SOA Governance & Security
How BPM Can Help

Philip Larson,
Director of Product Management,
Appian Corporation
Agenda

- SOA Intro
- How BPM And SOA Fit Together
- SOA Governance Challenges
  - Methodology, SLAs, Development Processes, Security & Access Controls, etc.
  - How Can BPM Help?
- Conclusion
Appian Corporation

Introduction to SOA
The Need for SOA

- Older applications without the principles of SOA have resulted in:
  - Inflexible applications that cannot quickly adapt to changing business needs
  - Complex logic embedded in application code; logic not reusable outside the application.
  - Stove-piped data stores making integration with other systems difficult.
SOA Introduction

- Service Oriented Architecture (SOA) is a style of designing, deploying and managing software infrastructure in which organizational resources are exposed as independent services that can be accessed in a standardized way by other people and systems.

- SOA is about designing and integrating applications and processes via this collection of shared business services.
What is a Service?

- A service is any well-bounded, defined and repeatable business task or function that can be invoked in a standard manner.
  - Modular
  - Well-defined
  - Repeatable (Reusable)
  - Standards-based

- NOTE: The scope of this function can range from very narrow to quite broad. It may be a simple, one-step task, such as updating an employee’s home address, or a more complex task involving several steps and a number of possible outcomes.
There are both service consumers and service providers

Services Allow for Platform Agnostic Communication

Location, Platform and Code are all irrelevant.
SOA Adoption

- SOA is NOT the end goal.
- Organizations are seeking strategies that enable operational agility and flexibility while also improving overall process visibility and consistency.
- SOA Deployments are typically incremental and evolutionary, building on past experiences while exploiting emerging standards and technology.
Benefits of SOA

- SOA’s Enable Corporate Agility
  - Agile System Delivery through composite applications is a primary focus of nearly all SOA initiatives.

- Services are Reusable
  - Increased reuse of common, shared services is also a major focus of SOA initiatives.

- Applications are Simpler to Maintain
  - Improved maintainability of core IT systems due to logical separation of business focused services from the underlying technology
  - New functionality or bug fixing may only effect a small number of services, not the entire application.
  - Modular systems are easier to modify and update, lowering maintenance costs.

- Enable Business-User Driven Applications
How BPM and SOA Fit Together
BPM Definition

- Business Process Management (BPM) refers to the design, execution, and optimization of cross-functional business activities that include people and systems.

\[
\text{Business Process Management (BPM)} = \text{Process-Centric Management Discipline} + \text{Process Technology}
\]
## Businesses Run on Processes

<table>
<thead>
<tr>
<th>Finance</th>
<th>Sales</th>
<th>Marketing</th>
<th>Manufacturing</th>
<th>Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable and Receivable</td>
<td>Contact and Lead Tracking</td>
<td>Advertising and Merchandise Management</td>
<td>Order and Vendor Management</td>
<td>Change and Configuration Management</td>
</tr>
<tr>
<td>Payroll and Expense Approval Processes</td>
<td>Contract Management</td>
<td>Promotions and Deal Management</td>
<td>Customer Service</td>
<td>Service Desk and Incident Management</td>
</tr>
<tr>
<td>Regulatory and Compliance Management</td>
<td>Pipeline Management</td>
<td>Event Management</td>
<td>Inventory Control and Supply Chain Management</td>
<td>Application and Security Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2006 Appian Corporation. All rights reserved. Proprietary and confidential.
“Cross-functional end-to-end processes are the ones that matter most to the bottom line: to overall efficiency, customer satisfaction, compliance, and responsiveness”

- Bruce Silver, “The 2006 BPMS Report”
BPM layers process capabilities on top of your SOA so you can get more out of your existing resources.
A composite application is an application built from components of existing applications orchestrated using additional business process logic.
Composite Application Architecture

Business Process Applications and Solutions
Composite Applications Using BPM & SOA

SARBANES-OXLEY COMPLIANCE

PROPOSAL MANAGEMENT

CONTRACT MANAGEMENT

CASE MANAGEMENT
Benefits: Corporate Agility

- Agility is the ability for an organization to sense change and respond efficiently to that change.

- Agile system delivery through composite applications is a primary goal for SOA initiatives.
Benefits: Corporate Agility

SOA & BPM lower the incremental cost of future process automation initiatives helping drive efficiency deeper into the organization.
Processes and services can be adapted, even in-flight, to continuously improve process execution or simply to handle one-off exceptions.

