

Visualising Security Threats using the Zachman Enterprise Architecture Framework

Bellua Cyber Security
Conference
Jakarta August 2006

John Grygorcewicz

johng@bisproconsulting.com

This document and the information it contains is presented commercial in confidence and contains information that is the intellectual property of Bispro Consulting and others. Its use out side of the purpose of discussion in any manner or any form constitutes a breach of copyright.

Why Use a Framework

Why Zachman

What is the Zachman Framework

How it Can help In Security Management

Questions

Content based on the work of Levent Ertaul and Raadika Sudarsanam from the University of California

Why Use a Framework ?

This document and the information it contains is presented commercial in confidence and contains information that is the intellectual property of Bispro Consulting. Its use out side of the purpose of discussion in any manner or any form constitutes a breach of copyright. Please contact Bispro on +62 21 3918330 for clarification.

Why Use a Framework ?

BCS 2006
Jakarta

- Business is becoming complex
- IT infrastructure and IT solutions integration is becoming complex
- Adds an additional layer of discipline to the management of security
- Give a single frame of reference for improved communication
- Ensures that structure is added to the analysis process.
- Help visualize the many security touch points, physical as well as logical.
- Assists in Policy formulation.

Why Use Zachman ?

This document and the information it contains is presented commercial in confidence and contains information that is the intellectual property of Bispro Consulting. Its use out side of the purpose of discussion in any manner or any form constitutes a breach of copyright. Please contact Bispro on +62 21 3918330 for clarification.







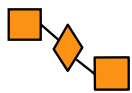
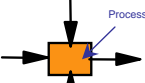
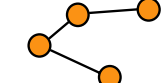
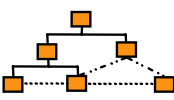
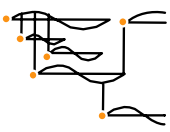
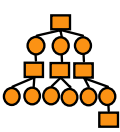
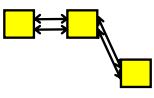
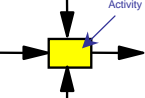
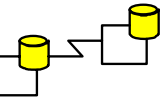
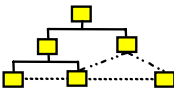
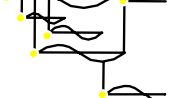
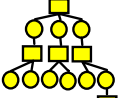
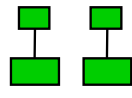
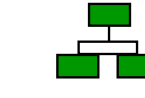
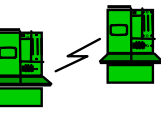
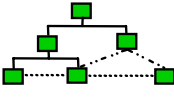

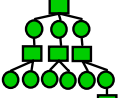






- You can use any framework that covers the 6 areas of Who What Why When Where How.
- Many organisations are realizing that they do not have full visibility into the organization and are looking at the Zachman framework due to its completeness.
- It has been around a long time, since 1987
- It focuses on Enterprise Architecture and the roles involved.

What is the Zachman Framework ?

This document and the information it contains is presented commercial in confidence and contains information that is the intellectual property of Bispro Consulting. Its use out side of the purpose of discussion in any manner or any form constitutes a breach of copyright. Please contact Bispro on +62 21 3918330 for clarification.

What is the Zachman Framework ?

