IBM Software Group

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

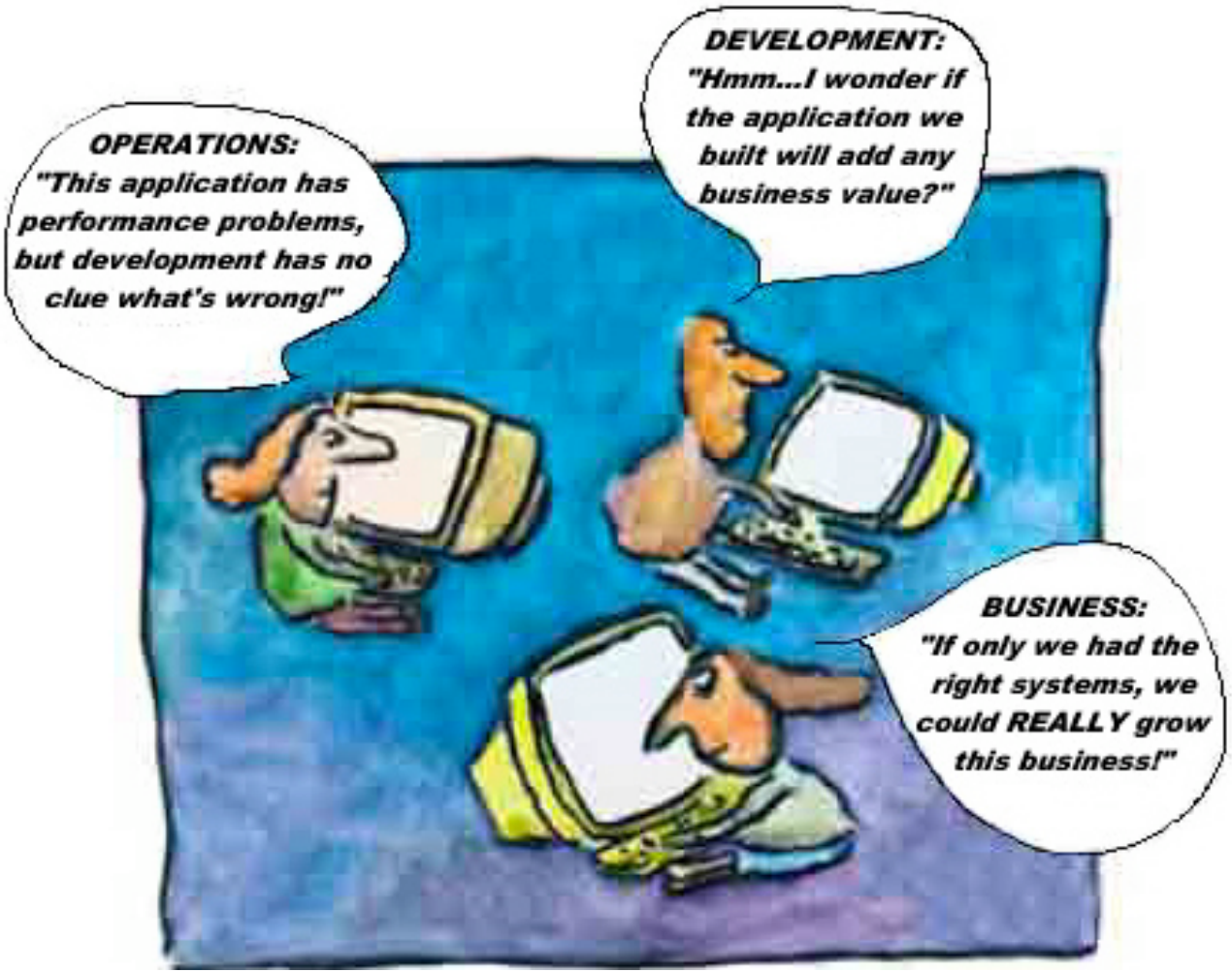
Rational. software

ON DEMAND BUSINESS

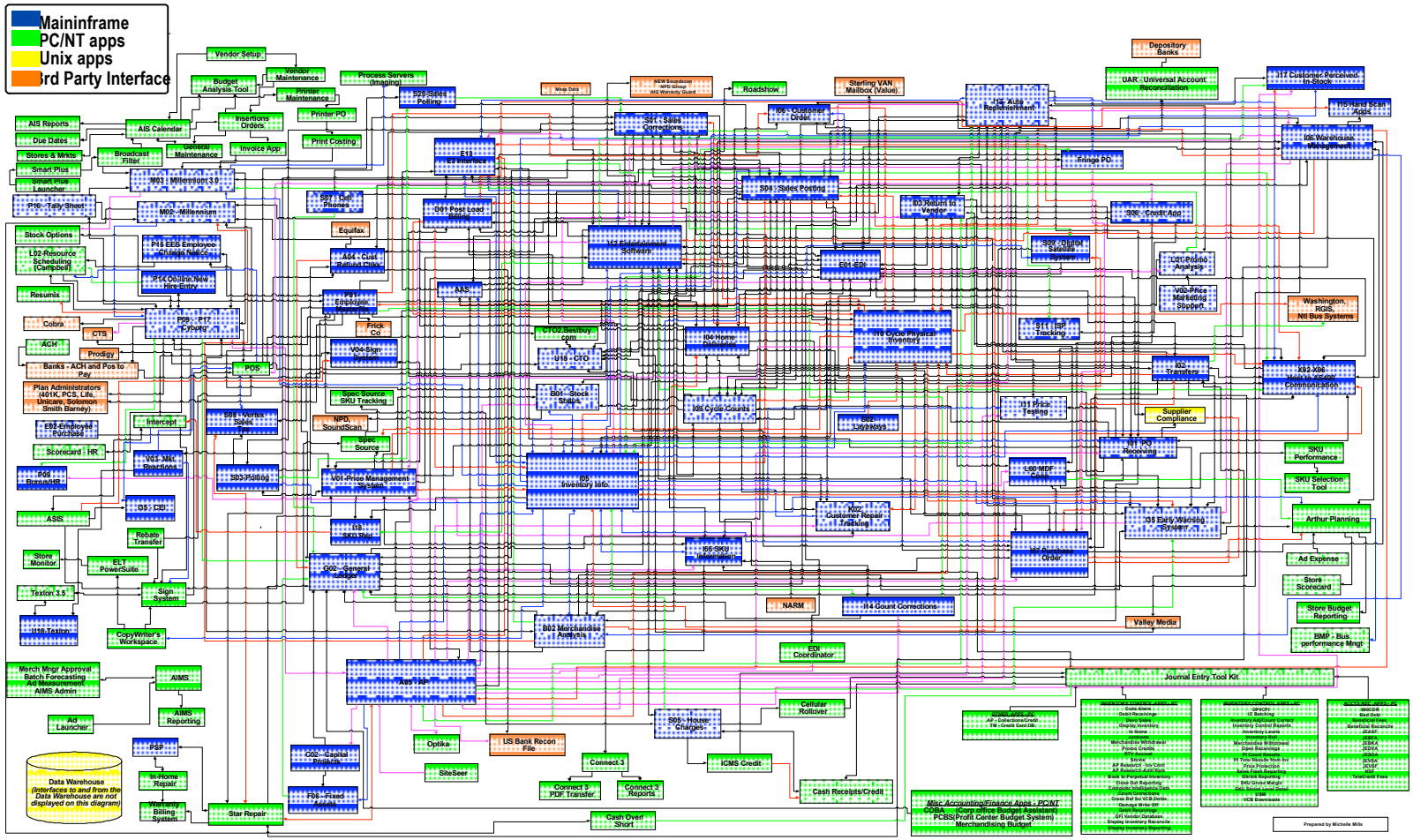
Topics Covered

- 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



