



*Security by Design*

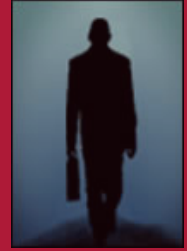
## **ENTERPRISE ARCHITECTURE'S ROLE IN COMPLIANCE**

version 1.0

**AegisSecurityWorks LLC**

### **Issue Overview:**

*Legal issues around meeting compliance objectives are driving organizations towards the use of frameworks to manage the security and regulatory process. The key frameworks for IT governance and security are – COBIT, ITIL, and ISO17799. There is a need to consolidate the ideas in the 3 frameworks and look for synergies within and across them. The majority of large-scale enterprises already have an Enterprise Architecture Management (EAM) process in place. This paper outlines a strategy to use the EAM methods as the “glue” that binds the frameworks together as well as providing strategic IT/business alignments.*



## Table of Contents

Summary.....	3
Enterprise Architecture Management.....	3
Governance Frameworks.....	4
COBIT – Control Objectives for Information and Related Technologies .....	4
ITIL – Information Technology Infrastructure Library .....	6
ISO 17799.....	8
Security Framework Overlap.....	9
EAM-Security Framework Integration .....	10
Security Policy Integration Process .....	10
Closing.....	11

## Summary

Many companies are turning to industry standard governance frameworks to fulfill compliance requirements. The primary frameworks for compliance and security are: Control Objectives for Information and related Technology (COBIT), IT Infrastructure Library (ITIL), and ISO 17799. Organizations are adopting the COBIT framework as an IT governance model precisely because of its affinity with Sarbanes-Oxley (SOX) legislation. COBIT however does not focus on IT operations or service management, this is the purview of ITIL. Lastly, what is missing from both COBIT and ITIL is the broad security coverage that is provided by ISO 17799. Clearly, one framework does not cover all the enterprise requirements and just as clearly business and IT leaders need a method to manage and rationalize each of these frameworks.

The goal of this paper is to show that a company's internal Enterprise Architecture (EA) group can use the current compliance environment to strengthen their role and relevance to the organization. EA is in the perfect position to create a comprehensive plan and methodology to organize the frameworks, tailor them to the enterprise requirements, and create a process where specific guidance can be syndicated to business and IT delivery areas. Specific guidance is required because none of the standards are prescriptive in nature; it is up to the individual organization to interpret and apply a practical approach to implementation – Enterprise Architecture can play a key role in shaping the frameworks for the company's implementation.

## Enterprise Architecture Management

It's common for most large corporations to have a department called Enterprise Architecture (EA) within their IT area. EA has numerous responsibilities, which at its core aims to provide linkages between strategic business objectives and technical plans. EA fulfills its mission in various ways, which include:

- ❑ Improving process efficiencies.
- ❑ Integrating delivery channels,
- ❑ Providing methods for a unified customer view,
- ❑ Improving integration points and minimizes overall complexities,
- ❑ Looking for reuse opportunities across the enterprise's technical and business environments.

Typically, Enterprise Architecture will develop a process called Enterprise Architecture Management (EAM). EAM is a set of processes and methods that provide guidance related to technology and its usage for the organization. The guidance will have linkages to the EA goals listed above. Enterprise Architecture direction can take the form of product/tool choices, development methods, design choices, and/or positions on topics such as security or open source usage.

While this is admittedly a very brief overview of EA and its goals, hopefully one can readily see how EA is in a unique position to assist with governance frameworks and their usage within the enterprise. EA's raison d'être is governance – EA provides

governance to the technical community thereby helping IT stay in alignment with business goals and objectives. It is the premise of this article that Enterprise Architects can and should step up to the task of integrating the various external governance frameworks into a coherent process for the companies they work for.

## Governance Frameworks

The industry standard governance frameworks that are getting the most attention due to their security and compliance requirements are COBIT, ITIL, and ISO 17799.

### **COBIT – Control Objectives for Information and Related Technologies**

COBIT is an open standard for IT governance with a supporting toolkit that is now in its 4<sup>th</sup> release. COBIT itself is based on the COSCO (Committee of Sponsoring Organizations of the Treadway Commission) standard. COBIT has its roots in the financial control/governance arena, which in the end is why it has gained in popularity as an IT governance and compliance model.

