SOA Health, Governance and Security

Ross Moodley
SOA Leader
IBM Global Business Services
Australia/New Zealand

Vinod Ralh
SOA Architecture Leader
IBM Software Group
Australia/New Zealand

SOA in Action
Get smart about SOA.

© 2009 IBM Corporation
IBM has harvested best practices from our vast number of global and local SOA projects

*Lessons learned help IBM understand clients’ SOA health*

Cross-IBM global deep dive analysis of 200 SOA deployment experiences:
- 750 Lessons Learned
- 650 Best Practices

*Regardless of Where You Are in the SOA Continuum*

Experience based on 5700 customers across Smart SOA*
The IBM Academy of Technology identified 5 best practices for successful SOA deployments:

1. **Develop an architecture with a vision for the future**

2. **Foresee linkages from IT to your business processes**

3. **Create an organisational culture and skills to support SOA**

4. **Build a scalable infrastructure**

5. **Enable operational visibility through governance and service management**

© 2009 IBM Corporation
SOA Maturity Assessment is driven by the **Service Integration Maturity Model (SIMM)**

- Caters to the whole spectrum of integration maturity from business to IT
- There are clearly defined attributes for each level of maturity to assess an organisation’s maturity level along the seven dimensions of an enterprise IT.
- SIMM addresses the people, process and technology aspects of an organisation’s maturity to transform into a service oriented enterprise.
Application and Services fitness for SOA

Healthy Attributes

- Optimise leverage of existing assets
- Build services with reuse in mind
- Specify services based on cross-LOB needs
- Services are being reused effectively
- Governance processes instituted
- Common service registries and repositories
- Common service security administration
- Secure Information Exchange
- Identities propagated and managed
- Transaction audit logging established and enabled
After your first SOA project you should…

<table>
<thead>
<tr>
<th>Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Align business with technology investment</strong></td>
<td>Look at SOA scenarios &amp; disciplines to address NFR’s of SOA platform.</td>
</tr>
<tr>
<td>Initial SOA projects often focus business requirements.</td>
<td>Ensure that incremental business function and IT investment is aligned.</td>
</tr>
<tr>
<td>Entry points are often people, process, information, reuse and connectivity.</td>
<td></td>
</tr>
<tr>
<td>Often minimum platform investment.</td>
<td></td>
</tr>
<tr>
<td><strong>Build governance roadmap based on reference architectures</strong></td>
<td>Assess your SOA governance maturity.</td>
</tr>
<tr>
<td>Initial SOA projects often do not look at SOA governance.</td>
<td>Use SOA governance reference model priritise SOA governance activity.</td>
</tr>
<tr>
<td><strong>Build security roadmap based on reference architectures</strong></td>
<td>Assess your SOA security maturity</td>
</tr>
<tr>
<td>Initial SOA projects often do not look at SOA security.</td>
<td>Use SOA security reference model to prioritise security activity.</td>
</tr>
<tr>
<td><strong>Use SOA health check to determine next steps</strong></td>
<td>Use SOA Health Check to understand as-is and to-be across SOA scenarios.</td>
</tr>
<tr>
<td>Organisations often have piecemeal approach to SOA.</td>
<td>Use this to build SOA platform roadmap.</td>
</tr>
</tbody>
</table>

SOA in Action
Get smart about SOA.

© 2009 IBM Corporation
Align business and infrastructure spend
A scenario on the importance of SOA governance - Step 1

1. Provide a currency service that fills a specific line of business (LOB)

* Scenario from Introduction to SOA Governance, Bobby Woolf.
A scenario on the importance of SOA governance - Step 2

1. Provide a currency service that fills a specific line of business (LOB)

2. Other LOBs start using the service
A scenario on the importance of SOA governance - Step 3

1. Provide a currency service that fills a specific line of business (LOB)
2. Other LOBs start using the service
3. LOBs increase use of services / quality suffers
A scenario on the importance of SOA governance - Step 3

1. Provide a currency service that fills a specific line of business (LOB)

2. Other LOBs start using the service

3. LOBs increase use of services / quality suffers

SOA in Action
Get smart about SOA.

