

# 5<sup>th</sup> SOA CoP

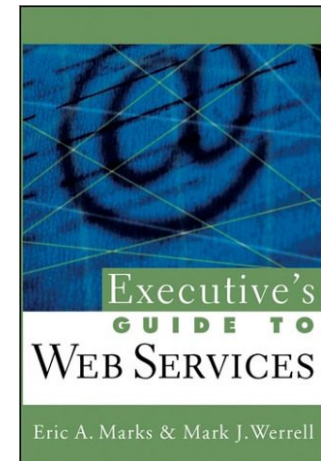
## Next Generation SOA Governance

*May 1, 2008*



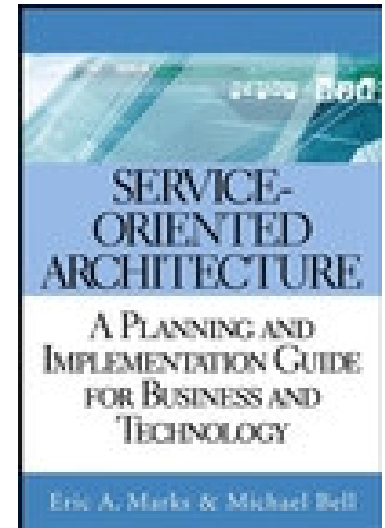
**AgilePath Corporation**  
38 Merrimac St.  
Newburyport, MA 01950

[www.agile-path.com](http://www.agile-path.com)



# What is SOA Governance?

- ***“SOA Governance refers to the organization, processes, policies, and metrics required to manage a SOA successfully.”***
- ***“...A SOA Governance model establishes the operating rules and guidelines of the organization and the SOA stakeholders, from architects and developers to service consumers and providers, and even applications and services themselves.”***
- ***These behavioral rules and guidelines are established via a body of defined SOA policies.***



New Definition from “**SOA Governance: Evolving Governance for the Services Driven Enterprise**” (2008, Wiley)

- SOA governance is the definition, implementation and ongoing execution of a **SOA stakeholder model and accountability framework** that **ensures an organization is pursuing an appropriate SOA strategy aligned with IT and business goals**, and is executing that strategy in accordance with guidelines and constraints defined by a body of SOA principles and policies.
- **SOA policies are enforced through various policy enforcement mechanisms such as governance boards and committees, governance processes, checkpoints and reviews, and governance enabling technology and tools.**

# Elements of a Complete Governance Model

- 1. Governance Strategy, Scope and Goals**
- 2. Governance Stakeholder Model**
- 3. Governance Goals, Principles and Policies**
- 4. Policy Enforcement and Provisioning Model**
- 5. Governance Enforcement Mechanisms**
  - a) Organizations and Boards**
  - b) Governance Processes, Events and Triggers**
  - c) Governance Enabling Technology and Tools**
- 6. Exception, Waiver, Escalation and Appeals Process**
- 7. Governance Metrics and Behavioral Model**
- 8. Governance Communications Model**
- 9. SOA Governance Feedback and Management Reviews**
- 10. Governance Performance Management and Sustainment**

# Next Generation Governance Challenges

- **Lack of industry standards for policies and policy enforcement**
  - Unified Policy Model
- **Naiveté vis-à-vis the structure of a “complete governance model” and the role of boards, tools and processes**
  - Integrated Policy Enforcement Model
- **Lack of integration of governance enabling technology and tools**
  - Policy provisioning from an enterprise policy model into enforcement by boards, processes and tools

# Unified Policy Model

- Unified view of policies from enterprise, compliance and business policies to EA policies, technical policies, and QoS policies
- Vertical integration and decomposition of policies, e.g . Security, business, and compliance into enforceable policies by boards and governance tools
- Horizontal integration of policies from design to QA/Testing to runtime

