White Paper

Information Security Integration within the Enterprise Reference Architecture Model Part 1

WP0073 | May 2013

Guy B. Sereff

Guy Sereff is an author, speaker and technology practitioner. His Technology Industry experience includes Application Research and Development, Large-Scale Technology Management, and Global Enterprise Architecture.

As well as a pragmatic blend of Strategy and Tactical execution, Guy also has extensive Architectural Domain experience which covers Business Architecture, Information Architecture, Solution Architecture and Enterprise Architecture.

In today's always on, digital-driven world, both the need for and the challenge of providing secure and reliable technology solutions is continually increasing. As our systems and platforms get more and more sophisticated, cyber criminals, 'hacktivists' and intelligent ne'er-do-wells grow equally more sophisticated in their ability to cause harm. The 'black hats' and fraudsters have come a long way from the early use of toy whistles to hack long distance phone service carriers to now managing complicated networks used to orchestrate synchronized assaults on institutions of all types. A continual barrage of perimeter penetration attacks hit infrastructure firewalls, where each day millions of attempts are made to locate a network vulnerability that can be exploited for some economic, social or political gain. Information security threats come from actors both outside and inside the organization as well, making it very difficult to sort out the trustworthy from the untrustworthy. The growing trend of hostile 'state' actors is quite disturbing and brings cyber threats to a whole new level of concern.

To be effective, Information Security must become a fundamental part of the Enterprise Architecture landscape, deeply embedded into platforms, services, networks and operations at all levels. Information Security must be an integral component within an organization's business, operation and technology strategies and solution delivery practices. In this two-part white paper series, we'll help architects, information security analysts, technology providers, business analysts and strategic risk managers

Access our **free**, extensive library at
www.orbussoftware.com/community

better understand how to incorporate Information Security into their organization's Enterprise Reference Architecture model.

In Part 1: Foundation, we'll cover a few key concepts that will provide the underpinning from which we'll be able to build our discussion on. These concepts include:

Fundamental Definitions and Relationships

- Enterprise Architecture
- Enterprise Architecture Frameworks
- Reference Models

Information Security Architecture Considerations

- Baseline Definitions
- Industry Certifications and Standards
- Information Security Architecture Framework Example

In Part 2: Implementation, we'll put the foundational principles from this document to work in the form of the Enterprise Reference Architecture Model and as an integral part of the Solution Delivery Process. We won't get into the details on specific information security practices or provide a 'one size fits all' list of reference architecture domain models that must be applied to an organization. Instead we'll discuss salient viewpoints to help successfully establish both an independent Information Security Reference Architecture domain and a means for successfully integrating Information Security into the broader Enterprise Reference Architecture Model.

Enterprise Architecture, Frameworks and Reference Models

Before we jump into Information Security Architecture, we will first set a common baseline context around Enterprise Architecture and its supporting frameworks and reference architecture models. An assumption has been made that readers are familiar with the general principles of Enterprise Architecture and that the definitions in this section serve only as a means of grounding ourselves to a common taxonomy. Occasionally architects and technologists use some of these terms and concepts interchangeably; our intent is to draw clear definitions and distinct relationships between (1) Enterprise Architecture, (2) Enterprise Architecture Frameworks, and (3) Enterprise Reference Architecture Models.

Enterprise Architecture

The field of Enterprise Architecture is an interesting if not fascinating intersection of business strategy, operations efficiency and technology

© Orbus Software 2013

"**Enterprise Architecture (EA)** is a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analyzing the execution of change toward desired business vision and outcomes. EA delivers value by presenting business and IT leaders with signature-ready recommendations for adjusting policies and projects to achieve target business outcomes that capitalize on relevant business disruptions. EA is used to steer decision-making toward the evolution of the future state architecture."[i]

optimization. While the Enterprise Architecture function is typically located in the Information Technology (IT) organization under the watchful eye of the Chief Technology Officer (CTO), its charter typically spans the full spectrum of the entity (or at least it should). Gartner paints a vivid picture with the following definition (left).

What I like about Gartner's description is that it is strategy-centric, rather than being overtly technology-centric. Although there are subtle variations in the domains that comprise various Enterprise Architecture definitions, they generally align to the domains of Business Architecture, Information Architecture, Solution Architecture, Application Architecture and Platform Architecture.[ii] For our discussion, think of Enterprise Architecture as the over-arching objective lens through which we attempt to view the enterprise's future state. Using this view, a model can be built to represent the organization's business, operation and technology disciplines, depicting their interdependencies and interaction models, underlying infrastructure and authoritative artifacts to drive tactical and strategic behavior.

Enterprise Architecture Frameworks

Because of its wide array of domains and disciplines, most organizations find the field of Enterprise Architecture to be quite daunting and at times rather vague, requiring the application of some consistent form of definition and approach. This is not too surprising, considering Enterprise Architecture spans such a wide swath across nearly all facets of the organization's ecosystem. Recognized best practices have emerged over time, encapsulated as frameworks that can help organizations bring proven structure to their Enterprise Architecture efforts. Even organizations that perceive themselves as being 'too small' or 'not for profit' can benefit from these frameworks as they force a series of conversations and self-assessments that ensure scarce resources are being invested in areas that will benefit the institution the most.

