Must-Have Policies

Structuring & Scaling SOA Adoption

Jason Bloomberg & Ron Schmelzer
ZapThink LLC

SOA09
SOASUMMIT2009
MAY 2009 | SCOTTSDALE, AZ

software AG

SOA Governance in the Narrow”

Governance of the SOA initiative

- Design time governance
  - Are developers and other personnel following the policies that apply to Services?
- Runtime governance
  - Are running Services and SOBAs conforming to runtime policies?
  - Automating policies specific to Services in the context of SOA

SOA Governance: Policies

Source: Wipro

The Power of the SOA Center of Excellence

- SOA experts who maintain a knowledge base of best practices
  - General and company-specific
  - Design time and runtime
- Drives SOA policy (either explicitly or implicitly)
- Can unify approaches across a large organization

The Challenge of Policy Automation

- Remember, policies are *business* concepts
- Governance is the way the *business* communicates & manages policies
- Challenge: What policies *can* and *should* be automated?

- SOA helps *automate* policy activities by treating policies as *metadata*

Steps for Automating Policies

- **Policy inventory**
- **Decide which policies are automatable**
- **Decide on level of granularity**
  - Message-level policies/Data-driven policies
  - Corporate-level policies/Governance & Security policies
  - Service-level policies/Performance, Security, Mediation, Transports, Response time / QoS / SLA
- **Translate policy into system-understandable format**
  - Pick an XML-based standard method
  - Develop your own XML-based spec
  - Encode directly into policy enforcement system
- **Figure out how to enforce policies in practice**
  - Policy mediation system
  - Registry-based system
- **Identify long-term policy maintenance**
  - Federated or centralized policy management?
  - How is policy going to be controlled?

Some Policy Standards

- WS-Policy
  - Allows web services to advertise policies & Web Service consumers to specify policy requirements
- XACML (XML Access Control Markup Language)
  - Access control policy language & a processing model describing how to interpret policies
- WS-SecurityPolicy
  - Used to publish security requirements & constraints of a Web Service
- WS-Management
  - Common way for systems to access & exchange management information across IT infrastructure
- WS-SecureConversation
  - Allows secure conversations between sites using Web Services

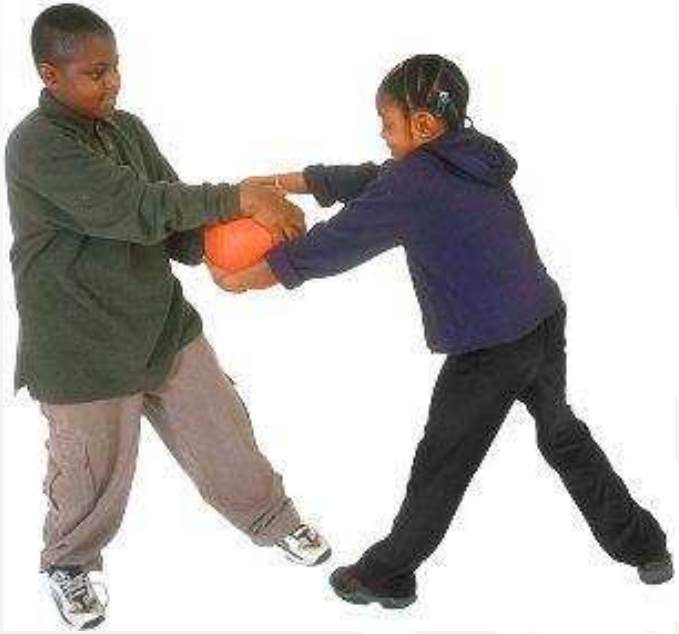
Design Time Policy Examples

- Reuse policies
  - Publication
  - Discovery
- Standards/WS-I compliance policies
- Contract creation policies
- Service testing & deployment policies
- Transaction policies

Business Driver: Reuse

- Reuse the old way: code reuse
  - Reusable code libraries and subroutines – the “Holy Grail” of programming
  - Branching code base reduces reusability
  - Hard to write reusable code, as requirements are never clear
- Reuse the new way: Service reuse
  - Reuse at runtime based upon contracted functionality
  - Loose coupling leads to flexible reuse
  - Appropriate governance and flexible metadata essential!

Challenge: Reuse = Sharing



We all learned to share in kindergarten…

But by the time we get to the working world, we forget how!

