Enterprise wide Security Architecture
 - There exists Enterprise, Software and Security architecture methods
 - There is methodology for information security and secure operations
 - The prescription of the Information Security Law and related legal rules can be implemented and maintained through the systematic and disciplined application of Architecture approach.

Thank You for Your Attention



...Questions?