

Security Planning Using Zachman Framework for Enterprises

Levent Ertaul

California State University,
Hayward,
Department of Mathematics
and Computer Science
25800 Carlos Bee Boulevard,
Hayward, CA 94542, USA
lertaul@csuhayward.edu ,
www.mcs.csuhayward.edu/~lertaul

Raadika Sudarsanam

California State University,
Hayward,
Department of Mathematics
and Computer Science
25800 Carlos Bee Boulevard,
Hayward, CA 94542, USA
rsudarsanam@horizon.csuhayward.edu

Abstract: *An “Enterprise” is a business association consisting of a recognized set of interacting business functions, able to operate as an independent, standalone entity. Security in an enterprise has elevated the interest in day-to-day business activities of today’s world, as the hackers threaten all kinds of valuable corporate information. The high profile attacks on the Internet and several physical attacks seems to have increased the security related issues on top of corporate agenda. Security is being achieved through the combination of technology and policy. The technology must be up to date and the policy must outline the procedures. The confronting major trends towards security are to integrate security throughout an organization, converge information security and physical security, and to emerge the importance of new security technologies. Zachman Framework is a logical structure for organizing the management of an enterprise and it controls and integrates all components of the system. This paper gives an overview of how Zachman’s Framework help define, design, and create tools for effectively securing an enterprise. Also, discussed in this paper is the incorporation of this framework in e-governance.*

Keywords: Enterprise Security Planning, Enterprise Security Management, Strategic Planning.

1. Introduction

Dramatic advances in computers and communications has paved the way for a plethora of sound security mechanisms for an enterprise. However, lack of logical structure for organizing the management of an enterprise, and the increase in the security attacks have led to the need for managing information security of an enterprise. Managing risk is the central issue of security. People around the world are looking for more agile and cost effective business operations. The urge to do more with less led in developing and using Enterprise Architectures as the “blueprint” for all enterprise engineering activities including data warehousing, software engineering, information engineering, commercial software evaluation, enterprise application integration, business to business and business to customer e-commerce, and the list is endless (Perkins, 2001). As the need for a comprehensive security plan for an enterprise increases, this paper builds a plan to secure an enterprise. The strategic framework for security planning can be employed using Zachman Framework for Enterprise Architecture taking into account various entities of the framework (DeLooze, 2001).

In 1987, John Zachman defined Framework as "simply 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” (Zachman, 1987), (Zachman, 1993). Zachman Framework is a two-dimensional classification schema diagramed in a six-by-six matrix format as shown in Figure 1. The rows represent the perspective of different players in the process

(Planner, Owner, Designer, Builder, Sub-Contractor, the System) while the columns represent aspects of the process (Data, Function, Network, People, Time, Motivation). The thirty-six frames at the core of the integrated Framework are referred to as cells. In this model, each cell is unique. The columns manage the complexity while the rows manage the changes.

The Framework is comprehensive, primitive, and generic. The framework distinguishes an issue by answering all the six primitive linguistic interrogatives *Who, What, Where, When, Why* and *How*, hence they cannot be fragmented further after analyzing. In addition to that, it is a logical structure for descriptive representations (i.e. models, or design artefacts) of any complex object and it is neutral with regard to the processes or tools used for producing the descriptions. For this reason, the Framework, as applied to Enterprises, is helpful for sorting out very complex, technology and methodology choices and issues that are significant both to general management and to technology management. This makes the framework generic. A brief description of the columns and rows are discussed below.































