UC EABok - Security Principles and Standards Review

Bo Pitsker, UCOP
Enterprise Security Architect
Bo.Pitsker@ucop.edu

July 12, 2016

Agenda

- Meeting objectives
- Presenter background
- Enterprise architecture intro
- Enterprise security architecture
- ITLC, ITAC and the OP EA team
- ITAC EaBok artifact structure and function
- Security artifact overview
- EA staff and resources for security
- Concluding remarks
- Q & A

Objectives for today’s presentation

- Introduce Enterprise Architecture (EA)
- Relate “Enterprise Architecture” to “Security Architecture”
- Introduce enterprise security frameworks
- Describe UC’s Enterprise Architecture Book of Knowledge (EABok) and its usage
- Motivate the use of UC EA security resources

Who are we?

- ITAC (the team formerly known as ITAG)
  – Information Technology Architecture Committee
  – A standing committee of ITLC
  – Campus representatives, appointed by local CIOs, responsible for creation and adoption of EA artifacts
- Enterprise Architecture group at OP
  – Formally part of OP ITS Strategic Planning organization
  – Architectural domains supported include business architecture, application architecture, data architecture, technology architecture, and security architecture
  – Supports ITAC, participates in Systemwide initiatives

Who am I?

- Enterprise Security Architect at OP for 2 years
- Involved with product security and services at Polycom
- Responsible for networking and security at San Francisco International Airport (SFO)
- Provided classified services at Lawrence Livermore National Laboratory (LLNL)
- Provided 1st managed security services and secure hosting at Pilot Network Services

What is “Enterprise Architecture”?

“An EA is a conceptual blueprint that defines the structure and operation of an organisation. Just as architecture provides a blueprint for constructing a building, Enterprise Architecture provides a blueprint and roadmap for aligning business strategy with IT. The aim of an Enterprise Architecture is to support the determination of how an organisation can most effectively achieve its current and future objectives. The Enterprise Architecture provides a guide to direct the evolution and transformation of enterprises with technology.”

Frameworks for enterprise architecture

- What is a framework?

“A structure for organizing information that defines the scope of the architecture (what the EA program will document) and how the areas of the architecture relate to each other.”

- TOGAF – The Open Group
- Zachman Framework – John Zachman

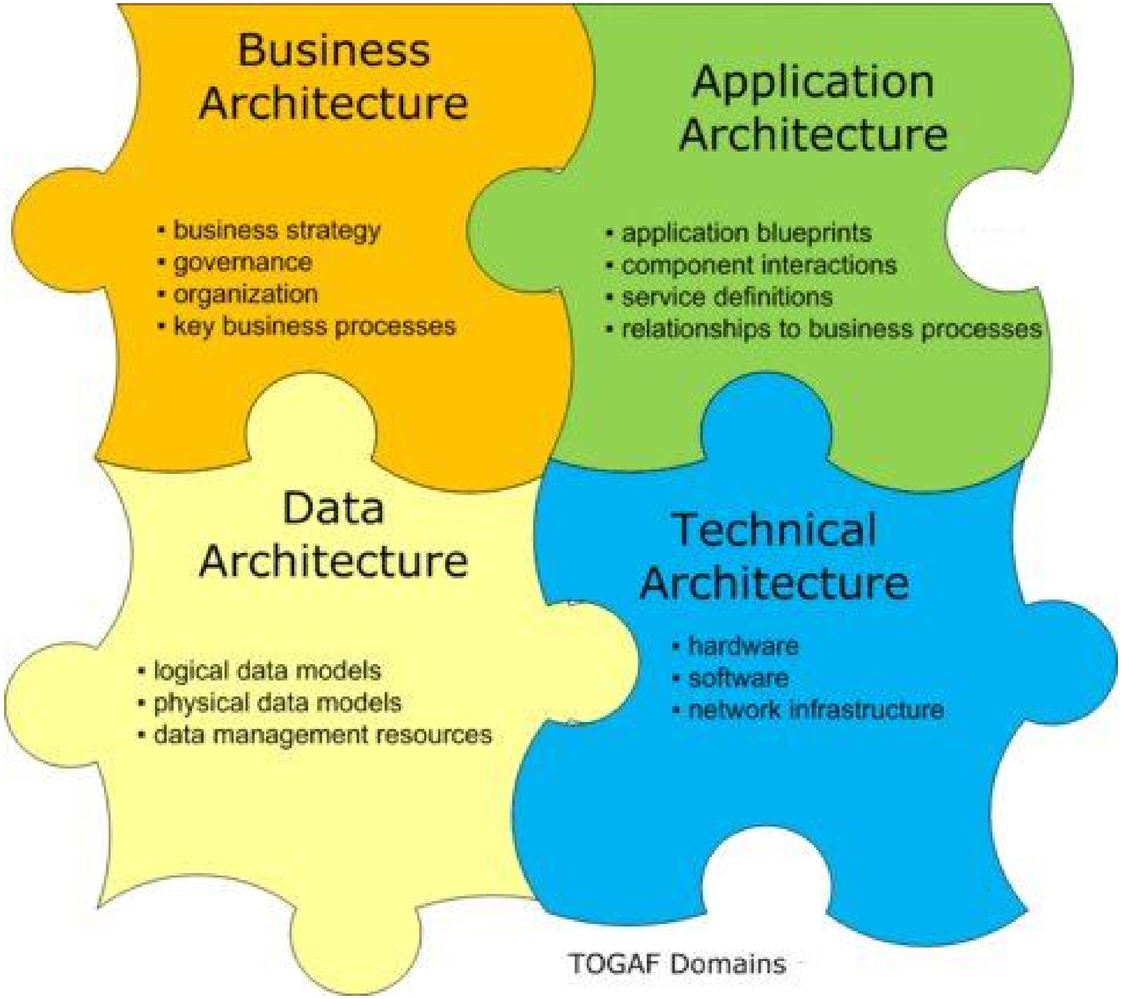
TOGAF

- What is TOGAF?

“The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture. TOGAF is a high level approach to design. It is typically modeled at four levels: Business, Application, Data, and Technology. It relies heavily on modularization, standardization, and already existing, proven technologies and products.”

- Principally process oriented
- Model-driven

TOGAF architectural domains



Business Architecture

- business strategy
- governance
- organization
- key business processes

Application Architecture

- application blueprints
- component interactions
- service definitions
- relationships to business processes

Data Architecture

- logical data models
- physical data models
- data management resources

Technical Architecture

- hardware
- software
- network infrastructure

TOGAF Domains

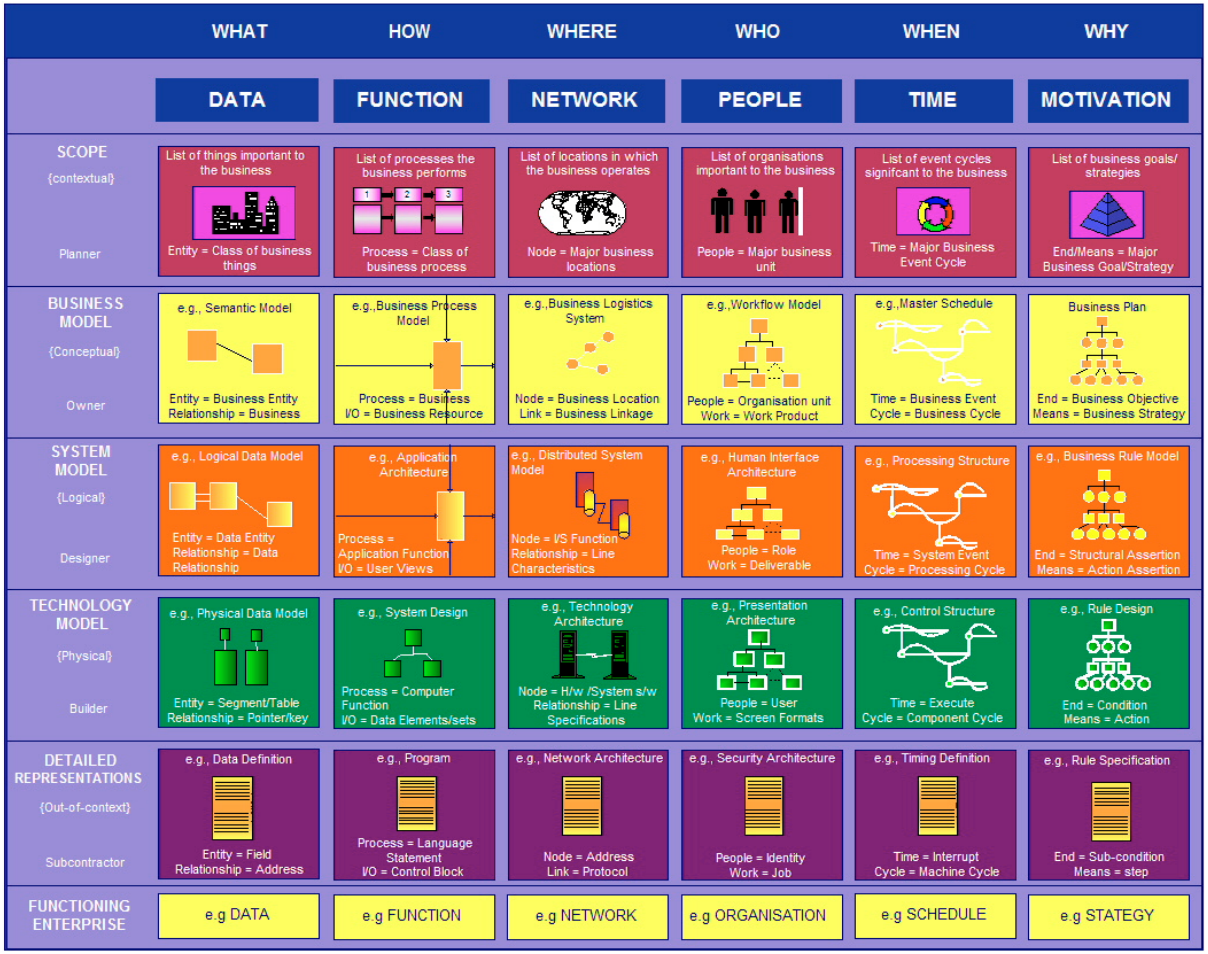
The Zachman Framework

- What is the Zachman Framework?