SOA Reuse Governance

- Reuse only important in practice
- Planning for reuse pointless without actual reuse!
- Developers would prefer to build anew
- Application assembly a new pattern
- Reuse governance covers:
  - Finding Services
  - Understanding Services
  - Composing Services
  - Publishing the resulting compositions

Reuse Challenges

- Many Services not designed for reuse
- Simply exposing Web Services does not increase reusability substantially
- Services are often too course grained to be reusable
- Core business systems do very different things and often don't need to share Services anyway!

Reuse over Time

New Composite Apps or Service-Enabled Existing Apps

- 1 2 3 6 7 9
- 2 5 7
- 3 4 5 9
- 1 3 8
- 1 5 8
- 4 6
- 1 2 6 7 8 9

Service Model

- Presentation Services: 3 8
- Coarse-Grained Business Services: 2 5 9
- Data Access Services: 1 6
- Legacy API Services: 4 7

Service Catalog

1 2 3 4 5 6 7 8 9

Source: BEA Systems

Run Time Policy Examples

- Service-Level Agreements
  - Availability policies
  - Response time policies
- Access control assertions & entitlements
- Threat prevention policies
- Commercial policies
- Auditing/logging policies

WS-SecurityPolicy Example

```
<wsp:Policy xmlns:wsp="..." xmlns:sp="...">
  <sp:SymmetricBinding>
    <wsp:Policy>
      <sp:ProtectionToken>
        <wsp:Policy>
          <sp:Kerberos sp:IncludeToken=".../IncludeToken/Once" />
            <wsp:Policy>
              <sp:WSSKerberosV5ApReqToken11/>
            <wsp:Policy>
          </sp:Kerberos>
        </wsp:Policy>
      </sp:ProtectionToken>
      <sp:SignBeforeEncrypting />
      <sp:EncryptSignature />
    </wsp:Policy>
  </sp:SymmetricBinding>
  <sp:SignedParts>
    <sp:Body/>
    <sp:Header Namespace="http://schemas.xmlsoap.org/ws/2004/08/addressing" />
  </sp:SignedParts>
  <sp:EncryptedParts>
    <sp:Body/>
  </sp:EncryptedParts>
</wsp:Policy>
```

Change Time Policy Examples

- Versioning policies
- Composition policies
- Sunsetting policies
- Policy management policies

Supporting Policy Changes

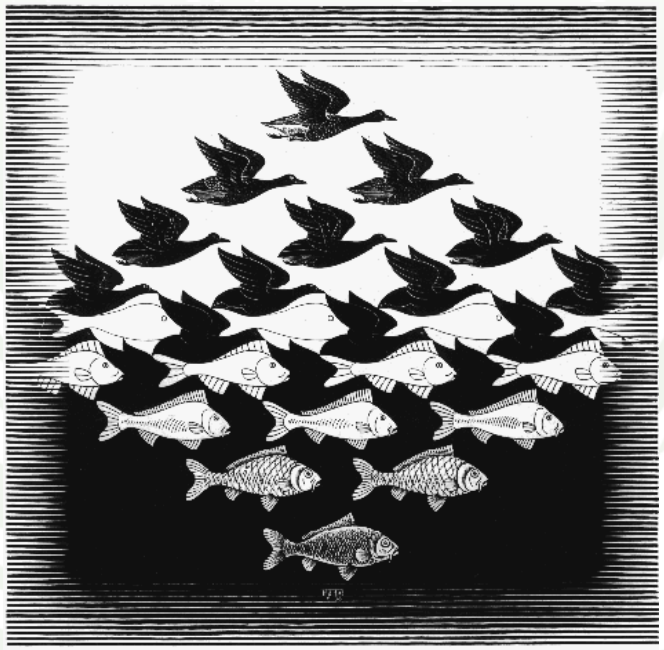
- How do you support changing policies?
  - Represent policies as metadata
  - Incorporate policy change into governance framework
  - Place scope of policy change into proper context

Remember, SOA means building for change

Governance Pitfall: Versioning

Without versioning policies:

- Service provider changes require consumer changes!



Bye-bye loose coupling!