Complexity is Forcing Change



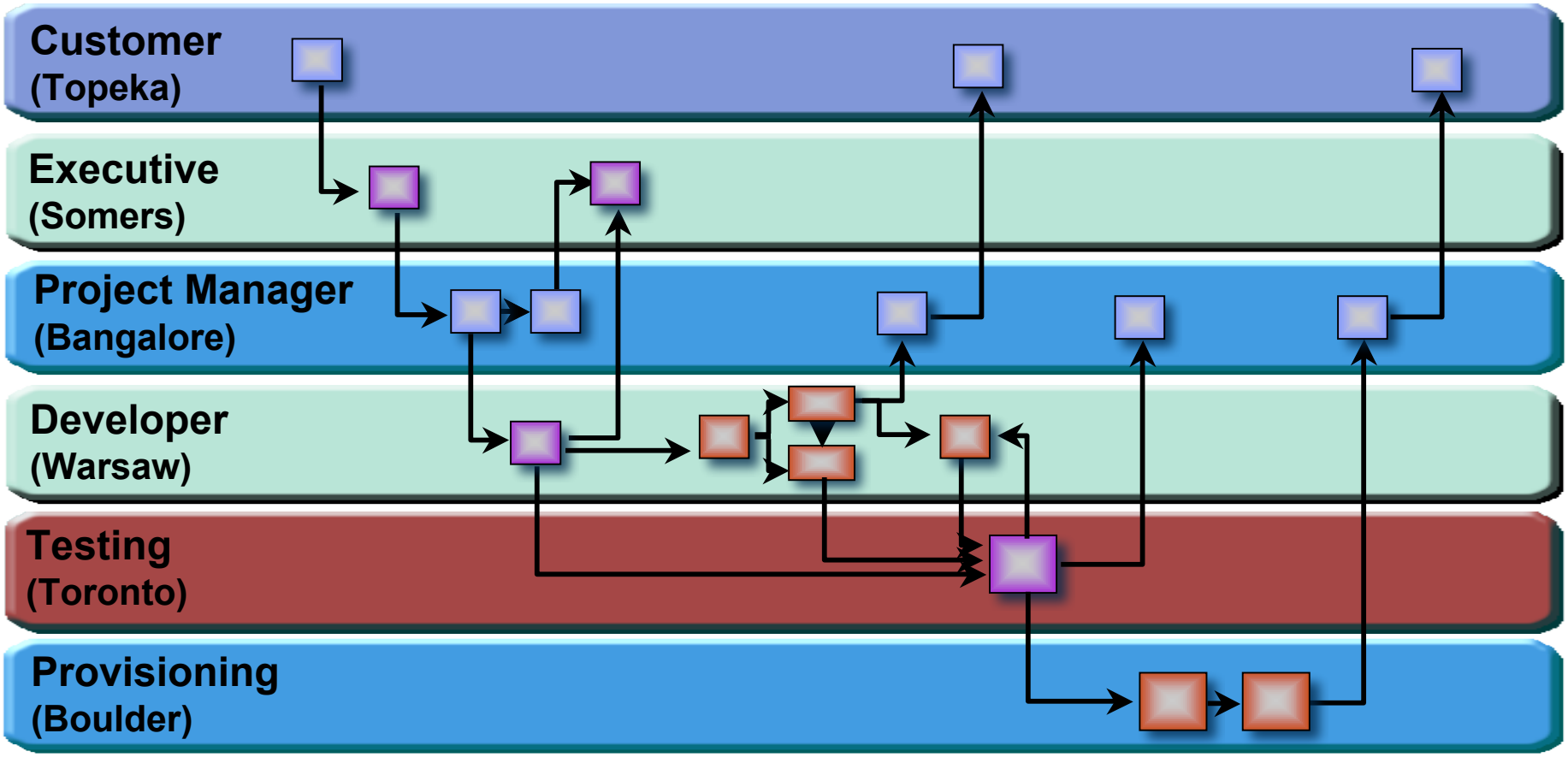
Actual Application Architecture

Initiatives Underway at IBM

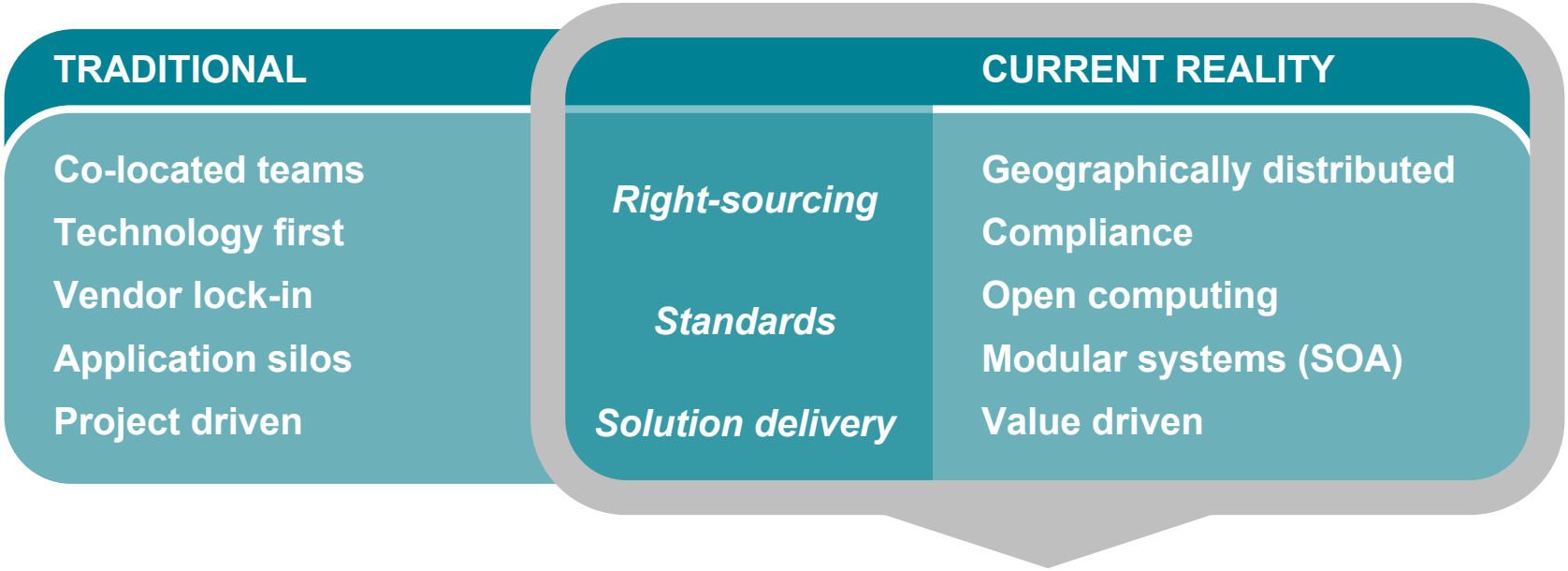
- Outside In Design (OID) – Scenario Driven
- Componentization – exploit open source or binary components as needed
  - Drive componentization and SOA standards
- End-end life cycle integration
- Move to SOA across and within products
- Model Driven Development, Deployment, Security, Management…
- Standards (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