Enterprise Architecture Frameworks are valuable as they bring a focused, repeatable analysis and artifact generation pattern that can aid an organization in taking a systemic and methodical approach when defining the components of their business. As shown in Figure 1, there are numerous Enterprise Architecture Frameworks to choose from, each having their own unique set of strengths and weaknesses. Framework implementation is not rigid, and many organizations have successfully established internal hybrid frameworks that take concepts from one or more of the published frameworks to meet their unique requirements. In contrast, architectural organizations that don't adopt at least some

© Orbus Software 2013

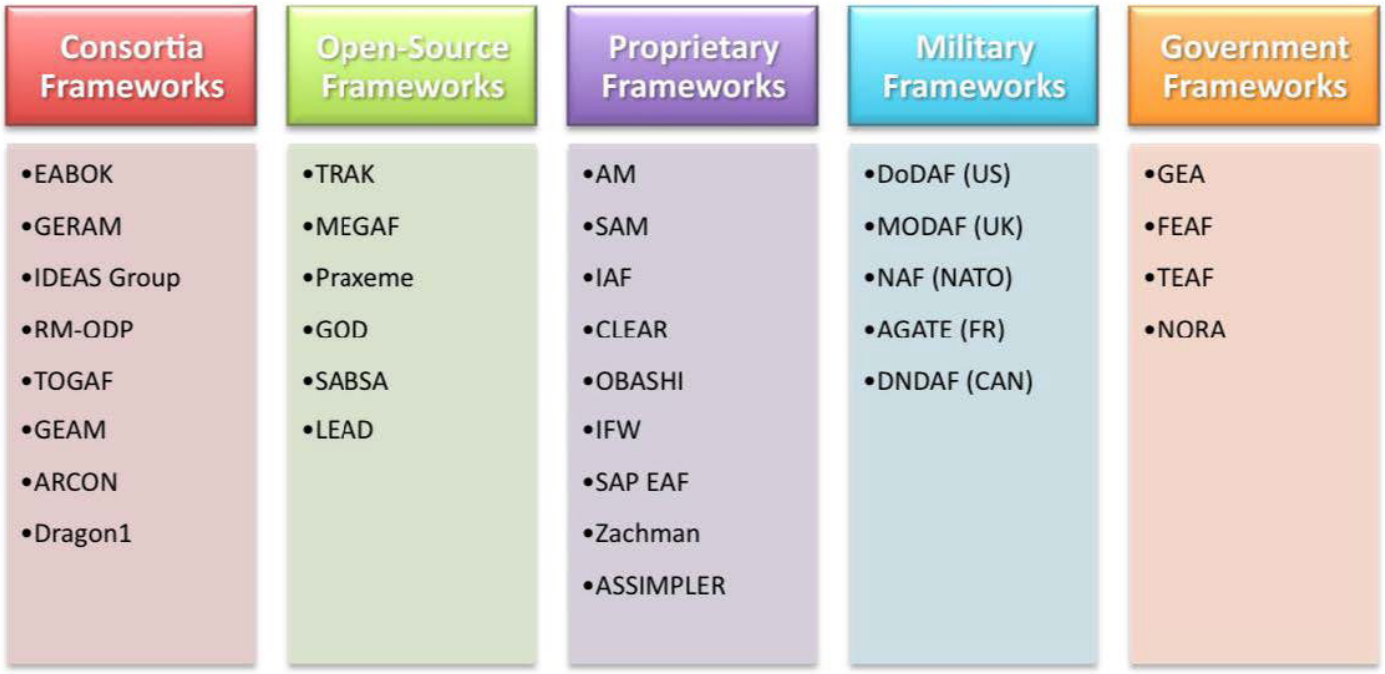


Figure 1 - Popular Enterprise Architecture Frameworks[iii]

baseline form of a consistent Enterprise Architecture framework often don't deliver their full potential, due to spotty subject coverage, inconsistent work product delivery and lack of governance.

Enterprise Architecture Framework "An architecture framework is a foundational structure, or set of structures, which can be used for developing a broad range of different architectures. It should describe a method for designing a target state of the enterprise in terms of a set of building blocks, and for showing how the building blocks fit together. It should contain a set of tools and provide common vocabulary. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks."[iv]

Choosing which framework to adopt or adapt is well beyond the scope of this document, as it is totally dependent on the unique nature of the organization. While not playing favorites, The Open Group provides a good, general definition of Enterprise Architectures Frameworks below that we can use for our purposes (left).

Where Enterprise Architecture represents a set of strategic objectives on a grand scale, the Enterprise Architecture Framework provides the methodology by which the organization's architecture community will operate. To be clear, the framework will not generally tell one how to address the needs of their organization per se, identify which Gang of Four[v] design pattern to use, or recommend one technology solution over another. Instead the frameworks acts as a guide through a series of critical subjects, providing a set of steps and questions designed to help produce a consistent and complete set of outputs to drive the next level of activity. At the end of the initial framework mapping activity, whether applied to a single program or to the business at large, the outputs from the Enterprise Architecture Framework collectively provide the definition of the Enterprise Architecture.

Doing this as a one-time event is certainly interesting, but to be effective this must be an evergreen process - one that is repeated consistently and regularly to reflect the dynamic nature of the organization itself. Imagine holding fast to a 'boom cycle' inspired Enterprise Architecture

© Orbus Software 2013

definition during an economic ‘down cycle’; it simply won’t provide the organization with the right strategic direction. Yes, some aspects of the defined architecture will change at a different pace than others, but this is by design, providing the resiliency needed to adapt to unavoidable change.

Enterprise Reference Architecture Model

Now that we’ve distinguished the relationship between Enterprise Architecture as a discipline and its various manifestations through frameworks, we turn our attention to the extended concept of referential architecture. As the name implies, Reference Architecture is a term that describes a discretely articulated set of constructs, or building blocks, that define particular functional and non-functional domains relevant to the entity. An organization’s Enterprise Reference Architecture Model is simply the collection of published Reference Architectures used to govern the generation of strategically aligned solutions.

