OSA Open Security Architecture

OWASP Switzerland Chapter Meeting
April 2009

OpenSecurityArchitecture.org

The OSA vision:

"OSA distills the know-how of the security architecture community and provides readily usable patterns for your application. OSA shall be a free framework that is developed and owned by the community.”

OSA approach is to bring clarity through visualization

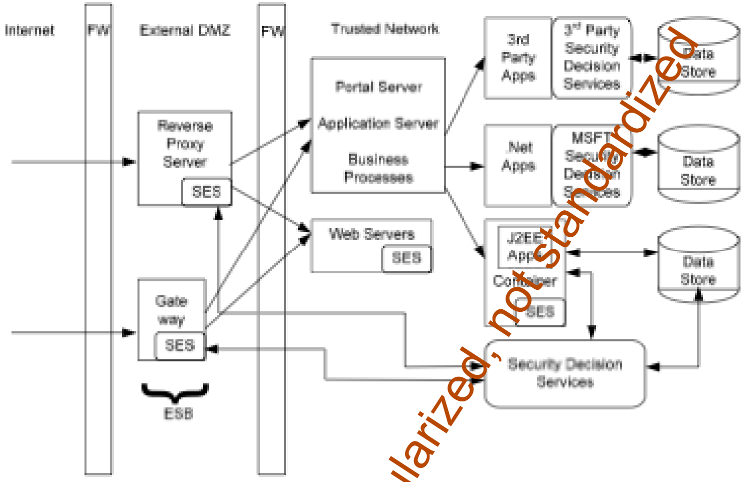


Figure 8: Gateway Based Migration to Infrastructure Managed Security

CP-5 **CONTINGENCY PLAN UPDATE**

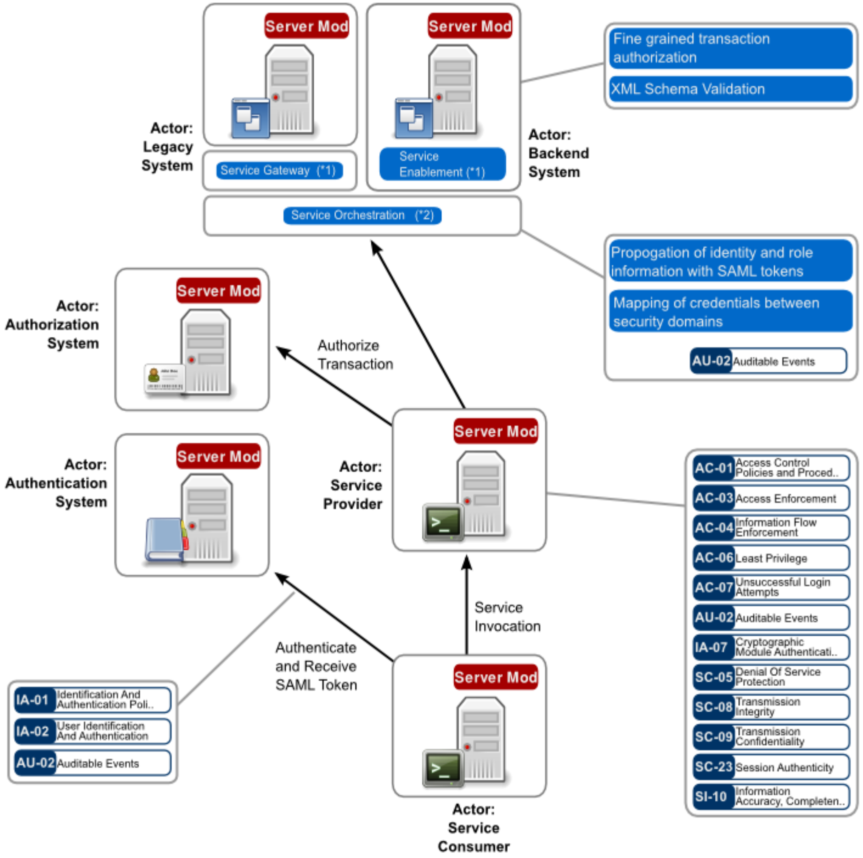
Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Control Enhancements: None.