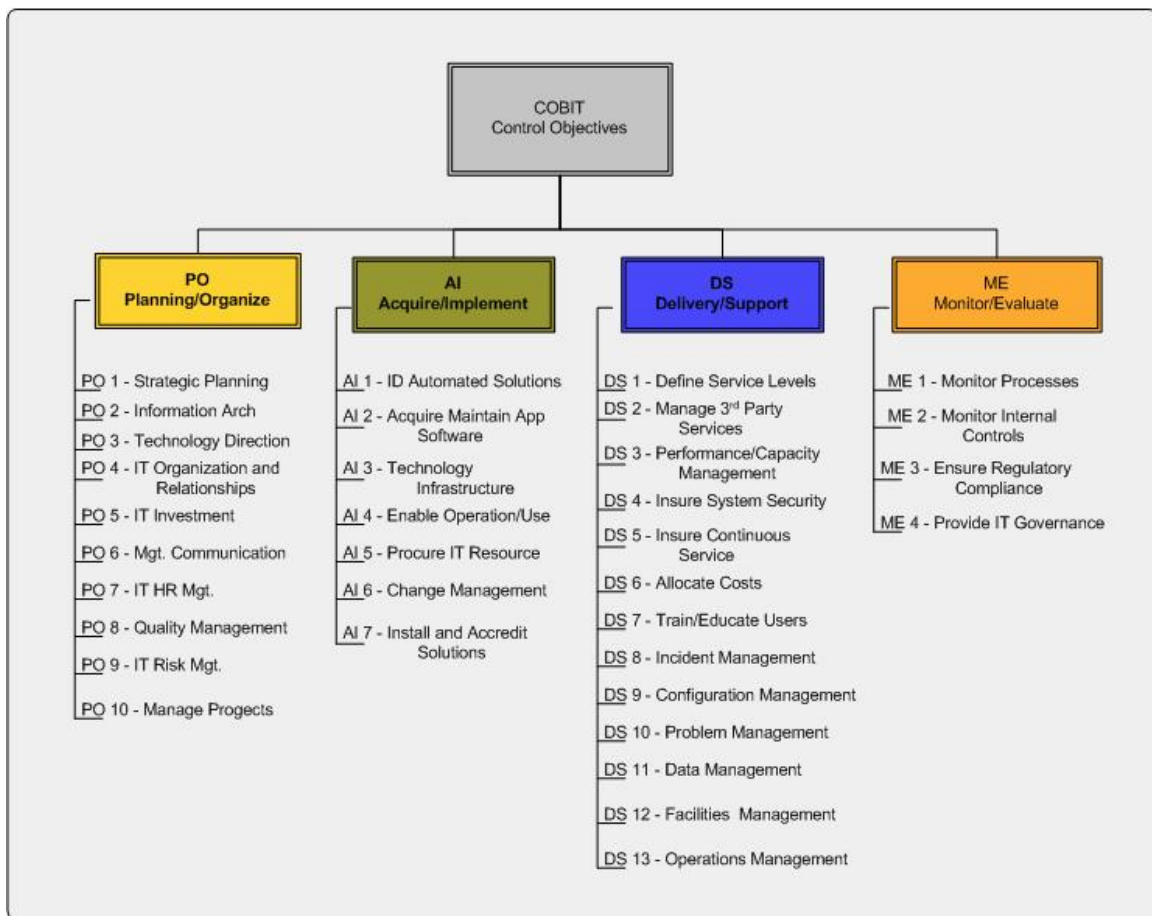
COBIT has a strong audit and control perspective, the earlier versions were usually pushed on (with much resistance from) IT by the audit department. However, COBIT has gained traction in recent years as Sarbanes-Oxley and other compliance legislation has gotten more attention.

COBIT begins by dividing the IT universe into 34 processes within 4 domains. The 4 COBIT domains are:

- ❑ *Plan/Organize (PO)*,
- ❑ *Acquire/Implement (AI)*,
- ❑ *Deliver/Support (DS)*
- ❑ *Monitor/Evaluate (ME)*.