BCS 2006
Jakarta

	DATA <i>What</i>	FUNCTION <i>How</i>	NETWORK <i>Where</i>	PEOPLE <i>Who</i>	TIME <i>When</i>	MOTIVATION <i>Why</i>	
SCOPE (CONTEXTUAL) <i>Planner</i>	List of Things Important to the Business  ENTITY = Class of Business Thing	List of Processes the Business Performs  Function = Class of Business Process	List of Locations in which the Business Operates  Node = Major Business Location	List of Organizations Important to the Business  People = Major Organizations	List of Events Significant to the Business  Time = Major Business Event	List of Business Goals/Strat  Ends/Mean=Major Bus. Goal/ Critical Success Factor	SCOPE (CONTEXTUAL) <i>Planner</i>
ENTERPRISE MODEL (CONCEPTUAL) <i>Owner</i>	e.g. Semantic Model  Ent = Business Entity ReIn = Business Relationship	e.g. Business Process Model  Proc. = Business Process I/O = Business Resources	e.g. Business Logistics System  Node = Business Location Link = Business Linkage	e.g. Work Flow Model  People = Organization Unit Work = Work Product	e.g. Master Schedule  Time = Business Event Cycle = Business Cycle	e.g. Business Plan  End = Business Objective Means = Business Strategy	ENTERPRISE MODEL (CONCEPTUAL) <i>Owner</i>
SYSTEM MODEL (LOGICAL) <i>Designer</i>	e.g. Logical Data Model  Ent = Data Entity ReIn = Data Relationship	e.g. Application Architecture  Proc. = Application Function I/O = user views	e.g. Distributed System Architecture  Node = I/S Function (Processor, Storage, etc) Link = Line Characteristics	e.g. Human Interface Architecture  People = Role Work = Deliverable	e.g. Processing Structure  Time = System Event Cycle = PROCESSING Cycle	e.g. Business Rule Model  End = Structural Assertion Means =Action Assertion	SYSTEM MODEL (LOGICAL) <i>Designer</i>
TECHNOLOGY MODEL (PHYSICAL) <i>Builder</i>	e.g. Physical Data Model  Ent = Segment/Table/etc. ReIn = Pointer/Key/etc.	e.g. System Design  Proc.= Computer Function I/O = Data Elements/Sets	e.g. Technology Architecture  Node = Hardware/System Software Link = Line Specifications	e.g. Presentation Architecture  People = User Work = Screen Format	e.g. Control Structure  Time = Execute Cycle = Component Cycle	e.g. Rule Design  End = Condition Means = Action	TECHNOLOGY MODEL (PHYSICAL) <i>Builder</i>
DETAILED REPRESENTATIONS <i>Sub Contractor</i>	e.g. Data Definition  Ent = Field ReIn = Address	e.g. Program  Proc.= Language Stmt I/O = Control Block	e.g. Network Architecture  Node = Addresses Link = Protocols	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	DETAILED REPRESENTATIONS (OUT-OF CONTEXT) <i>Sub-Contractor</i>
FUNCTIONING ENTERPRISE	e.g. DATA	e.g. FUNCTION	e.g. NETWORK	e.g. ORGANIZATION	e.g. SCHEDULE	e.g. STRATEGY	FUNCTIONING ENTERPRISE

The rows represent players who are a part of the process points of view. The players are

- someone who has undertaken to do business in a particular industry,
- the business people who run the organization,
- the systems analyst who wants to represent the business in a disciplined form,
- the designer, who applies specific technologies to solve the problems of the business,
- the builder of the system, and finally
- the system itself.

The Rows manage CHANGE

The columns represent the different aspects of the process. They are :

- the data manipulated by an organization (what),
- the organization's functions and processes (how),
- the organization's locations where business is conducted (where),
- the events that trigger business activities (when),
- the people and organizations involved (who),
- and the motivations and constraints which determine how the business behaves (why)

The Columns manage **COMPLEXITY**

The cells then are :

- all the various modeling techniques that are used within the Information Management domain
- they identify some places where we could use some new models.
- the translations required to go from row to row reveal interesting things about both how an organization does and how it should carry out its business

What is the Zachman Framework ?

BCS 2006
Jakarta

	Data (What)	Function (How)	Network (Where)	People (Who)	Time (When)	Motivation (Why)
Objectives / Scope	List of things important to the enterprise	List of processes the enterprise performs	List of locations where the enterprise operates	List of organizational units	List of business events / cycles	List of business goals / strategies
Model of the Business	Entity relationship diagram (including m:m, n-ary, attributed relationships)	Business process model (physical data flow diagram)	Logistics network (nodes and links)	Organization chart, with roles; skill sets; security issues.	Business master schedule	Business plan
Model of the Information System	Data model (converged entities, fully normalized)	Essential Data flow diagram; application architecture	Distributed system architecture	Human interface architecture (roles, data, access)	Dependency diagram, entity life history (process structure)	Business rule model
Technology Model	Data architecture (tables and columns); map to legacy data	System design: structure chart, pseudo-code	System architecture (hardware, software types)	User interface (how the system will behave); security design	"Control flow" diagram (control structure)	Business rule design
Detailed Representation	Data design (denormalized), physical storage design	Detailed Program Design	Network architecture	Screens, security architecture (who can see what?)	Timing definitions	Rule specification in program logic
	(Working systems)					
Function System	Converted data	Executable programs	Communications facilities	Trained people	Business events	Enforced rules

The Rules for Using the Framework :

- *Columns have no order*
- *Each column has simple, basic model*
- *Basic model of each column must be unique*
- *Each row represents a distinct, unique perspective*
- *Each cell is unique*
- *Combining the cells in one row forms a complete description from that view*