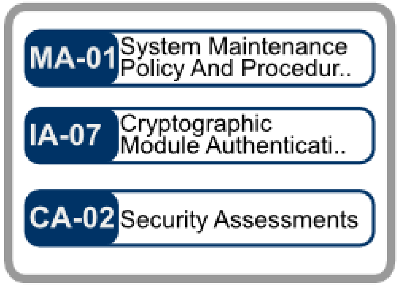
LOW CP-5	MOD CP-5	HIGH CP-5

Not coherent, not modularized, not standardized


Server Mod
Server Mod
Actor: Legacy System
Service Gateway (*1)
Service Enablement (*1)
Actor: Backend System
Service Orchestration (*2)
Fine grained transaction authorization
XML Schema Validation
Propogation of identity and role information with SAML tokens
Mapping of credentials between security domains
AU-02 Auditable Events
Actor: Authorization System
Server Mod
Authorize Transaction
Actor: Authentication System
Server Mod
Actor: Service Provider
Server Mod
Service Invocation
Authenticate and Receive SAML Token
Server Mod
Actor: Service Consumer
IA-01 Identification And Authentication Poli..
IA-02 User Identification And Authentication
AU-02 Auditable Events
AC-01 Access Control Policies and Proced..
AC-03 Access Enforcement
AC-04 Information Flow Enforcement
AC-06 Least Privilege
AC-07 Unsuccessful Login Attempts
AU-02 Auditable Events
IA-07 Cryptographic Module Authenticati..
SC-05 Denial Of Service Protection
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality
SC-23 Session Authenticity
SI-10 Information Accuracy, Completen..

08.02.19_Pattern_005_SOA_Internal_Usage.svg

How is OSA used?



MA-01 System Maintenance Policy And Procedur..

IA-07 Cryptographic Module Authenticati..

CA-02 Security Assessments

1) Agree baseline

Controls are mapped against governance best practice, security standards, laws and regulations

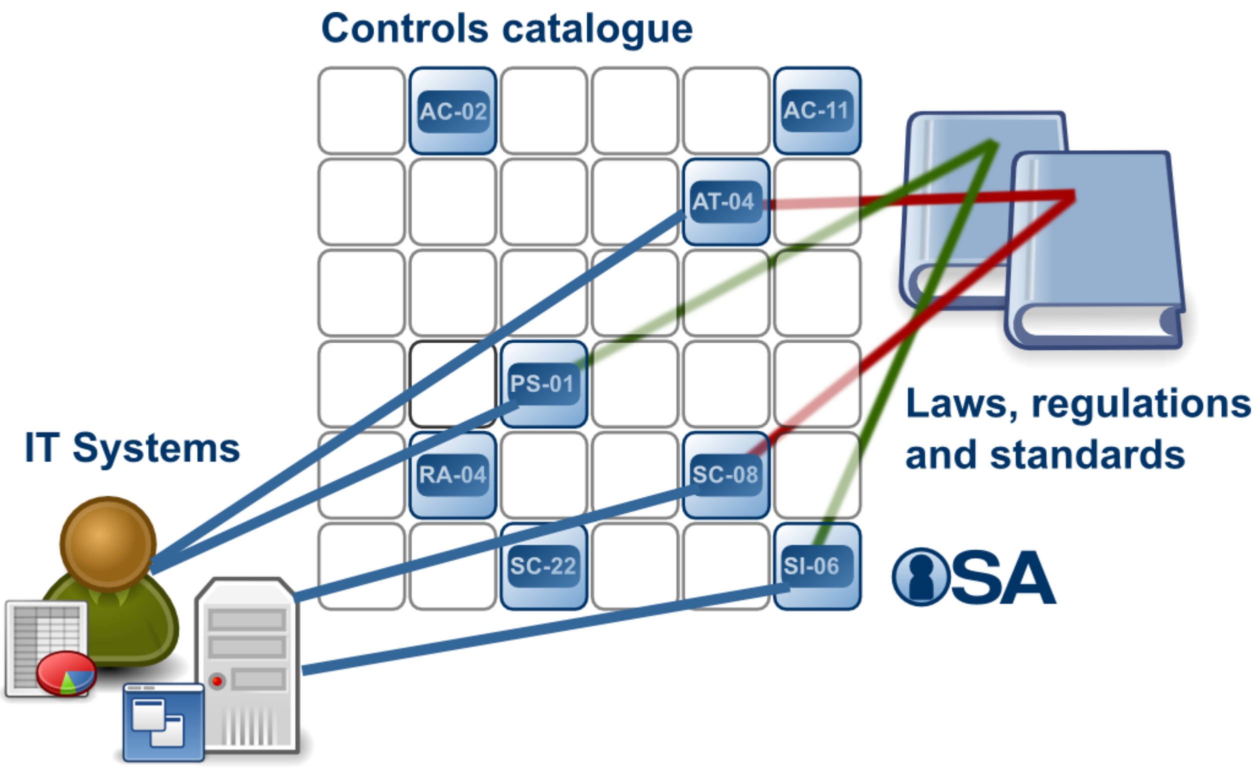
2) Choose Patterns

Patterns are generated for common security needs encountered in Industry verticals like Finance, Manufacturing and IT.