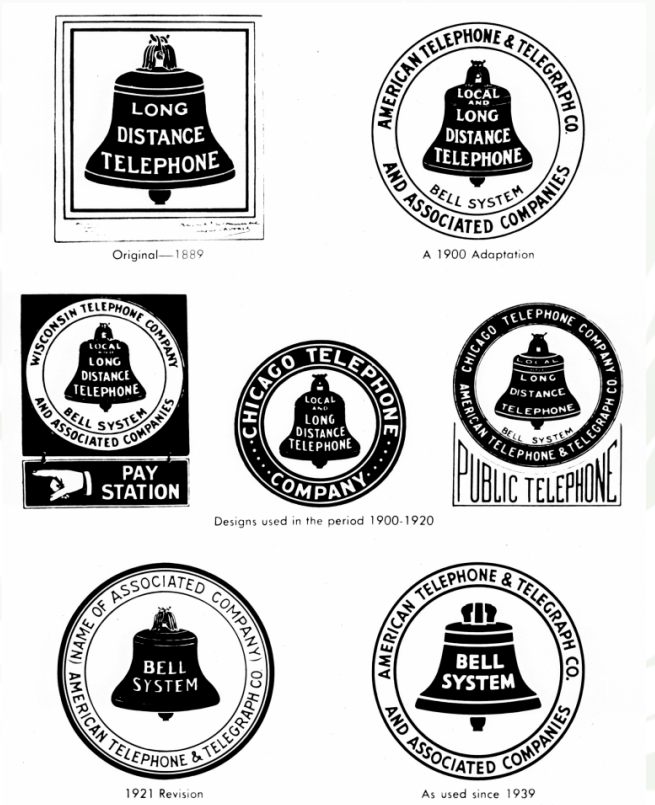
With versioning policies:

- Service providers & consumers change as per policy
- Maintains loose coupling

Challenge: Which Versioning Policies are Right for YOU?

Handling Service Versioning

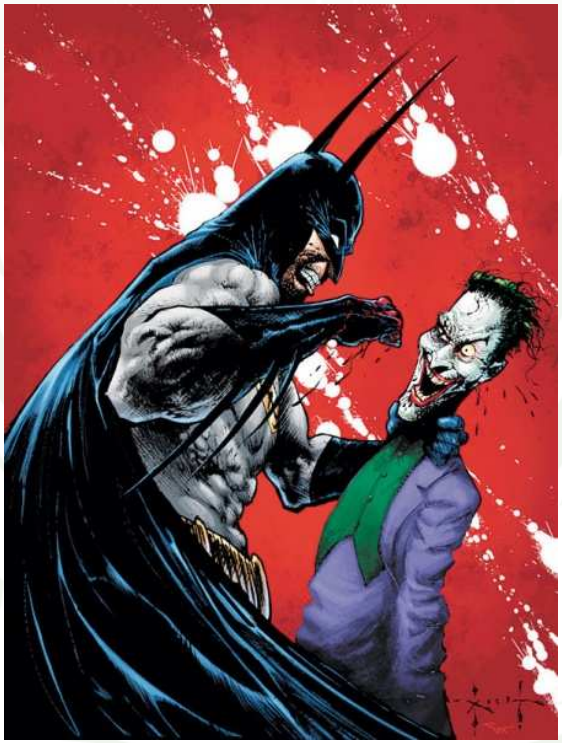
- New requirements may involve only process configuration changes
- Services may support multiple contracts
- New requirement may require new contract
- Policy drives version selection & deprecation



Service consumers must support versioning policies

Business Empowerment vs. IT Control

- IT management requires control
  - How to scale management control & avoid micromanagement?
- IT charged with empowering users
  - How to avoid policy breaches?
- Centralization of IT capabilities running into roadblocks
  - How to decentralize IT responsibility without leading to redundant or incompatible capabilities?



Governance essential for business empowerment

Governance: The Key to Business Empowerment

- Governance: creating, communicating, & enforcing policies
- SOA enables the formalization of policies as metadata