> “Briefly, a reference architecture consists of information accessible to all project team members that provides a consistent set of architectural best practices. These can be embodied in many forms: prior project artifacts, company standards, design patterns, commercial frameworks, and so forth. The mission of the reference architecture is to provide an asset base that projects can draw from at the beginning of the project life cycle and add to at the end of the project.“[vi]

The Reference Architecture defines the organization’s de facto architectural standards to be applied when delivering strategic capabilities within a particular discipline or domain. Paul Reed offers the following definition, which does a good job of encapsulating the core concepts for us. It is a little short on the roles of standardization and governance, but workable just the same.

First let’s discuss the Reference Architecture content. The following table provides a typical example of key elements a Reference Architecture template would likely contain - it is not intended to be exhaustive or comprehensive, but rather to provide a sense of content coverage. It is a combination of business, operational and technical information that defines scope, capabilities, and supporting technology components

Domain Meta Data - Description - Version - Stakeholders	**Business Capabilities** - Client-Facing Functionality - Transactional Tasks - Competitive Analysis	**Architectural Approach** - Guiding Principles/Patterns - Platform Independent Models - Applied Industry Model(s)
Domain Scope - In Scope / Out of Scope - Cross-Domain Dependencies - Critical Success Factors	**Operational Capabilities** - Process Mapping - Workflow Integration - Efficiency Drivers	**Technical Components** - Platform Specific Model - Approved Components - Buy/Hold/Sell Technical Assets
Strategy - Disruptive vs. Adoptive Approach - Strategic End State - Targeted Competency Level	**System Capabilities** - Functional - Non-Functional - Information Flow	**Conformance Roadmap** - Current State Analysis - End State Conformance Timeline - Program Alignment

© Orbus Software 2013

where required. Each organization will have to determine what the right level of content detail within their Reference Architecture should be.

This view isn't dissimilar from many existing framework models, other than its narrow focus on a particular domain. One of the distinguishing features of the Reference Architecture, however, is the very prescriptive list of Technical Components. Depending on the domain, this would typically dictate hardware selection, operating system specifications, application software packages, approved Open Source components, access controls, channel enablement tools and so forth. The goal is to have a domain template pre-populated and available for anyone needing to deploy the capabilities captured within that domain. This helps to (1) reduce variation across what should be common capability solutions and (2) accelerate solution delivery, as teams have a repository of pre-defined and pre-approved components. Deployment is accelerated even further if the domain has already been realized as a set of reusable shared services that can be quickly configured and provisioned to consumers (internal, external or both) in a flexible cloud or cloud-like environment.

To be fair, this all comes at a price and requires some diligent effort up front. A balance must be struck between too much and too little detail in the reference model. Make it too loose or abstract and downstream model consumers are emboldened to 'fill in the gaps' with potentially undesirable components or point solutions; Too tight or concrete and the reference model becomes brittle and difficult to maintain over time[vii]. Consequences must be weighed carefully to determine what components are non-negotiable (like critical Information Security components) and which can be afforded some leeway.

Just as the content of the Reference Architecture template must be determined, the organization must also determine what constitutes a Reference Architecture Domain. A common tendency is to establish the domains either along organizational lines to match the entity's existing corporate structure, or to match domains to existing processing platforms or applications (front-end, middleware, backend, data warehouse, etc.). This seemingly innocuous domain definition short cut may be initially easier to sell to the stakeholder community as it lacks much controversy, but it does little to challenge the status quo or to address organizational politics that may be propagating an unnatural set of boundaries. If the goal is thought leadership through enterprise driven architecture governance, then consider doing the hard work and aligning the domains along capabilities that define what the business does, even if the current systems are not set up as a corresponding match. Keep in mind that for each domain, there are

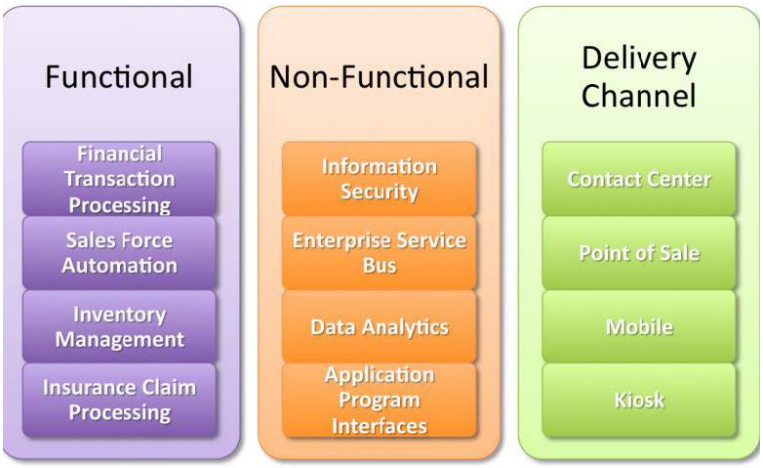


Figure 2 - Sample Reference Architecture Domains

© Orbus Software 2013

defined roadmap and end state elements. For those organizations that are not sure where to start, there are various commercially available reference models with varying degrees of content depth. Depending on the industry the organization is engaged in, these can be excellent accelerators; just be sure not to commoditize the organization's differentiating competencies or strategic advantages by adopting the same model as everyone else, especially competitors.