	DATA What	FUNCTION How	NETWORK Where	PEOPLE Who	TIME When	MOTIVATION Why	
SCOPE (CONTEXTUAL) Planner	List of Things Important to the Business  ENTITY = Class of Business Thing	List of Processes the Business Performs  Process = 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 Organization Unit	List of Events/Cycles Significant to the Business  Time = Major Business Event/Cycle	List of Business Goals/Strategies  Ends/Means = Major Business Goal/Strategy	SCOPE (CONTEXTUAL) Planner
BUSINESS MODEL (CONCEPTUAL) Owner	e.g. Semantic Model  Ent = Business Entity Rein = Business Relationship	e.g. Business Process Model  Proc. = Business Process IO = 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	BUSINESS MODEL (CONCEPTUAL) Owner
SYSTEM MODEL (LOGICAL) Designer	e.g. Logical Data Model  Ent = Data Entity Rein = Data Relationship	e.g. Application Architecture  Proc. = Application Function IO = User Views	e.g. Distributed System Architecture  Node = IS 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) Designer
TECHNOLOGY MODEL (PHYSICAL) Builder	e.g. Physical Data Model  Ent = Segment/Table/etc. Rein = Pointer/Key/etc.	e.g. System Design  Proc = Computer Function IO = Data Elements/Sets	e.g. Technology Architecture  Node = Hardware/Systems 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 Definition  End = Condition Means = Action	TECHNOLOGY MODEL (PHYSICAL) Builder
DETAILED REPRESENTATIONS (OUT-OF-CONTEXT) Sub-Contractor	e.g. Data Definition  Ent = Field Rein = Address	e.g. Program  Proc = Language Statement IO = 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  Ent = Sub-condition Means = Step	DETAILED REPRESENTATIONS (OUT-OF-CONTEXT) Sub-Contractor
FUNCTIONING ENTERPRISE	e.g. DATA	e.g. FUNCTION	e.g. NETWORK	e.g. ORGANIZATION	e.g. SCHEDULE	e.g. STRATEGY	FUNCTIONING ENTERPRISE

Figure 1 Zachman Enterprise Architecture Framework

The columns in the Zachman matrix refer to the interrogative questions asked by an enterprise. Answering these questions, complex situations and missing answers can be deduced without getting lost in details and without losing the awareness of interlinked entities within the same subject. The answers to these questions heavily depend upon the perspective. The columns descriptions are as follows:

- *Data (what):* This column answers to the interrogative question *what* – an enterprise is made of? It includes the list of things denoting the material composition of the enterprise that affects its direction and purpose. Also, it describes the entity relationship involved in each perspective of the enterprise.
- *Function (how):* This column answers to the interrogative question *how* – does it work? It describes how a process is transformed taking in the goals of an enterprise as the input that alters the output.
- *Network (where):* Each of the rows in this column describes about the geographical location, and the interconnection between the nodes of an enterprise. The nodes may comprise of business

offices, their service providers, and vendor connections.

- *People (who)*: This is the fourth column of the Framework answers the question *who* – is responsible? It describes the authority, responsibility or the workflow of the organization and the people who are involved in the business.
- *Time (when)*: The fifth column describes the most important axiom of business – *Time*. It denotes the time and event relationships between enterprises. The vertical axis of the infrastructure is the control axis and the horizontal axis the duration axis. It focuses on the scheduling of events, which are affected by triggers.
- *Constraints*: This column identifies the actions, which confines enterprises along with the external requirements of the organization.

The rows in the Zachman Framework represent a distinct, unique perspective. Each perspective defines the solution, taking into account other perspectives and restraints those perspectives impose. The rows represent the point of view of different players. They are:

- *Scope (Ballpark view)*: It defines the purpose and nature of the business from the planners view. The scope lists all the important things that manages and affects the business policies and its outcome.
- *Business Model (Owners view)*: This model defines the interaction between the entity and the business processes. The owner describes this relationship taking into consideration the desires of the users.
- *System Model (Architect's view)*: The architect analyzes both the business and technical perspectives of the enterprise and produces a design to the builder, from the specifications provided from the owner and the planner.
- *Technology Model (Designer's view)*: The designer takes the specifications from the architect and owners perspective to implement technology to address information processing.
- *Detailed Representation (Builder's view)*: This model produces the component from the architectural drawings and designs from the previous rows.
- *Functioning Enterprise*: This model depicts the operational system. This is the product of all planning, designing and development produced in the previous stages. It produces the final product from the user's perspective (Zachman & Sowa, 1992).

Due to security needs of today's world, every enterprise has to come up with some sort of security planning. Zachman Framework could work for those plans (DeLooze, 2001), (Zachman, 2001). In this paper, we give a security model to manage enterprise security based on Zachman Framework. First, we explain the rules of Zachman Framework. Second we discuss the security planning using Zachman Framework. Finally, conclusions are given.