"The Zachman Framework is an enterprise ontology and is a fundamental structure for Enterprise Architecture which provides a formal and structured way of viewing and defining an enterprise."

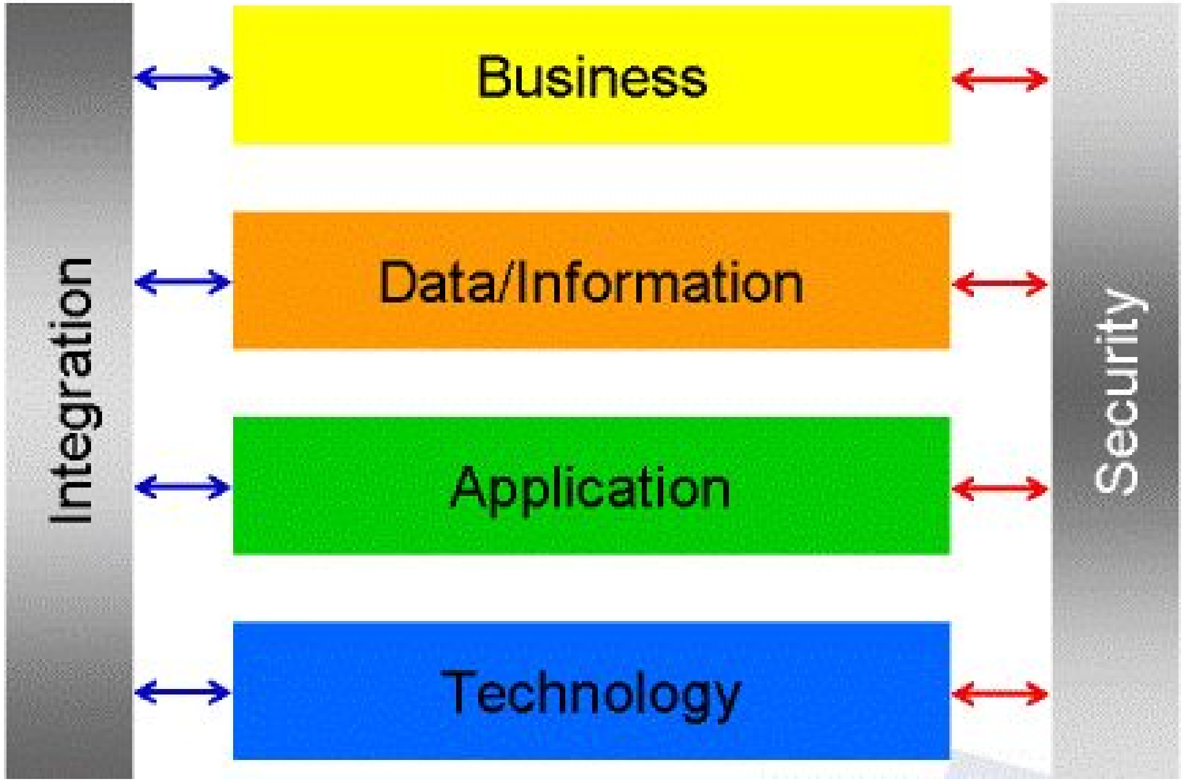
- It's not a framework, the title notwithstanding
- Zachman uses a 6 x 6 matrix to classify architectural artifacts, audiences, and models
- Zachman and TOGAF are complementary, not competitive

The Zachman matrix

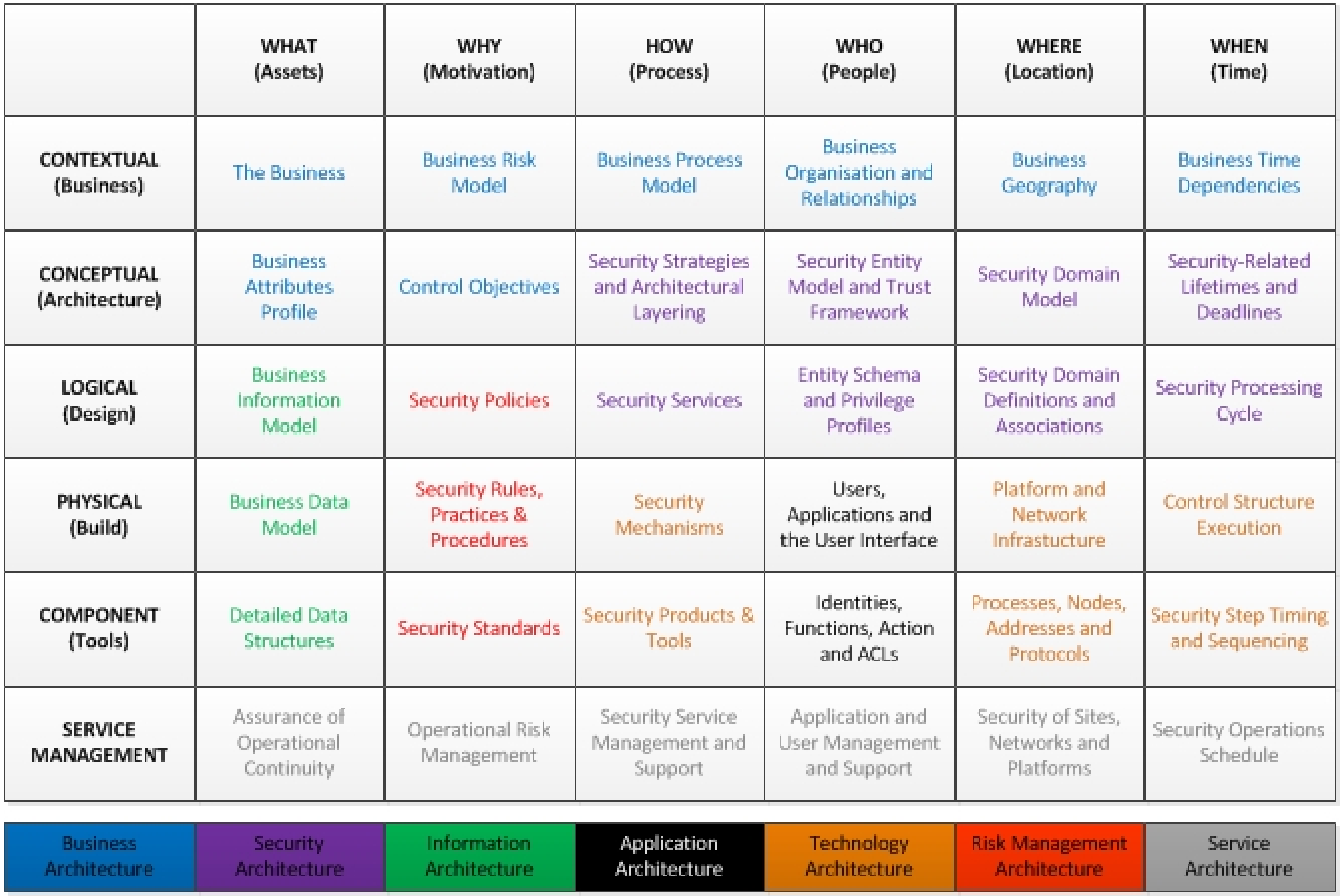


	WHAT	HOW	WHERE	WHO	WHEN	WHY
	DATA	FUNCTION	NETWORK	PEOPLE	TIME	MOTIVATION
SCOPE {contextual} Planner	List of things important to the business Entity = Class of business things	List of processes the business performs Process = Class of business process	List of locations in which the business operates Node = Major business locations	List of organisations important to the business People = Major business unit	List of event cycles signifcant to the business Time = Major Business Event Cycle	List of business goals/ strategies End/Means = Major Business Goal/Strategy
BUSINESS MODEL {Conceptual} Owner	e.g., Semantic Model Entity = Business Entity Relationship = Business	e.g.,Business Process Model Process = Business I/O = Business Resource	e.g.,Business Logistics System Node = Business Location Link = Business Linkage	e.g.,Workflow Model People = Organisation unit Work = Work Product	e.g.,Master Schedule Time = Business Event Cycle = Business Cycle	Business Plan End = Business Objective Means = Business Strategy
SYSTEM MODEL {Logical} Designer	e.g., Logical Data Model Entity = Data Entity Relationship = Data Relationship	e.g., Application Architecture Process = Application Function I/O = User Views	e.g., Distributed System Model Node = I/S Function Relationship = Line Characteristics	e.g., Human Interface Architecture People = Role Work = Deliverable	e.g., Processing Structure Time = System Event Cycle = Processing Cycle	e.g., Business Rule Model End = Structural Assertion Means = Action Assertion
TECHNOLOGY MODEL {Physical} Builder	e.g., Physical Data Model Entity = Segment/Table Relationship = Pointer/key	e.g., System Design Process = Computer Function I/O = Data Elements/sets	e.g., Technology Architecture Node = H/w /System s/w Relationship = Line Specifications	e.g., Presentation Architecture People = User Work = Screen Formats	e.g., Control Structure Time = Execute Cycle = Component Cycle	e.g., Rule Design End = Condition Means = Action
DETAILED REPRESENTATIONS {Out-of-context} Subcontractor	e.g., Data Definition Entity = Field Relationship = Address	e.g., Program Process = Language Statement I/O = Control Block	e.g., Network Architecture Node = Address Link = Protocol	e.g., Security Architecture People = Identity Work = Job	e.g., Timing Definition Time = Interrupt Cycle = Machine Cycle	e.g., Rule Specification End = Sub-condition Means = step
FUNCTIONING ENTERPRISE	e.g DATA	e.g FUNCTION	e.g NETWORK	e.g ORGANISATION	e.g SCHEDULE	e.g STATEGY

So where is the security architecture?



