



You Can't Buy Governance

Anne Thomas Manes

Vice President & Research Director

Application Platform Strategies

amanes@burtongroup.com

InfoWorld SOA Executive Forum
8 November 2007





You Can't Buy Governance

Thesis

- Governance is a human-oriented program
 - It helps people do things "right"
- Governance infrastructure supports the program
 - But tools, by themselves, won't give you governance
- Governance must be part of the normal process
 - Integrated with SDLC and IT management systems
- Governance must address the entire service lifecycle
 - Project selection through end of life
- Governance should be helpful and automatic
 - Make the right way the path of least resistance



You Can't Buy Governance

Agenda

- Fundamentals of a governance program
- Requirements of a SOA governance program
- Using technology to facilitate governance
- Recommendations



You Can't Buy Governance

Agenda

- Fundamentals of a governance program
- Requirements of a SOA governance program
- Using technology to facilitate governance
- Recommendations



What is governance?

- A risk mitigation strategy
 - A program to ensure that people do what's "right"
 - In compliance with laws, regulations, and best practices
- The need for governance is proportionate to risk
 - How easy/difficult is it to execute correctly?
 - What is the cost of failure or non-compliance?
- SOA is a very risky endeavor
 - Unfamiliar territory with disruptive cultural changes
 - Poor execution leads to increased complexity
 - Systems become more brittle and less flexible than before

Quality of execution is a reflection of governance

- Symptoms of poor execution
 - No planning and coordination of service projects
 - Single-use services and point-to-point connections
 - Proliferation of redundant services and data types
 - No metrics for measuring success
 - Inconsistent implementation of non-functional capabilities (security, reliability, transactions, logging, auditing, routing, filtering, etc)
 - Runtime service-level issues related to performance, scalability, reliability, availability, etc
 - Inability to isolate problems
 - Change management issues
 - Increased complexity



Quality of execution is a reflection of governance

- Symptoms of good execution
 - Well scoped projects that deliver recognizable business benefits
 - Sharing and reuse of services and data types
 - Reduction in redundant systems and point-to-point connections
 - Secure, reliable, available, performant systems
 - Ability to recognize and resolve issues before they become incidents
 - Well-coordinated management of service consumers, enabling consistent service-level delivery and well-transitioned enhancements and upgrades



What is a governance program?

- Policies
- Processes
- Metrics
- Organization



Policies define what's "right"

- Policies must address all stages in the service lifecycle
 - Project selection
 - Requirements
 - Design
 - Development
 - Deployment
 - Utilization
 - Operations
 - Enhancements
- Who gets to make these decisions?
 - Are they guidelines or law?
 - What's the waiver procedure?

Processes enforce policies

- Activities that provide an opportunity to test for compliance and make a go/no-go decision
 - SOA governance process should integrate with traditional SDLC and IT management processes
- Manual, human-driven processes
 - Design and code reviews, approval processes, etc
- Automatic processes
 - SDLC activities (code check-in, builds, tests, etc)
 - Runtime systems (dependency detection, runtime enforcement)



Metrics provide visibility into the governance process

- Required to ascertain compliance
- Keep watch on violations and waivers
- Also provide insight into and indications of
 - Trends
 - Process efficiency
 - Onerous or inappropriate policies and processes



Organizational culture must support the governance program

- Empowered governance police
- Formalized SDLC and IT management processes
- Consistent assessment and enforcement points
- Rewards for good behavior
- Punishments for bad behavior



You Can't Buy Governance

13

Agenda

- Fundamentals of a governance program
- Requirements of a SOA governance program
- Using technology to facilitate governance
- Recommendations



Scope: Governance applies to all stages in the services lifecycle

- Project selection
- Requirements management
- Service design and development practices
- Testing practices
- Configuration management
- Release management
- Contract management
- Service monitoring and control
- SLA management
- Runtime policy enforcement
- Incident management
- Change management



SOA Governance Requirements

Support, enable, and encourage

- Architectural best practices
- Technology and product selection guidelines
- Development best practices
- Quality management best practices
- Management of consumer/provider relationships
- Runtime policy enforcement
- Visibility into runtime operations