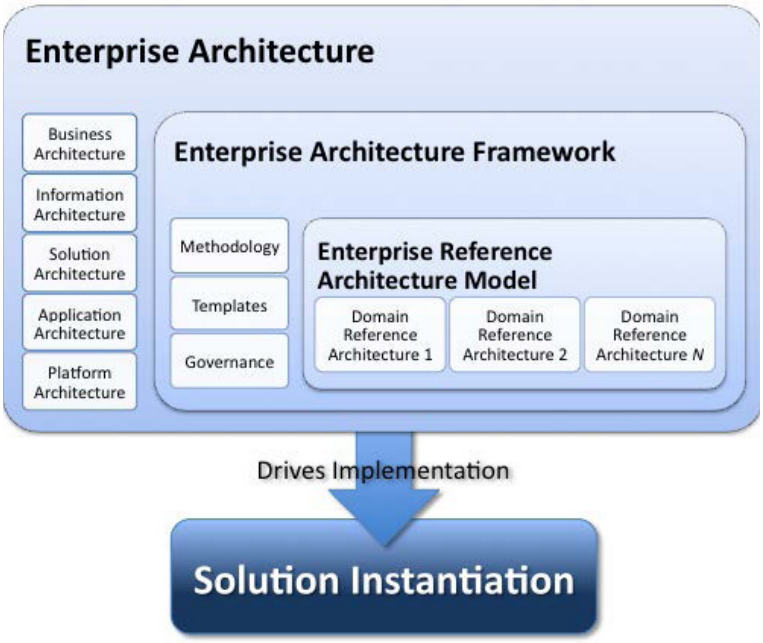


Figure 3 - Enterprise Architecture Influence on Solution Delivery

An Enterprise Architecture practice is only truly effective when it is able to influence organizational behavior in the intended direction. Assessing the existing state of affairs, creating reference architecture roadmaps and even publishing migration timelines are only the beginning steps of the process. A compelling business case must be raised to drive critical investment dollars into realizing and maintaining that desired end state, otherwise the architecture community may be perceived as not thinking like stakeholders and simply advocating technology projects for the sake of advocating technology projects. Depending on the needs of the organization, some reference architecture conformance activities are orchestrated through very explicit alignment initiatives. Other scenarios may depend on being able to 'weave' reference architecture components in over time, as resources are made available. Low priority roadmap items may remain unattended for a considerably long time, which is tolerable as long as higher value propositions are being realized along the way.

The key message of the roadmap is just that - a roadmap, which is designed to help chart the course from the current state to the end state for the greater good of the enterprise. Just don't be disappointed that when you finally get there at that elusive end state, the world has changed in the meantime and a new end state is required. This requires an iterative cycle that cannot be well served by point in time solutions or a set of one-time activities.

Information Security Architecture Considerations

Now that we have a shared view of what an Enterprise Reference Architecture Model is we will turn our attention more specifically to the topic of Information Security Architecture. As in the previous section, we'll ground ourselves with a few common definitions and then discuss resources available such as domain certifications, framework extensions,

© Orbus Software 2013

TREND: *"The information infrastructure - comprising computers, embedded devices, networks and software systems - is vital to operations in every sector. Global business and industry, governments indeed society itself cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed"*[viii]

Eric Goetz and Sujeet Shenoi (2010)

and standards to aid in the evaluation, definition and extension of existing information security capabilities. We are working under the assumption that the organization already has some level of information security awareness, and risk management and mitigation may in fact be quite rigorous. To that end we won't spend time on specific Information Security implementation topics such as secure communication protocols, preferred encryption methods or how to implement OpenID and such. Instead we will discuss topics related to the Information Security Architecture practice at large, leaving room as always for organizations to weigh their own needs and map their own best solution.

Baseline Definitions

"Security is all about protecting business goals and assets. It means providing a set of business controls that are matched to business needs, which in turn are derived from an assessment and analysis of business risk. The objective in risk assessment is to prioritize risks so as to focus on those [risks] that most require mitigation"[ix]

Before we go further, let's review a couple of relevant definitions. In their book, Enterprise Security Architecture: A Business-Driven Approach, Sherwood, Clark and Lynn offer this observation (left).

"Enterprise Information Security Architecture (EISA) is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. Although often associated strictly with information security technology, it relates more broadly to the security practice of business optimization in that it addresses business security architecture, performance management and security process architecture as well."[x]

For a slightly more academic toned definition, we have the following to consider as well (left).

The challenge when implementing security architecture at an enterprise level lies in the vast number of connections, components and actors involved, often on a global scale. Systems, operations and components require specific protection measures to safeguard the institution's digital perimeter. Once inside the firewall, there are a myriad of devices that have to securely communicate with one another in order to conduct operations. Messages communicated between devices must be authenticated and be guaranteed to be free of malicious content. Actions taken by the devices on the messages received must also be secured. Physical device locations must be securely constructed and monitored at all times. Data, one of the organization's most valuable assets, must be protected during its entire life cycle, including acquisition, in-memory manipulation, transmission, storage, retrieval and destruction. It is scary to think that we've barely scratched the surface in our discussion and we've yet to mention the most perilous of threats - human actors (and system actors posing as human actors, whether legitimately or illegitimately).

All of this comes down to understanding, establishing and executing

© Orbus Software 2013

effective risk assessment, prioritization and mitigation strategies. Even the fictitious, non-networked workstation locked inside the special vault deep in the interior of Fort Knox was no match for the Impossible Missions Force, who managed to manipulate security controls, commandeer HVAC systems, impersonate authorized emergency personnel and use social engineering to obtain the prized NOC list[1]. While it may have been an over-the-top set of Hollywood special effects to keep the storyline interesting, it does raise a good point for us to consider here. Most data centers are generally secure from average, unsophisticated threats and attempted assaults. However, installation security fortifications vary wildly from there, based on each organization's risk assessment (threat scenario likelihood and severity) and their propensity to invest in mitigating that risk. With finite resources available, it simply is not feasible to mitigate every risk identified, and informed judgment calls must be made.