SABSA builds on Zachman *and* TOGAF

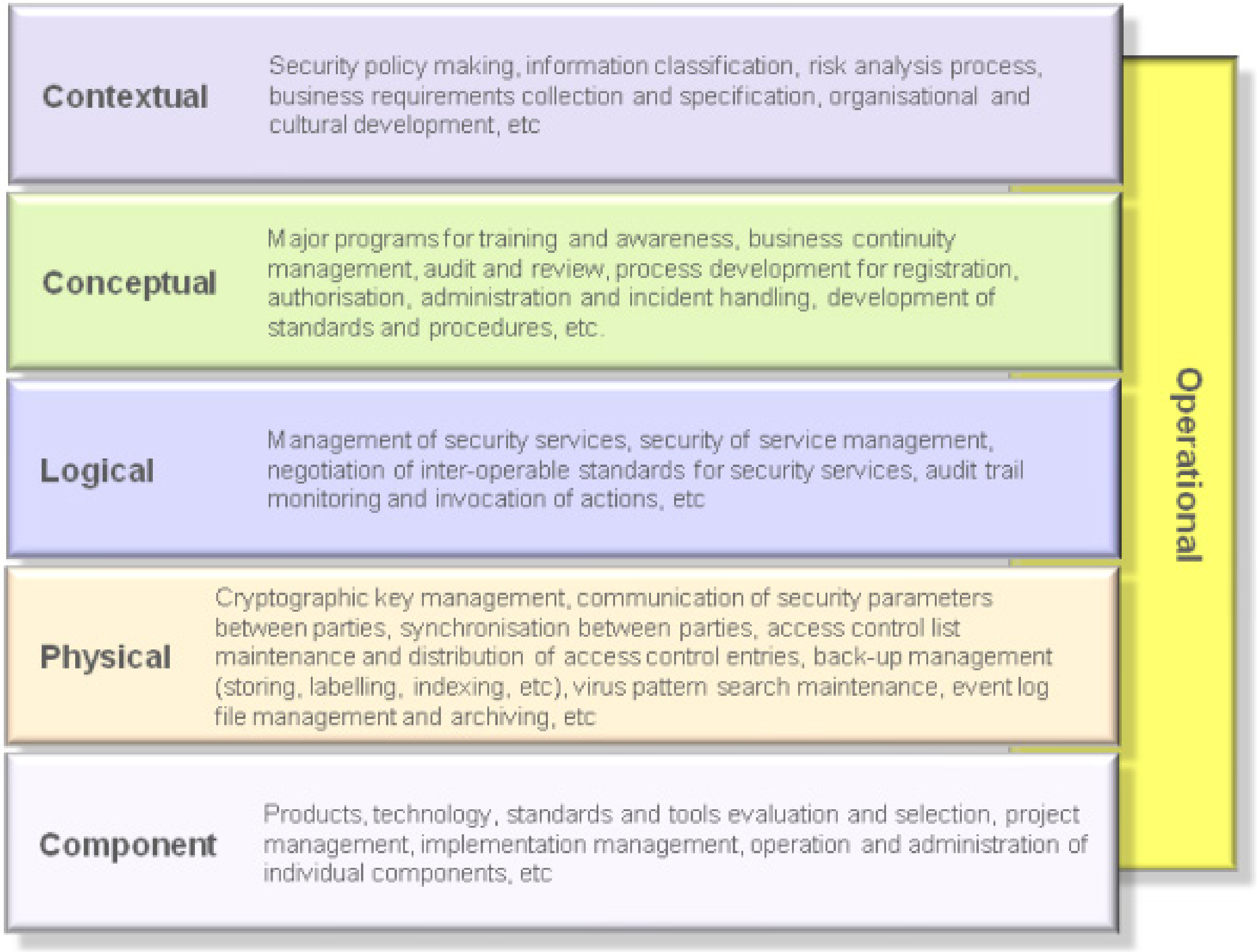


SABSA Model – Architecture Split

	WHAT (Assets)	WHY (Motivation)	HOW (Process)	WHO (People)	WHERE (Location)	WHEN (Time)
CONTEXTUAL (Business)	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
CONCEPTUAL (Architecture)	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
LOGICAL (Design)	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
PHYSICAL (Build)	Business Data Model	Security Rules, Practices & Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastucture	Control Structure Execution
COMPONENT (Tools)	Detailed Data Structures	Security Standards	Security Products & Tools	Identities, Functions, Action and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
SERVICE MANAGEMENT	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

Business Architecture	Security Architecture	Information Architecture	Application Architecture	Technology Architecture	Risk Management Architecture	Service Architecture

Collapsing SABSA into a single stack



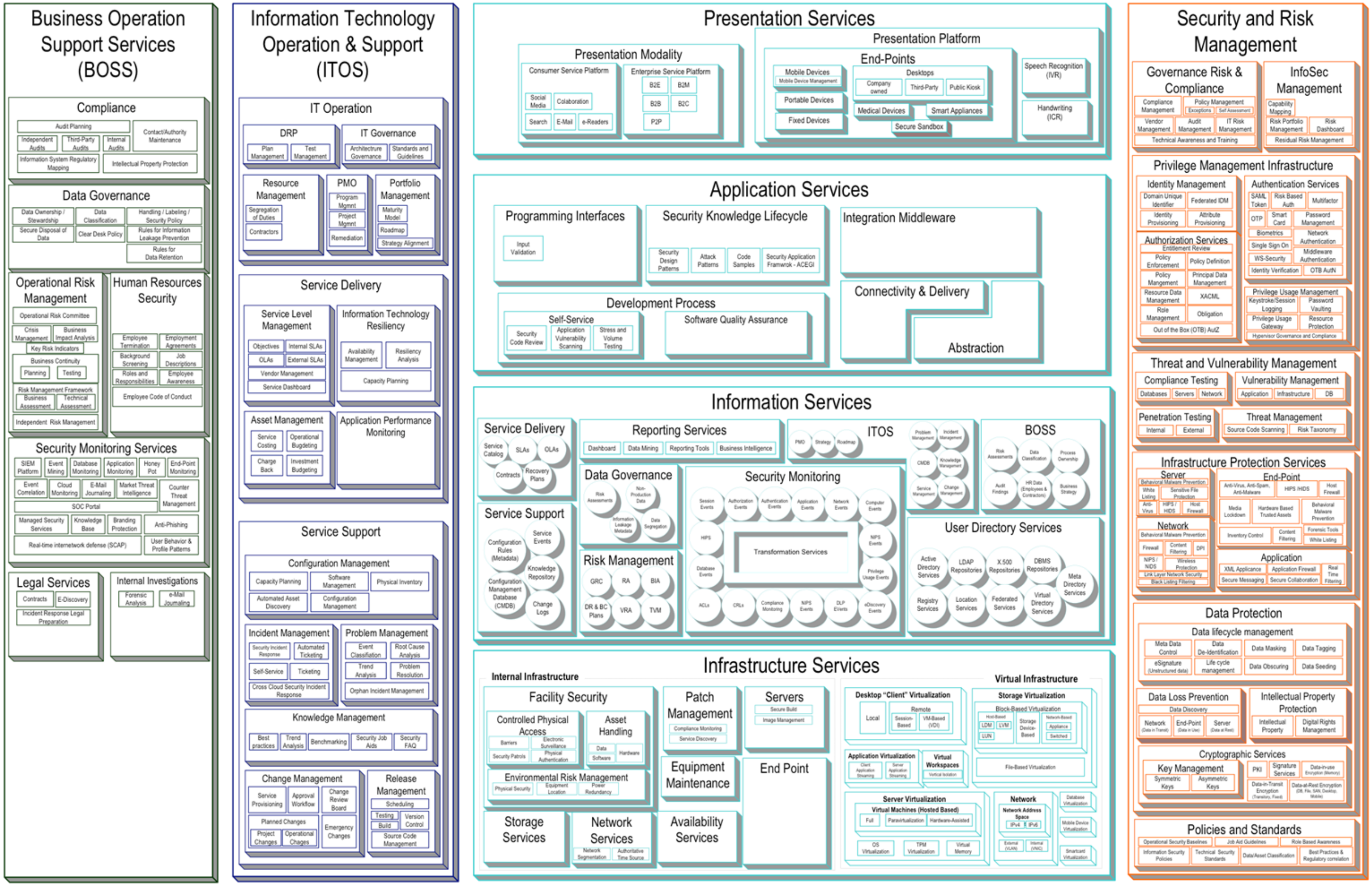
Contextual	Security policy making, information classification, risk analysis process, business requirements collection and specification, organisational and cultural development, etc
Conceptual	Major programs for training and awareness, business continuity management, audit and review, process development for registration, authorisation, administration and incident handling, development of standards and procedures, etc.
Logical	Management of security services, security of service management, negotiation of inter-operable standards for security services, audit trail monitoring and invocation of actions, etc
Physical	Cryptographic key management, communication of security parameters between parties, synchronisation between parties, access control list maintenance and distribution of access control entries, back-up management (storing, labelling, indexing, etc), virus pattern search maintenance, event log file management and archiving, etc
Component	Products, technology, standards and tools evaluation and selection, project management, implementation management, operation and administration of individual components, etc

