Enterprise Security Planning using the Zachman Framework – Builder's Perspective

L. Ertaul[1], **S.Vandana**[2] , **K. Gulati**[2] , **G. Saldamli**[3]
[1]Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[2]Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA
[3]MIS, Bogazici University , Istanbul, Turkey

Abstract - *In recent years enterprise architecture (EA) has acquired recognition as playing a pivotal role in change processes. Purported benefits of having enterprise architecture include improved decision making, improved adaptability to changing demands or market conditions, elimination of inefficient and redundant processes, optimization of the use of organizational assets and effectively achieve current and future objectives of the enterprise. By including security requirements in the EA process and security professionals in the EA team, enterprises can ensure that security requirements are incorporated into priority investments and solutions. Zachman Framework is a simple, logical and comprehensive enterprise architecture framework that can be used for enterprise security planning .This paper gives an overview of how Zachman's Framework helps in designing and implementing a streamlined, integrated enterprise security architecture. Also, discussed in this paper is a detailed specification of the security requirements from the builder's perspective of the Zachman Framework*

Keywords: Enterprise Architecture, Enterprise Security Planning, Zachman Framework

1 Introduction

In today's high-tech and interconnected world, every enterprise needs a well thought out security planning architecture. Security risks rise with the rise in the sophistication of enterprise products and enterprise as a whole. The rise of cloud computing, advancement of mobile, broadband and wireless communication clearly shows that enterprises need better control over the security mechanism.. Threats exist from both within the walls of each enterprise as well as from external sources such as hackers, competitors and foreign governments. The goal of enterprise security planning is to have a detailed representation of the procedures, guidelines and practices for configuring and managing security in your environment. By enforcing enterprise security planning, enterprises can minimize their risks and show due diligence to their customers and shareholders.

Enterprise architecture provides a framework for reducing enterprise system complexity and enabling enterprise information sharing. In today's environment, each department or system usually has a vertically integrated approach to data, process, and technology. For example, department A has an application with its own database and runs on its own computer. Department B has another application with its own database and runs on its own computer. The same is true for department C. The Zachman Framework, named after John Zachman, has emerged as a way to develop enterprise-wide architecture. This framework moves from this vertical, departmental approach to a completely opposite horizontal approach. Instead of representing the data, process and technologies as entirely separate entities; he organized them around the points of view taken by various players [1] [2].

The Zachman Framework would seem to provide a sensible way to approach the security of an enterprise as it can accommodate different players involved in securing the enterprise and each player's view of the enterprise security. Its overall simplicity belies its use. Each of the framework's thirty six cells produces at least one output document to describe the system from that particular viewpoint.

This paper is organized as follows. In section 2, we briefly describe the enterprise architecture. In section 3, we briefly describe the Zachman framework which is most popular enterprise architecture framework. In section 4, we briefly describe how the Zachman framework can be applied for enterprise security planning. In section 5, we discuss the tools, technologies and security specifications from the builder's perspective of the Zachman Framework.

2 Enterprise Architecture

Enterprise Architecture (EA) is a rigorous description of the structure of an enterprise, which comprises enterprise components (business entities), the externally visible properties of those components, and the relationships (e.g. the behavior) between them. EA describes the terminology, the composition of enterprise components, and their relationships with the external environment, and the guiding principles for the requirement (analysis), design, and evolution of an enterprise [3][4][5].

This description is comprehensive, including enterprise goals, business process, roles, organizational structures, organizational behaviors, business information, software applications and computer systems.

An Enterprise Architecture Framework (EA Framework) is a framework for an Enterprise Architecture which defines how to organize the structure and views associated with an Enterprise Architecture [6].

The three basic components of the enterprise architecture framework are:

-**Views**: provide the mechanisms for communicating information about the relationships that are important in the architecture [6].

-**Methods**: provide the discipline to gather and organize the data and construct the views in a way that helps ensure integrity, accuracy and completeness [6].

-**Training/Experience**: support the application of method and use of tools [6].