Architectural best practices

- Project identification and selection
- Identification of key stakeholders
- Requirements capture and management
- Types of services (application, data, composite, infrastructure)
- Standards, models, and patterns
- Application, service, data, and schema rationalization



SOA Governance Requirements

17

Technology and product selection guidelines

- Preferred technologies
- Technology selection guidelines
- Preferred products
- Product selection guidelines



Development best practices

- Standards and profile compliance
- Naming conventions
- Interface definition rules and recommendations
- Schema definition rules and recommendations
- Testing requirements
- Peer review requirements
- Techniques for supporting security, reliability, and transaction integrity requirements
- Reporting and visibility



Security drill-down

- How do you assess the risk associated with a particular service?
- What security precautions must be implemented to mitigate those risks?
- What's the maximum overhead that the security precautions can impose?
- What tools and technologies should be used to implement the security precautions?
- Who is responsible for implementing the security precautions?
- Who is responsible for ensuring that the security precautions have been implemented properly?
- What documentation must be generated for auditing compliance with security policies?



Quality management best practices

- Policy compliance testing
- Functional and non-functional testing
- Code coverage
- Interoperability and dependency testing
- Reporting and visibility

Managing consumer/provider relationships

- Service discovery and selection
 - Assumes proper service classification
- Negotiating utilization contracts
 - Usage plans
 - Service level agreements
 - Support agreements
 - Incident management
 - Enhancement agreements
 - Remuneration agreements
- Codification of runtime policies



Enforcing runtime policies

- Enabling information exchange among runtime systems
- Configuration of runtime policies and policy enforcement points

Visibility into runtime systems

- Instrumentation of runtime systems
- Anomaly detection
- Root cause analysis
- Incident creation and management



You Can't Buy Governance

23

Agenda

- Fundamentals of a governance program
- Requirements of a SOA governance program
- Using technology to facilitate governance
- Recommendations

SOA governance infrastructure (SGI) products

- Facilitate a governance program
 - Manage governance information
 - Service artifacts, metadata, and policies
 - Facilitate or automate processes
 - Enforce policies
 - Collect metrics
- Leading governance infrastructure products
 - Registries, repositories, and software asset management systems
 - Runtime management and mediation systems



Facilitating Governance

Using a reference architecture to design an infrastructure

- Define requirements
- Identify functional capabilities required
- Map alternatives to functional capabilities
- Design an infrastructure that implements required functional capabilities

