An Introduction to Information Security Architecture

Gartner The Future of IT Conference
October 4-6, 2011
Centro Banamex
Mexico City, Mexico

Notes accompany this presentation. Please select Notes Page view.
These materials can be reproduced only with written approval from Gartner.
Such approvals must be requested via email: vendor.relations@gartner.com.
Gartner is a registered trademark of Gartner, Inc. or its affiliates.

This presentation, including any supporting materials, is owned by Gartner, Inc.
and/or its affiliates and is for the sole use of the intended Gartner audience or
other authorized recipients. This presentation may contain information that is
confidential, proprietary or otherwise legally protected, and it may not be further
copied, distributed or publicly displayed without the express written permission
of Gartner, Inc. or its affiliates.

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved.
An Introduction to Information Security Architecture

There are many symptoms of inefficient or ineffective enterprise information security. Some examples include:

• Disparate security administration processes
• Duplicative or overlapping security tools
• Tools not working or not accepted by users
• Audit findings and lengthy audit proceedings
• Difficulty getting funding and approval for security initiatives

The reasons that enterprises may not be managing security effectively, making the right deployment decisions or sharing resources will vary. However, the root causes often have to do with failure to link security to business strategy, to identify security’s value to key stakeholders, making the right choices among competing solution alternatives, and managing projects effectively. Large and small organizations can use security architecture practice (a subset of enterprise architecture practice) to help make decisions about process, information and technology changes needed to support business strategy.

Enterprise architecture development (and, therefore, security and IAM architecture development) is a collaborative process that facilitates discussion and resolution among diverse groups of stakeholders enterprisewide, with the objective of ensuring a consistent approach to the execution of the business strategy.
Key Issues

1. What are the most effective contents and structures for security architecture?

2. How should enterprises practically model security architectures to ensure linkage to the business strategy and to adequately address risks?

3. What are security architecture pitfalls and best practices?
The term "architecture" is somewhat ambiguous, and can mean different things to different people. Within an IT context, architecture is probably commonly viewed as technology implementation design.
An effective enterprise information security architecture (EISA) practice, based on enterprise architecture (EA) principles, is a key tool for improving information security planning, implementation and operations. It improves the ability to make security design decisions that are aligned with business requirements. Security architecture is a continuous process, rather than a one-off activity. The focus is on developing and maintaining a set of evolving requirements, models, templates and principles, rather than delivering a set of static artifacts.

Security architecture is not a precise science. Practitioners get better as they learn what business requirements are, which solutions and approaches work, and which approaches are less effective. Hence, there is a need to focus on continuous improvement in the maturity of the EISA practice. And, while EISA practice (especially in the context of using EA principles) is still comparatively new in most organizations, it is not premature to identify maturity criteria that are specific to security architecture.
This model serves to convey some important principles of security architecture practice:

- The security architecture framework should enable planning and design via multiple iterations (levels of abstraction).
- The security architecture artifacts consist of the models, principles and documented requirements of various levels of abstraction.
- The architecture should address, at a minimum, the technical, business and information perspectives of the information security environment.
- The starting point for all security planning should be the business context, as formalized in a common requirements vision (CRV), strategic security principles and a common vision model.
- The solution architecture for any security implementation is a combination of the business, information and technology artifacts required for that implementation.

*Action Item: Treat security architecture as a continuous process.*
The EISA framework consists of a hierarchy of evolving documents containing models, requirements and templates. Documents higher up in the hierarchy tend to focus on concepts and tend to be less detailed and more stable. The lower down the hierarchy, the more detailed and dynamic the documents tend to be — that is, the more frequently they tend to be modified. In essence, changes in the strategic business requirements (less frequent) affect higher-level artifacts, while more-frequent changes in the technology and tactical business process landscapes affect lower-level artifacts. This dynamism alludes to the fact that the security architecture is a continuous process, rather than a single event or periodic activity.
In terms of content, the business context is described in an SRV, strategic security principles and a security program vision.

The artifacts in the SRV typically consist of matrices that replicate business strategies and external trends captured in the CRV of the EA (see "Toolkit: Bank XYZ Common Requirements Vision" G00146685), thereby linking them to explicit change, business and information requirement statements for the EISA. The slide illustrates a simplified example of an SRV.