The COBIT framework then breaks each process down, defining how it can be controlled, managed, and measured. COBIT provides a global view of information technology processes complete with RACI (Responsible, Accountable, Consulted, and Informed) charts to help clarify roles and responsibilities. Included in the most recent version of COBIT is a set of best practices and guidelines for managing and monitoring the functions within each domain. See diagram below for an outline of the COBIT 4.0 domains and processes.

COBIT 4.0 Domains and Processes



## ITIL – Information Technology Infrastructure Library

The Information Technology Infrastructure Library (ITIL) is a user customizable framework of IT best practices for infrastructure service creation, delivery, and management. The Office of Government Commerce in Norwich England created ITIL. Over the last 5 years ITIL has been gaining in popularity and adoption and is now a standard in the service delivery space.

Specifically, ITIL is a set of books that define the best practices around infrastructure (Data Center) management for service delivery to end customers – business users.

The ITIL books are:

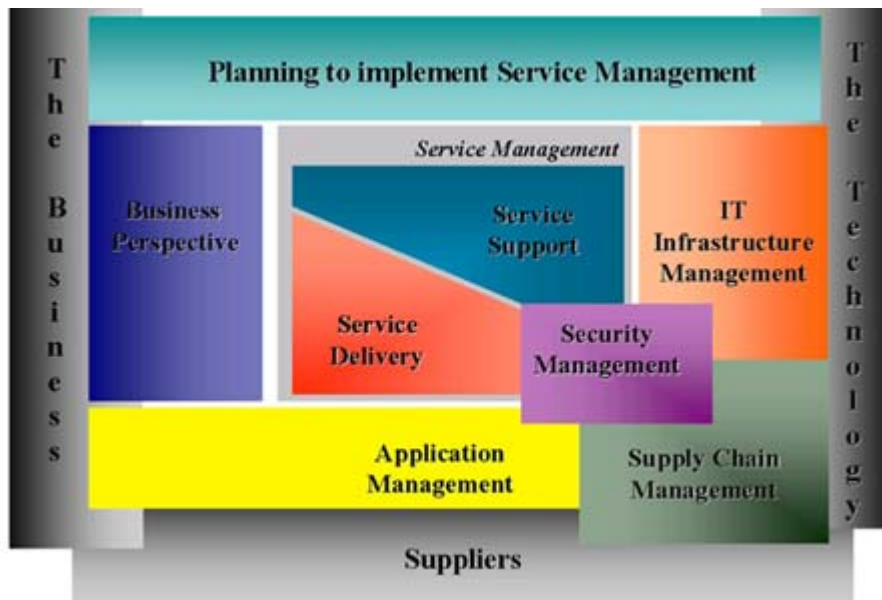
- ❑ **Service Delivery** – the services that the infrastructure unit(s) must deliver to the business units to support their current and projected needs are covered in this book.
- ❑ **Business Perspective** – the business unit's perspective is covered in this book with the desire to educate the business community on the use of ITIL and how it can fit into their plans and operations.
- ❑ **Service Support** – making sure the customers have access to those services is covered in the Service Support book.
- ❑ **Planning to Implement Service Management** – this book details the steps that are required to implement service management and ITIL.
- ❑ **IT Infrastructure Management** – This books covers the planning, building, and running of the environment with a service focus.
- ❑ **Security Management** – how are the services to be secured and CIA (Confidentiality Integrity, and Availability) assured are dealt with in this area.
- ❑ **Application Management** – how the software development lifecycle is managed is defined here.
- ❑ **Software Asset Management** – covers how software will be treated as an asset and managed through the lifecycle of introduction to retirement.

The graphic below illustrates the various ITIL components.

---

## ITIL Framework

---



Source: ITIL.com

The implementation of ITIL provides organizational benefits such as; common IT/business language for data center services, a contract around IT delivery of services, a pre-developed and globally tested framework for infrastructure management, and a basis measuring quality of service (QoS) for management purposes.