3) Optimise design

Architecture is optimised for the environment it will operate in.

A control catalog helps us understand business requirements



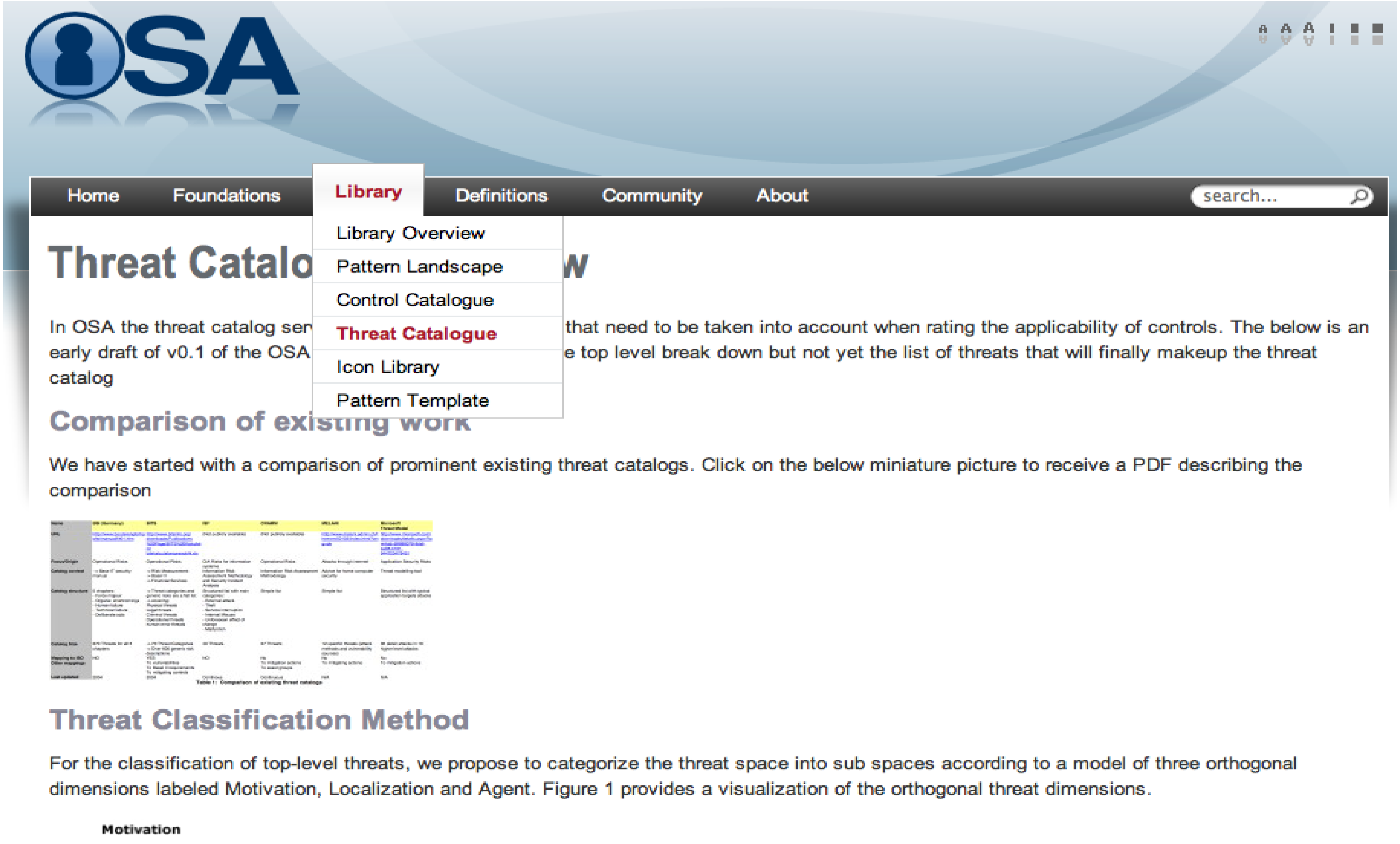
OSA serves corporate architects, auditors, and education