# Developing a Unified Model for Enterprise IT/SOA Policies

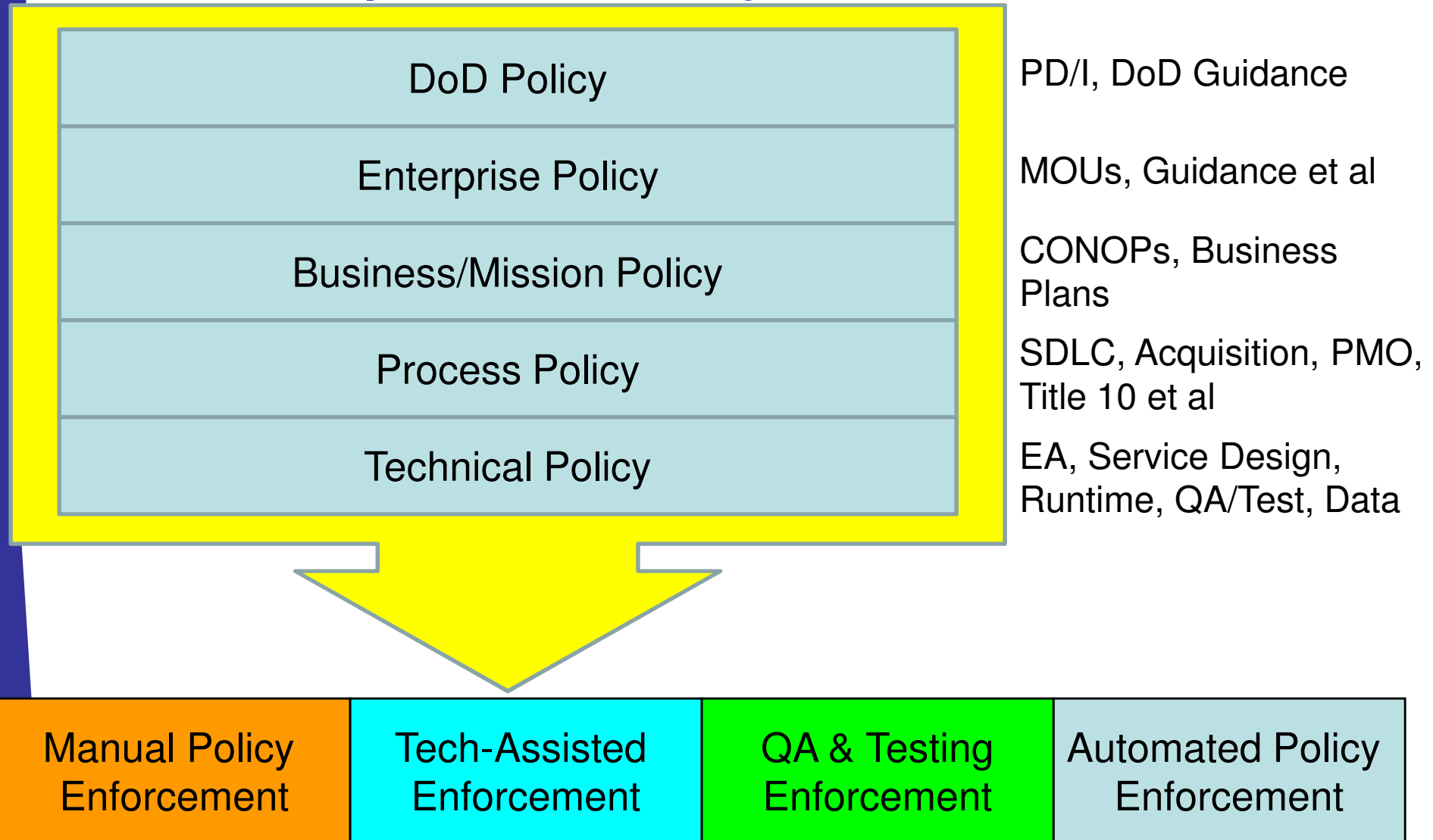
- IT/SOA “Policy” is a charged and misunderstood topic (almost as misunderstood as “Governance”)
- AgilePath has been working to unify the concept of enterprise/SOA “policies” vertically and horizontally in federated enterprises
- Vertical Policy Integration: compliance, business, process decomposed into technical policies
- Horizontal Policy Integration: alignment and integration of design time, QA/testing, and runtime policies
- Achieve **Integrated Governance, Policy Management and Enforcement** leveraging manual, collaborative and automated policy enforcement mechanisms

