Software & Systems Development Governance: An approach to improving Software Assurance

Sridhar Iyengar
IBM Distinguished Engineer
siyengar@us.ibm.com

OMG Software Assurance Day: February 15, 2006: Tampa, Florida

Rational software
Topics Covered

♣ Introduction to Governance – Why do we care

♣ What does Software Assurance have to do with Governance

♣ Model driven tools integration across the life cycle
  ▶ Enabling traceability and management of artifacts

♣ Model Driven Security – An example
If only we could link Business, Development & Operations

OPERATIONS: "This application has performance problems, but development has no clue what's wrong!"

DEVELOPMENT: "Hmm... I wonder if the application we built will add any business value?"

BUSINESS: "If only we had the right systems, we could REALLY grow this business!"
Complexity is Forcing Change

Actual Application Architecture
Initiatives Underway at IBM

- Outside In Design (OID) – Scenario Driven
- Componentization – exploit open source or binary components as needed
  - Drive componentization and SOA standards
- End-end life cycle integration
- Move to SOA across and within products
- Model Driven Development, Deployment, Security, Management…
- Standards (UML, SysML, UML Testing Profile, MOF, XMI, RAS, SAML, XACML, WS_Security…)
- Patterns, Transformations and Recipes
  - Modeling Tools : Abstract modeling level
  - Development Tools : Code & Artifact level
The world of many of our customers

*Governing a geographically distributed, service-oriented, open computing environment while ensuring regulatory compliance*
Transforming software and systems development

<table>
<thead>
<tr>
<th>TRADITIONAL</th>
<th>CURRENT REALITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-located teams</td>
<td>Geographically distributed</td>
</tr>
<tr>
<td>Technology first</td>
<td>Compliance</td>
</tr>
<tr>
<td>Vendor lock-in</td>
<td>Open computing</td>
</tr>
<tr>
<td>Application silos</td>
<td>Modular systems (SOA)</td>
</tr>
<tr>
<td>Project driven</td>
<td>Value driven</td>
</tr>
</tbody>
</table>

**Right-sourcing**

**Standards**

**Solution delivery**

**Business Driven Development**

Enabling organizations to *govern* the business process of software and systems *development*
Governance defined

Governance is the exercise of authority, responsibility and the communication of information

- Establishing chain of authority, accountability and responsibility
- Measurements and controls to enable people to carry out their authority and responsibility
Governance consists of

**Governance**

- Establishing chains of responsibility, authority and communication to **empower** people
- Executing measurement and control mechanisms to **enable** people to carry out their roles and responsibilities

**Governance**

- **Manage value**
  - Align business and software
  - At organizational and project levels
    - Balance risk and return
    - Provide clarity and accountability
- **Develop flexibly**
  - Leverage resources anywhere
  - Enable agile sourcing choices
  - Use iterative processes to reduce risk
- **Control risk and change**
  - Continuously measure to reduce risk
  - Enable lifecycle change management
  - Meet internal and external compliance needs
Innovation Insurance Team

Business Analyst
- Models business processes

Risk Analyst
- Analyze, define, and manage policies

Portfolio Manager
- Ensures development projects are aligned with business strategy

Integration Developer
- Assembles and implements solutions

Deployment Manager
- Deploys the solutions

IT Operations
- Maintains the Data Center

VP of Claims
- Reduces cost for claims processing

CSR
- Handles customer incident reports

VP of Development
- Reviews forecast vs actual and competitive products. Formulates actions to address

VP of Claims
- Establishes strategic goals and ensures company profitability

CIO
- Responsible for Technology Infrastructure

CFO
- Responsible for accounting and financial

Portfolio Manager
- Manages new development projects

Project Manager
- Ensures development projects are aligned with business strategy

CEO
- Reduces cost for claims processing

VP of Development
- Manages new development projects

Insurance Adjuster
- Handles claims that can be settled by phone or email

Field Adjuster
- Handles requests that require on-site inspection
Governance across life cycle: Project Flow

**Data, Security, Strategic, Business Governance**

**START**
- Policy Change
- Analyze policy
- Identify remediation plan (w/LOB)
- Identify requirements
- Validate plan & requirements

**IMPLEMENTATION FLOW**
- Prioritize projects
- Approve Project
- Decompose projects into tasks
- Generate Audit Package

**PROJECT APPROVAL FLOW**
- Initiate Project Request
- Estimate project costs
- Validate Service
- Deploy, Manage Service
- Manage Services Operations

**Development Governance**

**Development Governance**

**SOA (Service) Governance**

**Securing Services**

**IT Governance**

Feedback
Governance and processes are the keys to a successful transition to SOA

- Discover
- Construct & test
- Compose

- Gather requirements
- Model & simulate
- Design

- Financial transparency
- Business/IT alignment
- Process control
- SOA Governance Processes

- Integrate people
- Integrate processes
- Manage and integrate information
- Protect information

- Manage applications & services
- Manage identity & compliance
- Monitor business metrics
- Secure Apps & Services
Transforming to an SOA environment: How do we integrate Custom & COTS software

1.0 Identify Services
2.0 Identify Service Owners
3.0 Fund Services
4.0 Specify Services
5.0 Realize Services
6.0 Develop & Test Services
7.0 Deploy Services
8.0 Manage Services
9.0 Maintain Services
10.0 Manage Services Performance
11.0 Manage Service Level

Decompose business process and identify services required
Establish funding, project plans and resources
Codify business process and enforce standards
Develop iteratively, test to improve predictability, manage change to ensure traceability and auditability
Monitor composite application performance and adjust

Continuous Process Measurement and Improvement

Measure progress, manage change and adjust
Model Driven Development & Deployment

- **Design/Build**
  - Business Modeling (BPD, UML)
  - IT Modeling (UML, SQL, XSD)
  - J2EE/Web Services Development Wrapping Orchestration (J2EE)

- **Run/Manage**
  - Deployment J2EE App Svr Web Services
  - Management Component Mgmt App Mgmt

**Specific metadata Models**

- Traceability Links and Transformations (profiles, metamodels, Code Gen Templates)
- Serve up models, Components, processes On Demand
Application Life Cycle Integration Platform
A call to action  to the Eclipse Community

Language Tooling (J2EE, Web Services, Deployment)

Data Tools (RDBMS, XML...)