In the next section we discuss basic overview of the Zachman Framework which is the most popular enterprise architecture framework. We will also discuss the different perspectives and abstractions of the Zachman framework.

3 Zachman Framework Overview

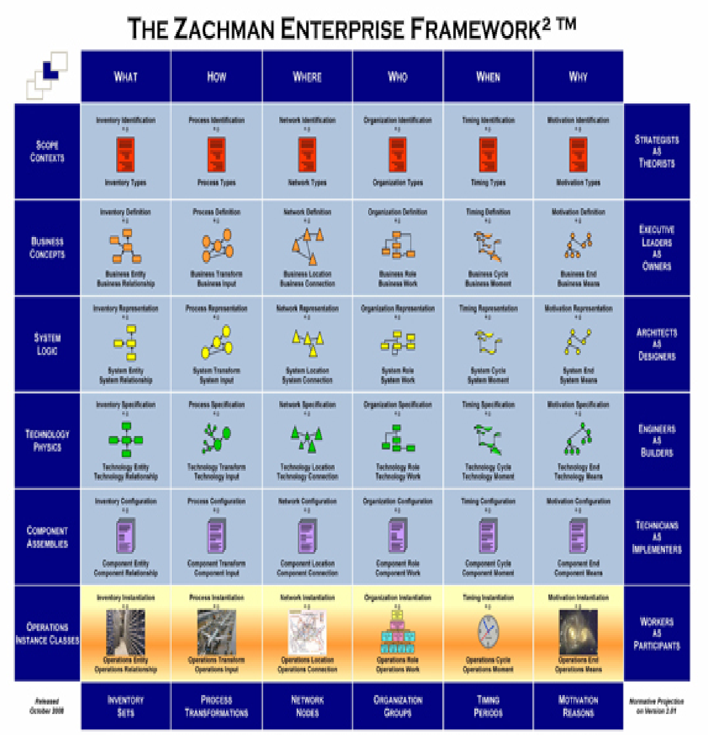
The Enterprise Architecture Framework (EA) frequently called the Zachman Framework, introduced in 1987 by John Zachman and extended by Sowa in 1992 (Sowa and Zachman 1992), as it applies to enterprises is a logical structure for classifying and organizing the descriptive representations of an enterprise that are significant to the management of the Enterprise as well as to the development of the enterprise’s systems. It was derived from analogous structures that are found in the older disciplines of Architecture/Construction and Engineering/Manufacturing that classify and organize the design artifacts created over the process of designing and producing complex physical products (ex., buildings or airplanes.) [7].

The units of the Framework can also be understood as organization scheme for all kinds of metadata involved in building and using an information system and have therefore become widely recognized during the last years [7].

The Zachman Framework provides the thirty-six necessary categories for completely describing anything; especially complex things like manufactured goods (e.g., appliances), constructed structures (e.g., buildings), and enterprises (e.g., the organization and all of its goals, people, and technologies). The framework provides six increasingly detailed views or levels of abstraction from six different perspectives as shown in Fig. 1[8].

It allows different people to look at the same thing from different perspectives. This creates a holistic view of the environment [8]. This Framework is intended being neutral in the sense that it’s defined totally independents from tools or methodologies and therefore any tool or any methodology can be mapped against it to understand what they are doing, and what they are NOT doing. The Zachman Framework cannot be considered as either a modeling language, or a methodology, or a modeling notation [7].

In the next section we will have a detailed description of the different perspectives (rows of the Zachman Framework) of viewing any complex thing like an enterprise.