Security Architect:
- Wide coverage
- Hot topics
- No BS
- Vendor neutral

Auditors:
- Control Catalog
- ISO/Cobit Mapping
- Risk based approach

Teaching:
- Foundations
- Visual patterns

OSA provides several coherent libraries



Threat Catalo w

In OSA the threat catalog ser that need to be taken into account when rating the applicability of controls. The below is an early draft of v0.1 of the OSA e top level break down but not yet the list of threats that will finally makeup the threat catalog

Comparison of existing work

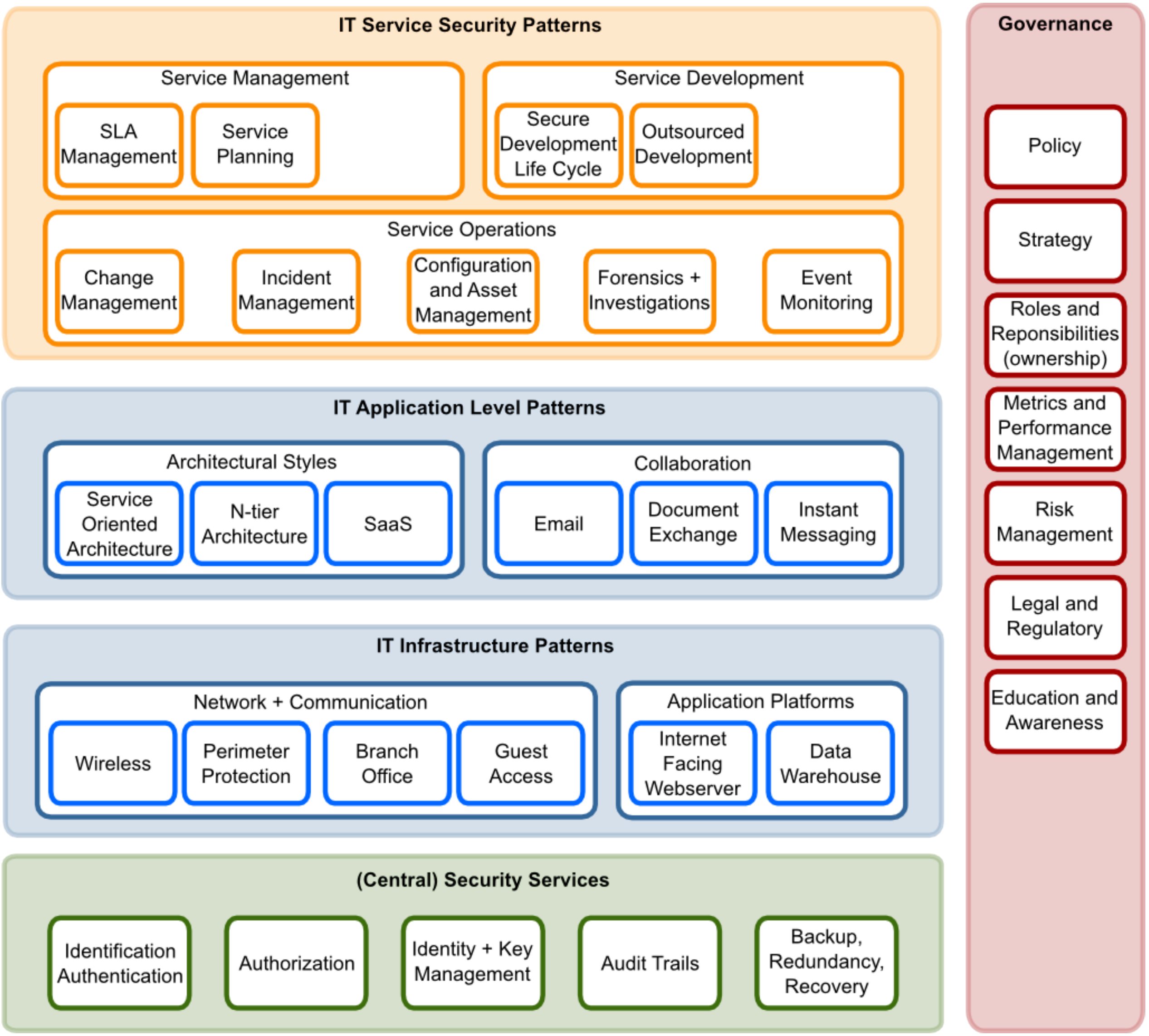
We have started with a comparison of prominent existing threat catalogs. Click on the below miniature picture to receive a PDF describing the comparison

Threat Classification Method

For the classification of top-level threats, we propose to categorize the threat space into sub spaces according to a model of three orthogonal dimensions labeled Motivation, Localization and Agent. Figure 1 provides a visualization of the orthogonal threat dimensions.