# Governance Unified Policy Model

Policy Enforcement Mechanism	SOA Policy Category	Multi-Level Policies
Governance Organizational Model & Boards	Compliance Policies Business Policies Process Policies	Security Policies Reuse Policies
Governance Boards and Governance Processes	Architecture Policies Technical Policies Design Policies	Reuse Policies Security Policies
Governance Enabling Technology and Tools	Design Policies QA/Test Runtime Policies	Security Policies



# Scope of Policy Unification



# Enterprise Policies Can be Decomposed into Technical Policies

Policy Definition,  
Management & Enforcement



Manual Policy  
Enforcement



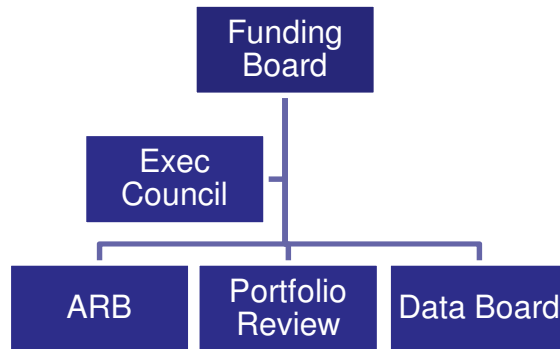
Automated  
Technical Policy  
Enforcement

- Company XYZ Security Policy will be followed for all enterprise Services
- Enforced during PMO reviews and lifecycle reviews
- Exceptions and waivers to SOA Executive Council
- WS-Security will be used
- SAML assertions/X.509 Certificate
- SSN will always be encrypted

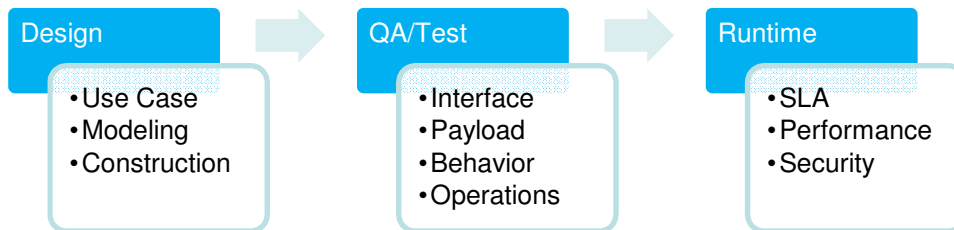
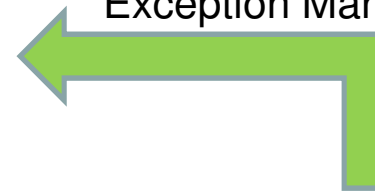
# Integrated Policy Enforcement Model

- Enforcing policies is not solely a governance technology problem
- Policies are enforced via an integrated fabric of boards, processes and governance enabling technology
- Integrating governance boards, governance processes and governance tools as a “fabric” of policy enforcement ensures complete policy coverage

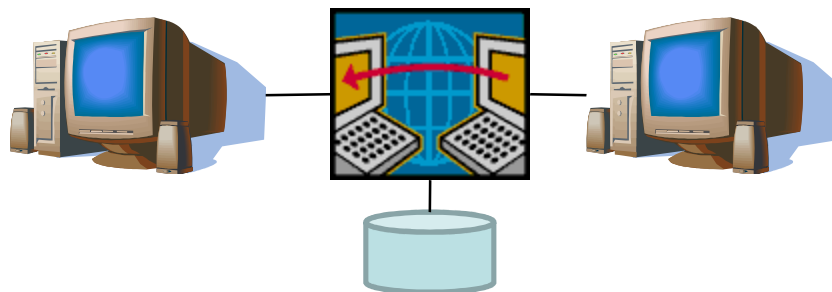
# Policy Enforcement



Manual Policy Enforcement and Exception Management



Manual Policy Enforcement (Design time)



Automated Policy Enforcement (QA/Test and Runtime)



# SOA Policy Enforcement Models

SOA Governance Policy Definition, Management  
& Enforcement (Policy Mgt. Model)



Policy Enforcement Model (PEM)



Manual Policy  
Enforcement  
(Boards)