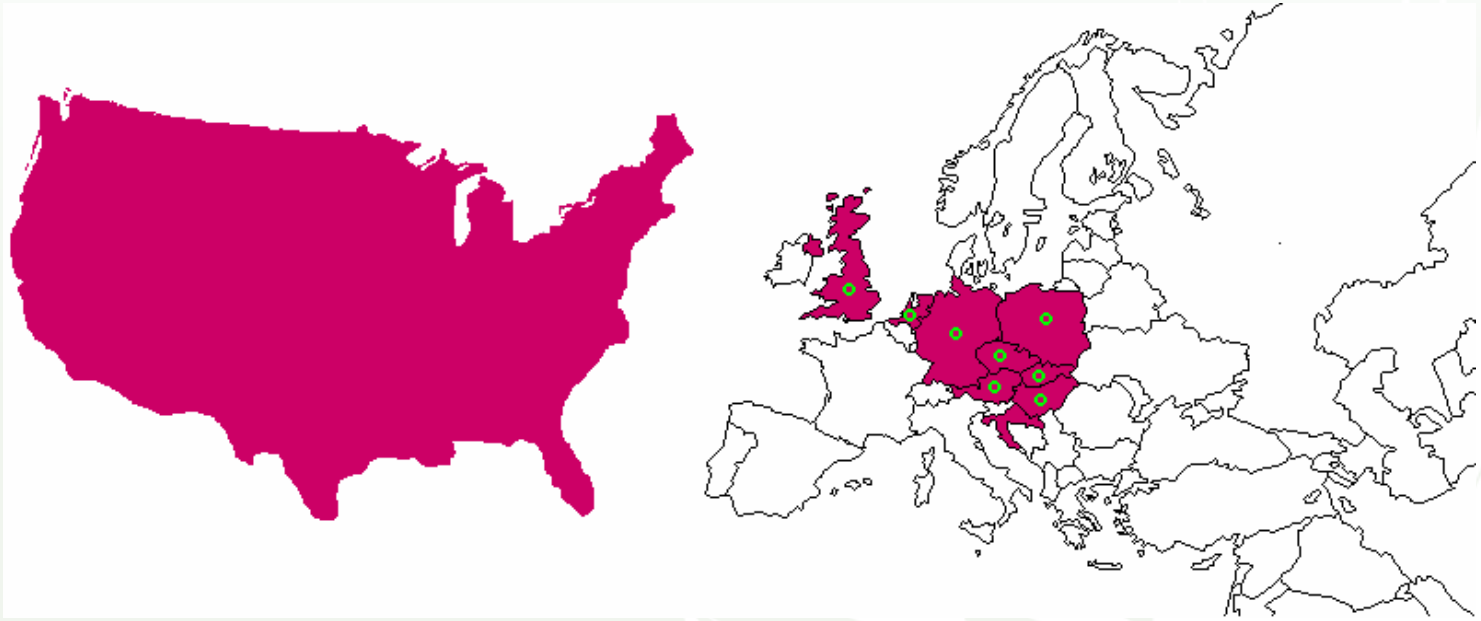
Practical SOA requires Governance
And
Effective Governance Requires SOA

Case Study: SOA Project Management & Governance at T-Mobile

Presented at ZapThink's

Practical SOA: Frankfurt, January 15, 2008

T-Mobile: A Worldwide Mobile Phone & Data Carrier



- T-Mobile Footprint:
  - ~ 110M subscribers in total, ~ 83M in Europe
  - Revenue close to 35 Billion Euro
  - Extremely competitive market

Why SOA?

Challenges	Requirements
Increasing efforts for maintenance decreasing capacity for innovation	■ Reduce effort and cost of maintenance ■ Reduce effort and cost of testing
Heterogeneous IT Landscape in TMO Countries	■ Harmonize technology, processes and architecture ■ Move to model-driven approaches
Lack of business flexibility Low reuse of business logic	■ Simplify Service use and re-use ■ Shorten release cycles
Integration of common business functions and additional LoBs	■ Better and easier integration of 3rd party / COTS components ■ Incorporate industry standards