Operational

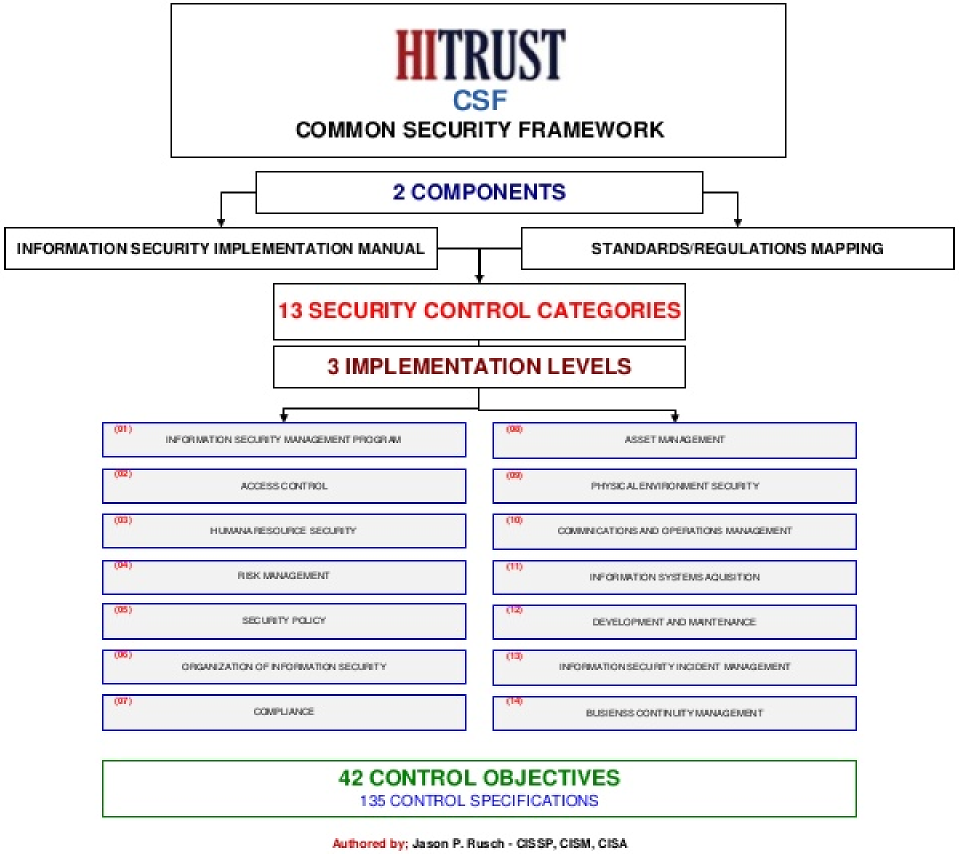
Other security frameworks lack an EA perspective but bring subject matter depth and rigor to the organization

- NIST/CSA Reference Architecture (for clouds)
- HITRUST CSF (for healthcare)
- NIST Cybersecurity Framework (NIST CSF)
- Note that many other standards and guidelines are *not* frameworks
  - ISO 27001/2
  - PCI DSS
  - SSAE 16 SOC2

NIST/CSA Reference Architecture



HITRUST CSF



HITRUST
CSF
COMMON SECURITY FRAMEWORK

2 COMPONENTS

INFORMATION SECURITY IMPLEMENTATION MANUAL

STANDARDS/REGULATIONS MAPPING

13 SECURITY CONTROL CATEGORIES

3 IMPLEMENTATION LEVELS

(01) INFORMATION SECURITY MANAGEMENT PROGRAM

(02) ACCESS CONTROL

(03) HUMANA RESOURCE SECURITY

(04) RISK MANAGEMENT

(05) SECURITY POLICY

(06) ORGANIZATION OF INFORMATION SECURITY

(07) COMPLIANCE

(08) ASSET MANAGEMENT

(09) PHYSICAL ENVIRONMENT SECURITY

(10) COMMINICATIONS AND OPERATIONS MANAGEMENT

(11) INFORMATION SYSTEMS AQUISITION

(12) DEVELOPMENT AND MAINTENANCE

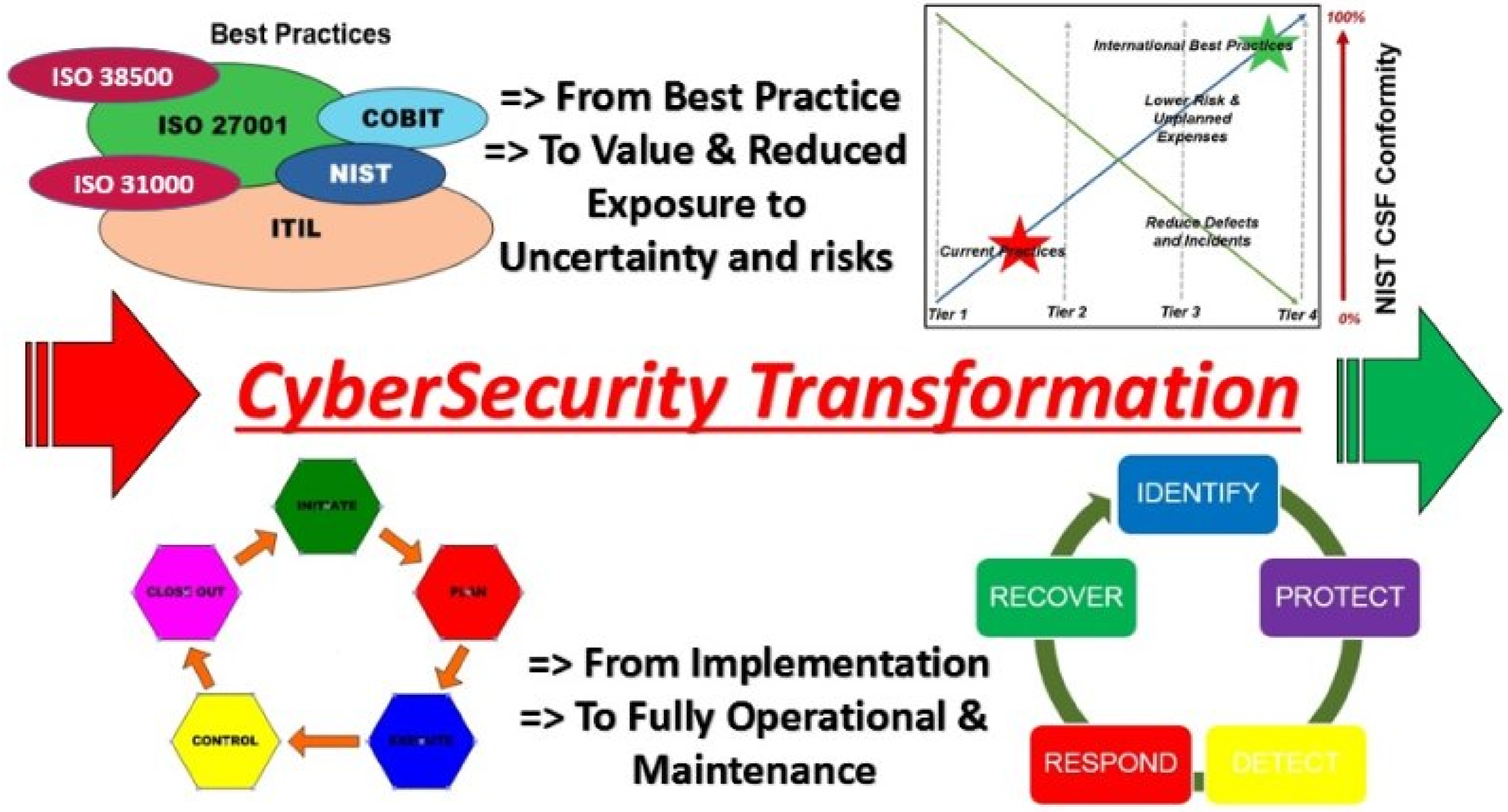
(13) INFORMATION SECURITY INCIDENT MANAGEMENT

(14) BUSIENSS CONTINUITY MANAGEMENT

42 CONTROL OBJECTIVES
135 CONTROL SPECIFICATIONS

Authored by: Jason P. Rusch - CISSP, CISM, CISA

The NIST Cybersecurity Framework (NIST CSF) has gained widespread acceptance, although it is not yet widely implemented