How it Can help In Security Management

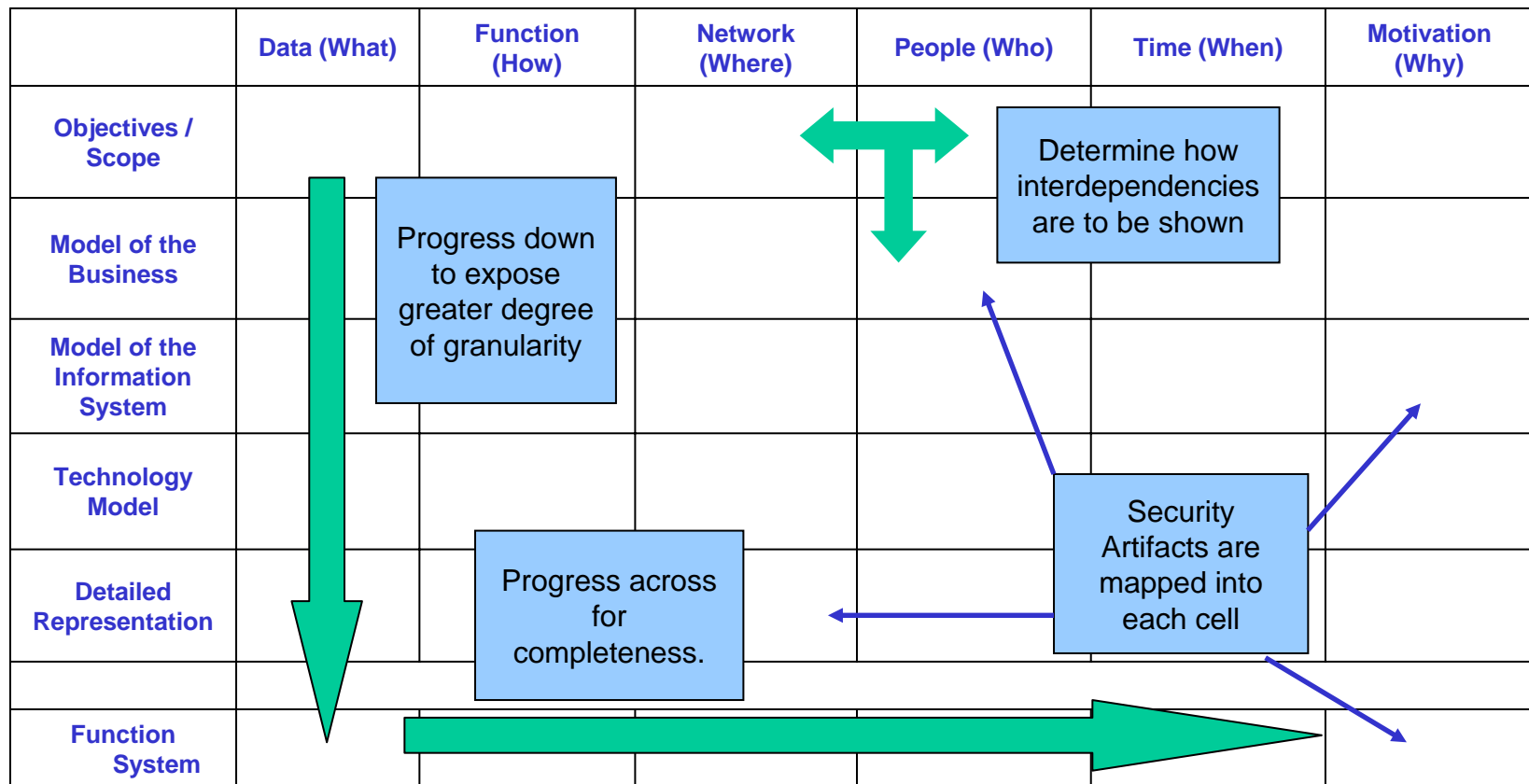
This document and the information it contains is presented commercial in confidence and contains information that is the intellectual property of Bispro Consulting. Its use out side of the purpose of discussion in any manner or any form constitutes a breach of copyright. Please contact Bispro on +62 21 3918330 for clarification.

How it Can help In Security Management

BCS 2006
Jakarta

Allows for an integrated enterprise wide, single frame view to allow for analysis of security touch points.