THE ZACHMAN ENTERPRISE FRAMEWORK² ™

	WHAT	HOW	WHERE	WHO	WHEN	WHY	
SCOPE CONTEXTS	Inventory Identification Inventory Types	Process Identification Process Types	Network Identification Network Types	Organization Identification Organization Types	Timing Identification Timing Types	Motivation Identification Motivation Types	STRATEGISTS AS THEORISTS
BUSINESS CONCEPTS	Inventory Definition Business Entity Business Relationship	Process Definition Business Transform Business Input	Network Definition Business Location Business Connection	Organization Definition Business Role Business Work	Timing Definition Business Cycle Business Moment	Motivation Definition Business End Business Means	EXECUTIVE LEADERS AS OWNERS
SYSTEM LOGIC	Inventory Representation System Entity System Relationship	Process Representation System Transform System Input	Network Representation System Location System Connection	Organization Representation System Role System Work	Timing Representation System Cycle System Moment	Motivation Representation System End System Means	ARCHITECTS AS DESIGNERS
TECHNOLOGY PHYSICS	Inventory Specification Technology Entity Technology Relationship	Process Specification Technology Transform Technology Input	Network Specification Technology Location Technology Connection	Organization Specification Technology Role Technology Work	Timing Specification Technology Cycle Technology Moment	Motivation Specification Technology End Technology Means	ENGINEERS AS BUILDERS
COMPONENT ASSEMBLIES	Inventory Configuration Component Entity Component Relationship	Process Configuration Component Transform Component Input	Network Configuration Component Location Component Connection	Organization Configuration Component Role Component Work	Timing Configuration Component Cycle Component Moment	Motivation Configuration Component End Component Means	TECHNICIANS AS IMPLEMENTERS
OPERATIONS INSTANCE CLASSES	Inventory Instantiation Operations Entity Operations Relationship	Process Instantiation Operations Transform Operations Input	Network Instantiation Operations Location Operations Connection	Organization Instantiation Operations Role Operations Work	Timing Instantiation Operations Cycle Operations Moment	Motivation Instantiation Operations End Operations Means	WORKERS AS PARTICIPANTS
Released October 2008	INVENTORY SETS	PROCESS TRANSFORMATIONS	NETWORK NODES	ORGANIZATION GROUPS	TIMING PERIODS	MOTIVATION REASONS	Normative Projection on Version 2.01

Figure 1. Zachman Framework published in year 2008 [8].

3.1 Rows of the Zachman Framework

John Zachman's "Framework" is diagrammed in Figure 1. The rows represent the points of view of different players in the systems development process, while columns represent different aspects of the process [8]. The players are:

- **Scope (Ballpark view)**: Definition of the enterprise's direction and business purpose. This is an industry view, concerned with the things that define the nature and purpose of the business. This is necessary to establish the context for any system development effort [8].

- **Model of the business (Owner's view):** This defines in business terms the nature of the business, including its structure, functions, organization, and so forth [8].

- **Model of the information system (Designer's view)**: This defines the business described in step 2, but in more rigorous information terms. Where row two described business functions, for example, as perceived by the people performing them, row three describes them specifically as transformations of data. Where row two described all the things of interest to the enterprise, row three describes those things about which the organization wishes to collect and maintain information, and begins to describe that information [8].

- **Technology model (Builder's view):** This describes how technology may be used to address the information processing needs identified in the previous rows. Here relational databases are chosen over network ones (or vice versa), kinds of languages are selected and program structures are defined, user interfaces are described, and so forth [8].

- **Detailed Description** (**Sub-Contractor's View)**: This is a view of the program listings, database specifications, networks, and so forth that constitute a particular system and implementation of the system is done. These are all expressed in terms of particular languages [8].

- **Functioning system**: Finally, a system is implemented and made part of an organization [8].

In the next section we will have a detailed description of the different columns of the Zachman Framework.

3.2 Columns of the Zachman Framework

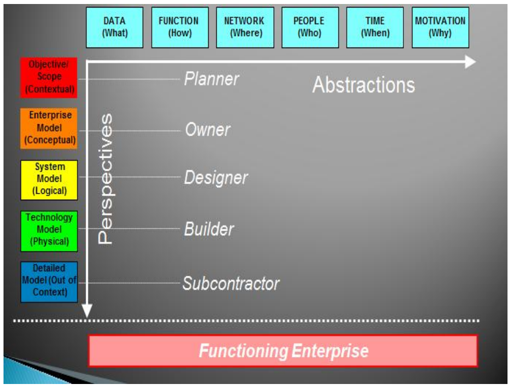


Figure 2. Perspectives and Abstractions of the Zachman Framework

The columns in the Zachman framework as shown in Fig 2 represent different areas of interest for each perspective. The columns describe the dimensions of the systems development effort. These are:

- **Data:** Each of the rows in this column address understanding of and dealing with any enterprise's data. This begins in row one with a list of the things that concern any company in this industry, affecting its direction and purpose. As you pass down through the rows, you move to progressively more rigorous descriptions of the data (row two is the business person's view, and row three is a disciplined translation of this), until you get to row four, where a specific design approach (and a specific database management system) is specified. Row five is the detailed representation of the data on the computer and row six is the working database [8].

- **Function:** The rows in the function column describe the process of translating the mission of the enterprise into successively more detailed definitions of its operations. Where row one is a list of the kinds of activities the enterprise conducts, row two describes these activities in a contiguous model. Row three portrays them in terms of data transforming processes, described exclusively in terms of the conversion of input data into output data. The technology model in row four then converts these data conversion processes into the definition of program modules and how they interact with each other. Pseudo-code is produced here. Row five then converts these into source and object code. Row six is where the code is linked and converted to executable programs [8].

- **Network**: This column is concerned with the geographical distribution of the enterprise's activities. At the strategic level (row one), this is simply a listing of the places where the enterprise does business. At row two, this becomes a more detailed communications chart, describing how the various locations interact with each other. Row three produces the architecture for data distribution, itemizing what information is created where and where it is to be used. In row four, this distribution is translated into the kinds of computer facilities that are required in each location, and in row five, these facilities requirements are translated into specification of particular computers, protocols, communications facilities, and the like. Row six describes the implemented communications facilities [8].

- **People**: The fourth column describes who is involved in the business and in the introduction of new technology. The row one model of people is a simple list of the organizational units and each unit's mission. In row two, this list is fleshed out into a full organization chart, linked to the function column. Here also, requirements for security are described in general terms. In row three, the potential interaction between people and technology begins to be specified, specifically in terms of who needs what information to do his job. In row four, the actual interface between each person and the technology is designed, including issues of interface graphics, navigation paths, security rules and presentation style. In row five, this design is converted into the outward appearance of each program, as well as the definitions of access permissions in terms of specific tables and/or columns each user can have access to. In row six, you have trained people, using the new system [8].

- **Time:** The fifth column describes the effects of time on the enterprise. It is difficult to describe or address this column in isolation from the others, especially column two. At the strategic (row one) level, this is a description of the business cycle and overall business events. In the detailed model of the business (row two), the time column defines when functions are to happen and under what circumstances. Row three defines the business events which cause specific data transformations and entity state changes to take place. In the technology model (row four), the events become program triggers and messages, and the information processing responses are designed in detail. In row five, these designs become specific programs. In row six business events are correctly responded to by the system [8].

- **Motivation:** As Mr. Zachman originally described this column, it concerned the translation of business goals and strategies into specific ends and means. This can be expanded to include the entire set of constraints that apply to an enterprise's efforts. In row one; the enterprise identifies its goals and strategies in general, common language terms. In row two, these are translated into the specific rules and constraints that apply to an enterprise's operation. In row three, business rules may be expressed in terms of information that is and is not permitted to exist. This includes constraints on the creation of rows in a database as well as on the updating of specific values. In row four, these business rules will be converted to program design elements, and in row five they will become specific programs. In row six, business rules are enforced [8].

In the next section we outline the rules of the Zachman Framework.

3.3 Rules of the Zachman Framework

The framework comes with a set of rules:

-**The columns have no order**: The columns are interchangeable but cannot be reduced or created [8].

- **Each column has a simple generic model**: Every column can have its own meta-model [8].

- **The basic model of each column must be unique**: The basic model of each column, the relationship objects and the structure of it is unique. Each relationship object is interdependent but the representation objective is unique [8].