- Governance boards
- Governance processes
- Governance reviews
- Manual enforcement processes
- Policy statements and guidelines

Tech-Assisted  
Enforcement  
(Processes)

- Collaboration tools
- Virtual board meetings
- Process automation and workflow
- Governance portals, dashboards and communication tools
- Community governance processes with collaboration tools

Automated Policy  
Enforcement  
(Technology)

- Web services Mgt platforms
- Service registries
- Security appliances and infrastructure
- Reliable messaging and intermediaries
- Policy engines
- Network infrastructure

13

# SOA Policy Enforcement Scenarios

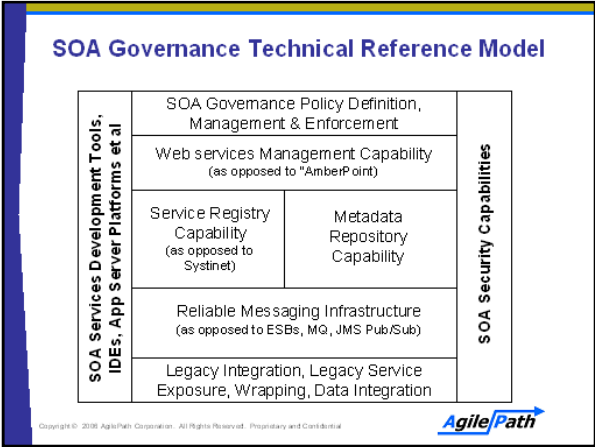
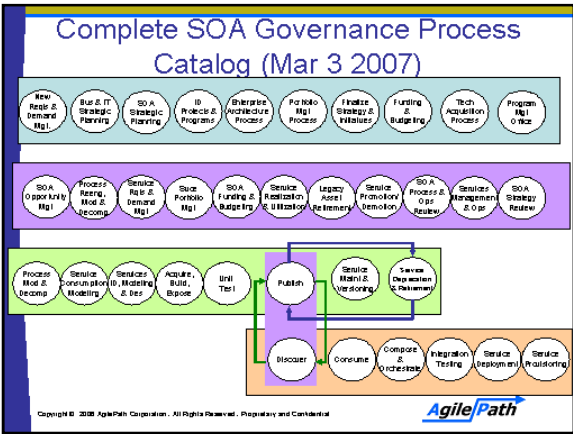
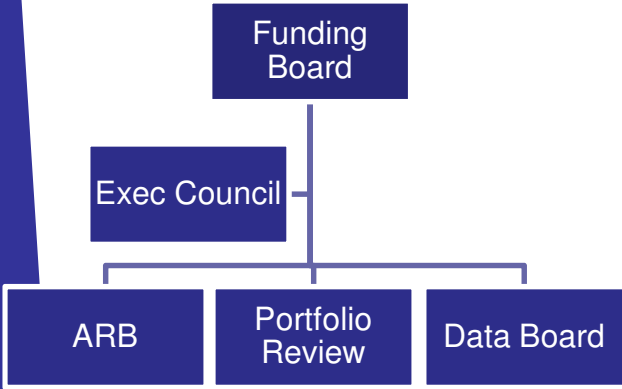
Policy Definition,  
Management & Enforcement



Manual Policy Enforcement

Process-Based Policy Enforcement

Automated Policy Enforcement



# SOA Policy Enforcement Scenarios

SOA Governance Policy Definition,  
Management & Enforcement



## Manual Policy Enforcement

- Governance boards
- Governance processes
- Governance reviews
- Manual enforcement processes
- Policy statements and guidelines