© 2009 IBM Corporation
A scenario on the importance of SOA governance - Step 4

1. Provide a currency service that fills a specific line of business (LOB)
2. Other LOBs start using the service
3. LOBs increase use of services / quality suffers
4. Service is fixed at provider’s expense

SOA in Action
Get smart about SOA.
A scenario on the importance of SOA governance - Step 5

1. Provide a currency service that fills a specific line of business (LOB)
2. Other LOBs start using the service
3. LOBs increase use of services / quality suffers
4. Service is fixed at provider’s expense
5. Fix works temporarily but problem reappears
A scenario on the importance of SOA governance - Step 6

1. Provide a currency service that fills a specific line of business (LOB)
2. Other LOBs start using the service
3. LOBs increase use of services / quality suffers
4. Service is fixed at provider’s expense
5. Fix works temporarily but problem reappears
6. Maintenance costs soar / provider ends service
SOA Governance Implementation Capability Pattern

**Plan & Organize**
- P01 – Service Transformation Planning
- P02 – Information Transformation Planning
- P03 – Technology Transformation Planning
- P04 – Service Processes, Organizations, Roles & Responsibilities
- P05 – Manage the Service Investment
- P06 – Business Vision & IT Alignment
- P07 – Service Portfolio Management
- P08 – SOA Ownership & Funding
- P09 – Service Governance Vitality
- P10 – Service Communication Planning
- P11 – Service Education & Training

**Program Management Controls**
- M01 – Enterprise Program Management
- M02 – Change Management
- M03 – Procurement of Resources
- M04 – Vendor Management
- M05 – Identify & Allocate Costs
- M06 – Monitor Business Benefits of SOA

**Service Development**
- D01 – Services Development Lifecycle Controls
- D02 – Requirements Gathering & Prioritization
- D03 – Service Identification
- D04 – Service Specification
- D05 – Service Realization
- D06 – Service Certification

**Service Operations**
- O01 – Service Execution Monitoring
- O02 – Service Operational Vitality
- O03 – Service Support

---

SOA in Action
Get smart about SOA.

© 2009 IBM Corporation
A Typical SOA Governance Project

Tailor SGMM

Create Project Proposal

Execute the “SOA Governance Project”

Identify SOA Business and IT Principles

Determine Existing Governance Structure

Define CoE Structure

Create the SOA Governance Framework

Roles

Processes

Policies

Metrics

Checkpoints

Implement Tools and Infrastructure

WebSphere

Lotus

Rational

Tivoli

Refine Operational Environment

SOA in Action
Get smart about SOA.

© 2009 IBM Corporation
Example of SOA Governance Enforcement at Runtime

Dynamic Endpoint Selection based on response time

1. A message is received
2. Invokes a selection mediation
3. Read Policy information
4. Executes matching algorithm to identify the provider service for requestor service
5. Message is transformed and routed to the selected endpoint
6. Monitor Response time
7. Update Service Attributes
Security and SOA Pilots

- Many pilots are done “without security”
  - In many controlled environments this is quite acceptable.

- However, if there is >1 domain, there is an identity flow issue to resolve
  - Doing a SOA pilot that includes only one domain is not likely to be representative of the enterprise requirements
  - Recommendation is to address identity flow early in the development process
How does Identity flow between services?

Propagating Identity Across SOA
IBM SOA Security Reference Model
Identity-Aware ESB

- Add *User Identity* to the set of technical issues “abstracted” from the business applications into the Enterprise Service Bus
  - Identity and Token Mediation
  - Coarse-grain authorization also possible

---

**Diagram:**

- **Service A**
- **Service B**
- **Enterprise Service Bus**
- **WESB/XI50/WMB**
- **Security Token Service**
- **Authorization Service**
- **Tivoli Federated Identity Mgr**
- **Tivoli Access Manager**

**Exchange this representation of the user from Service A for one that Service B will understand**

**New representation of user identity (for Service B)**

**Authorized?**

**Yes/No**

**Diagram Notes:**

1. **Identity and Token Mediation:**
   - Integrates identity and token management into the service bus.
2. **Coarse-grain authorization:**
   - Enables more flexible access control based on broader criteria.
Boundary Security

- Traditional firewalls protect against network-level attacks, but do not protect against XML/SOAP level attacks/errors
- Validation of identity and coarse-grained authorization can be added to the boundary
- Logical extension of Identity-Aware ESB pattern
### Findings
- **Align business with technology investment**
  - Initial SOA projects often focus business requirements.
  - Entry points are often people, process, information, reuse and connectivity.
  - Often minimum platform investment.