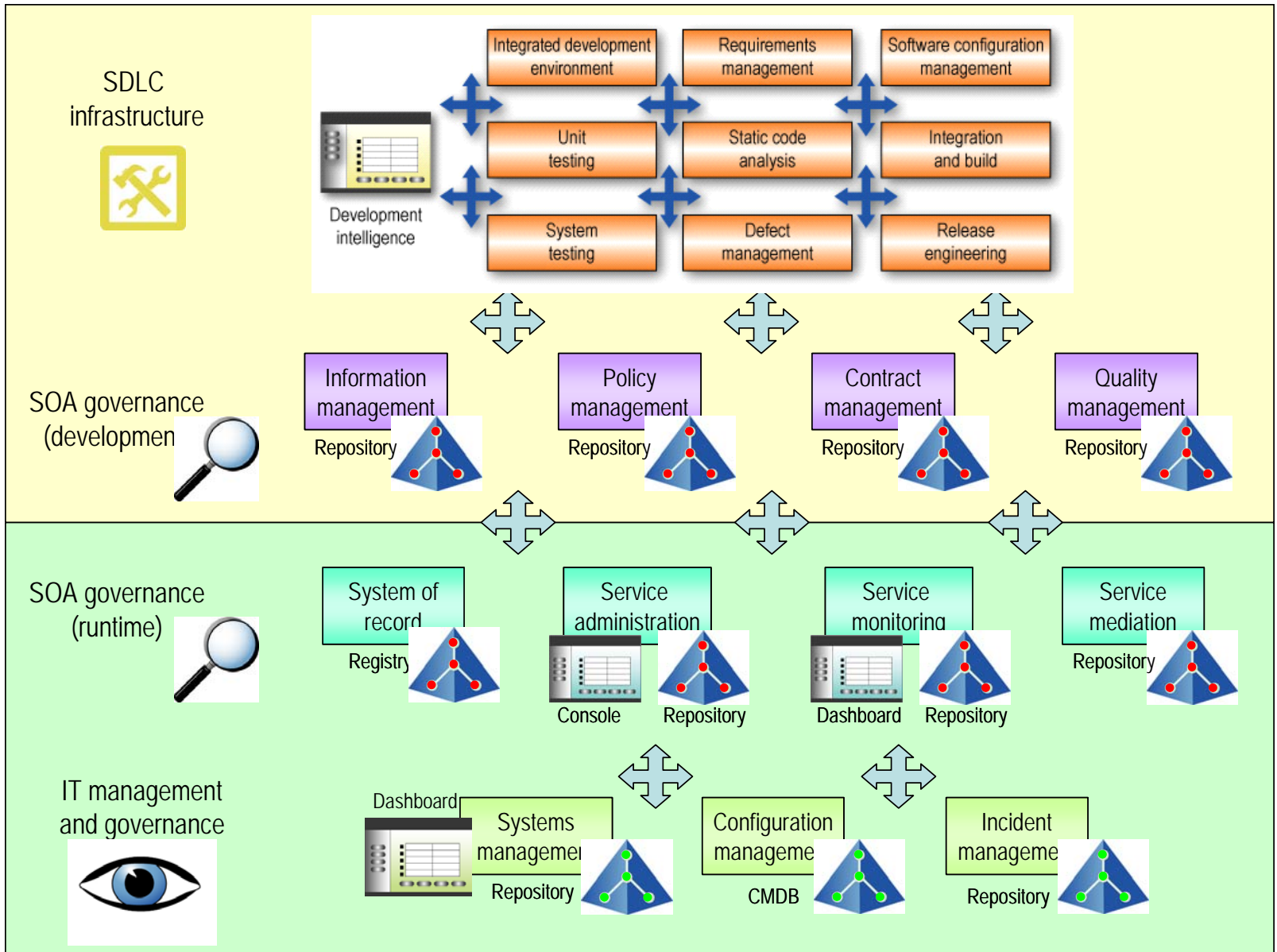


Required functional capabilities

- Enable sharing of services and service artifacts
- Manage the lifecycle of services and artifacts
- Manage quality of services and artifacts
- Define and manage policies
- Associate policies with services and artifacts
- Ensure policy compliance
- Manage contracts between consumers and providers
- Administer and configure services and their policies
- Ensure automatic enforcement of runtime policies
- Monitor runtime systems
- Integrate SOA governance with traditional SDLC and IT management processes
- Gather metrics and enable reporting



SGI Functional Model



Development-time functional infrastructure components

- Information management
 - Enable sharing, support lifecycle management, support discovery
- Policy management
 - Policy definition, attachment, and enforcement
- Contract management
 - Contract definition, negotiation, and codification
- Quality management
 - Testing of new and enhanced services and artifacts

Runtime governance functional components

- System of record
 - Enable information exchange among runtime components
- Service administration systems
 - Administer and configure services and runtime components
 - Reconfigure the environment in response to anomalies
- Service monitoring systems
 - Collect runtime metrics
 - Provide visibility into the environment via dashboards
- Service mediation systems
 - Intercept in-flight messages and enforce runtime policies
 - Security, reliability, transactions, auditing, etc

Alternatives

- Development time
 - Home-grown solutions
 - Registry/repository
 - Policy management systems
 - Quality management systems
- Runtime
 - SOA management systems
 - XML gateways
 - ESBs