## QA & Testing Enforcement

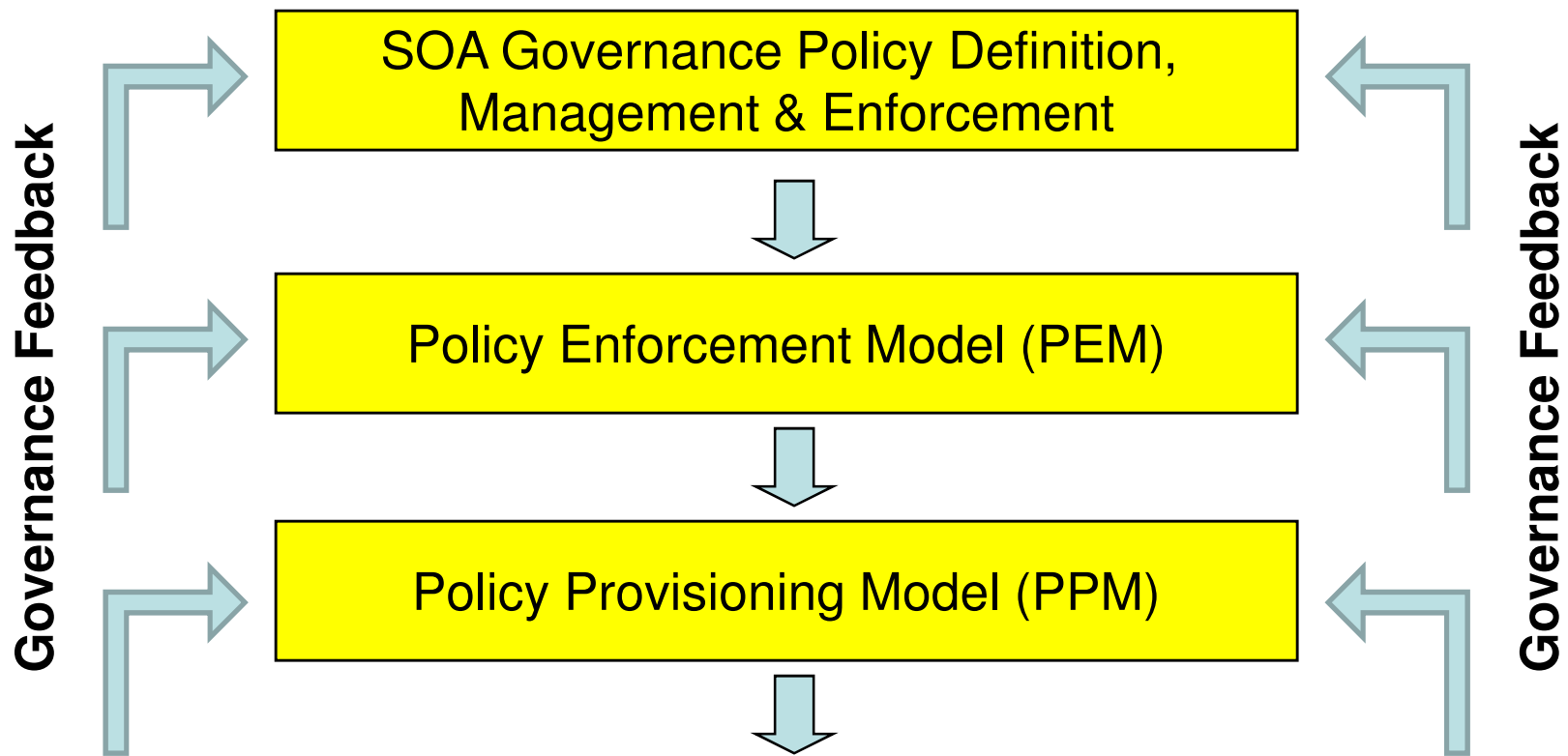
- Continuous QA and testing solutions
- Service interfaces, payloads and message integrity
- SLA and contract conformance and assurance
- Service performance under load
- Etc.

## Automated Policy Enforcement

- Web services Mgt platforms
- Service registries
- Security appliances and infrastructure
- Reliable messaging and intermediaries
- Policy engines
- Network infrastructure

15

# SOA Policy Provisioning Model



Manual Policy Enforcement

Process-Based Policy Enforcement

QA & Testing Enforcement

Automated Policy Enforcement



# Lack of integration of governance enabling technology and tools

- Once governance tool requirements are identified and tools are selected, integrating them is one thing; integrating and enforcing policies across them is another
- Multiple classes of governance tools and technologies
  - Repositories and Registries
  - Runtime tools, e.g. security appliances, ESBs, WSM et al
  - Quality assurance and testing tools
- Multiple processes , e.g. portfolio management, service lifecycle management, SDLC governance