=> From Best Practice
=> To Value & Reduced Exposure to Uncertainty and risks

=> From Implementation
=> To Fully Operational & Maintenance

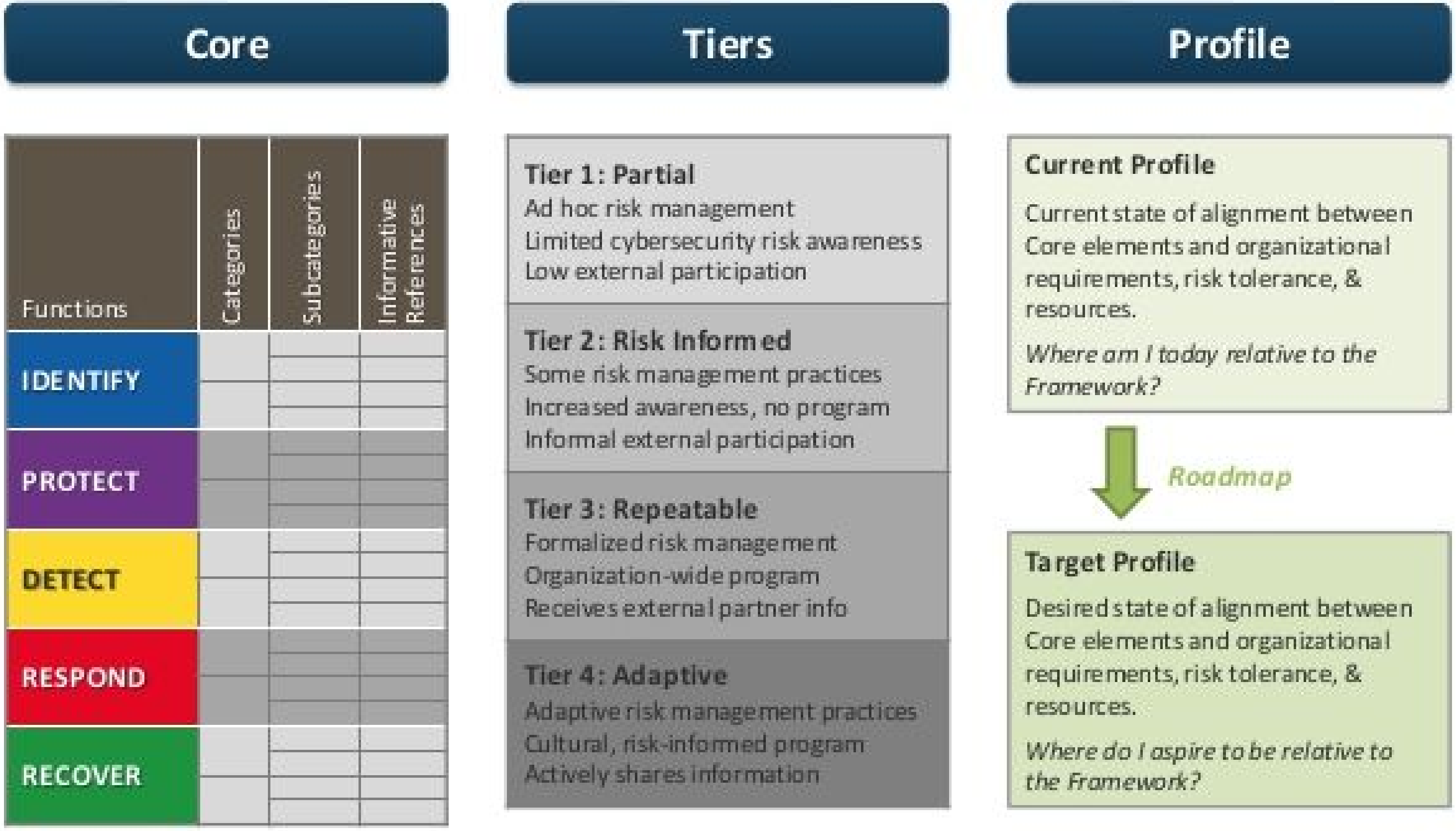
UC has adopted the NIST CSF

- The CRGC approved the NIST CSF as a formal guidance document for all locations
- Because of its breadth, implementation of the NIST CSF will be distributed across many organizations and disciplines
- The UC EA team is planning to develop supporting artifacts, such as a crosswalk between UC EABoK artifacts and the NIST CSF

Key components of the NIST CSF

- The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references
- *Framework Implementation Tiers* provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.
- A *Framework Profile* represents the outcomes based on business needs.

NIST Cybersecurity Framework (CSF)



Core

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Tiers

Tier 1: Partial
Ad hoc risk management
Limited cybersecurity risk awareness
Low external participation

Tier 2: Risk Informed
Some risk management practices
Increased awareness, no program
Informal external participation

Tier 3: Repeatable
Formalized risk management
Organization-wide program
Receives external partner info

Tier 4: Adaptive
Adaptive risk management practices
Cultural, risk-informed program
Actively shares information

Profile

Current Profile

Current state of alignment between Core elements and organizational requirements, risk tolerance, & resources.

Where am I today relative to the Framework?

Roadmap

Target Profile

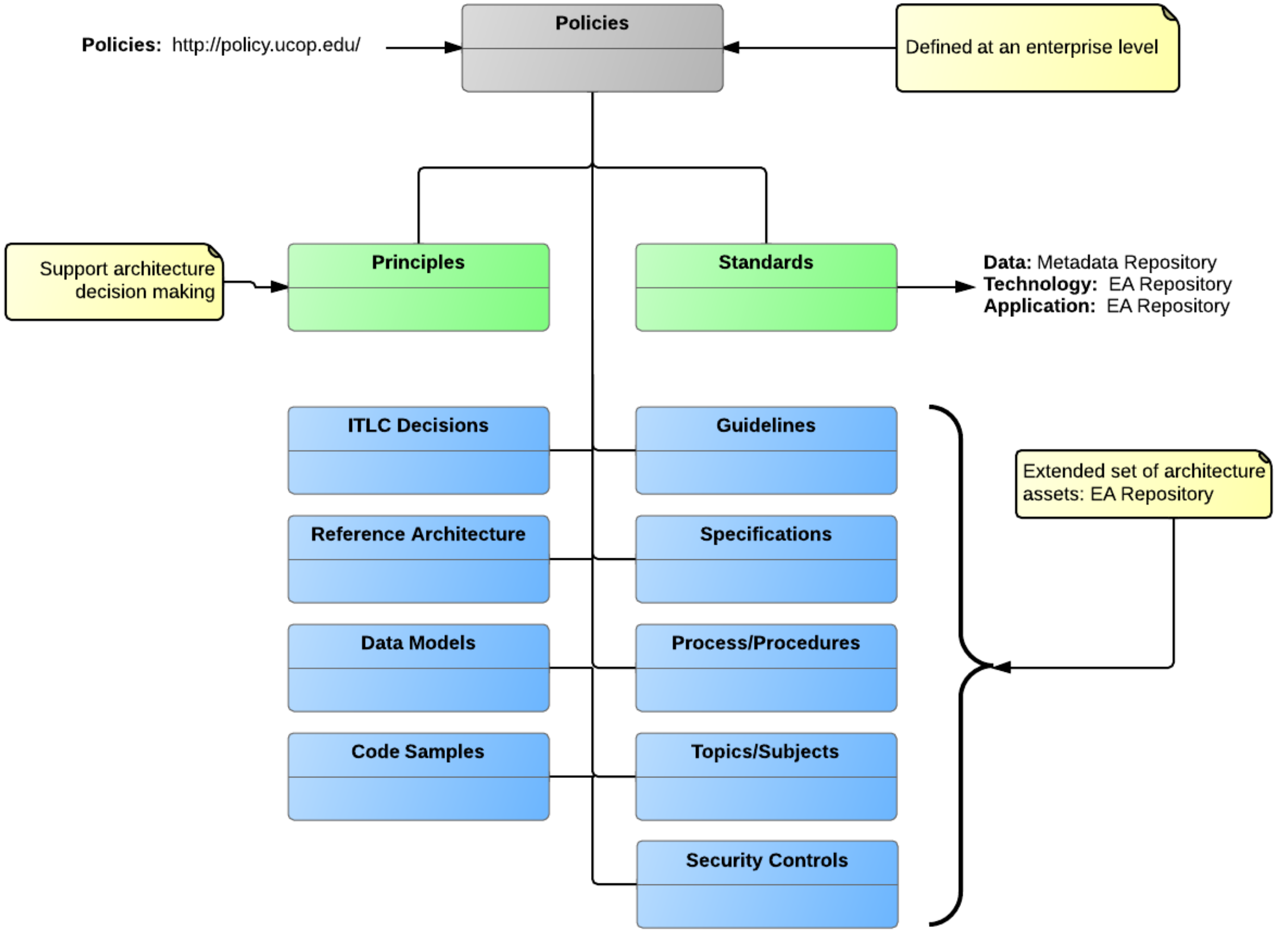
Desired state of alignment between Core elements and organizational requirements, risk tolerance, & resources.

Where do I aspire to be relative to the Framework?

The EA team and IT Architecture Committee (ITAC) developed a framework to manage the end-to-end lifecycle of architecture artifacts

- An Enterprise Architecture Assets Framework (EAAF) was created for lifecycle management of assets that may advance consistency, reuse or interoperability
- The EAAF is loosely modeled after TOGAF
- The collection of Enterprise Architecture Assets established an EA Body of Knowledge (EABoK)

Types of Enterprise Architecture Assets (EAAs) developed or planned


Policies: http://policy.ucop.edu/
Policies
Defined at an enterprise level
Support architecture decision making
Principles
Standards
Data: Metadata Repository
Technology: EA Repository
Application: EA Repository
ITLC Decisions
Guidelines
Extended set of architecture assets: EA Repository
Reference Architecture
Specifications
Data Models
Process/Procedures
Code Samples
Topics/Subjects
Security Controls