ITIL implementations that I have seen have all been partial implementations or customizations of the modules to suite the adopting enterprise. This by itself is not a bad strategy – it allows the organization to plan an iterative rollout and incorporate modules that make the most sense for them. You should not be adopting ITIL with the expectation of great cost savings, as a matter of fact the net affect would most likely be an increase in cost. However you should see an increase in the quality of service your organization is delivering across the infrastructure spectrum.

The COBIT Framework's focus is on auditing and controlling the technical environment whereas ITIL is focused on service management and delivery. ITIL and COBIT are not opposing frameworks but should be seen as complementary in nature.

## ISO 17799

ISO17799 provides a set of recommendations for security practitioners, IT leaders, and business staff members for the implementation and maintenance of security standards within the organization. ISO 17799 provides a framework or starting point for security like the other frameworks discussed here it can be extended or adopted in pieces.

The ISO 17799 document is organized into 10 sections with the lowest level of detail being a list of *controls* listed within each of the sections. ISO 17799 instructs the practitioner to select controls from each section to reduce risk to appropriate levels for the organization. The document provides examples as to how an organization may go about managing its risk and encourages the practitioner to perform a risk analysis to understand security requirements before controls are decided upon.

The 10 sections of the ISO 17799 document are defined below:

- ❑ **Security Policy** – this section is devoted to providing management with clear policy objects with respect to information security.
- ❑ **Organizational Security** – This section covers information security infrastructure, third party access, and outsourcing of technical operations. The objective here is to develop a method to communicate and foster cooperation and team work between individuals and departments within/across the enterprise including outside business partners.
- ❑ **Information Asset Classification** – data classification schemes are recommended within this section. The goal is to provide staff with a short hand method to understand how a particular piece of information should be handled and controlled.
- ❑ **Personnel Security** - this section of ISO 17799 defines staff security controls that should be maintained in the organization. These controls include employee and staff screening methods, confidentiality agreements, training methods, security violation reporting and responsibility process.
- ❑ **Physical Security** – the controls described here protect staff and property from a breach in physical security, “acts of god” as well as deliberate violations are described. Controls such as clean desk/clean screen policy, maintenance of property, physical control of assets on and off site are discussed.
- ❑ **Communication and Operational Controls** – Operational duties, procedures, change control methods are defined in this section. Securities of data at rest and in transit including retention policies are discussed.
- ❑ **Access Controls** – Rules, regulations, and responsibilities concerning data access and acceptable methods for information access are enumerated.
- ❑ **Systems Development** – this is a very broad category within ISO 17799 that outlines the security requirements around system development including cryptography, key management, risk analysis, security requirements gathering, and change management. Interestingly, the software development Life Cycle (SDLC) is not mentioned within this section. Many of the controls defined here would be covered within the SDLC.



- ❑ **Business Continuity Planning** – Methods for creating, testing, and refreshing the business continuity plan are discussed.
- ❑ **Compliance** – This section deals with the understanding compliance requirements and the development of methods to remain in regulatory compliance.



## Security Framework Overlap

If we were to take the 4 COBIT Domains – Plan/Organize, Acquire/Implement, Delivery/Support, and Monitor/Evaluate – and compare how ITIL and ISO 17799 cover each domain we can begin to see the overlap between frameworks, see diagram below.

*Framework Overlap Diagram*

		---- COBIT Process Number ----												
COBIT Domain		1	2	3	4	5	6	7	8	9	10	11	12	13
Plan/Organize 10 Processes			✓	✓	✓	✓	✓	✓	✓	✓	✓			
Acquire/Implement 7 Processes		✓	✓	✓	✓	✓	✓							
Delivery/Support 13 Processes		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Monitor/Evaluate 4 Processes		✓	✓											

 = Covered by ISO 17799      = Covered by ITIL

 No process for given domain.      Not covered by ITIL or ISO.