2. Rules of Zachman Framework

The Zachman Framework is influenced by principles of classical architecture that establish a common vocabulary and set of perspectives for describing complex enterprise systems. This influence is reflected in the set of rules that govern an ordered set of relationships that are balanced and orthogonal. By designing a system according to these rules, the architect can be assured of a design that is clean, easy to understand, balanced, and complete in it. Zachman's Framework provides the blueprint, or architecture, for an organization's information infrastructure. This section explains the rules involved with the architecture framework.

- *Columns have no order*: Order creates bias and implies priority. Few programmers tend to have bias towards function while few others towards data of the framework. There is no particular order in the architecture. The order implies the strategies, which values the judgment of the

enterprise. All the columns are equally important, for all are abstractions of the same enterprise.

- *Each column has simple, basic model:* The abstraction of each column corresponds to basic entities suggested by the interrogatives. In addition to this their connection is also important for the design. Each column has basic model that constitutes a generic metamodel.
- *Basic model of each column must be unique:* No entity or connector in the basic column model is repeated in name or concept. They may be related as they are the abstractions of the enterprise but they are separate and unique.
- *Each row represents a distinct, unique perspective:* Each row of the framework represent different perspective of the owner, designer, builder etc. The definition of each entity reflects the perspectives of different constraints.
- *Each cell is unique:* Each cell in the framework is unique as each column has a unique aspect and each row has a unique perspective.
- *Combining the cells in one row forms a complete description from that view:* The main significance of this rule is that when additional columns are defines each new cell must be consistent with the perspective of the row. Each cell is dependent upon the above cell, below cell and cell in the same row. Any change in a cell would have effect on the dependent cells of the row (Zachman & Sowa, 1992), (Zachman, 1993).

3. Security Planning using Zachman Framework

The following is a generalized plan for a secured enterprise using the Zachman Framework by mapping the defined artefacts of security onto the Framework. Figure 2 provides the overview of the security artefacts mapped onto each cell of the Zachman Framework. We map on the attributes of the Figure 2 by following a path downwards, by producing a conceptual view of the owner from the physical view of the planner. Notice that, in Figure 2, we have included a new column discussing about the External Requirements and Constraints faced by the enterprise, in place of the motivation of the Zachman column. The following is the detailed description of the security perspective of all the players of an enterprise or the individual rows of the Zachman Framework:

3.1. Scope:

The scope of an organization is defined in the first row of the Zachman Framework as shown in Figure 2. The planner addresses the security management policy in the scope by providing information to the architect with few of the following constraints. They include customer requirements, financial responsibilities and limitations imposed by regulations and so forth. Using the analogy of constructing a building, the maximum number of stories built depends on the strength of its foundation, as it integrates the building supporting structure (Imon, Zachman & Geiger, 1997). Similarly, the system must ensure appropriate level of information in its scope to build the other rows of the framework.

The first column of scope addresses detailed planning of the 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. The data which may be included in this cell are sales, regulatory information, intellectual property, expenses, events, assets, revenue, human resources, resource and development, legal and partner's information, competitors, suppliers, customers, lobby data, subcontractors and the internal and external data of the enterprise. In addition, enterprises' mission and strategy will also be incorporated in the scope of the organizational security policy.

Column two includes all processes including operations, manufacturing, research, production, and legal that need to be secured and also the cross-functional processes that oversee and interconnect all the processes.

Column three addresses the location of an enterprise, which includes the corporate headquarters connections, regional and national offices, vendor connections, like third party and partners authority involved in accessing the data. It also addresses the service providers, which includes carriers and other entities that require special attention because of potential government policies.

Column four addresses users of various departments of the enterprises and their network accessibility. The different departments includes human resources, facilities, finance, sales, marketing, technical support, partners and legal authorities, customers and suppliers and the government authorities and users of these departments who operate on the data. The threat of security increases as the numbers of access points to operate the data extends. Hence, the level of security is maintained in accordance to the authority of the personnel.

Column five addresses the list of events, sequencing the timing of the processes and flows, significant to the business. This includes business process planning cycle, contingency planning, market fluctuations and strategic planning of the enterprise.