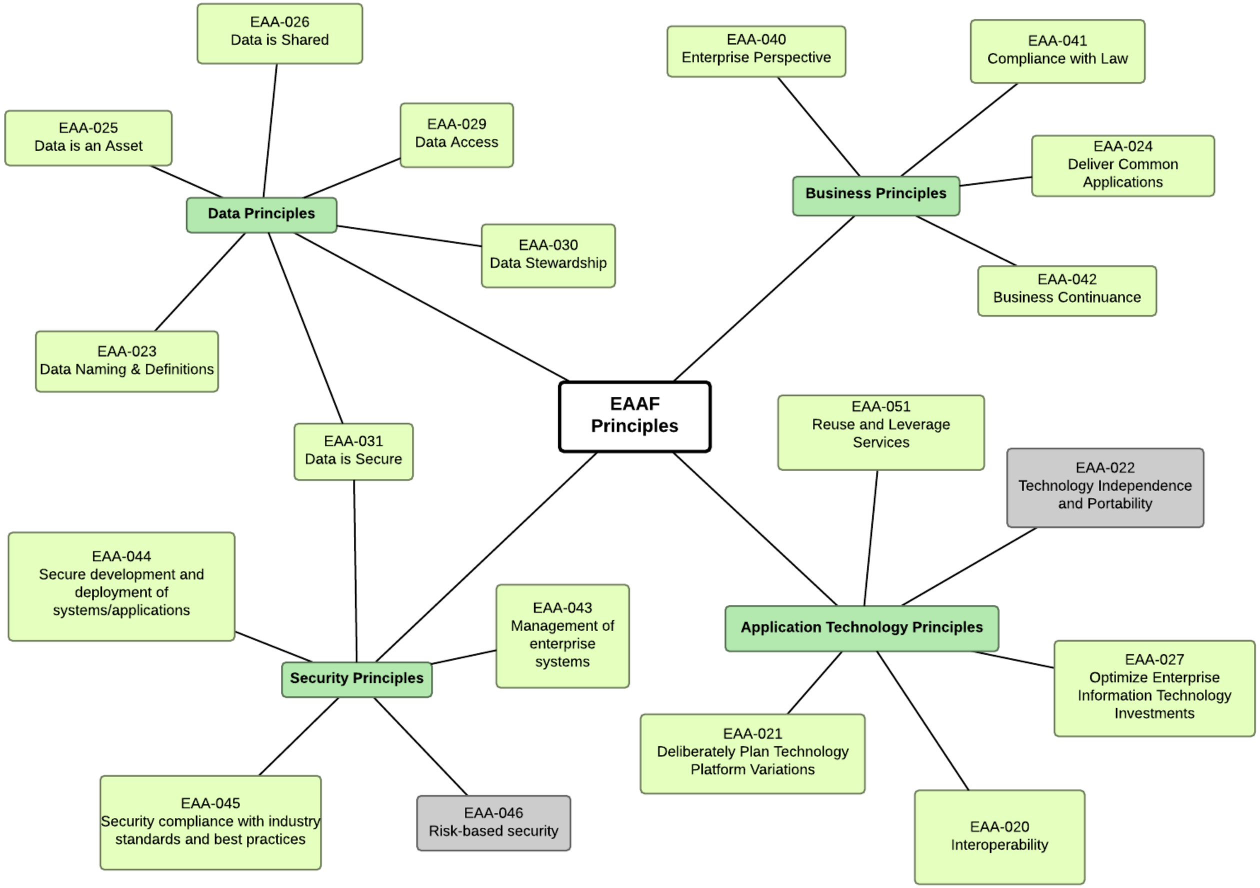
What is a principle?

“A generalized type of business driver, a principle is any statement that is thought, by senior leadership, to be useful guidance for the organization to consider when making business decisions.”

- Principles are value statements, not directives
- Principles are long-term, enduring and seldom amended
- Principles are enforced with policies, standards, and procedures

Architectural principles anchor the EAAF – All EAAs should trace back to a principle

Architectural principles mind map


EAAF Principles
Data Principles
EAA-026 Data is Shared
EAA-025 Data is an Asset
EAA-029 Data Access
EAA-030 Data Stewardship
EAA-023 Data Naming & Definitions
EAA-031 Data is Secure
Business Principles
EAA-040 Enterprise Perspective
EAA-041 Compliance with Law
EAA-024 Deliver Common Applications
EAA-042 Business Continuance
Application Technology Principles
EAA-051 Reuse and Leverage Services
EAA-022 Technology Independence and Portability
EAA-027 Optimize Enterprise Information Technology Investments
EAA-021 Deliberately Plan Technology Platform Variations
EAA-020 Interoperability
Security Principles
EAA-044 Secure development and deployment of systems/applications
EAA-043 Management of enterprise systems
EAA-045 Security compliance with industry standards and best practices
EAA-046 Risk-based security

What is a standard?

“A mandatory requirement”

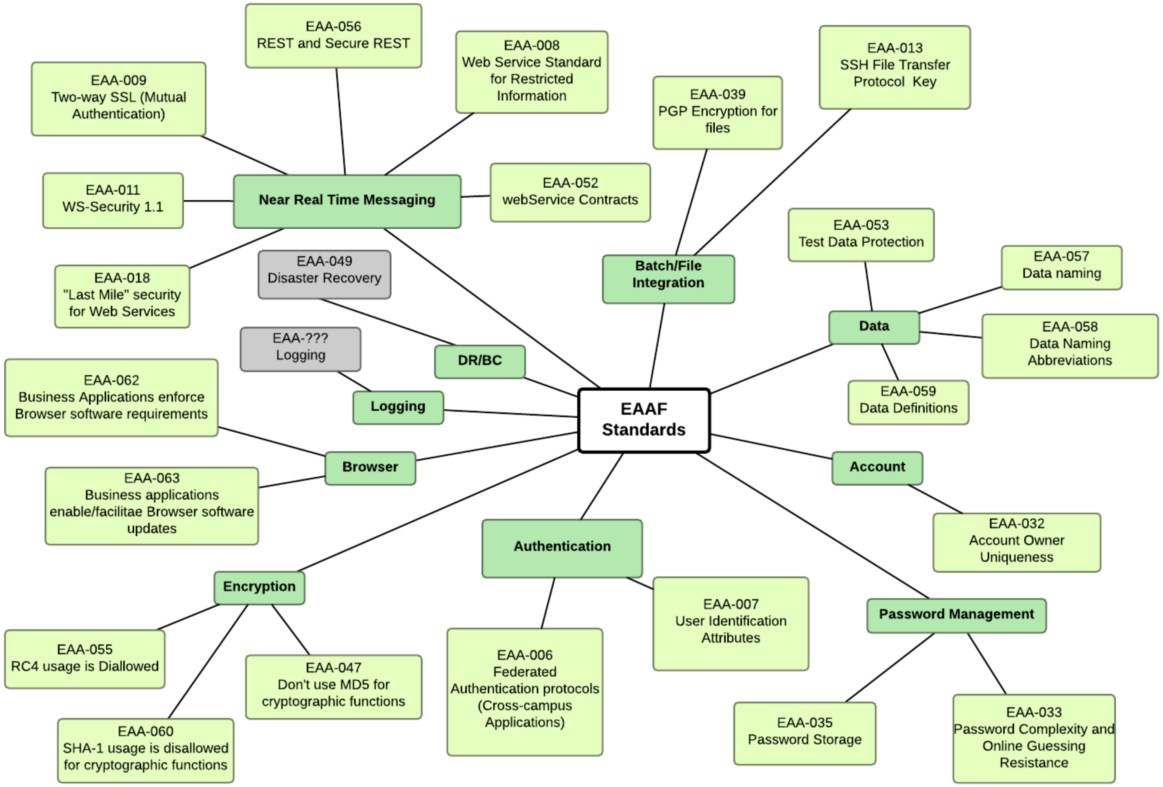
“Set by policies that help produce the procedures that will be followed to carry out the objectives of the policies. Standards attempt to tie the procedures with their policies.”

“*A collection of specific and detailed requirements that must be met.*

Specifies the minimum set of administrative, technical, or procedural controls required to meet the related policy.”

The next level of EAAs are Standards and Guidelines

Security standards mind map



EAAF Standards

- Near Real Time Messaging
  - EAA-009 Two-way SSL (Mutual Authentication)
  - EAA-056 REST and Secure REST
  - EAA-008 Web Service Standard for Restricted Information
  - EAA-011 WS-Security 1.1
  - EAA-052 webService Contracts
  - EAA-018 "Last Mile" security for Web Services
- DR/BC
  - EAA-049 Disaster Recovery
- Logging
  - EAA-??? Logging
- Browser
  - EAA-062 Business Applications enforce Browser software requirements
  - EAA-063 Business applications enable/facilitae Browser software updates
- Encryption
  - EAA-055 RC4 usage is Diallowed
  - EAA-060 SHA-1 usage is disallowed for cryptographic functions
  - EAA-047 Don't use MD5 for cryptographic functions
- Authentication
  - EAA-006 Federated Authentication protocols (Cross-campus Applications)
  - EAA-007 User Identification Attributes
- Batch/File Integration
  - EAA-039 PGP Encryption for files
  - EAA-013 SSH File Transfer Protocol Key
- Data
  - EAA-053 Test Data Protection
  - EAA-057 Data naming
  - EAA-058 Data Naming Abbreviations
  - EAA-059 Data Definitions
- Account
  - EAA-032 Account Owner Uniqueness
- Password Management
  - EAA-035 Password Storage
  - EAA-033 Password Complexity and Online Guessing Resistance

What is a guideline?

