Enterprise Security Planning with TOGAF-9

L. Ertaul[1], A. Movasseghi[2], and S. Kumar[2]
[1]Math & Computer Science, CSU East Bay, Hayward, CA, USA
[2]Math & Computer Science, CSU East Bay, Hayward, CA, USA

Abstract. *Enterprise security architecture is a unifying framework and reusable services that implement policy, standard and risk management decision. The purpose of the security architecture is to bring focus to the key areas of concern for the enterprise, highlighting decision criteria and context for each domain. TOGAF-9 architecture framework provides guidance on how to use TOGAF-9 to develop Security Architectures and SOA's. This paper addresses the enterprise architect of what the security architect will need to carry out their security architecture work. It is also intended as a guide to help the enterprise architect avoid missing a critical security concern.*

Keywords*:* Enterprise Security Planning, Enterprise Architectures, TOGAF

1. Introduction

The Open Group Architecture Framework (TOGAF) is a framework - a detailed method and a set of supporting tools for developing enterprise architecture **[1].** TOGAF 9 is much different from other architecture frameworks such as Zachman, as it is lot more process driven and gives you a way to essentially codify architectural patterns **[2].** Key enhancement in TOGAF 9 is the introduction of a seven-part structure and reorganization of the framework into modules with well-defined objectives. This will allow future modules to evolve at different speeds and with limited impact across the entire blueprint -- something that's needed if you're looking to create architecture within compartments and have those compartments operating independently **[1],[3],[5].** TOGAF 9, first of all, is more business focused. Before that it was definitely in the IT realm, and IT was essentially defined as hardware and software. The definition of IT in TOGAF 9 is the lifecycle management of information and related technology within an organization. It puts much more emphasis on the actual information, its access, presentation, and quality, so that it can provide not only transaction processing support, but analytical processing support for critical business decisions **[4].**

2. TOGAF Structure

As shown in Fig 1, TOGAF structure consists of;

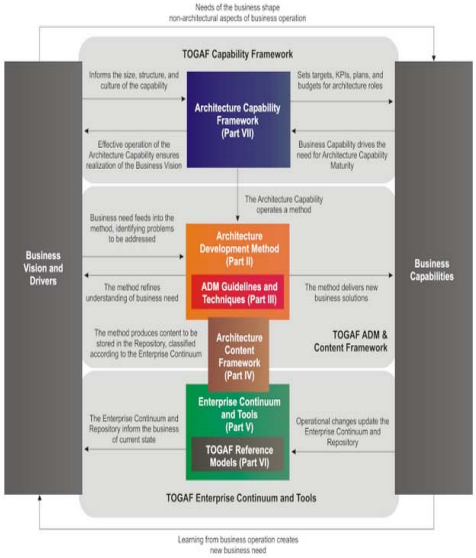

Figure 1. TOGAF Structure

PART I (Introduction) -This part provides a high-level introduction to the key concepts of enterprise architecture and in particular the TOGAF approach. It contains the definitions of terms used throughout TOGAF and release notes detailing the changes between this version and the previous version of TOGAF.

PART II (Architecture Development Method) - This part is the core of TOGAF. It describes the TOGAF Architecture Development Method (ADM) - a step-by-step approach to developing enterprise architecture.

PART III (ADM Guidelines and Techniques) This part contains a collection of guidelines and techniques available for use in applying TOGAF and the TOGAF ADM.

PART IV (Architecture Content Framework) This part describes the TOGAF content framework, including a structured metamodel for architectural artifacts, the use of re-usable architecture building blocks, and an overview of typical architecture deliverables.

PART V (Enterprise Continuum & Tools) This part discusses appropriate taxonomies and tools to categorize and store the outputs of architecture activity within an enterprise.

PART VI (TOGAF Reference Models) This part provides a selection of architectural reference models, which includes the TOGAF Foundation Architecture, and the Integrated Information Infrastructure Reference Model (III-RM).