Column six addresses the external requirements and the constraints faced by an enterprise. Typical external requirements will include regulatory compliances, technological restrictions, security and privacy regulations, etc. Time and funding becomes the typical constraints of the whole enterprise at all levels.

	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 (CONTEXTUAL) <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 and National offices. Service Providers and Carriers. Vendors Connections 	<ul style="list-style-type: none"> Security Policies Authority and responsibility of executive department, HR, Sales, Marketing, Research Development, Finance and various other departments of the company Corporate Governance 	<ul style="list-style-type: none"> Business planning process cycle Contingency plans (disaster recovery, software upgrade) Market fluctuations Strategic Planning (outsourcing) 	<ul style="list-style-type: none"> Business plan. Security and privacy regulation. Regulatory compliance (IEEE, ISO) Technological restrictions Time Funding
ENTERPRISE / BUSINESS MODEL (CONCEPTUAL) <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"> Interconnection of business location Voice, Voice Security Data, Data Security Logistics network security 	<ul style="list-style-type: none"> Organization chart Who does what? Authorizations Responsibilities 	<ul style="list-style-type: none"> Business cycles (Corporate calendar, Product life cycle, Demand cycle) Budget Sales and marketing 	<ul style="list-style-type: none"> Government policies Corporate ethics Industrial threat analysis Business relationships Pending legislations Political Standards (ex IEEE, ISO) International trade regulations
SYSTEM MODEL (LOGICAL) <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 control 	<ul style="list-style-type: none"> Physical security Link Types: Internet, Satellite, Wireless, Telephone, Fiber/Link Security (VPN, SSL, Encryption) Link Quality of Service End-to-end security Node Security Node Types Logic Security (Acknowledgment, transportation) 	<ul style="list-style-type: none"> Hierarchy Separation of duties User access control Deliverable metrics User auditing 	<ul style="list-style-type: none"> Software upgrades Test and detect tracking Real time alerts Reengineering Timeline Dependency Milestone 	<ul style="list-style-type: none"> Jurisdictional issues Threat Frequency Technology Funding Application risk analysis
TECHNOLOGY MODEL (PHYSICAL) <i>Builder</i>	<ul style="list-style-type: none"> Meta-data model Database Schema Storage management Data encryption 	<ul style="list-style-type: none"> Intrusion detection process Response of disaster recovery process Asset management Insurance policy 	<ul style="list-style-type: none"> Bio-metric Identification Authentication Server Link security Intrusion Detection System Operating Systems 	<ul style="list-style-type: none"> Work flow Presentation format Client interface requirements 	<ul style="list-style-type: none"> Security awareness program Password management policy Timely backups Information lifecycle management Risk mitigation analysis Key management 	<ul style="list-style-type: none"> Construction Technological Available resources
DETAILED REPRESENTATIONS (OUT-OF-CONTEXT) <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"> Single sign on process Backup devices Smart cards Programs Data Encryption Standards (DES, RSA, PKI BIOS) Software Inventory 	<ul style="list-style-type: none"> Security Protocols (VPN, SNMP) End security protocols Logistics hub management Authentication service product Kerberos 	<ul style="list-style-type: none"> Identity and access management Authorization management 	<ul style="list-style-type: none"> Machine cycle Interrupt management Rotation of assignment 	<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

Figure 2. Enterprise Security Planning using Zachman Framework

3.2. Enterprise Model:

The enterprise model is the business process model of the enterprise. The owner is the intended recipient of the final product that is built. The Owner provides information about the product/services and its usage (O'Rourke, Fishman & Selkow, 2003). It is clear from Figure 2 that the conceptual model should be placed below the physical model of the planner.

In the first column, the owner dictates his/her requirements of data list, which are applied in the business, by classifying the data according to the level of security and confidentiality. Integrity and availability of the data is ensured by taking backup of the data. Implementing a data-auditing model in this cell keeps track of all the data accessed.

Column two addresses the process of the enterprise. This model moulds the input classified data (Column 1), producing an output depending on the market triggers, which are applied on the process. The processes are classified according to the level of criticalness.

Column three defines the location of the business nodes where the systems are used. The connection links between the nodes may be in the form of data, voice or logistics. The transfer of information between the nodes of the enterprise requires high level of security.