Motivation

OSA comes with taxonomy, landscape and foundational articles



IT Service Security Patterns

- Service Management
  - SLA Management
  - Service Planning
- Service Development
  - Secure Development Life Cycle
  - Outsourced Development
- Service Operations
  - Change Management
  - Incident Management
  - Configuration and Asset Management
  - Forensics + Investigations
  - Event Monitoring

IT Application Level Patterns

- Architectural Styles
  - Service Oriented Architecture
  - N-tier Architecture
  - SaaS
- Collaboration
  - Email
  - Document Exchange
  - Instant Messaging

IT Infrastructure Patterns

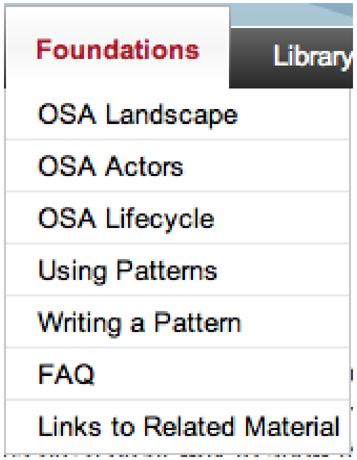
- Network + Communication
  - Wireless
  - Perimeter Protection
  - Branch Office
  - Guest Access
- Application Platforms
  - Internet Facing Webserver
  - Data Warehouse

(Central) Security Services

- Identification Authentication
- Authorization
- Identity + Key Management
- Audit Trails
- Backup, Redundancy, Recovery

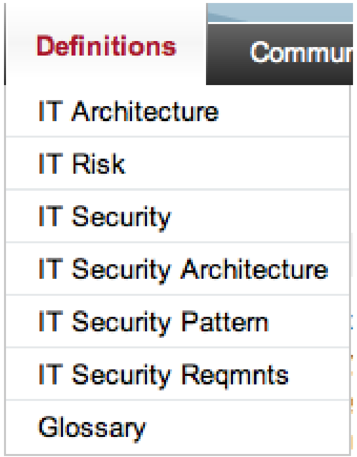
Governance

- Policy
- Strategy
- Roles and Reponsibilities (ownership)
- Metrics and Performance Management
- Risk Management
- Legal and Regulatory
- Education and Awareness



Foundations | Library

- OSA Landscape
- OSA Actors
- OSA Lifecycle
- Using Patterns
- Writing a Pattern
- FAQ
- Links to Related Material



Definitions | Commun

- IT Architecture
- IT Risk
- IT Security
- IT Security Architecture
- IT Security Pattern
- IT Security Reqmnts
- Glossary

10 Patterns Currently Available

- Cloud Computing
- Identity Management
- Privacy Mobile Device
- Public Web Server
- SOA Internal Service
- SOA Publication and Location
- Wireless- “private secure network” and “Using a public hotspot”