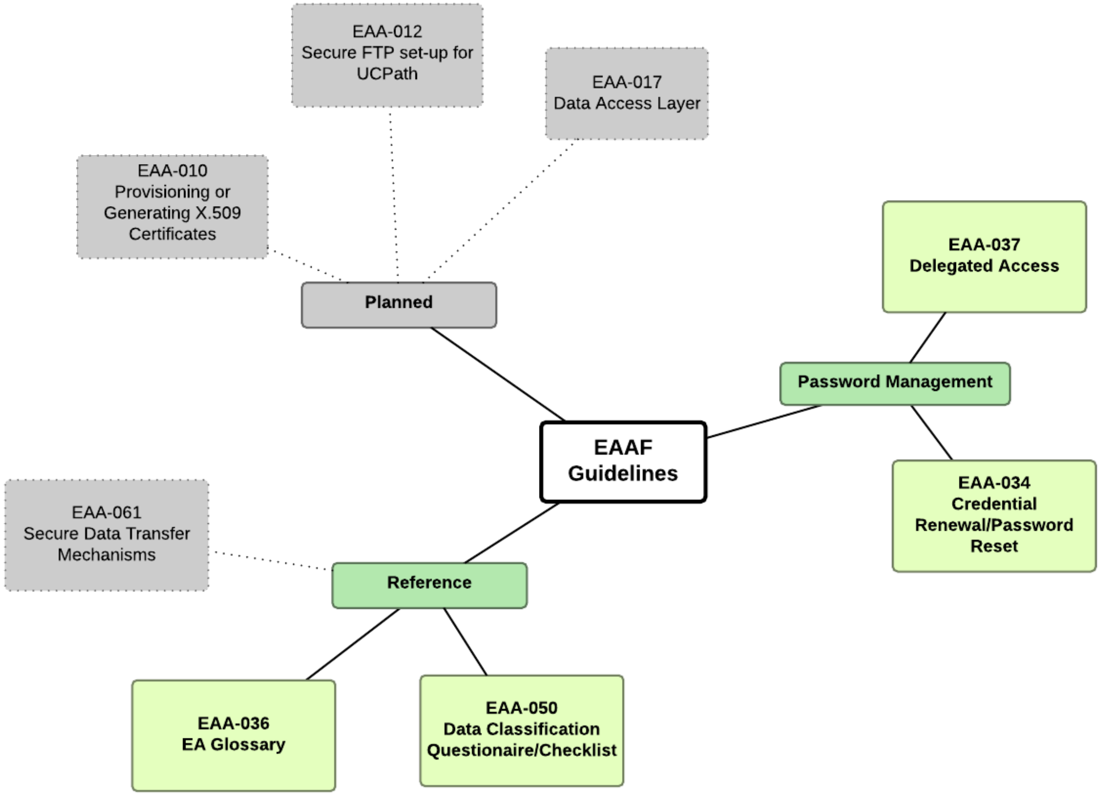
“Recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.”

“A document describing best practice, which recommends what should be done. Compliance with a guideline is not normally enforced.”

“A description of a particular way of accomplishing something that is less prescriptive than a procedure”

The next level of EAAs are Standards and Guidelines (continued)

Security guidelines mind map


EAA-012
Secure FTP set-up for UCPath
EAA-017
Data Access Layer
EAA-010
Provisioning or Generating X.509 Certificates
EAA-037
Delegated Access
Planned
Password Management
EAAF Guidelines
EAA-034
Credential Renewal/Password Reset
EAA-061
Secure Data Transfer Mechanisms
Reference
EAA-036
EA Glossary
EAA-050
Data Classification Questionaire/Checklist

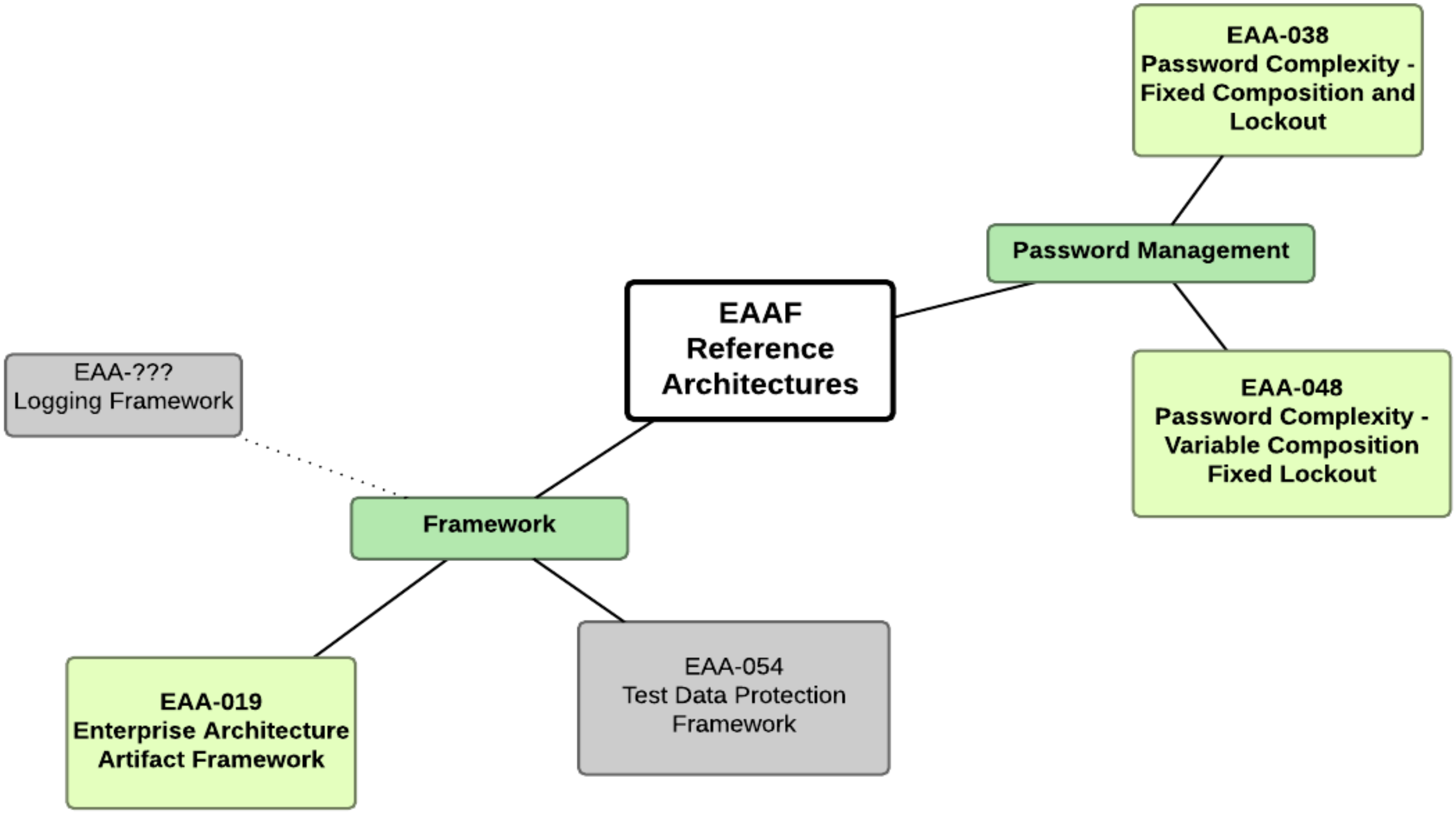
What is a reference architecture?

“[A] Reference Architecture is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.”

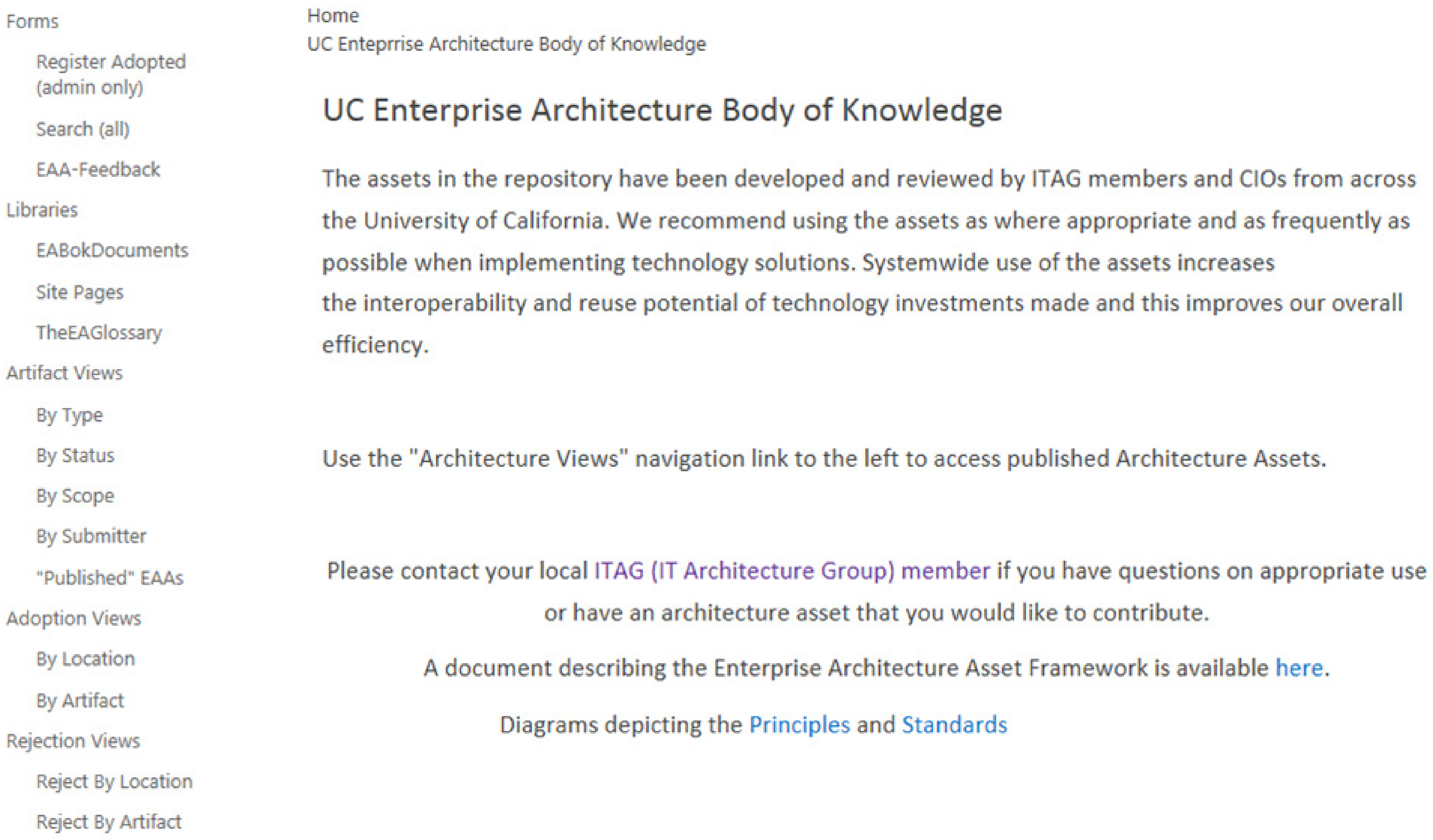
“A reference architecture models the abstract architectural elements in the domain of interest independent of the technologies, protocols, and products that are used to implement a specific solution for the domain.”