- **Each row describes a distinct, unique perspective:** Each row describes the view of a particular business group and is unique to it. All rows are usually present in most hierarchical organization [8].

- **Each cell is unique**: The combination of 2, 3 & 4 must produce unique cells where each cell represents a particular case. Example: A2 represents business outputs as they represent what are to be eventually constructed [8].

- **The composite or integration of all cell models in one row constitutes a complete model from the perspective of that row:** For the same reason as for not adding rows and columns, changing the names may change the fundamental logical structure of the Framework [8].

- **The logic is recursive**: The logic is relational between two instances of the same entity [8].

In the next section we will briefly describe how the Zachman framework can be used for Enterprise Security Planning.

4 Security Planning using Zachman Framework.

For security architecture modeling purposes, the columns of the Zachman matrix (data, function, network, people, time and motivation) are extremely useful. They provide the answers to what data assets the organization controls, how they are used, where they are located, the people involved and means to achieve a secured organization.

Similarly, the first five rows of the matrix give a unique perspective of a particular security challenge. The highest level, the Ballpark View, defines a clear and coordinated boundary (domain) of the system for the purposes of identifying the people, subsystems, and needs impacted by the system.

The Owner’s View captures the business and organizational relationships, and their external interfaces. It also documents sources of system requirements, including those derived from legacy systems.

The Designer’s View defines the functional capabilities of the system and establishes required interactions between subsystems. The Designer's View also establishes and documents the security architectural design and provides a basis for system measurement.

Finally, the Builder’s View provides a detailed description of the design and methodology for monitoring and correcting system performance.

Each layer in the framework relates to a tool that can be used to secure the system. For example, an overall organizational security policy would be implemented in the Ballpark View. A tailored security policy and detailed descriptions are handled by the other rows.

5 Builder’s Perspective

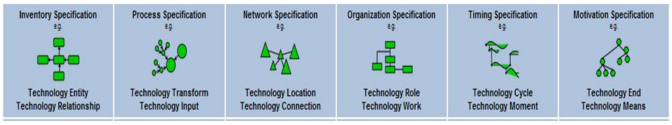


Figure 3 . Row 4 (Builder’s View) of the Zachman Framework

The technology model of the Zachman Framework defines the physical representations of the things in the enterprise as shown in Fig 3.. The builder specifies the technology to solve the problems. The builder applies the physical constraints of what is possible to the designer’s artifacts and implements the product or service by understanding its environment [8]. The Builder integrates all the data sources evolved from different platforms and operating systems for providing a common enterprise wide view.

In the next sub section we will describe builder’s view of the data column and specify possible tools and technologies from an enterprise security view point

5.1 Builder – Data Column

The builder specifies the tools and technology that can be used to ensure the confidentiality, integrity, availability, authenticity and non-repudiation of the designer’s logical data model. The builder is concerned about the digital and physical data security.

Figure 4. Builder – Data Cell

To ensure data confidentiality and authentication services the builder decides which data has to be encrypted and specifies type of encryption based on the sensitivity of the data. This includes encryption, decryption, certificate management, key management and data recovery services in case the encrypted data is not available for any reason. Standard database security techniques are employed to prevent unauthorized access and denial of service attacks. The builder handles data storage management system and also specifies security mechanism and policies to be adopted if the data is stored in cloud computing enviroment.The builder specifies data backup and recovery tools to ensure data availability. For non-repudiation services the builder specifies the use of digital signatures and certificates.

Table 1 specifies some of the tools and technologies that can be used for ensuring data confidentiality, data integrity, data availability, data authenticity and non-repudiation of data .The tools and technologies based on the designer’s logical data model and industry security standards.