PART VII (Architecture Capability Framework) This part discusses the organization, processes, skills, roles, and responsibilities required to establish and operate an architecture function within an enterprise.

The intention of dividing the TOGAF specification into these independent parts is to allow for different areas of specialization to be considered in detail and potentially addressed in isolation. Although all parts work together as a whole, it is also feasible to select particular parts for adoption whilst excluding others. For example, an organization may wish to adopt the ADM process, but elect not to use any of the materials relating to architecture capability **[1].**

3. TOGAF-9 Security Architecture

Security Architecture is a cohesive security design which addresses the requirements and in particular the risks of a particular environment/scenario and specifics what security controls are to be applied where. The design process should be reproducible. This definition is intended to specify only that, architecture is a design, which has a structure and addresses the relationship between the components **[6][7].**

3.1 Security for Architecture Domains

All groups of stakeholders in the enterprise will have security concerns. These concerns might not be obvious as security-related concerns unless there is special awareness on the part of the IT architect. It is desirable to bring a security architect into the project as early as possible. In TOGAF 9, throughout the phases of the ADM, guidance will be offered on security-specific information which should be gathered, steps which should be taken, and artifacts which should be created. Architecture decisions related to security, like all others, should be traceable to business and policy decisions, which should derive from a risk analysis.

3.2 Areas of Concerns for Security Architecture

Authentication: The authenticity of the identity of a person or entity related to the system in some way **[8],[7].**

Authorization: The definition and enforcement of permitted capabilities for a person or entity whose identity has been established.

Audit: The ability to provide forensic data attesting that the system was used in accordance with stated security policies.

Assurance: The ability to test and prove that the system has the security attributes required to uphold the stated security policies.

Availability: The ability of the system to function without service interruption or depletion despite abnormal or malicious events.

Asset Protection: The protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use.

Administration: The ability to add and change security policies, add or change how policies are implemented in the system, and add or change the persons or entities related to the system.

Risk Management: The organization's attitude and tolerance for risk. (This risk management is different from the special definition found in financial markets and insurance institutions that have formal risk management departments.)

3.3 Security Architecture Artifacts

Typical security architecture artifacts should include. 1.) Business rules regarding handling of data/information assets. 2.) Written and published security policy. 3.) Codified data/information asset ownership and custody. 4.) Risk analysis documentation. 5.) Data classification policy documentation.

3.4 ADM Security Architecture Requirement Management

Security Policies and security standards are one of the most important part of enterprise requirement management process. Security policies are established at executive level and have the characteristics like durability, resistant to impulsive change, and not technology specific. Once established act as a requirement for all architecture projects. Security standards are highly dynamic and state technological preferences used to support security policies. Security standards will manifest themselves as security-related building blocks in the Enterprise Continuum. Security patterns for deploying these security-related building blocks are referred to in the Security Guidance to Phase E.

New security requirements arise from many sources:

1. A new statutory or regulatory mandate
2. A new threat realized or experienced
3. A new IT architecture initiative discovers new stakeholders and/or new requirements.

In the case where 1. and 2. above occur, these new requirements would be drivers for input to the change management system discussed in Phase H. A new architecture initiative might be launched to examine the existing infrastructure and applications to determine the extent of changes required to meet the new demands. In the case of 3. above, a new security requirement will enter the requirements management system.

4. Security Architecture and ADM

Security architecture and ADM have eight different phases as explained below

4.1 Preliminary Phase

As shown in Fig 2**,** this phase is responsible for the defining and documenting applicable rules and security policies requirements. In TOGAF 9, **ISO/IEC 17799:2005** is used for the formation of security policies. In order to implement these policies there is need to identify a security architect or security architecture team. Security considerations can conflict with functional considerations and a security advocate is required to ensure that all issues are addressed and conflicts of interest do not prevent explicit consideration of difficult issues. If the business model of organization does encompass group of other organizations, then a common ground should need to be established between architects of different organization so they can develop interfaces and protocols for exchange of security information related to federated identity, authentication and authorization. So, the inputs to this phase would be written security policy, relevant statutes, list of applicable jurisdictions and outputs comes out in form of list of applicable regulations, list of applicable security policy, security team roaster, list of security conditions and boundary conditions. **[7][9].**