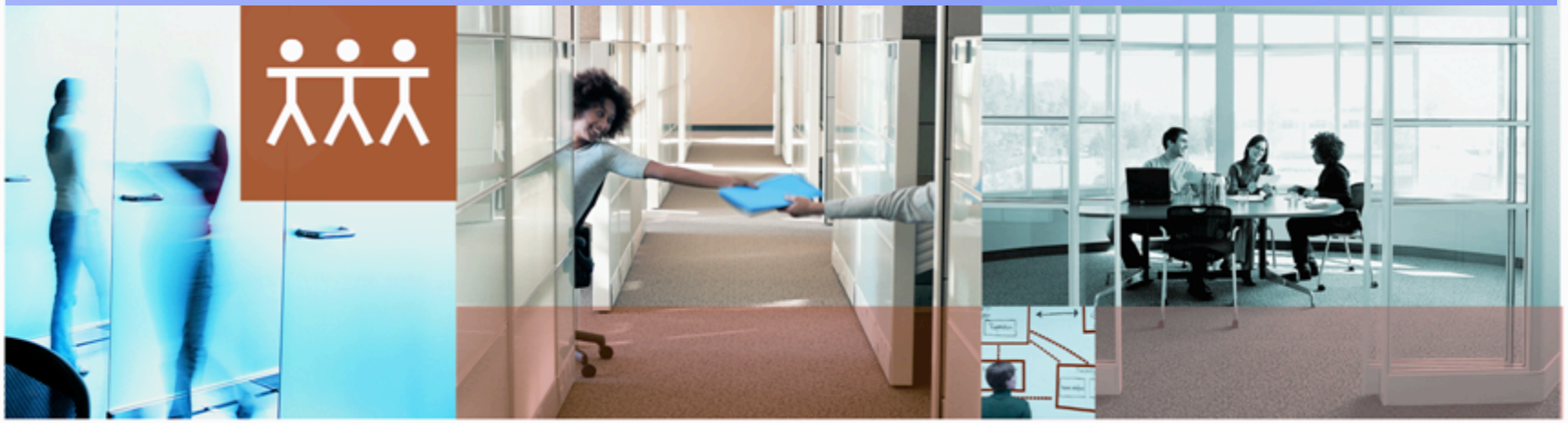


Business Driven Development

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

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

Innovation Insurance Team

CEO

Establishes strategic goals and ensures company profitability

Business Analyst

Models business processes

Risk Analyst

Analyze, define, and manage policies

CIO

Responsible for Technology Infrastructure

CFO

Responsible for accounting and financial

Portfolio Manager

Ensures development projects are aligned with business strategy

Project Manager

Manages new development projects

Integration Developer

Assembles and implements solutions

Deployment Manager

Deploys the solutions

VP of Claims

Reduces cost for claims processing

CSR

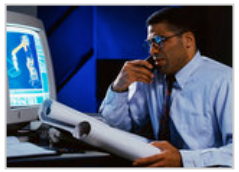
Handles customer incident reports

Insurance Adjuster

Handles claims that can be settled by phone or email

IT Operations

Maintains the Data Center



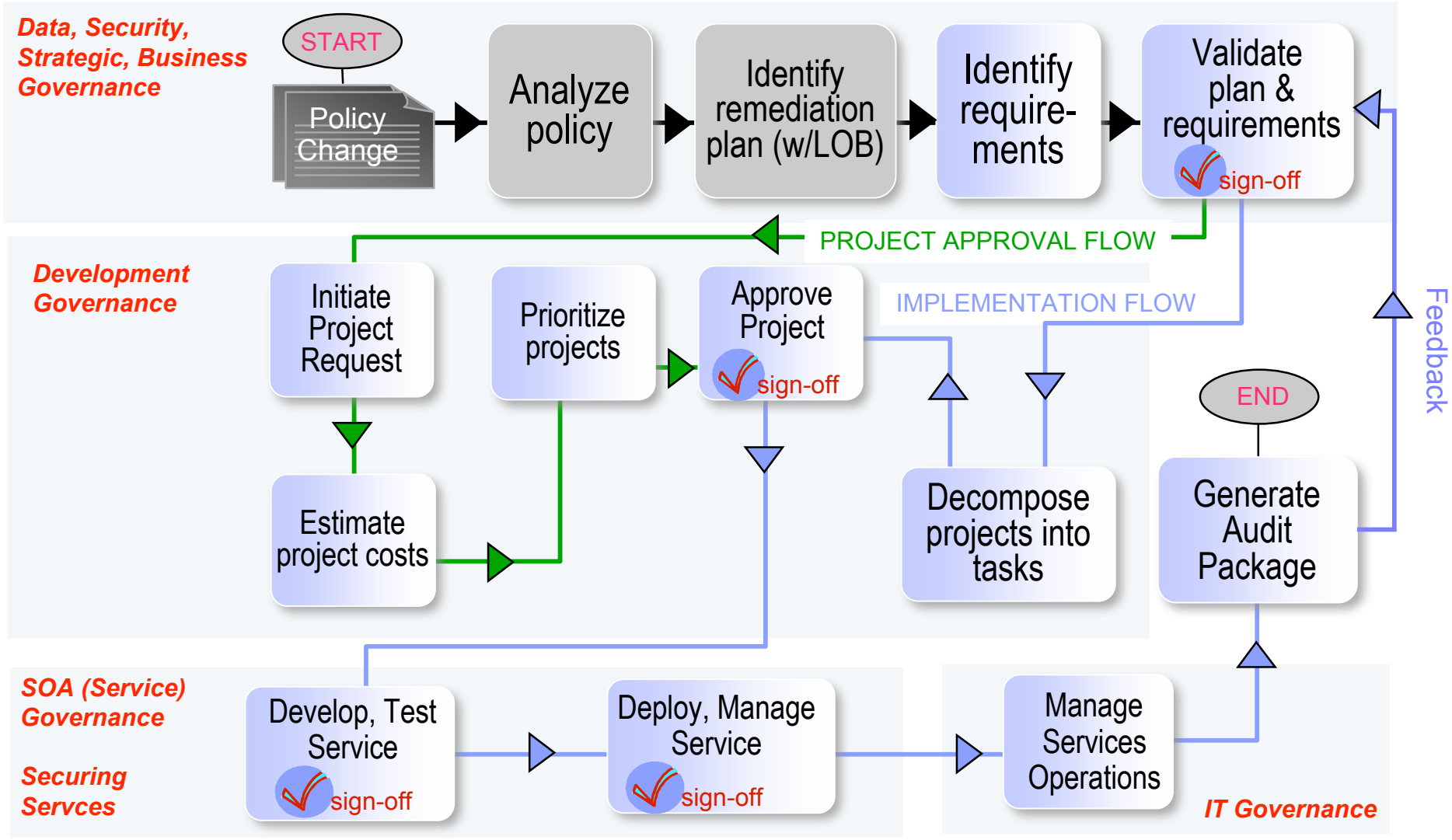
VP of Development

Reviews forecast vs actual and competitive products. Formulates actions to address

Field Adjuster

Handles requests that require on-site inspection

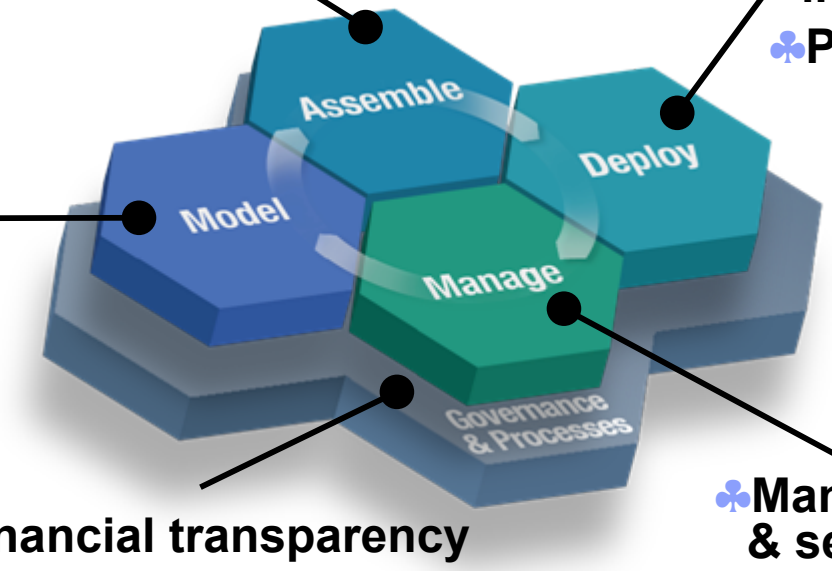
Governance across life cycle : Project Flow