In Column four, the owner distributes the authority and responsibility of the human resources within the company by creating an organization chart. This chart provides information of the desired flow within the enterprise by clearly outlining the characteristics of who does what work.

Column five describes the time dimension of an enterprise. Time dimension may be of two forms. One of the forms represents the snapshot of a point in time and the other defines a period. Business cycles over a period include corporate calendar, product and demand lifecycle, whereas the balance sheet information is for a small period of time.

Column six discusses the corporate ethics, which plays a central role in employee decisions. The policies of the government, political influences, pending legislations and industrial standards could be a constraint, as it would have adverse effect towards the progress of the organization. Industrial competition results in a price war, which shifts the market shares and productivity growth.

The objectives of the enterprise defined by the owner must focus on information quality as depending on this information, the designer and the builder builds the whole system. Hence the analysis concludes that the owner's view describes the business requirements of the enterprise and thus is related to the business model.

3.3. System model:

As it is suggested in Figure 2, the System model is placed in the third row of the Security Framework, as the functionality of this fully attributed model is to reflect the enterprise model of the above row. The system analyst (Designer) represents the business in a disciplined form. Due to the increase in the number of users and complex IT environment, installing a firewall can no longer be the solution of security measures. In the next row of the Zachman Framework, the Designer hardens the applications and the operating system of the enterprise to ensure reliable security operations. The Designer is an engineer or architect of the final product or service. He/she is intermediary understanding both the business perspective of the owner and the technical needs of the builder, who takes the design from the architect and builds the product or system in the next row, Row 4. The designer represents the laws of nature, the system or the logical constraints of the product or service's design (O'Rourke, Fishman & Selkow, 2003).

Column one of the logical data model describes the systems view of interest by transforming the real description of the product into its built in specifications. The entities of Row 3, Column 1 associate to the other entities mentioned in the same column of the above rows. The classified data obtained from the owner is validated for accuracy and authentication. The backup are scheduled for regular updates and patches.

Column two discusses the information security policy function of the enterprises which needs to mandate the backups of all data available at all times. This includes data archiving process to ensure no loss of data due to physical thefts or natural disasters. Data auditing helps mitigate the significant business risks associated with requirements for regulatory compliance and the use of corporate data assets. A comprehensive audit trail for critical data activity including data access, data changes, data viewing (who is looking at what data) and changes to database structure must be provided.

Column three addresses the available links between the nodes of the system locations and the security of its nodes and their links. The business linkage attribute could be a satellite link connecting two continents or countries or it could be a wire line or a wireless link between the business locations within the country, or it could also be dedicated optical fibre connectivity between the nodes of the system within a network. Encryptions based on end-to-end security that are independent of the network, provide robust and efficient solution for end security. Security of the nodes not only protects against thefts, but also against vandalism, unauthorised access, and media removal. Security during transportation of freight ensures high physical level of security.

Column four is the Human Interface architecture cell of the row. It separates the duties of the organization, listed in Row 2 Column 4. This cell defines the “Roles”, that is, skill set of the person, which discusses the business-level responsibilities of the organization. Roles are assigned to users who perform a job with those responsibilities. Only after receiving a role the user can perform the tasks defined in the role. The “Roles” defined in Column 4, Row 3, are performed by the organization units in Column 4, Row 2. At the system level of Row 3, we know the “Data Entities” (Column 1) accessed by the “Roles” and the “Application function” executed by them in Column 2 and in Column 3 the “IT Components” employed by them and the “System events” initiated by the “Roles” and constrains faced by them (Zachman, 2001).

In Column five, the designer plans the system events to be scheduled on a timely basis depending on the security level of the information. The survival and growth of an organization in an increasingly turbulent environment depends upon the utilization of information for aligning the organizational structure. Therefore, it is necessary to upgrade the software and the hardware components with necessary patches or modules to assure optimal performance of the product. Reengineering, which is a key concept of identifying the process enablers and barriers addressing the people, technology, facilities, etc., are addressed at this level. To establish a strategic assessment of the enterprise, the performance of risk management are tracked and evaluated to measure the frequency of its occurrence, failure of which may have adverse impact on the product or service.