Figure 2. TOGAF Security Architecture and ADM

4.2 Phase A (Architecture Vision)

In Phase A, the main intention of security architect is to obtain management support for security measures. All the security related architecture decision should be documented and the concern management peoples and executives should need to identified and frequently updated about the security related aspects of project. Tension between delivery of new business functions and security policies do exist. So the processes solving such disputes must be established at the early stage of the project. Other architects and management need to

identify that the role of security architect is safeguard the assets of enterprise. Any existing disaster recovery and business continuity plan must be understood and their relationship with the planned system must be defined and documented. All the architecture decisions must be made between the context of environment within which system will be placed and operate. So the physical, business and regulatory environment must be defined **[7][9].**

4.3 Phase B Business Architecture

Phase B help to locate the legitimate actors who will interact with the product/service/process. Many subsequent decisions regarding authorization will rely upon a strong understanding of the intended users, administrators, and operators of the system, in addition to their expected capabilities and characteristics. It must be borne in mind that users may not be humans; software applications may be legitimate users. Those tending to administrative needs, such as backup operators, must also be identified, as must users outside boundaries of trust, such as Internet-based customers. The business process regarding how actors are vetted as proper users of the system should be documented. Consideration should also be made for actors from outside the organization who are proper users of the system. The outside entities will be determined from the high-level scenarios developed as part of Phase A. Security measures, while important, can impose burden on users and administrative personnel. Some will respond to that burden by finding ways to circumvent the measures. Examples include administrators finding ways to create "back doors" or customers choosing a competitor to avoid the perceived burden of the infrastructure. The trade-offs can require balancing security advantages against business advantages and demand informed judicious choice. Identify and document interconnecting systems beyond project control. Assets are not always tangible and are not always easy to quantify. Examples include: loss of life, loss of customer good will, loss of a AAA bond rating, loss of market share. Determine and document appropriate security forensic processes in order to proper implementation of security policies which in turn helps to catch the security breaches. Determine and document how much security (cost) is justified by the threats and the value of the assets at risk **[7][9].**

4.4 Phase C Information Systems Architectures

A full inventory of architecture elements that implement security services must be compiled in preparation for a gap analysis**.** Every state change in any system is precipitated by some trigger. Commonly, an enumerated set of expected values of that trigger initiates a change in state. However, there are likely other potential trigger inputs that must be accommodated in non-normative cases. Additionally, system failure may take place at any point in time. Safe default actions and failure modes must be defined for the system informed by the current state, business environment, applicable policies, and regulatory obligations. Safe default modes for an automobile at zero velocity may no longer be applicable at speed. Safe failure states for medical devices will differ markedly from safe failure states for consumer electronics. Standards are justly credited for reducing cost, enhancing interoperability, and leveraging innovation. From a security standpoint, standard protocols, standard object libraries, and standard implementations that have been scrutinized by experts in their fields help to ensure that errors do not find their way into implementations. From a security standpoint, errors are security vulnerabilities. Presumably, in the event of system failure or loss of functionality, some value is lost to stakeholders. The cost of this opportunity loss should be quantified, if possible, and documented**.** Existing business disaster/continuity plans may accommodate the system under consideration. If not, some analysis is called for to determine the gap and the cost if that gap goes unfilled **[7][9].**

4.5 Phase D (Technology Architecture)

Security architect should assess and baseline current security-specific technologies (enhancement of existing objective), revisit assumptions regarding interconnecting systems beyond project control, identify and evaluate applicable recognized guidelines and standards. Every system will rely upon resources that may be depleted in cases that may or may not be anticipated at the point of system design. Examples include network bandwidth, battery power, disk space, available memory, and so on. As resources are utilized approaching depletion, functionality may be impaired or may fail altogether. Design steps that identify non-renewable resources, methods that can recognize resource depletion, and measures that can respond through limiting the causative factors, or through limiting the effects of resource depletion to non-critical functionality, can enhance the overall reliability and availability of the system **[7] [9]**.