- Changes may be necessary because of changes in:
  - Customer Demands
  - Market Dynamics
  - Competitive Landscape
  - Regulatory/Compliance Requirements
Benefits: Service Reuse

Processes control interaction with services that may be reused in other processes and applications

- Reduce Development/Go-to-Market costs
- Consistent Service Execution
- Reuse enables best practices
Summary

- Composite applications (SOA + BPM) are the next generation framework for rapidly building agile apps.
Challenges: SOA Governance
SOA Governance Intro

- The essence of governance is the assignment of responsibility for certain decisions and creating accountability for the results.

- According to Gartner, SOA Governance requires identifying the RACI for the individual services...
  - Who is **R**esponsible for the service?
  - Who is **A**ccountable?
  - Who is **C**onsulted?
  - Who is **I**nformed?

- The larger the SOA, the more it needs comprehensive governance.
BPM Helps Secure & Govern the SOA

Enterprise Security Architecture

BPM Suite Security Engine

Firewall

Web Service

Database

Web Service

Web Service

BPM Suites should play a pivotal role in securing and governing access to services exposed through an SOA.
Although BPM Alone is Not Enough…

PKI Infrastructure

SSL Encryption

Web Service Consumer

Unencrypted Message → Certificate → Encrypted Message → Certificate → Decrypted Message Delivered

SOA Governance: Methodology

- There is no single, mature, well-defined SOA methodology available today.
- The Methodology Chosen Must Address
  - Prioritization – Which Services Do I Implement First?
  - Funding – Who is Paying for All This?
  - Ownership – Who Owns These Services Moving Forward?
SOA Governance: Prioritization of Services

- What Services Do I Start With?
  - Exposing all of an organization's core systems will take a long, long time.
  - Companies must realize that some of their infrastructure and legacy applications are not worth exposing as services. The benefits won’t outweigh the costs.
  - Prioritization requires a clear articulation and communication of the strategic business objectives based on the processes to be improved.
Prioritization: How BPM Can Help?

- BPM can help...
  - Organizations approach SOA top-down rather than bottom-up.
  - Organizations prioritize the services that will have the greatest impact in the organizations business processes.
  - Prevent spending scarce IT resources on services that won’t be incorporated into future composite applications or enterprise processes.
  - Ensure that business users are driving the service implementation priorities rather than just IT.
SOA Governance: Funding

- Who is Paying for All This?
  - SOA projects need to be justified by measurable business value. But who covers development costs, maintenance costs, and operational costs?
  - Management funding decisions are different for service-oriented composite applications (particularly when cross-functional) than standard applications.
Funding: How BPM Can Help?

BPM can help…

- Identify who benefits the most from a particular service or set of services.
- Monitor service usage across processes and applications.
- Implement and manage chargeback arrangements, in which costs of reusable services are split among various application owners, proportional to the service usage.
SOA Governance: Ownership

- **Who Owns the Service?**
  - Does the ownership change from development to operation to maintenance (life-cycle management)?
  - If the service in a process is business-related (e.g. say a policy rule), does IT or business own the right to change the service parameters?
    - Must Business Notify IT of all changes?
  - How does the help desk for service support work? Who are the problems routed to? What if the service is from a third party? How do you maintain seamless customer support in a world of glued together services.
Ownership: How BPM Can Help?

- BPM can help…
  - Define and manage the ownership of the service including the RACI.
  - Enforce service policies in terms of who can adjust what in the context of different processes.
  - Automatically notify relevant parties when changes do occur. (e.g. The “I” in RACI)
  - Implement help desk processes in which problems are routed to the appropriate person depending on the specific problem w/ the service.
SOA Governance: Processes & Policies

- SOA governance implies putting in place new, specific processes & policies in which both IT and business players are involved.
- The processes supported must include:
  - Service Management Policies (performance, monitoring, availability, SLAs)
  - Service Life-Cycle Processes
  - New Development Policies
SOA Governance: Service Mgmt (incl. SLAs)

- SOA Governance requires the ability to create and enforce process-based SLAs with their internal and external service providers.
  - Web Services and SOA aggravates the problem by making more services. More moving parts can sometimes mean greater complexity.
  - SOA governance must identify the decision-makers responsible for determining the service levels required, performance requirements & access controls.
  - SLAs can vary greatly, including rule-based changing requirements of service response times and up-time.
Service Management Hypos

- HYPO 1: perhaps only HR workers can invoke services providing information on employee ranking.
- HYPO 2: if a bank only does wire transfers at 2 p.m., they may expect more network traffic a little after 2 p.m. How can they create rules that if the performance degrades to less than 95% of the SLA, send an e-mail to the sys. admin and automatically kick in the backup services?
SLAs: How BPM Can Help?