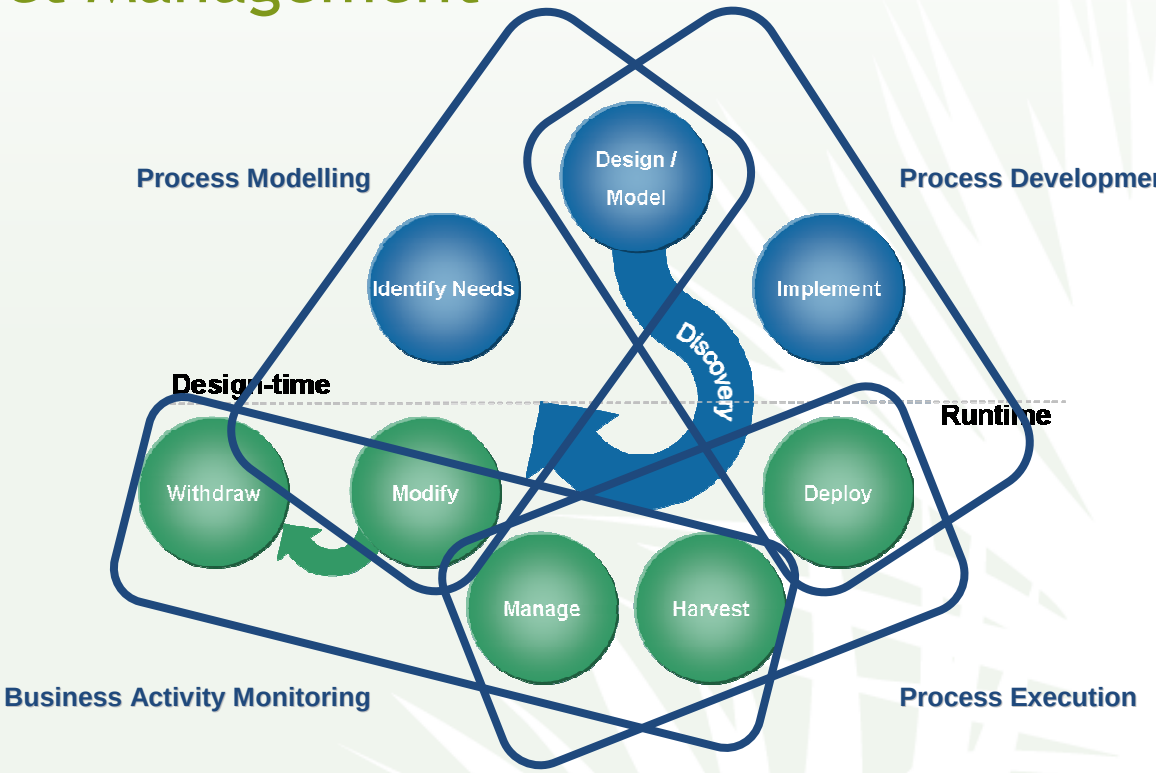
Strategy: Unify SOA & BPM Approaches

- **T-Mobile SOA Efforts**
  - Enables creation, composition and governance of loosely coupled business Services
  - Supports IT to manage complexity while connecting people, processes and systems
  - Provides a layer of control and governance over BPM efforts

- **T-Mobile BPM Efforts**
  - Enables creation, execution and optimization of business processes
  - Allows continuous improvement of business processes driven by line of business
  - SOA simplifies BPM implementations significantly

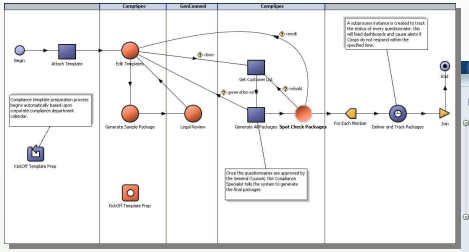
For T-Mobile, BPM approach is a way to build composite SOA applications

T-Mobile SOA/BPM Iterative Project Management

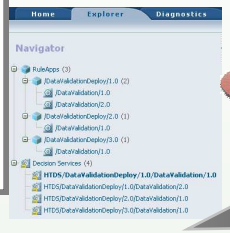


The Iterative SOA Lifecycle: Detail

Process Modeling



Process Modeling, Simulation and Documentation

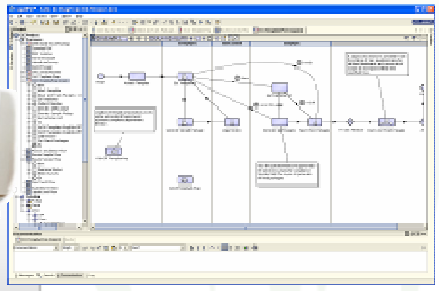


Business Rules Definition

Business Analysts

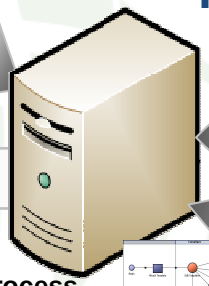
Solution Architect

Process Development

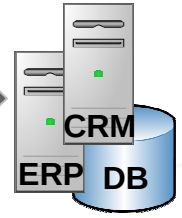


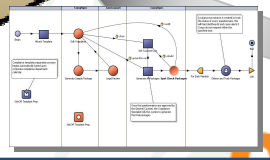
Process Development and Solution Definition