Visualization of interdependencies



A number of tools can be used to deploy the framework

- Least sophisticated and costly is using static design tools such as Microsoft Office
 - Interdependency mapping is manual
 - relationships are not contained in the models
 - model dependencies are manual
 - models are static
 - manageable for small deployments
- Most Sophisticated is using dynamic design tools such as enterprise modelers
 - Interdependency mapping is managed by the tool
 - relationships are contained in the models
 - model dependencies are managed by the tool
 - models are dynamic
 - normally have scalable single object repository
 - should be considered for medium to large deployments



High Level overview of cell structure

This document and the information it contains is presented commercial in confidence and contains information that is the intellectual property of Bispro Consulting. Its use out side of the purpose of discussion in any manner or any form constitutes a breach of copyright. Please contact Bispro on +62 21 3918330 for clarification.

Objectives / Scope

Addresses the visualization requirements and high level WHY.

	Data (What)	Function (How)	Network (Where)	People (Who)	Time (When)	Motivation (Why)
Objectives / Scope	List of data (things) that affects the direction and purpose of an enterprise, which are to be secured depending on the level of sensitivity of the data.	List of processes that need to be secured and also the cross-functional processes that oversee and interconnect all the processes.	List of locations where the enterprise operates and which ones need to be secured	List of organizational units and external parties and their security levels down to individual roles	List of list of events, sequencing the timing of the processes and flows, significant to the business and what are the security implications	List of business external requirements and the constraints faced by an enterprise including the security requirements and plans

Define the interrelationships and dependencies

Business Model

Addresses the business requirements that need to be met

	Data (What)	Function (How)	Network (Where)	People (Who)	Time (When)	Motivation (Why)
Business Model	Addresses the definition of confidentiality and security requirements for the items in row 1	Addresses process criticality definition as well as input and output measurement definition	Addresses types of links between nodes of the system locations & security requirements of nodes & links.	Addresses what are the access policies at unit and role level. Also defines situational information flow characteristics	Addresses sequencing of events in line with security requirements. Retention periods, type requirements such as design vs deployment for product.	Addresses the individual policies that impact the organizations

Again define the interrelationships and dependencies

Systems Model

Addresses the technology and architecting requirements of the upper rows

	Data (What)	Function (How)	Network (Where)	People (Who)	Time (When)	Motivation (Why)
Systems Model	Addresses the specification design to achieve the required security	Addresses design of policy implementation for areas such as availability, backup, access etc	Addresses the design of the security aspects for link types. Looks at encryption and hardware as well as physical protection	Addresses the role definitions from a security perspective and assigning of roles to users	Addresses the updating side of the equation for software hardware, patches, processes etc Also looks at the retention and destruction of information and underlying data	Addresses the internal and external threat issues such as links, server, storage etc

Again define the interrelationships and dependencies

Technology Model

Addresses the physical layer and implements the technology and requirements of the upper rows

	Data (What)	Function (How)	Network (Where)	People (Who)	Time (When)	Motivation (Why)
Technology Model	Addresses areas such as encryption type to use, hardware to use, software to use, type of intrusion detection etc	Addresses usage and function of the system. Plus, disaster recovery plans and links to BCP, recovery activities how damaged equipment is to be handled.	Addresses control devices, biometric systems, identification systems, protocols etc	Addresses requirements for password control, risk assessment etc	Addresses risk mitigations through sequential awareness programs, system reviews, training etc	Addresses constraints based on technology, resources, product construction etc

Again define the interrelationships and dependencies

Detailed Representations

Addresses the actual build based on the specifications and requirements of the upper rows

	Data (What)	Function (How)	Network (Where)	People (Who)	Time (When)	Motivation (Why)
Detailed Representations	Addresses the Data Definition coming from Physical data model above. Looks at database models and use of security control models	Addresses the algorithms to be used and key control mechanisms , LDAP and single sign on, storage media, configuration of software etc	Addresses hub and message management as well as physical access systems, guards, alarm systems, data authentication, services security etc	Addresses the implementation of the Identity management systems described in the upper rows	Addresses machine cycles, load balancing, failover etc	Addresses constraints such as environmental or legal related to realization