### Recommendations
- Look at SOA scenarios & disciplines to address NFR’s of SOA platform.
- Ensure that incremental business function and IT investment is aligned.

### Findings
- **Build governance roadmap based on reference architectures**
  - Initial SOA projects often do not look at SOA governance.

### Recommendations
- Assess your SOA governance maturity.
- Use SOA governance reference model to prioritise SOA governance activity.

### Findings
- **Build security roadmap based on reference architectures**
  - Initial SOA projects often do not look at SOA security.

### Recommendations
- Assess your SOA security maturity.
- Use SOA security reference model to prioritise security activity.

### Findings
- **Use SOA health check to determine next steps**
  - Organisations often have piecemeal approach to SOA.

### Recommendations
- Use SOA Health Check to understand as-is and to-be across SOA scenarios.
- Use this to build SOA platform roadmap.
## SOA Diagnostic within IBM SOA services offerings

<table>
<thead>
<tr>
<th>OFFERING NAME</th>
<th>FOCUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOA Strategy</strong></td>
<td>Helps the C-level executives lay out a business blueprint, complete with an SOA strategy, architecture and governance roadmap to guide the transformation of the organization and its systems to a service-oriented model using component-based business models</td>
</tr>
<tr>
<td><strong>SOA Diagnostic</strong></td>
<td>Helps an organization assess its current state in service orientation, integration and business process management to evaluate how it’s doing and make recommendations for corrective action, if warranted</td>
</tr>
<tr>
<td><strong>SOA Implementation Planning</strong></td>
<td>Helps a line of business develop a robust implementation plan that includes a high-level solution architecture review and the definition of scope in terms of process, service and governance to successfully realize an SOA solution</td>
</tr>
<tr>
<td><strong>Business Process Management (BPM) Enabled by SOA</strong></td>
<td>Helps businesses plan, design, model, simulate, measure and optimize core processes across the organization to achieve maximum operational effectiveness in an SOA environment</td>
</tr>
<tr>
<td><strong>SOA Design, Development, and Integration Services</strong></td>
<td>Helps an organization design, build and integrate the targeted SOA application and infrastructure</td>
</tr>
<tr>
<td><strong>SOA Management Services</strong></td>
<td>Helps an organization establish the management framework and supporting infrastructure to sustain the SOA environment, helping to ensure ongoing value and benefits realization</td>
</tr>
</tbody>
</table>
The SOA Diagnostic has three focus areas covering maturity assessment, BPM review and technical review

- Understand current environment
- Understand current and planned IT transformational initiatives
- Conduct diagnostic interviews/workshops
- Assess maturity using SIMM
- Refine scope and concerns to be investigated
- Perform business process benchmarking
- Evaluate process models against industry reference models
- Conduct Business Process Modeling and Requirements Definition Assessment
- Refine scope, identifying concerns that merit further investigation
- Review current architectural and design documentation
- Conduct interviews and workshops
- Identify preliminary gaps and improvement areas
- Prepare and review findings and recommendations
Roadmap for assessing your SOA Health

Choosing the right path for your needs

START

Existing SOA Project?

YES

Known Problem Area?

YES

NO

NO

SOA Strategy and Planning Services

SOA Diagnostic / Healthcheck Workshops

Specialised Diagnostic Healthchecks

Treatments

SOA in Action
Get smart about SOA.
IBM SOA Health, Governance and Security

Vast internal and external engagement experience

IBM Intellectual Capital  
Best Practices IT Principles  
Architecture & Standards  
Patterns  
Innovative Products  
Integrated Solutions  
Clients

Point of View – “The full picture”

How to best apply technology and methods to improve your SOA cost, flexibility, and service level.

www.ibm.com/soa/healthcheck

© 2009 IBM Corporation
Thank You

SOA in Action
Get smart about SOA.

© 2009 IBM Corporation