Process Execution

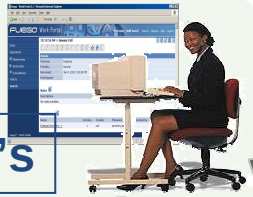


Process Server and Monitoring Repository



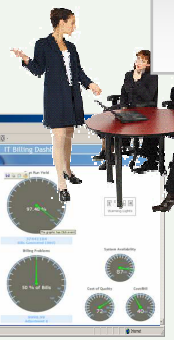


Process Participants

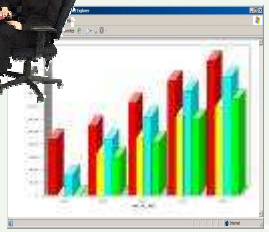


Business KPI's

Business Owners



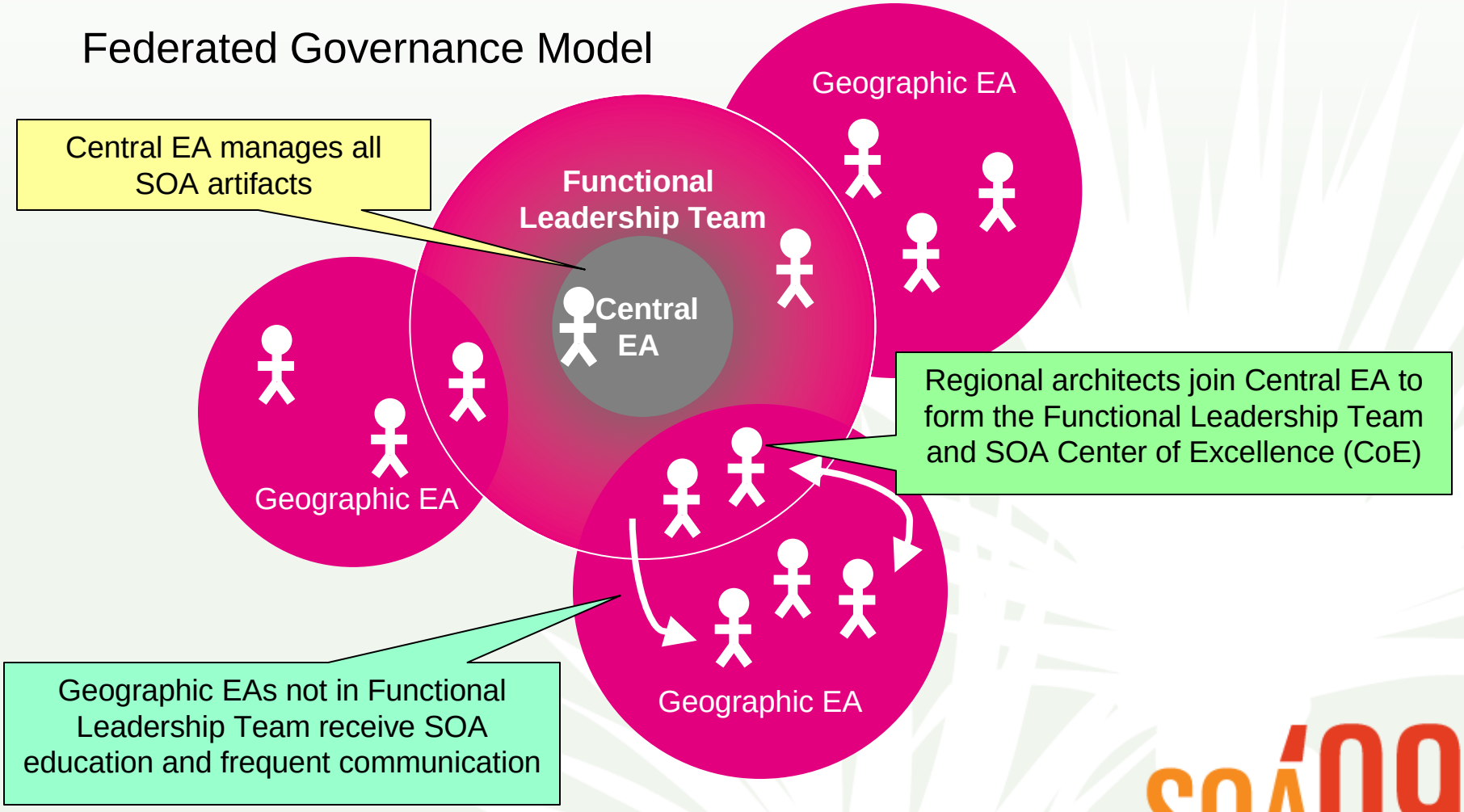
Process Management and Real-Time BAM



Historical & Trend Analysis

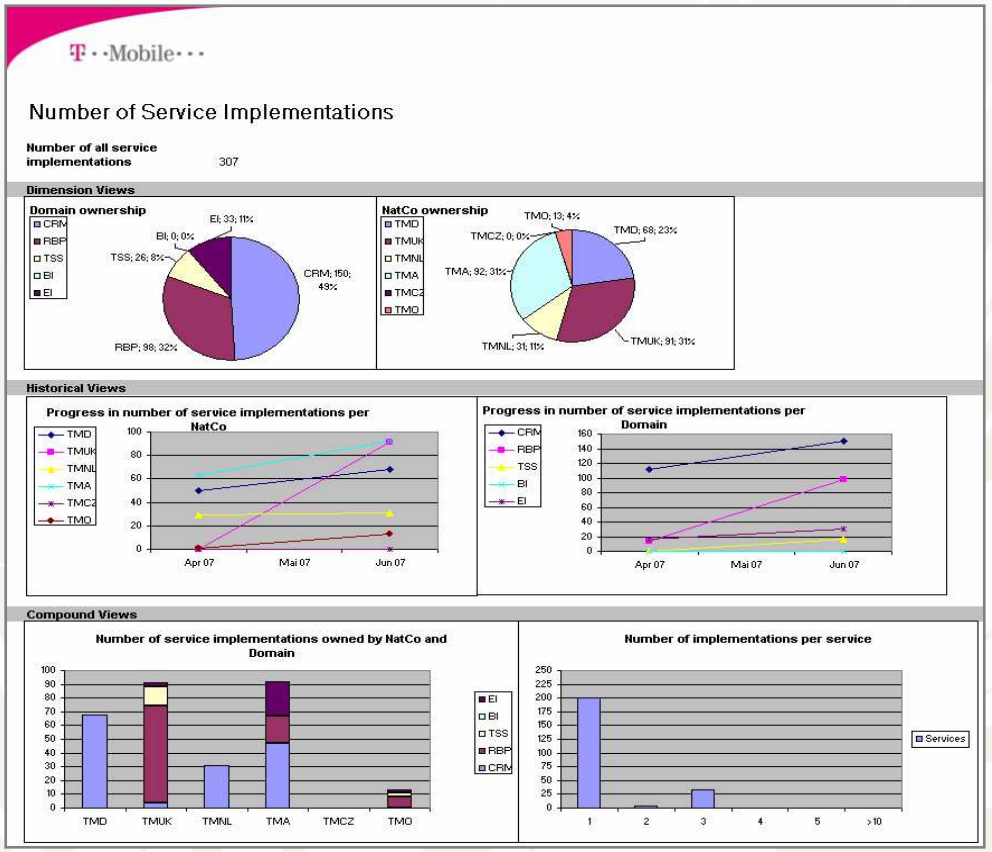
T-Mobile: Organizational Approach to Governance

Federated Governance Model



SOA Dashboard helps to govern SOA

- Leverages central Repository to measure SOA progress
- KPIs are defined and used to steer SOA development
- Architectural design and service portfolio is actively influenced
- Focus on SOA objectives such as “Reuse” and “Harmonize”
  are steered rather than staying wishful thinking



Findings and Lessons Learned

- Actual Results (July 07):
  - Reduced redundancy by 13%
  - Increased # of deployed Services / applications by 47%
  - Service usage increased by 39%
  - Amount of reused services: 34%

- Lessons Learned
  - You won't get to SOA Governance without a working IT Governance.
  - SOA Governance is one aspect in a holistic Enterprise Architecture Management
  - Introduce and enforce technical standards as early as possible.
  - Neither believe in miracles nor rely on consultants entirely.
  - There is no one-size-fits-all approach.
  - You will need to undertake massive activities to get buy-in from business.
  - Don't go for "Lowest Common Denominator (LCD)" compromise.
  - You can't avoid friction in your enterprise totally.
  - Prepare for a "long distance run".

ZapThink is an industry advisory & analysis firm focused exclusively on SOA, EA, and Enterprise 2.0.

Register for an upcoming *Licensed ZapThink Architect* course and obtain your LZA Credential!

Thank You!

Jason Bloomberg

jbloomberg@zapthink.com

Ronald Schmelzer

rschmelzer@zapthink.com