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

- Discover
- Construct & test
- Compose

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

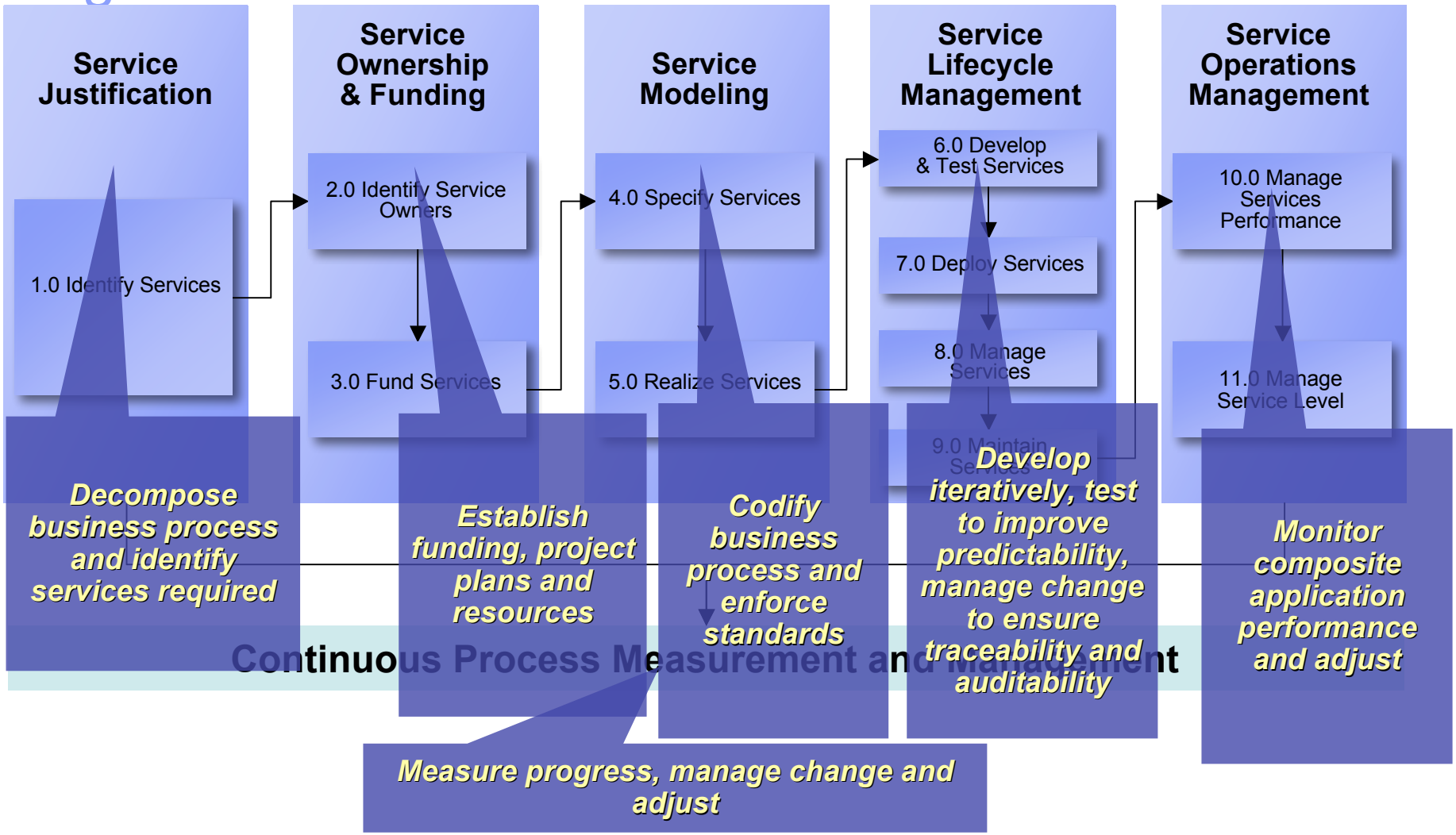


- Gather requirements
- Model & simulate
- Design

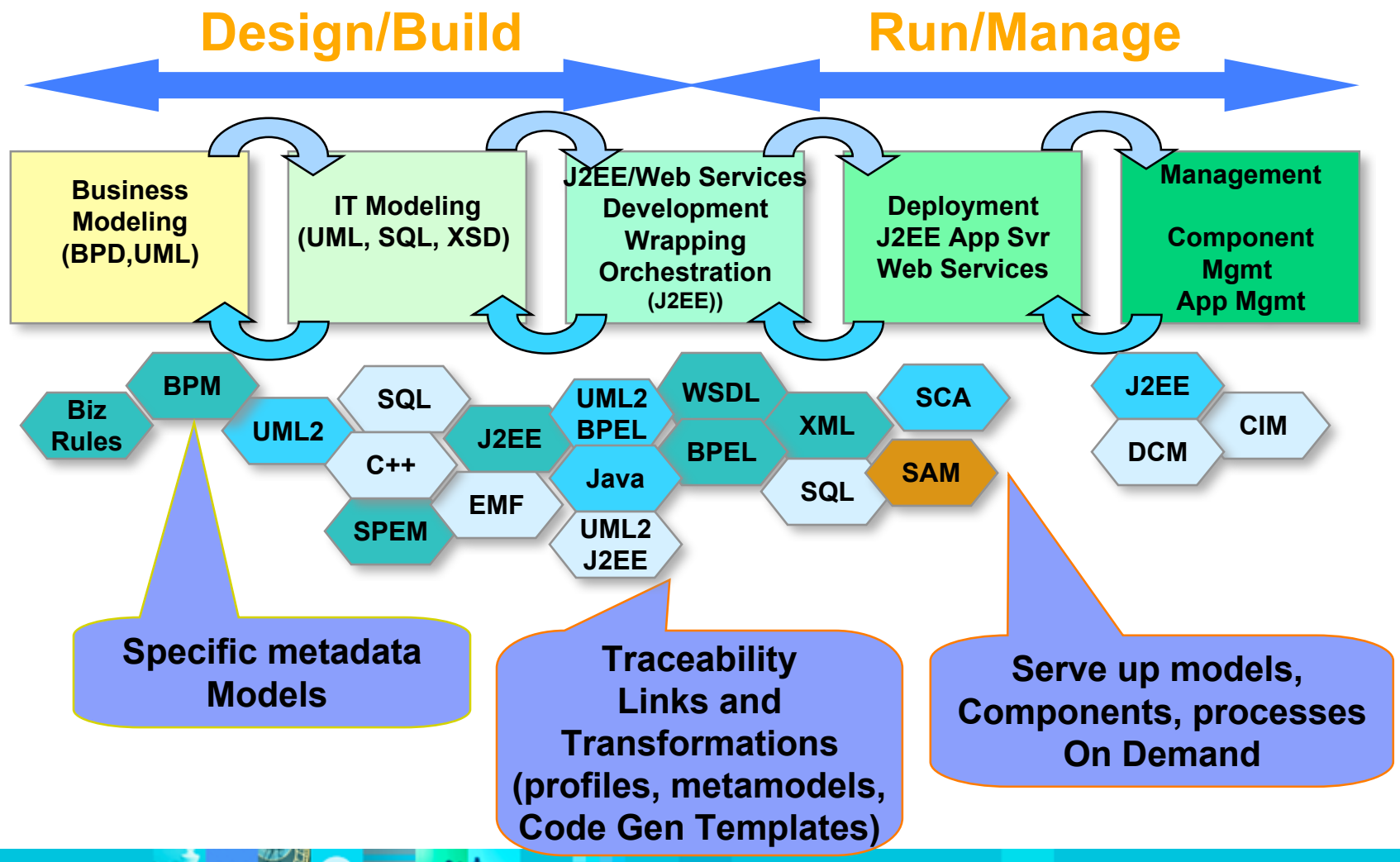
- Financial transparency
- Business/IT alignment
- Process control
- SOA Governance Processes