Table 1 : Security tools and techniques for Builder – Data cell

Data Encryption :
Symmetric encryption : AES /3DES / blowfish
Public key encryption : RSA
Disk/File encryption : Microsoft EFS and Bit locker encryption system.
DBMS column encryption : Oracle 11g transparent data encryption/ Sybase column encryption
Digital Signatures
Data Recovery/Availability
RAID,Windows Data Recovery,Recuva (Windows)
Mirrored data servers
Data in the cloud computing environment(storage as a service):
Cloud safety box,Open solaris VPC gateway,Trend micro secure cloud 1.1
Data logging and monitoring
SIEM,CA Log manager,Event Viewer
Data Authentication
eTrust Siteminder
Single sign on,RSA Secure id,Kerberos Authentication
Physical Security - Use of shredders to dispose data
Data Access Control
Biometrics,Oracle database vault
Intrusion Detection System , Intrusio Prevention System

In the next sub section we will describe builder’s view of the function column and specify possible tools and technologies from an enterprise security view point

5.2 Builder – Process column

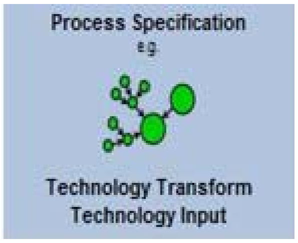


Figure 5. Builder – Process Cell

Column two of the Technology model describes the usage and functioning of the system [9]. This cell addresses the disaster recovery plans of the organization. The restoration activities include identifying the internal and external resources to handle damaged equipment and media in order to minimize the loss [9].It also addresses operational security processes, training processes involved in the organization with asset management and data security processes. Table 2 lists the processes for builder-process cell.

Intrusion Detection Process
Network based – SNORT
Host based –
OSSEC(Open Source Host based intrusion detection system)
Tripwire
AIDE(Advanvced Intrusion detection Environment)
Prelude Hybrid IDS
Disaster Recovery Process:
NetBackup
NetBackup PureDisk
NetBackup Real Time
Cluster Server
Backup Exec
Backup Exec System Recovery Server Edition
Storage Foundation
Volume Replicator
Operational Security Processes
Hardware Controls
Software Controls
Input/Output controls
Media controls
Data Auditing Process
ACL
Audit Exchange
ActiveData CAAT software
RemoteSysInfo
Data Archiving Process
Tape Storage
Disk Storage
Cloud archiving
Asset Management Process
Radio Frequency Identification
GPS
VANET
Training Process

Table 2. Security processes for Builder –Process cell

In the next sub section we will describe builder's view of the network column and specify possible tools and technologies from an enterprise security view point.

5.3 Builder - Network

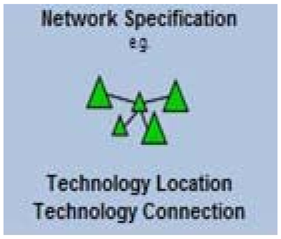


Figure 6. Builder – Network Cell

Column 3 of the technology model is concerned about the tools and technologies that can be used to secure the communication between the enterprise entities that are geographically distributed. The builder specifies tools/techniques to secure the communication links, the networking infrastructure, network monitoring and access control mechanism to be employed with the security policies. Table 3 specifies the tools/techniques to be used for builder – network cell.

Table 3. Security entries for Builder – Network cell

Wireless Security :
-disable SSID broadcast
-user authentication – 802.1X,EAP/EAP-fast,ACS for AAA
-transport encryption -802.11,AES,TKIP,MFP,WPA/WPA2
-detect and prevent rogue APs,clients,ad-hoc networks –Audits,RF Scanning,wireless IPS
-VPN's for remote access
Wired and Wireless Security :
-VPN for remote encryption
Link encryption – Cisco Fiber channel link encryption (uses 128 bit AES)
Email Security : PGP
Network device hardening
Network Intrusion detection – SNORT ,Fragrouter
Network Management
-SNMP v3
-Syslog
-RMon
Physical Security for Network Infrastructure
-Biometrics
-Video Surveillance
-Sensors
-Incident Response
Harware device specification(eg : routers,switches)
-Network Availability ,MTTR(Mean time to repair),MTBF(mean time between failures)
Logistics Security
- TMW Suite – Enterprise transportation software
-Roadnet Transportation Software

In the next sub section we will describe builder's view of the Time column and specify possible tools and technologies from an enterprise security view point.