Column six maps the jurisdictional issues, which may have adverse effect on the requirements of the organization. External security threats, which may comprise of server attacks or storage threats, could have devastating effect on the company. Application risk analysis caused by inadequate security of access points and interfaces acts as a constraint for the organization.

3.4. Technology Model:

The technology model of the Zachman Framework defines the physical representations of the things in the enterprise. The builder specifies the technology to solve the problems. The builder applies the physical constraints of what is possible to the designer’s artefacts and implements the product or service

by understanding its environment (O'Rourke, Fishman & Selkow, 2003). The Builder integrates all the data sources evolved from different platforms and operating systems for providing a common enterprise wide view.

Column one answers the question, What data is to be encrypted? Depending on the sensitivity of the data, standard encryption services are employed. This will include encryption, decryption and certificate management services. Secrecy, in the context of database security, includes a variety of threats incurred through unauthorized access that may lead to unauthorized release of information or even Denial of Service (DoS) attacks. The builder also handles the storage management system by partitioning the data, derived from the previous rows of this column, into internal or external hard drives. The meta-data present in Row 4, Column 1 of the framework should be safeguarded against unauthorized use of computers and networks other than those employed in Row 4, Column 3 by implementing Intrusion detection systems (IDS) at Column 2. The IDS discovers and reports unauthorized activity, such as log-on attempts by unauthorized users other than the users in column 4, by recording system logs and generates audit reports in Column 5.

Column two of the Technology model describes the usage and functioning of the system. 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.

Column three secures the business nodes by implementing access control devices such as various types of biometric systems. Authentication server reconciles the evidence of identity by authenticating data to its client. The communication links between the server nodes handles the data of Column 1 by implementing protocols for secure connection between the client and the server.

Column 4 is fulfilled by the "Users", the "Roles" from Row 3, at the "Presentation Architecture" of this row. Scheduling risk analysis and change in passwords on a sequential basis reduces the risks at this layer to an acceptable level.

Column five addresses risk mitigation analysis, the greatest concern to management, to identify and safeguard and mitigate vulnerabilities. Conducting security awareness program in a scheduled basis to the employees, by taking into account the needs and current levels of training and understanding of the employees and management, increases the consciousness of all employees regarding ways to protect information and information processing resources (Tipton & Krause, 1999).

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

3.5. Detailed Representations:

The Detailed Representations list the specifications of the technology model. The subcontractor assembles and fabricates the individual components of the enterprise derived from the above layers of the framework. The subcontractor creates the detailed descriptions that disassociate the parts or pieces of the complex object for the purposes of manufacturing the product and service (O'Rourke, Fishman & Selkow, 2003).

Column one addresses the "Data Definition" language specified in the "Physical Data Model" of Row 4. The relational database management system (RDBMS) and OO database models make use of security control models like discretionary access control (DAC) policy or mandatory access control (MAS) policy to secure information by assigning sensitivity levels to data entities (Tipton & Krause, 1999).

Due diligence investigations not only protect the current and future intellectual property, they also safeguard the company's reputation.

Column two of the subcontractor row defines the "Language Statement" for the input and output control blocks. An enterprise finds suitable algorithms to accept most jurisdictions worldwide, to protect the integrity of its messages. Algorithms such as Advanced Encryption Standard (AES), RSA, and Public-Key Infrastructure (PKI) help any enterprise to meet the challenges of protecting the most sensitive information assets. They also employ emergency key-recovery features. Single sign-on is a process employed to protect passwords. In this process the user needs to type their password only once and it is characterized by the advantages of convenience and centralized administration (Tipton & Krause, 1999). Data backup devices such as magnetic tapes and removable media like CD-ROMs etc., are used to restore the disaster recovery process defined by the builder in Row 4.

Column three addresses the node security by using logistics hub management, where hubs are able to manage inbound and outbound operations for source-to-consumption supply chain execution and optimisation. Manned guarding and access control systems such as burglar alarms increases building node security. Data authentication and confidentiality ensures implementation of end security protocols like Point-to-Point Protocol (PPP) and Secure Sockets Layer (SSL). Kerberos is a network access control and authentication protocol designed for client-server applications based on secret-key cryptography.