Facilitating Governance

Capability/Product Matrix

	Registry	Repository	Policy Mgmt	Quality Mgmt	SOA Mgmt	XML gateway	ESB
Information Mgmt		3					
Policy Mgmt		varies	3		varies	varies	
Contract Mgmt		varies			varies		
Quality Mgmt				3			
System of Record	3						
Service Admin					3		
Service Monitoring					3	1	
Service Mediation					2	2	2



Facilitating Governance

Home-grown solutions

- Pen and paper
- File systems
- Collaboration systems
- Custom-built governance solutions

Registry/Repository

- Different capabilities – often conflated
- Registry
 - Runtime system of record
 - Standards-compliance (UDDI) enables information exchange
- Repository
 - Information management
 - Lifecycle management
 - Policy management (maybe)
 - Contract management (maybe)
- Leading vendors
 - BEA ALER, HP Systinet, IBM WSRR, Software AG Infravio
 - LogicLibrary, SOA Software Workbench



Policy management systems

- Pure-play policy management
 - Define, manage, and codify policies
 - Attach policies to artifacts
 - Automate compliance testing
 - Integrate with SDLC and runtime systems
- Only one vendor:
 - WebLayers

Quality management systems

- Testing and diagnostic tools for SOA systems
 - Functional, regression, load, stress, performance, security, and interoperability testing
- Built-in IDE testing features
 - Limited quality management capabilities
- Specialized SOA quality systems
 - Amberpoint, Borland, Crosscheck, Empirix, HP/Mercury, IBM, iTKO, Mindreef, Parasoft, Solstice

SOA management systems

- Supported functional components
 - Service administration
 - Service monitoring
 - Service mediation
 - Policy management (sometimes/limited)
- Leading vendors:
 - AmberPoint
 - BEA ALSM
 - Progress Actional
 - SOA Software
 - Software AG Infravio X-Broker
 - Tibco ActiveMatrix Policy Manager



XML gateways

- Supported functional components
 - Service mediation
 - Policy management (sometimes/limited)
- Leading vendors
 - Cisco
 - Forum Systems
 - IBM
 - Layer 7
 - Vordel

ESBs

- Supported functional components
 - Service mediation (limited support for policy-driven mediation)
- Leading vendors
 - BEA, IBM, Microsoft, Oracle, Progress, SAP, Software AG, Tibco
 - Cape Clear, Fiorano, IONA, iWay, Rogue Wave, Sun, Vitria
- Open Source
 - Apache ServiceMix, Apache Synapse, Fuse, JBoss, Mule, WSO2



You Can't Buy Governance

39

Agenda

- Fundamentals of a governance program
- Requirements of a SOA governance program
- Using technology to facilitate governance
- Recommendations



Recommendations

Develop a SOA governance plan

- Obviously it won't happen overnight
- Assemble a cross-functional team
- Assess your current SDLC & IT governance programs
- Identify opportunities to add new policies and processes to current program
- Develop a plan to implement additional governance efforts
- Plan funding for governance infrastructure

Develop SOA policies

- Address all aspects of the service lifecycle
 - Project selection, requirements, design, development, testing, configuration, consumption, operations, versioning, retirement
- Establish priorities for what must be tackled first
- Corporate culture will influence decisions



Helpful hints

- Policies must be flexible
 - Define a waiver process up front
- Document the reasoning for each policy
- Be prepared to reassess and change policies over time

- A policy management system can be invaluable

Make processes painless

- Governance processes should be as automatic and painless as possible
 - Make the right way the path of least resistance
- E.g., Automatic governance processes:
 - Compliance checking during code check-in, builds, unit tests
 - Configuration of new services for security and mgmt
 - Propagation of runtime policies to policy enforcement points
 - Compliance checking of in-flight messages
 - Detection of dependencies and relationships
- Integration with tooling makes it simpler for developers to identify and fix compliance issues



Conclusion

- SOA is a high-risk endeavor
 - Huge potential benefits
 - But many initiatives will be derailed by culture and politics
- Success will require strong governance
- SOA governance products won't give you strong governance by themselves
- Governance depends on people, policies, and processes
 - SGI facilitates the program