5.4 Builder - Time

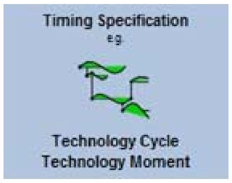


Figure 7. Builder – Time Cell

Time cell is the physical representation of the system events and physical processing cycles expressed as control structures [10].

Table 4. Security entries for Builder – Time cell

Regular Patch updates
Regular Backups
Password Management-Enterprise password safe
Key Management
Monitoring
People training
Information life cycle management – SAP Netweaver, Oracle 11g ILM
Risk/Vulnerability Analysis – SSL Digger,Scuba,Site digger
Task Management
Resource Management

In the next sub section we will describe builder's view of the network column and specify possible tools and technologies from an enterprise security view point.

5.5 Builder - People

Organization Specification
e.g.
Technology Role
Technology Work

Figure 8. Builder – People cell

This cell is concerned with the physical representation of the work flow of the enterprise from security viewpoint.The below Table 5 presents the security entries for the builder – people cell.

Table 5. Security entries for builder – people cell

Workflow specification Specification of access privilages -Electronic access – access list , smart cards ,firewalls / routers -Physical access - sensors , alarms , ID Client User interface Metrics – performance,survey,bonuses Role specification

In the next section we will discuss the builder's view of the motivation column.

5.6 Builder – Motivation

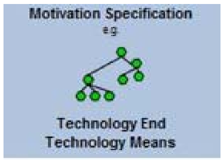


Figure 9. Builder – Motivation cell

Column six deals with the constraints implied due to technological limitations and with the availability of resources and product construction[10].

Table 6 : Security entries for Builder- Motivation cell

Business Constrained Rules Budget Technological Constraints Availability of Hardware and Software Government Policies,Legal Changes Security Policies Environmental Regulations,Government Regulations Industry Standards

6 Conclusion

Zachman framework is simple and comprehensive framework and fits well to model the security of the enterprise. The six perspectives and abstractions bring out all the necessary security mechanism and policies to be adopted for securing the enterprise. Though the Zachman framework seems to be a document heavy approach it still lets the enterprise assess its current state of security and make changes for a more secured environment. It would be better if the framework can be tweaked to fit the enterprise security planning (for e.g. : we could add a customer row to the framework as well) but this is a limitation of using this framework. Though the Zachman Framework looks comprehensive enough to model the enterprise security other frameworks like Department of Defense Architecture Framework (DODAF) and TEAF can also be considered for enterprise security planning.

7 References

[1] Hay, David C., THE ZACHMAN FRAMEWORK: AN INTRODUCTION, Essential Strategies, Inc.;

[2] http://www.tdan.com/view-articles/4140/

[3] Giachetti, R.E., Design of Enterprise Systems, Theory, Architecture, and Methods, CRC Press, Boca Raton, FL, 2010.

[4] Enterprise Architecture Research Forum, http://earf.meraka.org.za/earfhome/defining-ea

[5] MIT Center for Information Systems Research, Peter Weill, Director, as presented at the Sixth e-Business Conference, Barcelona Spain, 27 March 2007

[6] Stephen Marley (2003). Architectural Framework. NASA /SCI. Retrieved 10 Dec 2008.

[7] http://www.mega.com/wp/active/document/company/wp_mega_zachman_en.pdf

[8] http://www.essentialstrategies.com/documents/zachman2000.pdf

[9] http://www.mcs.csueastbay.edu/~lertaul/ESP/article%252014.pdf

[10] https://apps.adcom.uci.edu/EnterpriseArch/Zachman/ZIFA03.pdf

[11] http://www.sans.org/reading_room/whitepapers/modeling/applying-security-enterprise-zac

[12] citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.4113&rep...

[13] http://www.zachmanframeworkassociates.com/

[14] *The Zachman Framework, For Enterprise Architecture: Primer for Enterprise Engineering and Manufacturing,* John A. Zachman, Zachman International, Metadata Systems Software Inc., 2001-2006