- Manage applications & services
- Manage identity & compliance
- Monitor business metrics
- Secure Apps & Services

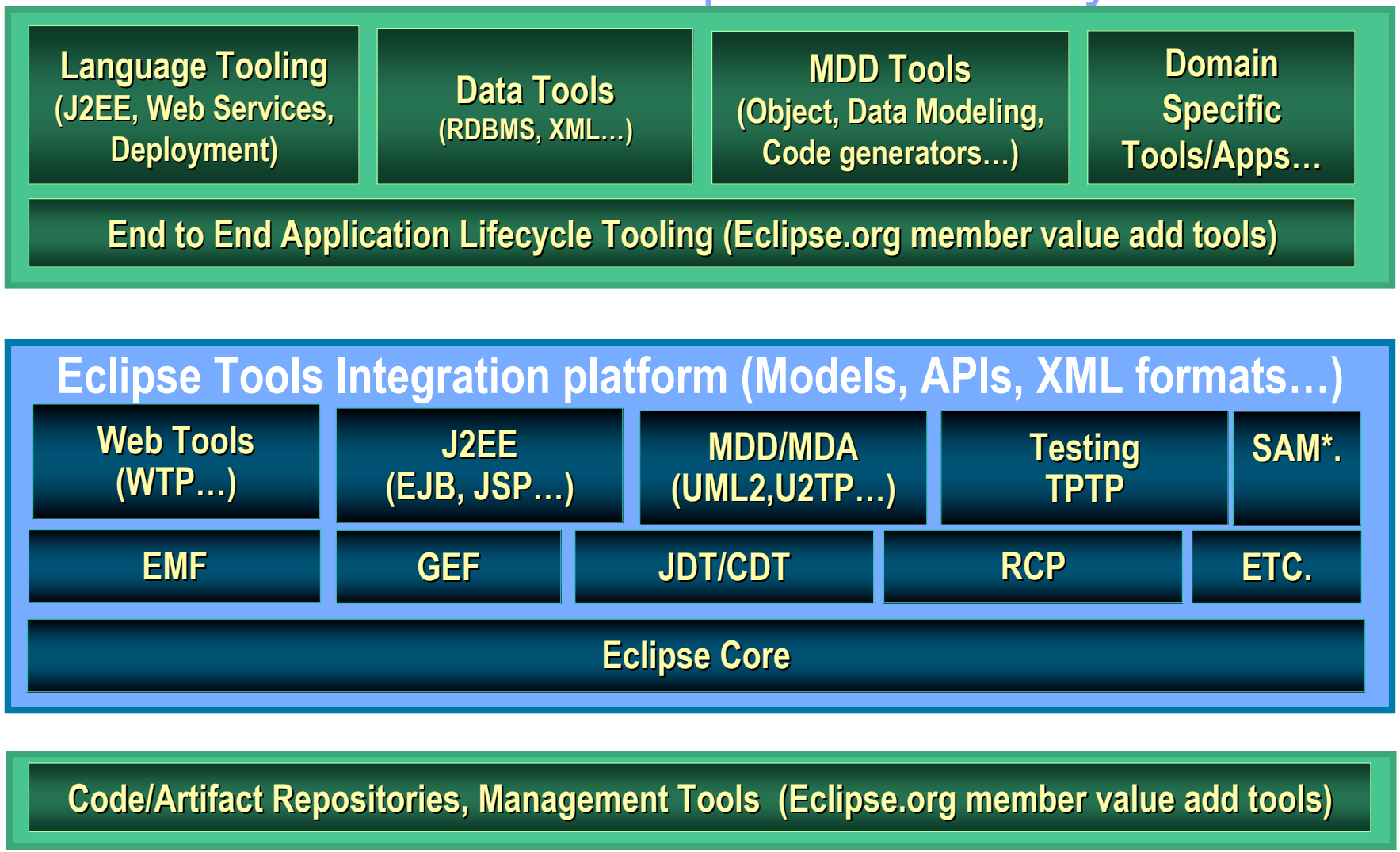
Transforming to an SOA environment : How do we integrate Custom & COTS software