Action Item: Use the SRV to document high-level security solution requirements that are explicitly linked to business strategies, environmental and technology trends, and security best practices.
Strategic security architecture principles guide decisions made during the architecture development, design and implementation stages. They should be derived from, and validated against, the principles articulated in the EA. These principles establish the foundational guidance for developing the security architecture. They guide a security architecture strategy that moves from various disconnected security activities to an aligned future state by:

- Aligning with business goals and risks
- Meeting multiple requirements with a common set of controls
- Providing a common reporting infrastructure for a single version of the truth (that is, the agreed-on controls, policies, processes and technologies)
- Being as noninvasive as possible, and using automation of controls where possible, instead of manual testing and surveying
- Clarifying roles, responsibilities and accountability

Action Item: Link your strategic security principles to the relevant business, information and technology principles derived from the EA.
The program vision model creates the basis for developing the strategic security principles (see "Toolkit: Strategic Security Architecture Principles Worksheet" G00158890), and it contributes to the development of the security requirements vision (see "Security Architecture: Developing the Requirements Vision" G00160066).
In many client organizations, the group responsible for developing architecture may not include the appropriate security subject matter expertise. There may not be a security architect on the EA team. Although security content for Bank XYZ was appropriately identified in the higher-level business documents, the security elements of conceptual, logical and implementation-level models were incomplete or inconsistent among models. Of course, it was never Gartner's intent for the Bank XYZ architecture collection to be exhaustive in detail. However, the lack of detail is useful for our purpose — that is, to demonstrate how security architects can work with the EA team, and to analyze current architecture work to identify where security can be improved.

For the remainder of this presentation, we'll analyze the initial set of Bank XYZ models associated with bringing in new customers, and we'll highlight IAM changes that might be identified by a security architecture team working with the EA team.

*Action Item: Identify "weak" spots in existing EA models, pull them out and bolster them by modeling IAM-specific artifacts."
The original "new customer" business process is an example of a business viewpoint EA artifact. Analysis of this model reveals that little in the way of security was designed into this business process. Although there are mentions of "verifying access," no banks would grant a loan to someone whose identity they didn't verify to an appropriate level of assurance. Also, once the customer's real-world identity has been verified and an account created, future interactions should require the customer to authenticate his or her identity before conducting transactions.

Action Item: Identify "weak" spots in existing EA models, pull them out and bolster them by modeling IAM-specific artifacts.
This model is an example in which identity proofing and authentication are added as a subset of the overall new customer business process. In this example, the new customer may make initial contact through the Web or through an agent assisting the customer with the registration process. The in-person process offers an opportunity to check physically for government-issued identity documents to add an extra layer of assurance. The online channel only allows for use of an identity-proofing function to verify real-world identity.
The slide is a marked-up version of the original Bank XYZ future-state network technology architecture model. It's noteworthy because of what's included and what's missing. The red circles highlight security technologies that were included in the original model — notably firewalls and virtual private networks (VPNs). None of the IAM components (such as the identity verification components) are illustrated, and there's only a passing reference to "security and access managers."

**Action Item:** Identify "weak" spots in existing EA models, pull them out and bolster them by modeling IAM-specific artifacts.
The business process and information flow models highlighted the need for identity-proofing services, authentication capabilities, and a tie-in with security information and event management (SIEM) systems. The trust model for Bank XYZ indicated the need to support multiple forms of authentication. The Bank XYZ mergers have brought in multiple legacy authentication technologies. Therefore, one future-state design consideration is to flexibly support multiple forms of authentication and to abstract the authentication service from the endpoint authentication technologies. This calls for the use of a versatile authentication service (VAS). This component — one instantiation for customers and another for internal employees — is illustrated here, along with associated directory services, and the identity-proofing service and SIEM systems that were identified in the information and business process models.