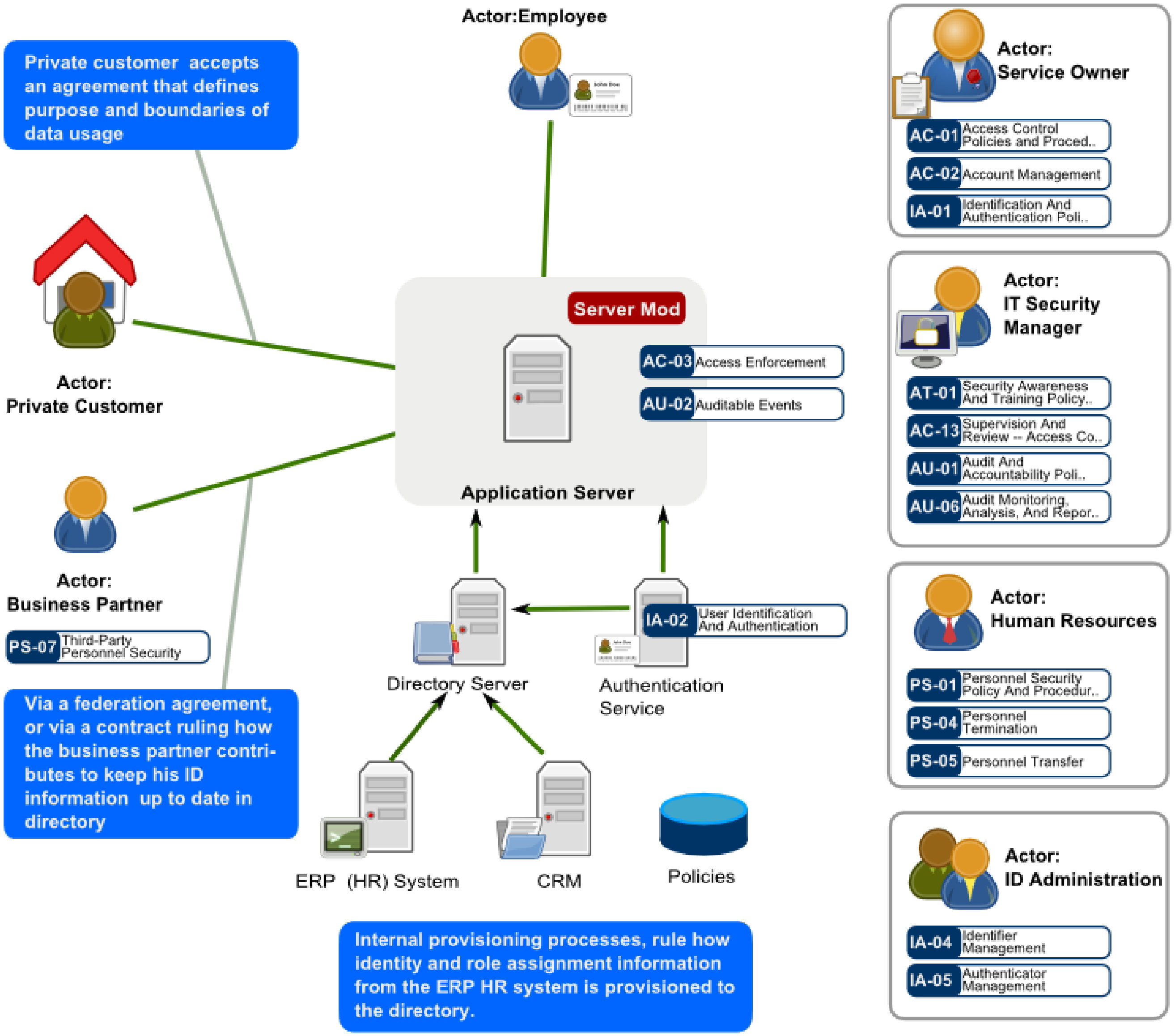
Modules:

- Client
- Server

Upcoming:

- Secure SDLC
- Data Security

Pattern Example: Identity Mgmt



Actor:Employee
Actor:
Service Owner
AC-01 Access Control Policies and Proced..
AC-02 Account Management
IA-01 Identification And Authentication Poli..
Actor:
Private Customer
Server Mod
AC-03 Access Enforcement
AU-02 Auditable Events
Application Server
Actor:
IT Security Manager
AT-01 Security Awareness And Training Policy..
AC-13 Supervision And Review -- Access Co..
AU-01 Audit And Accountability Poli..
AU-06 Audit Monitoring, Analysis, And Repor..
Actor:
Business Partner
PS-07 Third-Party Personnel Security
Directory Server
IA-02 User Identification And Authentication
Authentication Service
Actor:
Human Resources
PS-01 Personnel Security Policy And Procedur..
PS-04 Personnel Termination
PS-05 Personnel Transfer
ERP (HR) System
CRM
Policies
Actor:
ID Administration
IA-04 Identifier Management
IA-05 Authenticator Management