# Policy Standards Gaps and Challenges

- WS-Policy is not enough
- Proprietary schemes are insufficient
- Vendor consortia and ad hoc standards won't get the job done, e.g. GIF, SOA Link et al
- All approach policy from a technical perspective, not a business or enterprise perspective
- ***Need a unified policy model and integration standards for business, compliance, process and technical policies provisioned to all possible policy enforcement mechanisms***

# Exploring Next Generation Policy Enforcement Scenarios: Quality Assurance and Testing

## SOA Governance Policy Definition, Management & Enforcement

### Manual Policy Enforcement

- Governance boards
- Governance processes
- Governance reviews
- Manual enforcement processes
- Policy statements and guidelines

### QA & Testing Enforcement

- Continuous QA and testing solutions
- Service interfaces, payloads and message integrity
- SLA and contract conformance and assurance
- Service performance under load
- Etc.

### Automated Policy Enforcement

- Web services Mgt platforms
- Service registries
- Security appliances and infrastructure
- Reliable messaging and intermediaries
- Policy engines
- Network infrastructure

# Exploring Next Generation Policy Enforcement Scenario: Runtime Security Policy Enforcement

SOA Governance Policy Definition,  
Management & Enforcement



## Manual Policy Enforcement

- Governance boards
- Governance processes
- Governance reviews
- Manual enforcement processes
- Policy statements and guidelines

## QA & Testing Enforcement

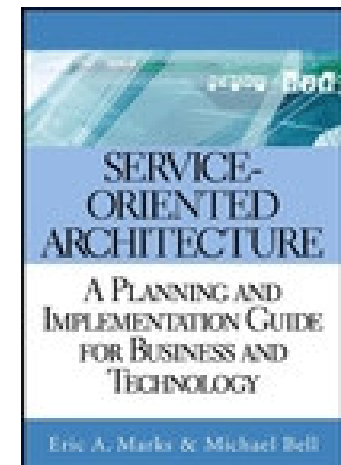
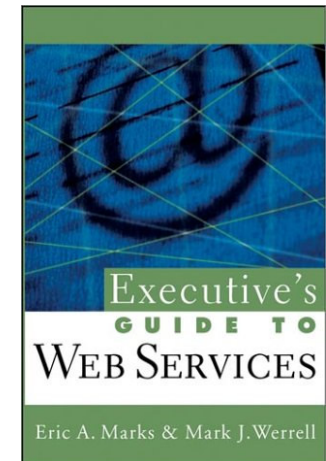
- Continuous QA and testing solutions
- Service interfaces, payloads and message integrity
- SLA and contract conformance and assurance
- Service performance under load
- Etc.

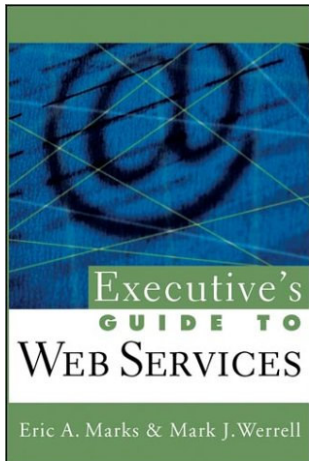
## Automated Policy Enforcement

- Web services Mgt platforms
- Service registries
- Security appliances and infrastructure
- Reliable messaging and intermediaries
- Policy engines
- Network infrastructure

# AgilePath Corporation Facts

- Founded and incorporated 2003
- Headquarters: Newburyport, MA
- President, CEO and Founder: Eric A. Marks, Co-Author of “Executive’s Guide to Web Services” (2003)
- Co-Author of SOA: A Planning and Implementation Guide for Business and Technology, (Marks and Bell, 2006)
- **Coming in April 2008: “SOA Governance : Evolving Governance in the Services-Driven Enterprise”**
- Privately Held
- Web Site: [www.agile-path.com](http://www.agile-path.com)





# Thank You!

**Eric A. Marks**  
**AgilePath Corp.**  
[emarks@agile-path.com](mailto:emarks@agile-path.com)  
[www.agile-path.com](http://www.agile-path.com)