In addition to shear costs, it can also be quite challenging to mitigate risks while maintaining a positive user experience and providing a productive operating environment. Organizations simply cannot effectively function in isolation from the rest of the world in today's marketplace and must stay digitally connected with their customers, regulators, and supply chain partners. This requires certain trade offs between 'ultimate' security, and 'secure enough' in order to meet the business objectives while protecting the assets of the firm. This drives the need for an Information Security Architecture paradigm that not only reflects the risks inherent in the existing and planned platforms, but also accommodates a risk mitigation-weighting schema that provides some level of guidance on prioritization. This guidance needs to explicitly address all of the high-level components similar to those shown in Figure 4 below, even if the plan is to 'handle manually' or 'accept the unmitigated risk' at the business operation level. Choosing to take a risk is not the same as not knowing about or simply not planning for it; it simply memorializes the intention not to mitigate the risk and accept the potential consequences. Available audit resources should be consulted early to ensure that accepted risks are tolerable within the organization's policies and procedures.

© Orbus Software 2013

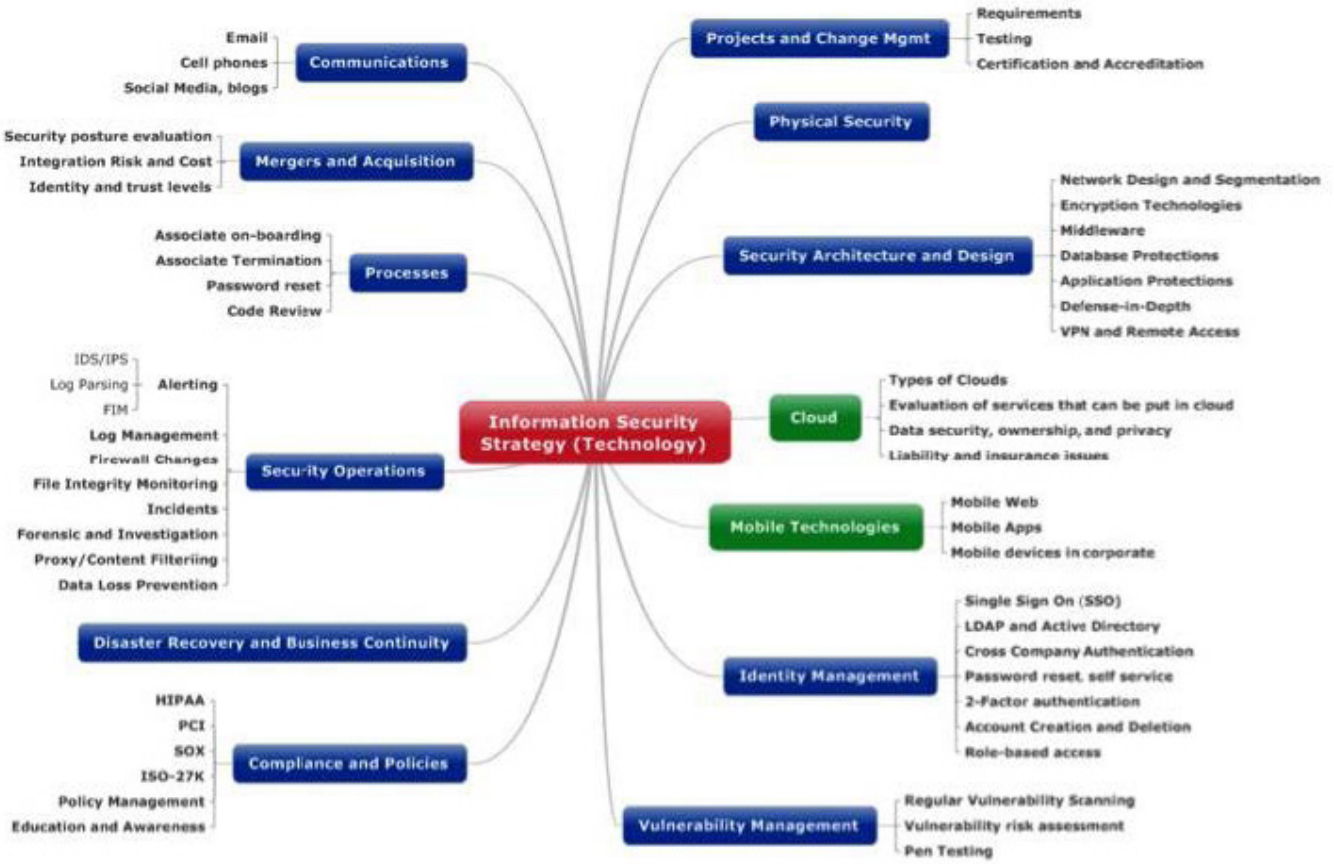


Figure 4 - High Level Components of Information Security Strategy[xi]