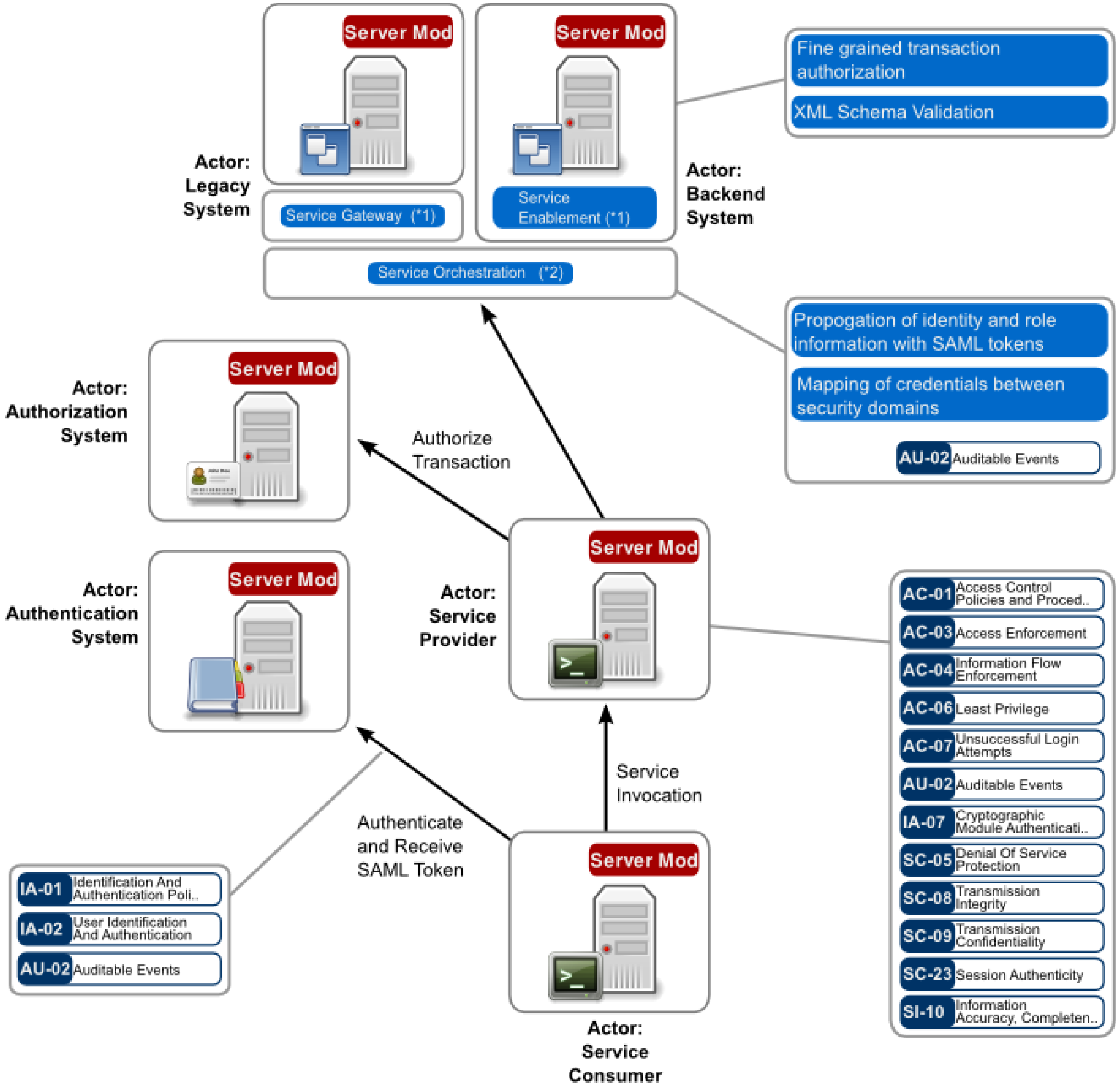
Private customer accepts an agreement that defines purpose and boundaries of data usage

Via a federation agreement, or via a contract ruling how the business partner contributes to keep his ID information up to date in directory

Internal provisioning processes, rule how identity and role assignment information from the ERP HR system is provisioned to the directory.

Pattern: 08_02_Pattern_010_31_Identity_Management.svg

Pattern example: SOA security


Server Mod
Server Mod
Fine grained transaction authorization
XML Schema Validation
Actor: Legacy System
Service Gateway (*1)
Service Enablement (*1)
Actor: Backend System
Service Orchestration (*2)
Propogation of identity and role information with SAML tokens
Mapping of credentials between security domains
AU-02 Auditable Events
Server Mod
Actor: Authorization System
Authorize Transaction
Server Mod
Actor: Authentication System
Actor: Service Provider
Server Mod
AC-01 Access Control Policies and Proced..
AC-03 Access Enforcement
AC-04 Information Flow Enforcement
AC-06 Least Privilege
AC-07 Unsuccessful Login Attempts
AU-02 Auditable Events
IA-07 Cryptographic Module Authenticati..
SC-05 Denial Of Service Protection
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality
SC-23 Session Authenticity
SI-10 Information Accuracy, Completen..
Service Invocation
Authenticate and Receive SAML Token
Server Mod
IA-01 Identification And Authentication Poli..
IA-02 User Identification And Authentication
AU-02 Auditable Events
Actor: Service Consumer