Column four, "The Security Architecture", identifies the "Identity" of the person who can access which "Fields" of Column 1, the "Language Statements" they could execute, and what "Addresses" (Column 3) they were authorized to access. Identity management solutions manage the users to help address the rapid growth in users of an enterprise system. These solutions improve security, reduce IT costs, enhance revenues, help with regulatory compliance and increase overall business agility.

Column five addresses the "Timing Definition", the definition of interrupts and machine cycles. It employs the machine cycle of the system by calculating the time taken to carry out an instruction. In a computer, the CPU gets input from the computers memory, processes its mathematical calculation using ALU (Arithmetic Logic Unit) and outputs the results of calculation to another system. Interrupt management simulates interrupts by maintaining an even queue together with a simulated clock. Rotation of assignment is an essential function to ensure staff backup by periodically alternating the individuals for essential tasks.

Column six discusses the constraints of the subcontractor during integration or implementation of the product or service which might occur due to environmental or legal issues.

3.6. Functioning Enterprise:

The functioning enterprise is the final system implemented and made part of the operational system environment. It is the physical materialization of the product or service and it is the result of the articulated artefacts (descriptive representations and models). Certification is a formal declaration from the designer, builder, and subcontractor to the owner that the functioning enterprise is as the owner described. Therefore the functioning enterprise should reassemble the owner's perspective with the other perspectives attempting to make what the owner desired in reality. Row 6 is therefore the reality and it is what the users of the enterprise's product or service experience physically (O'Rourke, Fishman & Selkow, 2003).

4. Conclusions

Security is a never-ending process that requires constant monitoring, updates, investment, research and implementation of new technologies. The Zachman Framework is based on an open architecture, which ensures solutions that can be easily extended to an enterprise's security policy of today and that of the future. It is shown that Zachman Framework best fits to plan security architecture for an enterprise as any evolving changes in technology can be implemented onto the Zachman Framework without affecting the direction of the enterprise. For this reason, the security planning using the Zachman Framework applied to enterprises is helpful for sorting out complex technology and methodology issues that are significant both to general and technology management.

The above planned Zachman Security Framework can be mapped with a government enterprise architecture establishing standard security services, increasing the level confidence, integrity and availability for IT across government.

References

DeLooze, L.Lori. (2001). Applying Security to an Enterprise using the Zachman Framework. *SANS Institute*.

Inmon, H. William, & Zachman, A. John, & Geiger, G. Jonathan, 1997, Data Stores Data Warehousing and the Zachman Framework Managing Enterprise Knowledge, McGraw-Hill.

O'Rourke, Carol, & Fishman, Neal, & Selkow, Warren, 2003, Enterprise Architecture Using the Zachman Framework, Course Technology.

Perkins, Alan, 2001, Enterprise Architecture Engineering.

Tipton, F. Harold, & Krause, Micki, 1999, Information Security Handbook, Auerbach Pub.

Zachman, John. (1987). A Framework for Information Systems Architecture. *IBM Systems Journal*, vol. 26, no.3. IBM Publication.

Zachman, A. John. (1993). The Framework for Enterprise Architecture: Background, Description and Utility.

Zachman, J.A., & Sowa, J.F. (1992). Extending and Formalizing the Framework for Information Systems Architecture. *IBM Systems Journal*, Vol. 31, No.3.

Zachman, A. John. (2001) Security and the Zachman Framework. *DataToKnowledge Newsletter*, Vol. 29, No. 6. (Business Rule Solutions LLC, November/December 2001).

Levent Ertaul. He is currently a full time faculty at California State University, Hayward, in the department of Math & Computer Science. He is actively involved in security projects nationally and internationally. His current research interests are Enterprise Security Planning, Mobile Agents Security, and Wireless Security. He has numerous publications in Security issues.

Raadika Sudarsanam She is currently pursuing her MSc degree in Department of Computer Science at California State University, Hayward. Her research interests are ESP and Network Security.

My sincere thanks to all the students for their active and enthusiastic participation in the discussion of "Security Planning for an Enterprise Architecture using Zachman Framework" in the project (CS/TC 6899) class held at California State University, Hayward in winter 2005 quarter.