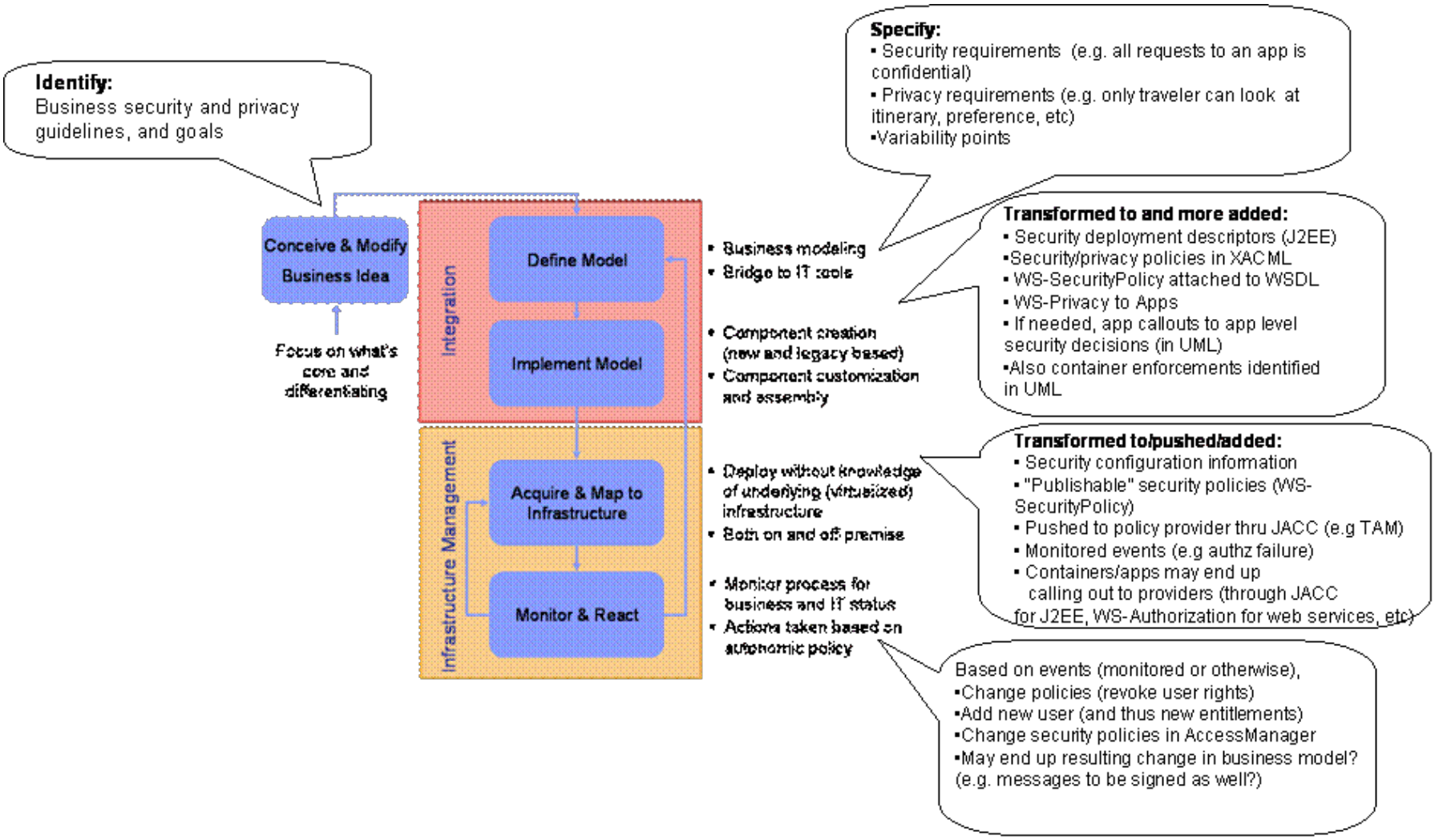
Model Driven Development & Deployment



Application Life Cycle Integration Platform
A call to action to the Eclipse Community



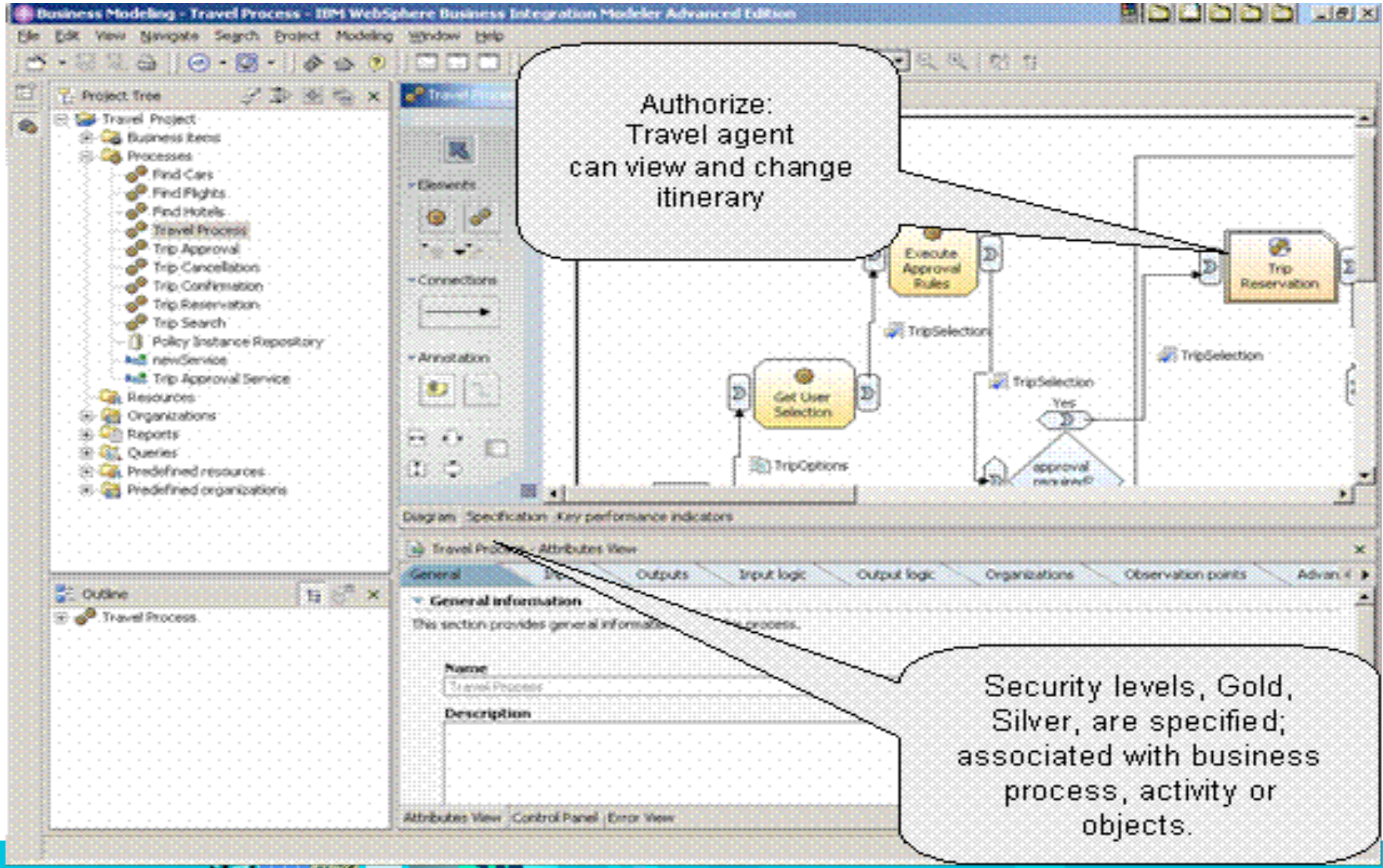
Model Driven Security – Life Cycle



Security Roles in an Organization

Organization	Roles
Business Strategy and decision making	Chief Security Officer, Security Policy Officer, Security Architect, Security Auditor
Development	Business analyst, Application programmer, Identity/Security developer
Operations and Administration	Security Administrator, System/Application Administrator, Operator