- BPM can help...
  - Define the SLA using role-based and rule-based access control to invoking services, based on the context of the parent process.
  - Enforce the SLA through process rules, rule-based notifications and by monitoring and auditing service performance.
  - Enable alert-based reporting on the level of adherence to the SLA as well as standard process dashboards and reporting.
  - Send automatic notifications or help define graceful exception handling when the SLAs break down.
Outsourcing is the practice of shifting an organization's operations to a third party vendor.

Core Processes

Non-Core Processes

Outsource

Human Resources

Data Entry

Call Center

Order Fulfillment

Focus
BPM Secures SOA at the Application Level

BPM secures web services at the application level by requiring authentication. BPM Suites employ username/password, PKI, and other authentication mechanisms.
BPM Secures SOA at the Process Level

BPM secures processes and the incorporated services at the application level using role-based access control restrictions.
BPM Secures SOA at the Service Level

**PROCESS MODEL SECURITY**

<table>
<thead>
<tr>
<th>Process Model Role Map</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SA</strong></td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>Edit/Save</td>
</tr>
<tr>
<td>Publish</td>
</tr>
<tr>
<td>Start Process</td>
</tr>
<tr>
<td>simulate</td>
</tr>
<tr>
<td>delete</td>
</tr>
<tr>
<td>archive</td>
</tr>
<tr>
<td>Attach</td>
</tr>
<tr>
<td>removeAttach</td>
</tr>
<tr>
<td>view</td>
</tr>
<tr>
<td>viewReport</td>
</tr>
<tr>
<td>overrideLock</td>
</tr>
<tr>
<td>changeRole</td>
</tr>
</tbody>
</table>

**SERVICE SECURITY**

<table>
<thead>
<tr>
<th>Service Role Map</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SA</strong></td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>view</td>
</tr>
<tr>
<td>assignall</td>
</tr>
<tr>
<td>assignpool</td>
</tr>
<tr>
<td>reject</td>
</tr>
<tr>
<td>override</td>
</tr>
<tr>
<td>addAttach</td>
</tr>
<tr>
<td>removeAttach</td>
</tr>
<tr>
<td>complete</td>
</tr>
<tr>
<td>changeRole</td>
</tr>
<tr>
<td>IFM</td>
</tr>
</tbody>
</table>

BPM secures each role’s privileges for all objects of the suite. This includes processes, services, documents, pages, etc.
Service Life-Cycle Processes

- Life-cycle management processes must support multiple versions of a service implementation running at the same time running in multiple versions of the parent processes.
- As the complexity of the systems grows, the interdependencies become more fragile.
- Service life-cycle processes includes the ability to discover, define and manage the relationships b/w assets to eliminate this fragility.
- More ownership issues at different points in the life-cycle.
Dev. & Life-Cycle Mgmt: How BPM Can Help?

- BPM can help...
  - Keep track and report on which service versions are being used for each process in real-time.
  - Audit these transactions for historical review or use in help-desk processes.
  - Track when new versions are incorporated into processes to see the “evolution” and optimization of the services over time.
SOA Governance: New Development Processes

- Governance requires setting up new development processes to ensure the testing and removing of vulnerabilities in Web Services. Processes should recommend security enhancements to WSDL, for instance.
- How do you enforce new policies to encourage service reuse in applications?
- How do you enforce new practices for ensuring services are developed in a consistent way at the right level of granularity?
Service Development: How BPM Can Help?

- BPM can help…
  - Enforce the processes for governing the testing of Web Services, including recommendations on how to improve security of the WSDL or XML Schemas.
  - Enforce development policies regarding appropriate application design and appropriate areas for service reuse.
Conclusions
Conclusions

- Composite applications (BPM + SOA) are the next generation framework for agile business apps.
- BPM’s position in the overall architecture can be used as an additional layer of security to protect access to the services exposed in your SOA.
- BPM can help address add’l SOA governance concerns, including:
  - Defining and managing roles and access controls to services used in composite applications
  - Enforcing SOA Governance Methodology
  - Providing visibility into service execution and enforcement of SLAs
  - Enforcing New Processes for the Development, Testing and Deployment of new services in your SOA
Thank You for Your Participation

- Philip Larson
  - Director, Product Management
  - Appian Corporation
  - larson@appian.com
  - (703) 442-1057 / www.appian.com