08.02.19_Pattern_005_SOA_Internal_Usage.svg

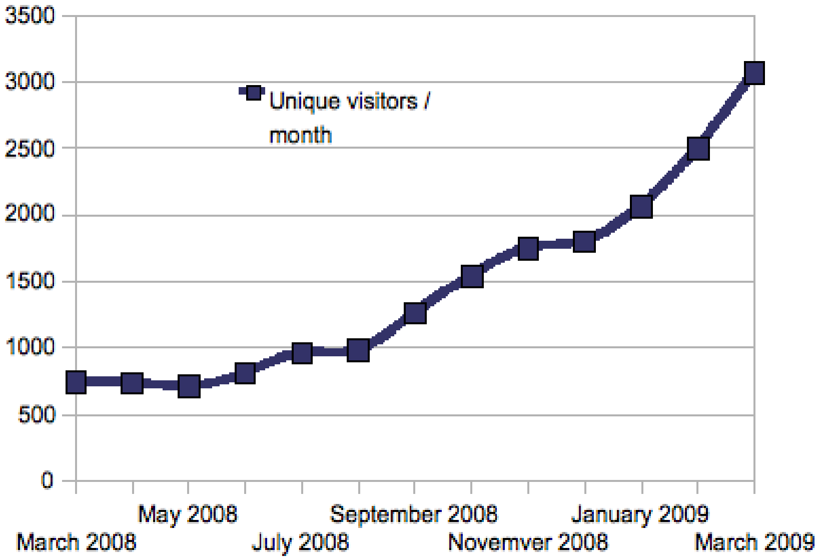
Currently Under Development: SDLC

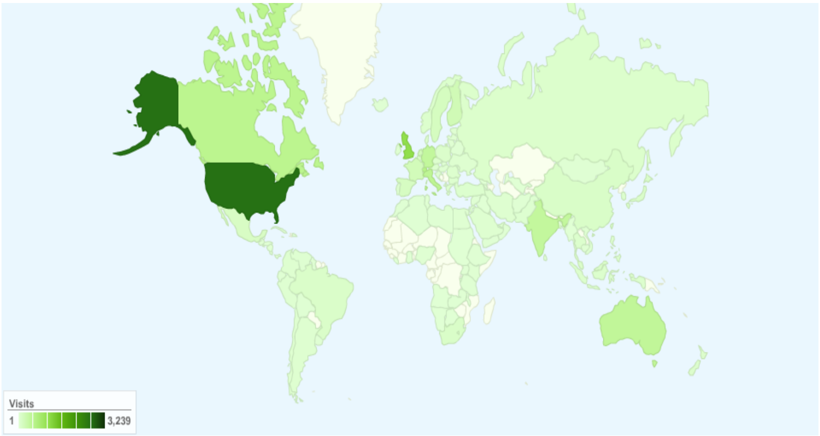
OSA SDLC: Core controls for secure solution development

Roles	Training	Requirement	Design	Implementation	Verification	Release	Response
Business application Owner	Business process Essentials	Strategic risk analysis Privacy policy	Role and permission design			Residual solution risk acceptance	Service Level Management
Service manager		SLA definition				Residual service risk acceptance	SLA monitoring
Project manager		Project risk analysis				Hand over risk sheets to service manager	
Analyst		Solution risk analysis	Abuse case definitions	Analysis of coverage of automated tests			
SW and Infrastructure Architect		Technology risk analysis	Capacity planning Disaster recovery Planning		Verify SLA fulfillment capabilities		
SW Engineering		Technology prototyping		Code review Static source analysis	Verify abuse cases		
QA Engineering	Process framwork	Define quality gates			Automated black box and white box testing	Verify claimed security attributes and sign-off release	
Security Specialist	Secure development Principles Security policy	Security requirements elicitation Attack surface identification Define trust boundaries	Security design review Threat modelling		Penetration testing	Response plans as part of operational security guide	Security Incident Management
Operations							Change Management (incl. Vulnerability Management) Continuos Monitoring

Definitions:	Solution risk	A risk posed by the deployed solution to the business that it serves or to other stake holders
	Project risk	A risk that threatens the goal of the project (which is put in place to develop the solution)
	Penetration testing	A manual testing process that requires knowledge of potential vulnerabilities

A fast growing community effort





- 5-10 new patterns per year.
- More than 300 registered members
- More than 3000 unique visitors per month
- Most visitors from US and EU

Take home message:

- OSA is a consistent foundation
- OSA helps you to get up to speed quickly
- You can help make it better :-)