*Action Item:* Identify "weak" spots in existing EA models, pull them out and bolster them by modeling IAM-specific artifacts.
When the time comes to build or buy solutions, implementers need to know what the organization supports in terms of standard components and services. It isn't enough to just identify a product, or for example, an international standard. To be effective and help drive adoption, components and services should be defined in ways that help the intended recipient to understand the context of the standardization. Here, we show a sample implementation-level component catalog entry (formerly known as a "brick") for the VAS. Note that the entry includes the capability description and the product information, and that it also includes:

- The architectural patterns and services it supports, so that its usefulness for other appropriate use cases can be realized.
- The temporal context — what implementers should use this service for today, and what should be done one, two, and three to five years from now. This helps provide the longer-term picture, and is better than merely identifying a standard that may lose favor as the market and internal business requirements change.

Not pictured here, but included in related research, are other data elements in the standard component template (such as the architectural requirements that this component fulfills), as well as a list of the other products that were evaluated prior to selection, and why the selection was made.
**Architecture principles** represent the highest level of guidance for IT planning and decision making. Principles are simple statements of an organization's beliefs about how it wants to use identity and directory services over the long term, and are derived from business goals and corporate values. They provide the primary link between business technology strategies, and they drive the development of technical positions and templates.

A **technical position** can be thought of as a stand or a "stake in the ground" decision: an organization's expressed choice between competing technical alternatives and the justifications for that choice. Taken together, the answers to all the statements of position in one technical position document constitute the organization's established position on that particular issue. For example, an organization's disposition of the "Directory Integration" technical position may call for use (or nonuse) of custom metadirectory services, and the "User Management" technical position disposition would specify when to use delegated administration or existing databases for user registration.

**Templates** are "blueprints" or models of the identity and directory architecture, depicting how multiple system or application components relate to each other. Templates are useful in showing the structure of any IT environment. Templates graphically illustrate the identity and directory infrastructure that results from the complete collection of technical positions. In a well-developed architecture, templates are consistent with the technical positions.
Many architecture development efforts fail because the initial effort is scoped too broadly, making it difficult to quickly deliver guidance to implementations. Architecture efforts also fail when these efforts are viewed as one-time developments. Deliverables age and become irrelevant as the business climate changes. Architecture must be treated as an ongoing programmatic concern. Too much time spent on how architecture deliverables (artifacts) will be organized and formatted can also be wasted time and can prevent the architecture from delivering value in a timely manner. It is trite to say that we don't implement technology for technology's sake; however, many architecture efforts to date have focused simply on establishing technology standards with nonexistent or only vague associations to the business requirements. Focus instead on a set of deliverables that not only will help guide one or more key projects, but also have the potential to guide future projects. Begin with business change requirements, move to develop design principles and conceptual models, and then use those high-level models to drill-down and focus more-detailed architectural work on specific projects.
An Introduction to Information Security Architecture

Tactical Guideline: Integrating the security architecture into the enterprise architecture, although desirable, is seldom practical.

**Obstacles to Closer Enterprise Architecture Alignment**

- **Language**
  - Different communities
- **Understanding**
  - Distrust and politics
- **Resources**
  - No time to architect
- **Organization structure**
  - Security design done by security team
- **Architecture tool immaturity**

Strategies for getting closer to EA:

- Collaborate/join in new projects — e.g., planning for cloud computing, establishing a trust community.
- Leverage the corporate focus on IT governance.
- Align structure and terminology.
- Attend an EA course.
- Learn to use the EA methodology of your organization.
- Place a team member on the EA team.
- Hold workshops with EA — common processes, process interfaces and terminology.

*Action Item: Make a conscious decision about the level of alignment and integration of your security architecture with your EA that you will aim for today and in the midterm.*
Your Action Plan

Monday Morning
- *Reach out* to your EA colleagues.

Next 90 Days
- *Investigate* the feasibility of setting up a dedicated security architecture function.
- *Define* and *resource* the security architecture process.
- *Publish* the business context.

Next 12 Months
- *Develop* and *use* security artifacts as and when required.
Related Gartner Research

- Aligning Security Architecture and Enterprise Architecture: Best Practices
  Tom Scholtz (G00162519)

- The Structure and Content of an Information Security Architecture Framework
  Tom Scholtz (G00158226)

- Security Architecture: Developing the Requirements Vision
  Tom Scholtz (G00160066)

- Toolkit: Program Vision Model for Security Architecture
  Tom Scholtz (G00168698)

- Toolkit: An IAM Example of Security Architecture Development
  Greg Kreizman, et al (G00157703)