Security Definitions at the Business Process Level



Security Constraints captured in UML

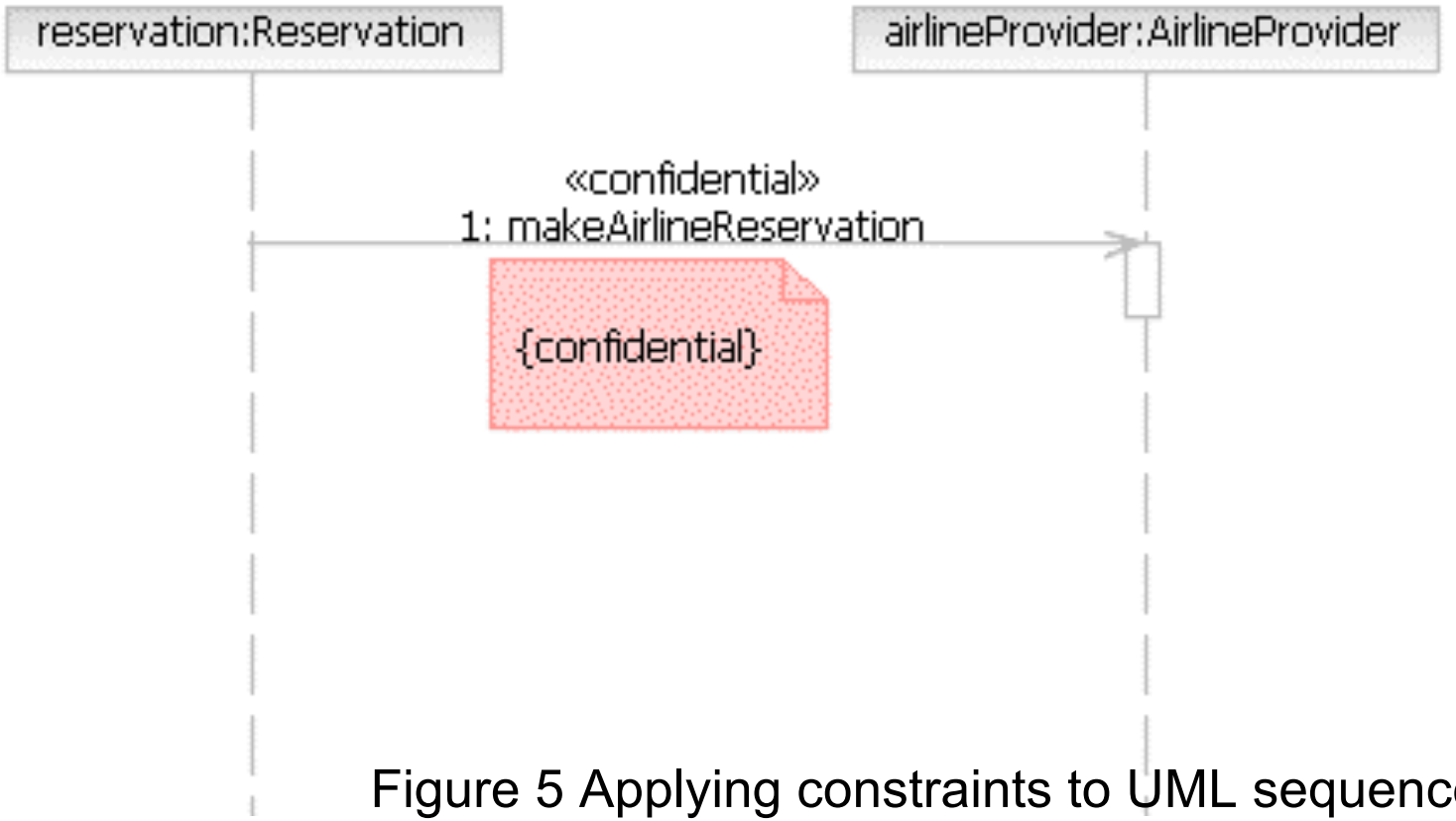


Figure 5 Applying constraints to UML sequence diagram

Sample XACML generated from Annotated Model

XACML for security policies

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

```
<Policy PolicyId="P1"
        PolicyCombiningAlgoId=
  "path-more-specific-deny-overrides-with-propagation">
 <Target>
  <Subjects><Subject>
   <SubjectMatch MatchId="user-role-match">
    <SubjectAttributeDesignator AttributeId="subject-id"
                                DataType="string"/>
     <AttributeValue DataType="string">traveller
     </AttributeValue>
     <AttributeValue DataType="string">
          http://myUserRoleMapping</AttributeValue>
   </SubjectMatch>
  </Subject></Subjects>
  <Resources><AnyResource/></Resources>
  <Actions><Action>
   <ActionMatch MatchId="action-id">
    <ActionAttributeDesignator AttributeId="subject-id"
                               DataType="string"/>
    <AttributeValue DataType="string">view
    </AttributeValue>
   </ActionMatch>
  </Action></Actions>
 </Target>
 <Rule RuleId="R1" Effect="Permit">
 <Target>
  <Resources><Resource>
   <ResourceMatch MatchId="path-match">
    <AttributeValue DataType="pattern-path">
                                /Itinerary</AttributeValue>
     <ResourceAttribugteDesignator
       DataType="simple-path" AttributeId="resource-id"/>
   </ResourceMatch>
  </Resource></Resources>
 </Target>
</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