Information Security Certifications

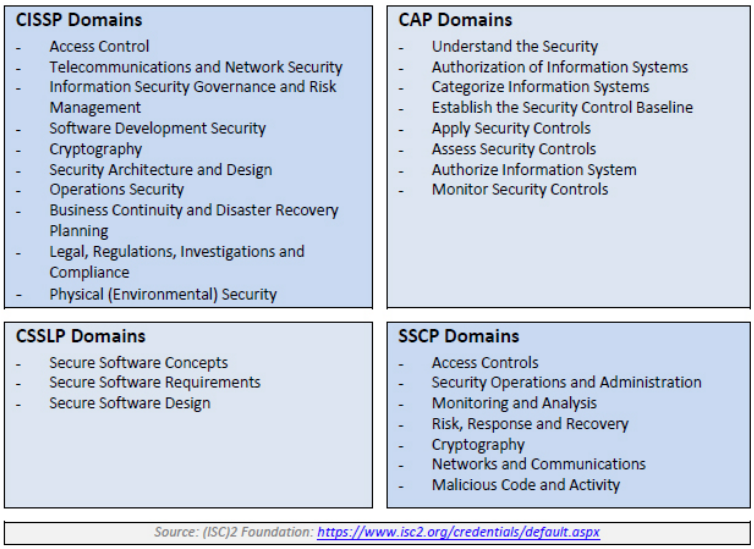
As Information Security has risen in to the level of critical core competency, several bodies of knowledge have emerged, resulting in professional certification. While we won't review them all here, a good place to start when looking for relevant Information Security Architecture domain topics are within the various certification areas of expertise as outlined by the International Information Systems Security Certification Consortium, or (ISC)[2®]. They currently confer the following certifications:

- CISSP: Certified Information Security Professional
- CAP: Certified Authorization Professional
- SSCP: Systems Security Certified Practitioner
- CSSLP: Certified Secure Software Lifecycle Professional

The intent here is not to endorse this particular set of certifications, but rather to call them out as a good example of how crosscutting and pervasive the area of information security really is. You'll notice that some of the domains overlap, either explicitly or implicitly with contextual variation as needed for the area of expertise. Many vendors also offer proprietary security-related certifications for their products or platforms, which can be very beneficial depending on how pervasive that product is used across the enterprise.

Certified professionals are trained on how to assess and address the domains listed below, creating an instant Center of Information Security Excellence within the organization they belong to. Keep in mind,

© Orbus Software 2013



Authentication: *"The substantiation of the identity of a person or entity related to the system in some way."*

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.)"*

however, that this training is generalized and will not provide them with business context or industry-specific risk knowledge. The key is, however, that they have demonstrated a proven level of competency and are equipped to perform analysis of specific security subject areas in a methodical, standardized manner.

Information Security and TOGAF

Recall from our previous section that one of the prominent Enterprise Architecture Frameworks is TOGAF (The Open Group Architecture Framework). Although recognized as a critical omission in earlier iterations of TOGAF, Security Architecture was added to version 9 in 2009 (see Chapter 21). This chapter of TOGAF is largely based on a white paper published in 2005 by The Open Group as a supplement to TOGAF 8 (Guide to Security Architecture in TOGAF ADM)[xii]. Chapter 21 provides specific security architecture steps for each of the nine TOGAF phases in terms of key considerations, inputs and outputs. They also provide the following list of areas Security Architects (left - by title or by role) should address:[xiii]

Rather than embed the Information Security steps directly into each phase of the TOGAF framework, they are treated as extensions to the phase itself. The warning flag this raises is the potential perception that Information Security is somehow optional, or not as critical as the other architectural components already engrained in the phases. The message to the organization must be clearly reinforced that Information Security Architecture needs to be cared for at every point along the architectural life cycle. In my experience, shifting organizational technology is often not as difficult as shifting organizational culture; if there isn't an enterprise-wide sensitivity and appreciation for the criticality of Information Security today, shifting that point of view needs to start right away.

Organizations that try to work security considerations into the architecture late in the process will struggle with getting the right level of risk prioritization and mitigation set, as many of the key architectural decisions may have already been made. Retrofits can be quite costly, depending upon how fundamentally flawed the current state is and

© Orbus Software 2013

how far along in the life cycle things have progressed. Stakeholders will generally agree that Information Security is important, but will offer only a tepid response regarding interest in funding the rework; this type of rework generally does not add perceptible functionality enhancements and correctly raises the question as to why it wasn't designed correctly in the first place. Just as trying to inspect quality into a process at the end is not effective, the same principle applies to Information Security, but often with much higher negative potential impact to the organization.

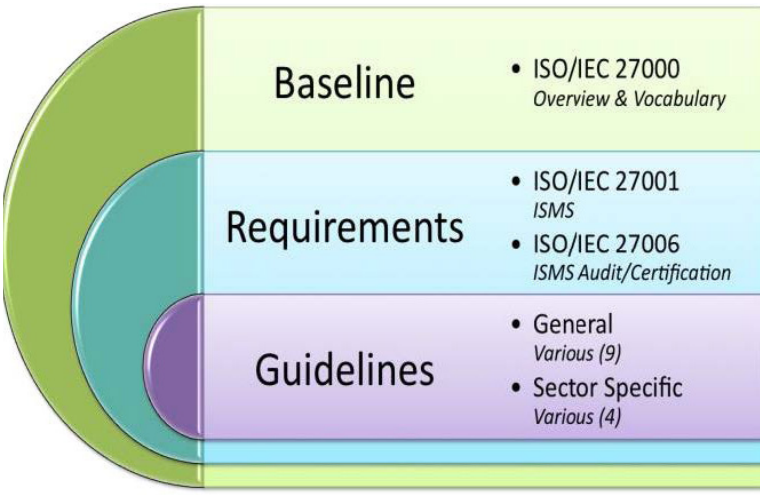


Figure 5 - ISO/IEC ISMS Standards

ISO IEC 27000

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly published a collection of Information Security standards based on best practices observed across industries and geographic boundaries. This collection of various published and pending standards make up a body of information security knowledge referred to as the Information Security Management System (ISMS) family of standards.[xiv]

Regardless of whether or not an organization adopts any or all of the ISMS standards, reviewing ISO/IEC 27000:2012 is recommended, as it provides an overview of each of the subsequent standards. A vocabulary is also included, which may prove useful in establishing a universal Information Security taxonomy within the organization if one doesn't exist or it lacks precise definitions (i.e. Risk Management Process versus Risk Treatment Process). Reading through this standard will also provide a good indication of which of the ISMS standards would likely apply or benefit the organization. Two of the standards specify ISMS requirements (ISO/IEC 27001, ISO/IEC 27006), while the remaining standards provide general and sector-specific guidelines.