## EAM-Security Framework Integration

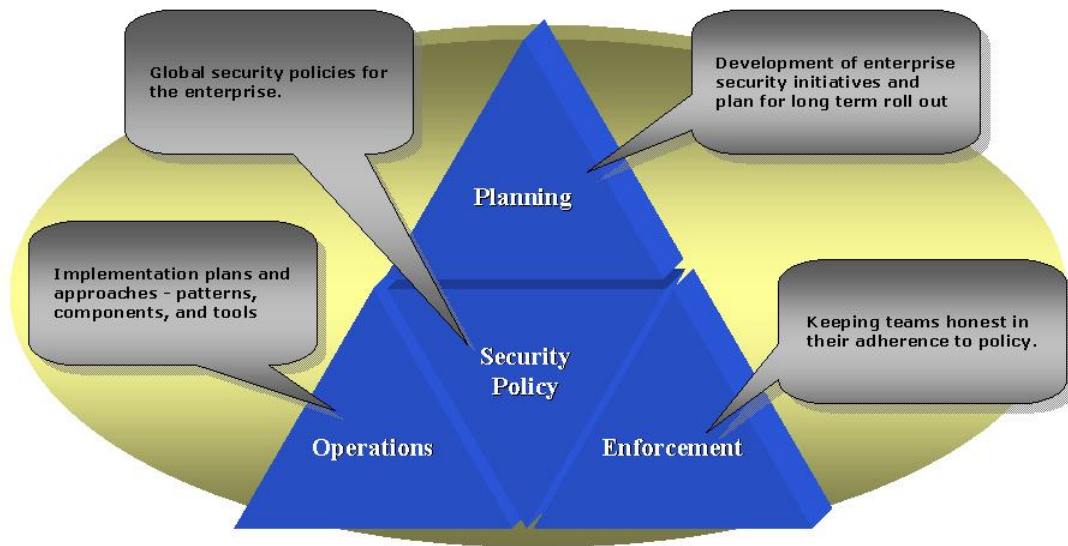
Understanding the individual frameworks, how each framework overlaps and complements one another has been a key ingredient to our clients' framework integration plan.

The Enterprise Architecture (EA) group with its mandate for strategic technology and business process integration across a time span that are longer than an individual project can be key to the framework introduction and usage practice. EA should have architecture management processes in place and should be looking for ways to incorporate ISO 17799 and ITIL components into the enterprise; this can be done by developing a policy management integration plan such as the one described below.

---

### *Policy Management Integration*

---



### Security Policy Integration Process

The process of integrating a company's EAM plans with the security frameworks starts with the development of security policies. The organization's security policies are foundational to the integration of security frameworks. Without sufficient policy definition security framework integration/adoption will be haphazard at best.

The other three support functions can then be put into place.

- ❑ **Planning** – determining the long term vision and how best stage the implementation of that vision
- ❑ **Operations** – the implementation and monitoring of the planned activity
- ❑ **Enforcement** – how to enforce the policies that have been put into place

Within this integration structure you should first look at the items listed below

- ❑ **Leverage the existing** – If you have already adopted one framework leverage that work to show linkages back to the other where they have overlaps. If the framework you have adopted is lacking where the other is strong the course of action is obvious. If you already have design reviews make sure to include the new framework requirements into the existing corporate control points for example.
- ❑ **Document the process** – As we have seen, ISO 17799 and ITIL don't tell you exactly how to accomplish the defined tasks these standards document *what* needs to be done. The EA group should document *how* the standard(s) will be implemented. The processes will vary depending on the size and maturity of the organization.
- ❑ **Governance model** – A typical organization would already have a governance model in place and the new procedures and policies would need to be added to this process.
- ❑ **Look for redundancies** – eliminate redundancies within your processes as the new frameworks are instituted. It is very common for individuals to layer new processes over existing and creating redundant and in some cases policies and procedures may even conflict with each other.
- ❑ **Develop communication plan** – A communication and training plan will be necessary as these frameworks and their corresponding policies and procedures are rolled out. Plan a to have early and often communication sessions with employees including training sessions.

## Closing

A company's Enterprise Architecture department is in a unique position to manage the roll out and integration of industry standard security frameworks. Understanding the company's current processes along with the standard security frameworks will assist in this effort. EA will enhance its value to the organization while working to insure the security of the enterprise's critical assets.