MDD Tools (Object, Data Modeling, Code generators...)

Domain Specific Tools/Apps...

End to End Application Lifecycle Tooling (Eclipse.org member value add tools)

Eclipse Tools Integration platform (Models, APIs, XML formats...)

Web Tools (WTP...)

J2EE (EJB, JSP...)

MDD/MDA (UML2,U2TP...)

Testing TPTP

SAM*

EMF

GEF

JDT/CDT

RCP

ETC.

Eclipse Core

Code/Artifact Repositories, Management Tools (Eclipse.org member value add tools)
Model Driven Security – Life Cycle

Identify:
Business security and privacy guidelines, and goals

Conceive & Modify Business Idea
Focus on what’s core and differentiating

Define Model
- Business modeling
- Bridge to IT tools

Implement Model
- Component creation (new and legacy-based)
- Component customization and assembly

Acquire & Map to Infrastructure
- Deploy without knowledge of underlying (virtualized) infrastructure
- Both on and off premise
- Monitor process for business and IT status
- Actions taken based on automatic policy

Monitor & React

Specify:
- Security requirements (e.g. all requests to an app is confidential)
- Privacy requirements (e.g. only traveler can look at itinerary, preference, etc)
- Variability points

Transformed to and more added:
- Security deployment descriptors (J2EE)
- Security/privacy policies in XACML
- WS-SecurityPolicy attached to WSDL
- WS-Privacy to Apps
- If needed, app callouts to app level security decisions (in UML)
- Also container enforcements identified in UML

Transformed to/pushed/added:
- Security configuration information
- "Publishable" security policies (WS-SecurityPolicy)
- Pushed to policy provider thru JACC (e.g. TAM)
- Monitored events (e.g. authz failure)
- Containers/apps may end up calling cut to providers (through JACC for J2EE, WS-Authorization for web services, etc)

Based on events (monitored or otherwise):
- Change policies (revoke user rights)
- Add new user (and thus new entitlements)
- Change security policies in AccessManager
- May end up resulting change in business model? (e.g. messages to be signed as well?)
<table>
<thead>
<tr>
<th>Organization</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Strategy and decision making</td>
<td>Chief Security Officer, Security Policy Officer, Security Architect, Security Auditor</td>
</tr>
<tr>
<td>Development</td>
<td>Business analyst, Application programmer, Identity/Security developer</td>
</tr>
<tr>
<td>Operations and Administration</td>
<td>Security Administrator, System/Application Administrator, Operator</td>
</tr>
</tbody>
</table>
Security Definitions at the Business Process Level

Authorize:
Travel agent can view and change itinerary

Security levels, Gold, Silver, are specified; associated with business process, activity or objects.
Security Constraints captured in UML

Figure 5 Applying constraints to UML sequence diagram
Sample XACML generated from Annotated Model

**XACML for security policies**

"Traveller can view /Itinerary and descendant pages: (Traveller, (View, /Itinerary))"

```xml
<Policy PolicyId="P1"
   PolicyCombiningAlgId="path-more-specific-deny-overrides-with-propagation">
  <Target>
    <Subjects><Subject>
      <SubjectMatch MatchId="user-role-match">
        <SubjectAttributeDesignator AttributedId="subject-id"
          DataTypes="string"/>
        <AttributeValue DataTypes="string">traveller</AttributeValue>
      </SubjectMatch>
    </Subjects>
    <Resources><AnyResource/>
    <Actions><Action>
      <ActionMatch MatchId="action-id">
        <ActionAttributeDesignator AttributedId="subject-id"
          DataTypes="string"/>
        <AttributeValue DataTypes="string">view</AttributeValue>
      </ActionMatch>
      <Action/>
    </Actions>
  </Target>
  <Rule RuleId="R1" Effect="Permit">
    <Target>
      <Resources><Resource>
        <ResourceMatch MatchId="path-match">
          <AttributeValue DataTypes="pattern-path">Itinerary</AttributeValue>
        </ResourceMatch>
      </Resource>
    </Target>
    <Rule/>
  </Rule>
</Policy>
```
Software Assurance : Some Relevant OMG Standards

- UML 2.0 : Architecture, Design & Requirements Capture
- UML Testing Profile : Test automation
- KDM : Metadata about existing systems
- MOF & XMI : Metadata Infrastructure
- SysML : System design, Requirements
Governance consists of

**Governance**

- Establishing chains of responsibility, authority and communication to **empower** people
- Executing measurement and control mechanisms to **enable** people to carry out their roles and responsibilities

**Governing Development, Deployment & Management**

**Manage value**
- Align business and software
- At organizational and project levels
  - Balance risk and return
  - Provide clarity and accountability

**Develop flexibly**
- Leverage resources anywhere
- Enable agile sourcing choices
- Use iterative processes to reduce risk

**Control risk and change**
- Continuously measure to reduce risk
- Enable lifecycle change management
- Meet internal and external compliance needs