4.6 Phase E (Opportunities and Solution)

Identify existing security services available for re-use. From the Baseline Security Architecture and the Enterprise Continuum, there will be existing security infrastructure and security building blocks that can be applied to the requirements derived from this architecture development engagement. For example, if the requirement exists for application access control external to an application being developed, and such a system already exists, it can be used again. Statutory or regulatory requirements may call for physical separation of domains which may eliminate the ability to re-use existing infrastructure. Known products, tools, building blocks, and patterns can be used, though newly implemented. Also, Engineer mitigation measures addressing identified risks. Having determined the risks amenable to mitigation and evaluated the appropriate investment in that mitigation as it relates to the assets at risk, those mitigation measures must be designed, implemented, deployed, and/or operated. Since design, code, and configuration errors are the roots of many security vulnerabilities, taking advantage of any problem solutions already engineered, reviewed, tested, and field-proven will reduce security exposure and enhance reliability **[7] [9].**

4.7 Phase F (Migration Planning)

In a phased implementation the new security components are usually part of the infrastructure in which the new system is implemented. The security infrastructure needs to be in a first or early phase to properly support the project. Secondly, during the operational phases, mechanisms are utilized to monitor the performance of many aspects of the system. Its security and availability are no exception. Security of any system depends not on design and implementation alone, but also upon installation and operational state. These conditions must be defined and monitored not just at deployment, but also throughout operation **[7][9].**

4.8 Phase G (Implementation Governance)

Establish architecture artifact, design, and code reviews and define acceptance criteria for the successful implementation of the findings. Implement methods and procedures to review evidence produced by the system that reflects operational stability and adherence to security policies. To achieve all those things it is necessary to trained people to ensure correct deployment, configuration, and operations of security-relevant subsystems and components; ensure awareness training of all users and non-privileged operators of the system and/or its components**[7][9].**

4.9 Phase H (Architecture Management)

Incorporate security-relevant changes to the environment into the requirements for future enhancement (enhancement of existing objective) **[7] [9].**

5. Conclusions

Unless the security architecture can address a wide range of operational requirements and provide real business support and enablement, rather than just focusing upon short-term point solutions, then it will likely fail to deliver what the business expects. This type of failure is a common phenomenon throughout the information systems industry, not just in the realm of security architecture. Yet it is not sufficient to compile a set of business requirements, document them and then put them on the shelf, and proceed to design a security architecture driven by technical thinking alone. Being a successful security architect means thinking in business terms at all times, and setting up quantifiable success metrics that are developed in business terms around business performance parameters, not technical ones.

6. References

1. TOGAF version 9 Enterprise edition**,http://www.opengroup.org/architecture/togaf9-doc**
2. http://www.infoworld.com/t/platforms/open-group-upgrades-enterprise-architecture-402.
3. http://www.infoworld.com/d/architecture/togaf-9-means-better-architecture-555
4. http://www.zdnet.com/blog/gardner/togaf-9-advances-it-maturity-while-offering-more-paths-to-architecture-level-it-improvement/2808
5. http://www.opengroup.org/architecture/togaf9-doc/arch/chap04.html
6. http://www.isss.ch/fileadmin/publ/agsa/Security_Architecture.pdf
7. http://www.opengroup.org/architecture/togaf9-doc/arch/

8. W. Stallings, “Cryptography and Network Security Principles and Practices”, fourth edition, Prentice Hall, 2010
9. http://www.slideshare.net/MVeeraragaloo/togaf-9-security-architecture-ver1-0-5053593