Again define the interrelationships and dependencies

How it Can help In Security Management

BCS 2006
Jakarta

ENTERPRISE SECURITY PLANNING USING ZACHMAN FRAMEWORK

	DATA <i>What</i>	FUNCTION <i>How</i>	NETWORK <i>Where</i>	PEOPLE <i>Who</i>	TIME <i>When</i>	External Requirements and constraints
SCOPE <i>(CONTEXTUAL)</i> <i>Planner- Ball Park View</i>	<ul style="list-style-type: none"> ~ Things that affect the direction and purpose of an enterprise. ~ Mission, Goals and Strategies. ~ Customer, Business and Employee, Internal and External data. 	<ul style="list-style-type: none"> ~ Operational Processes ~ Planning, Development, Research Process ~ Production, Quality, Marketing, Sales Process ~ Legal Process ~ Cross-functional process 	<ul style="list-style-type: none"> ~ Geographic locations of the Enterprise's Headquarters, Regional 	<ul style="list-style-type: none"> ~ Security Policies ~ Authority and responsibility of 	<ul style="list-style-type: none"> ~ Business planning process cycle ~ Contingency plans (disaster recovery upgrade) ~ Operations ~ Outsourcing (outsourcing) 	<ul style="list-style-type: none"> ~ Business plan ~ Security and privacy regulation. ~ Regulatory compliance (IEEE, ISO) ~ Technological restrictions ~ Time ~ Funding
ENTERPRISE / BUSINESS MODEL <i>(CONCEPTUAL)</i> <i>Owner</i>	<ul style="list-style-type: none"> ~ Classification of Data according to secure level ~ Data Confidentiality (Encryption, Password etc.) ~ Data Integrity (Backup, Archive) ~ Data Availability (speed, performance etc.) ~ Data Access Control (Secure or Insecure Access) ~ Data Auditing Model (to keep track of the accessed data) 	<ul style="list-style-type: none"> ~ Classification of Process ~ Input and Output of Data ~ Control Parameters (Triggering events, Time) 	<ul style="list-style-type: none"> ~ Internal ~ External ~ Virtual ~ Distributed ~ Local 			<ul style="list-style-type: none"> ~ Government policies ~ Corporate ethics ~ Industrial threat analysis ~ Business relationships ~ Pending legislation ~ Political ~ Standards (IEEE, ISO)
SYSTEM MODEL <i>(LOGICAL)</i> <i>Designer</i>	<ul style="list-style-type: none"> ~ Data verification model ~ Data workflow model ~ Data relationship models ~ Data backup demands (scheduling) 	<ul style="list-style-type: none"> ~ Disaster recovery process ~ Access Control Process ~ Data archiving process ~ Data auditing process (Audit trail) ~ Confidentiality, Availability and Integrity processes ~ Internal and External Process 	<ul style="list-style-type: none"> ~ Physical security ~ Link Types: Internet, Satellite, Wireless, Telephone, FiberLink ~ Security (VPN, SSL, Encryption) ~ Link Quality of Service ~ End-to-end security ~ Node Security ~ Node Types 	<ul style="list-style-type: none"> ~ Hierarchy ~ Separation of duties ~ User access control ~ Deliverable metrics ~ User auditing 	<ul style="list-style-type: none"> ~ Security ~ Threat ~ Risk ~ Assets ~ Re-engineering ~ Timeline ~ Dependency ~ Milestone 	<ul style="list-style-type: none"> ~ Jurisdictional Issues ~ Threat frequency ~ Technology ~ Funding ~ Application risk analysis
TECHNOLOGY MODEL <i>(PHYSICAL)</i> <i>Builder</i>	<ul style="list-style-type: none"> ~ Meta-data model ~ Database Schema ~ Storage management ~ Data encryption 				<ul style="list-style-type: none"> ~ Awareness program ~ Management policy ~ Updates ~ Lifecycle management ~ Non analysis ~ Element 	<ul style="list-style-type: none"> ~ Construction ~ Technological ~ Available resources
DETAILED REPRESENTATIONS <i>(OUT-OF-CONTEXT)</i> <i>Sub-Contractor</i>	<ul style="list-style-type: none"> ~ Database models ~ Data definition language ~ Firewall backup ~ Due diligence 	<ul style="list-style-type: none"> ~ Data Encryption Standards (DES, RSA, PKI BIOS) ~ Software Inventory 	<ul style="list-style-type: none"> ~ Kerberos 			<ul style="list-style-type: none"> ~ Implementation ~ Integration
FUNCTIONING ENTERPRISE	<ul style="list-style-type: none"> ~ Data 	<ul style="list-style-type: none"> ~ Function 	<ul style="list-style-type: none"> ~ Network 	<ul style="list-style-type: none"> ~ Organization 	<ul style="list-style-type: none"> ~ Schedule 	<ul style="list-style-type: none"> ~ Constraints

Each entry in the cell would have its own design or reference document

Illustrative

Version and revision control must be strong and contained in a single documents repository or directory

Questions ?

This document and the information it contains is presented commercial in confidence and contains information that is the intellectual property of Bispro Consulting. Its use out side of the purpose of discussion in any manner or any form constitutes a breach of copyright. Please contact Bispro on +62 21 3918330 for clarification.



*Performance
Pure & Simple*