Organizations have been successful in applying the ISO/IEC ISMS standards as an extension or clarification of their existing practices and Information Security Architecture. It can also be advantageous in situations where an internationally recognized security standard is critical to the nature of the organization and its perception in the marketplace, such as a bank or major healthcare provider. The final point we'll make is that these are auditable standards, meaning operations can be certified and independently audited. Passing an ISO/IEC 27000 audit or achieving certified accreditation is no guarantee that the institution is impervious to threats and that all risks have been mitigated or neutralized. However, it does provide an objective assessment of the institution's Information Security practices.

© Orbus Software 2013

NAIP - National Information Assurance Partnership[xv]

The National Information Assurance Partnership (NAIP) program was established as a coalition between the public and private sectors to validate how well IT products adhere to certain security-related international standards related to Information Security. This program, called the Common Criteria Evaluation and Valuation Scheme (CCEVS) for IT Security has published a series of documents that provide a means of evaluating the security capabilities of software products. Organizations can evaluate and potentially enhance the software-related components of their Information Security Architecture by reviewing NAIP's CCEVS publications and applying the specified criteria to their own platforms. The CCEVS is embodied in four documents:

Common Methodology for Information Technology Security Evaluation

- Part 1: Introduction and General Model
- Part 2: Security Functional Components
- Part 3: Security Assurance Components
- Evaluation Methodology

One of the strengths of the NAIP CCEVS is that it follows a repeatable pattern that can provide consistent evaluation of different platforms and their ability to protect assets. The evaluation criteria can also be used to help an organization drive their Information Security requirements.

SABSA - Sherwood Applied Business Security Architecture

The last model we'll mention in this section is the Sherwood Applied Business Security Architecture model, or SABSA.[xvi] The SABSA model is a deliberate extension to the Zachman Framework metamodel, segmenting the organization's Enterprise Architecture into a very similar multi-dimensional matrix to thoroughly describe and define risks and threats within the construct of an Information Security Architecture paradigm. The SABSA and Zachman models both identify essentially the same architectural layers:

© Orbus Software 2013

SABSA	Zachman Framework[xvii]
Contextual Security Architecture	Scope (Contextual) - Planner
Conceptual Security Architecture	Business Model (Conceptual) - Owner
Logical Security Architecture	System Model (Logical) - Designer
Physical Security Architecture	Technology Model (Physical) - Builder
Component Security Architecture	Detailed Representations (Out-of-Context) - Subcontractor
Operational Security Architecture	Functioning Enterprise

The other axis of the SABSA Matrix supports the 'what-why-how-who-where-when' points of view that are applied to each architectural layer. Methodically working through this matrix builds a comprehensive set of artifacts that essentially outline the organization's Information Security Architecture in a well-defined manner.

SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

© 1995 – 2009 SABSA Limited | info@sabsa.org

Figure 6 - The SABSA Matrixx[viii]

The purpose of sharing the SABSA model here is twofold. First, the matrix provides a solid tool for assessing and defining the organization's Information Security model from a business and risk management perspective. Whether the model is formally adopted or not, it can be

© Orbus Software 2013

used to compare an organization's existing approach to confirm topical coverage and to identify potential gaps that need to be addressed. Second, for those organizations already following the Zachman enterprise metamodel framework or some customized variation thereof, the SABSA model would be a fairly natural extension to the existing framework approach already in place. Architects would benefit from the similarity of their current practice and, just as TOGAF required additional structure to formally incorporate Information Security into their architectural process, pairing up SABSA with Zachman ensures that Information Security Architecture is explicitly cared for in the overall Enterprise Architecture process.

TREND: *"Why can't the targeted institutions, some of which have extremely sophisticated technology, defend themselves against the onslaught?*

The main answer, as we've noted in many previous articles, lies in the massive volume of the attacks, which unleash a torrent of data at websites with the goal of overwhelming them.

'Twelve months ago, the maximum protection [from cyber assault attempts] for a major financial institution was 10 gigabytes per second,' says Dave Ostertag, a global investigation manager with Verizon. 'Now we're averaging 40 to 50 gigabytes per second. The entire industry has changed.'"[xix]

David Browdie, Bank Technology News, American Banker (2013)

In closing, we reiterate that these models and industry tools are presented here not by way of endorsement or recommendation, but rather to give organizations a sense of what tools are out there to help them define Information Security Architecture for their enterprise. Clearly not all models are a good fit for all situations, but it is unlikely that none of the models, standards and/or tools would be a good fit either, even if some level of customization or modification were required.

The bottom line is that the Information Security Architecture must be tailored and scaled to meet the unique risk profile of the institution. Some institutions will have the luxury of adopting models and frameworks as 'off the shelf' solutions straight away, while others will have to make customizations to meet their organization's needs. Either way, consider that even with an extremely talented pool of architects and designers, Information Security Architecture should not be driven by intuition, experience and skill alone - equip the organization to succeed with known best practices and industrial-strength tools as well.

