Architecture Plus Symposium
October 7, 2008

*Bringing the Enterprise Architecture, Security, and Privacy Communities Together*

Dr. Scott Bernard
Deputy CIO, Chief Architect, ISSO
Federal Railroad Administration
U.S. Department of Transportation
scott.bernard@dot.gov
Recent EA Writing Projects

February 2009

Coherency Management
Architecting the Enterprise for Alignment, Agility, and Assurance

Gary Doucet, John Getze, Pallab Saha and Scott Bernard
Foreword by John Zachman

Quarterly

Journal of Enterprise Architecture
February 2008 | Volume 4, Number 1

Feature
Architect’s Spotlight: Mike Lowe 4

Articles
Framework Standards – What’s it all About? 7
John Zachman

The Organization’s Compass - Enterprise Architecture 11
Sion Eng Khai Lim, Von On Chin, Pooy See-Heng, and Chong Chai-Fing

A Goal-Oriented Way to Define Metrics for an Enterprise Architecture Program 20
Niina Hämäläinen and Tommi Kärkkäinen

Integrating Enterprise Architecture and IT Portfolio Management Processes 27
George Makian

Case Study
Enterprise Architecture and IT Governance Considerations for Mergers and Acquisitions in Integrating Sarbanes-Oxley Granite Downs 41

A quarterly publication of the Association of Enterprise Architects
An Educational Forum for Enterprise Architects

www. enterprisean .org

Summer 2009

EA³
An Introduction to Enterprise Architecture
Third Edition
Scott A. Bernard
Updating the FEA SPP

The Federal Enterprise Architecture – Security and Privacy Profile (FEA-SPP) was developed by the Office of Management and Budget and the Federal CIO Council to provide best practices and recommendations that promote the successful incorporation of information security and privacy into an organization’s enterprise architecture and to ensure appropriate consideration of security and privacy requirements in agencies’ strategic planning and investment decision processes. FEA-SPP v2.0 was published in June 2006.

FEA-SPP v3.0 is in development to be ‘embedded guidance’ on security and privacy controls in the FSAM and in NIST SP-800-37, 39, and 53. There is also an assessment tool in work.
The FEA asks Federal agencies to look at their operations from common business, performance, service, technology, and data views; which are incorporated into Reference Models. The FEA-SPP works within and across all five of the FEA Reference Model areas to identify enterprise, segment, and system level security / privacy requirements and solutions.
Information Security and Data Privacy Framework

- Federal Enterprise Architecture
- Performance Architecture (PRM)
- Business Architecture (BRM)
- Service Component Architecture (SRM)
- Data/Information Architecture (DRM)
- Technology Architecture (TRM)

Enterprise Architecture Guidance and Supporting Documentation

Enterprise Level “Common Controls” for Security/Privacy

- Segment Level Controls
- Solution / System Level Controls

Governance Process

Lifecycle Development & Maintenance Process

NIST Risk Mgmt. Framework
- Security / Privacy Control Development
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor
The Risk Management Framework

**Starting Point**

- **CATEGORIZE Information System**
  Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

- **SELECT Security Controls**
  Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

- **IMPLEMENT Security Controls**
  Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

- **ASSESS Security Controls**
  Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

- **AUTHORIZE Information System**
  Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

- **MONITOR Security State**
  Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
The FEA and the RMF Working Together

RISK EXECUTIVE FUNCTION
Enterprise-wide Oversight, Monitoring, and Risk Management

Architecture Description
- Architecture Reference Models
- Segment and Solution Architectures
- Mission and Business Processes
- Information System Boundaries

Organizational Inputs
- Laws, Directives, Policy Guidance
- Strategic Goals and Objectives
- Priorities and Resource Availability
- Supply Chain Considerations

RMF
RISK MANAGEMENT FRAMEWORK

Common Security Controls
(Inherited by Information Systems)
Questions ?