Conclusion

Information Security is crucial to an organization's survival in today's digital economy. Stakeholders, shareholders, partners and customers expect the organization to protect their assets, keep their secrets safe and to not expose them to fraud or undue risk. Yesterday's security measures and countermeasures are no longer enough to defend the organization from tomorrow's sophisticated and massive attacks. Organizations will always be faced with limited resources and unable to eliminate or mitigate all possible risks, requiring a business-oriented risk management approach that drives the right level of investment into Information Security.

© Orbus Software 2013

In Part 1, we clarified the distinction between Enterprise Architecture, Enterprise Architecture Frameworks, and Enterprise Reference Architecture models. We also reviewed several resources and bodies of knowledge to help establish a comprehensive Information Security center of excellence. In Part 2 we discuss proactive steps needed to make Information Security Architecture a vital part of the Enterprise Architecture Model.

While there are no guarantees, adapting and applying these principles to an organization's Enterprise Reference Architecture Model practice will help strengthen their level of Information Security competency. However, being competent is not enough - protecting the collateral, interests, and constituents of an organization requires constant and deliberate execution of risk management and threat neutralization techniques with minimal business and operational friction or disruption.

References

[1] Mission Impossible; Paramount Pictures (1996)

[i] Gartner. (2012). Gartner IT Glossary - Defining the Industry. Gartner, Inc. http://www.gartner.com/it-glossary/enterprise-architecture-ea/. Accessed April 5, 2013

[ii] Sereff, Guy B. (2012). Launching an Enterprise Business Architecture Practice: A Playbook for Getting Started. P. 18. Franklin, TN, USA: Guy B. Sereff

[iii] Wikipedia. Enterprise Architecture Framework. Wikipedia - The Free Encylopedia. http://en.wikipedia.org/wiki/Enterprise_Architecture_framework. Accessed April 5, 2013

[iv] The Open Group. (2009). TOGAF Version 9 - The Open Group Architecture Framework (TOGAF). P. 41. Zaltbommel, NL: van Haren Publishing

[v] Gamma, Erich, Richard Helm, Ralph Johnson, John Vlissides. (1994). Design Patterns: Elements of Reusble Object-Oriented Software. Upper Saddle River, NJ: Addison-Wesley.

[vi] Reed, Paul. (2002). Reference Architecture: The Best of Best Practices. IBM developerWorks.

[vii] Muller, Gerrit. (2013). A Reference Architecture Primer. P. 10-12. Kongsberg, Norway: Buskerbund University College

[viii] Goetz, Eric and Sujeet Shenoi (2010) Critical Infrastructure Protection. P. XIX. New York, NY: IFIP International Federation for Information Processing / Springer

[ix] Sherwood, John, Andrew Clark and David Lynn. (2005). Enterprise

© Orbus Software 2013

Security Architecture: A Business-Driven Approach. P. 16. San Francisco, CA: CMP Media LLC

[x] World Wizzy. (2013). Enterprise Information Security Architecture. World Wizzy. http://worldwizzy.com/learn/index.php/Enterprise_Information_Security_Architecture. Accessed April 3, 2013

[xi] Rehman, Rafeeq. (2011). High Level Components of Information Security Strategy. CISO Leadership, Strategy, and Research. http://rafeeqrehman.wordpress.com/2011/01/05/information-security-strategy/. Accessed 4/2/2013.

[xii] The Open Group Security Forum. (2005). Guide to Security Architecture in TOGAF ADM. San Francisco, CA: The Open Group.

[xiii] The Open Group. (2009). TOGAF 9. P 232-3. San Francisco, CA: The Open Group

[xiv] ISO/IEC. (2012). International Standard ISO/IEC 27000:2012 Information Technology - Security Techniques - Information Security Management System - Overview and Vocabulary. 2nd ed. P. iv. Geneva, CH: International Organization for Standardization

[xv] NAIP, (2012). National Information Assurance Partnership Common Criteria Evaluation & Validation Schema. NAIP. http://www.niap-ccevs.org/ Accessed 4/2/2013.

[xvi] Sherwood, John, Andrew Clark and David Lynas. (2009). White Paper - Enterprise Security Architecture. P. 9.

[xvii] Zachman, John A. (2011). The Zachman Framework for Enterprise Architecture. Zachman International. http://www.zachman.com/images/ZI_PIcs/ZF3.0.jpg Accessed 4/10/2013.

[xviii] Sherwood, P. 16.

[xix] Browdie, Brian. (2013) Why Cyberattacks Continue to Overpower Banks' Security Tech. American Banker; Bank Technology News. http://www.americanbanker.com/issues/178_66/why-cyberattacks-continue-to-overpower-banks-security-tech-1058072-1.html?zkPrintable=1&nopagination=1. Accessed 4/5/2013.

© Orbus Software 2013

Recommended Reading

Enterprise Security Architecture: A Business-Driven Approach
John Sherwood and Clark (2005)

Guide to NIST Information Security Documents
National Institute of Standards and Technology (2009)

Guide to Security Architecture in TOGAF ADM
The Open Group (2005)

Model-Based Management of Information System Security Risk
Nicolas Mayer (2012)

Information Security: A Conceptual Architecture Approach
Oracle (2011)

© Copyright 2013 Orbus Software. All rights reserved.

No part of this publication may be reproduced, resold, stored in a retrieval system, or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

Such requests for permission or any other comments relating to the material contained in this document may be submitted to: *marketing@orbussoftware.com*

Orbus Software
3rd Floor
111 Buckingham Palace Road
London
SW1W 0SR
United Kingdom

+44 (0) 870 991 1851
enquiries@orbussoftware.com
www.orbussoftware.com

orbus software