Yet another EAA type is the Reference Architecture

Reference architecture mind map


EAA-038
Password Complexity - Fixed Composition and Lockout
Password Management
EAAF Reference Architectures
EAA-048
Password Complexity - Variable Composition Fixed Lockout
EAA-???
Logging Framework
Framework
EAA-019
Enterprise Architecture Artifact Framework
EAA-054
Test Data Protection Framework

EABoK Screen Shots – home page



UC Enterprise Architecture Body of Knowledge

The assets in the repository have been developed and reviewed by ITAG members and CIOs from across the University of California. We recommend using the assets as where appropriate and as frequently as possible when implementing technology solutions. Systemwide use of the assets increases the interoperability and reuse potential of technology investments made and this improves our overall efficiency.

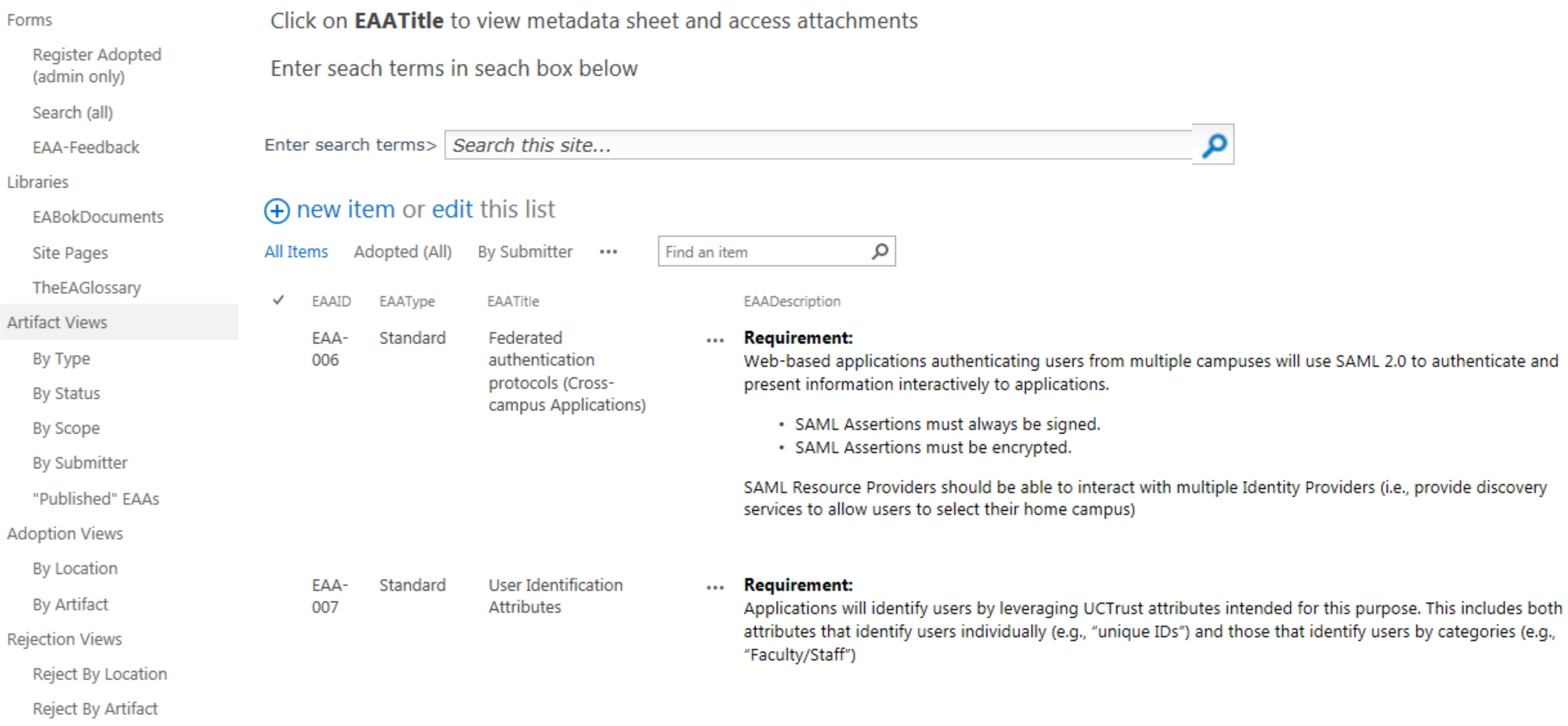
Use the "Architecture Views" navigation link to the left to access published Architecture Assets.

Please contact your local ITAG (IT Architecture Group) member if you have questions on appropriate use or have an architecture asset that you would like to contribute.

A document describing the Enterprise Architecture Asset Framework is available here.

Diagrams depicting the Principles and Standards

EABoK Screen Shots – EAA list



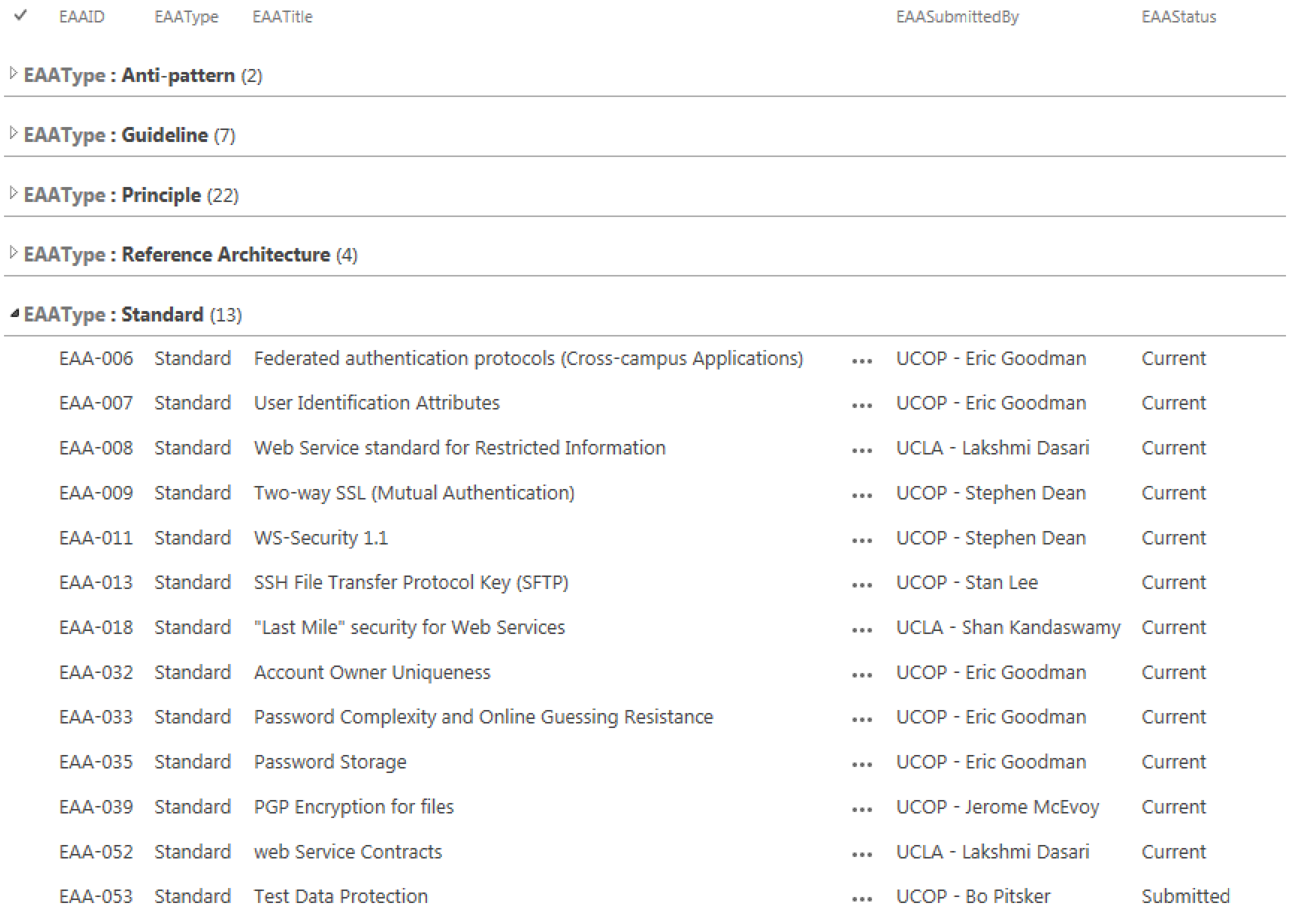
Click on **EAATitle** to view metadata sheet and access attachments

Enter seach terms in seach box below

Enter search terms> *Search this site...*

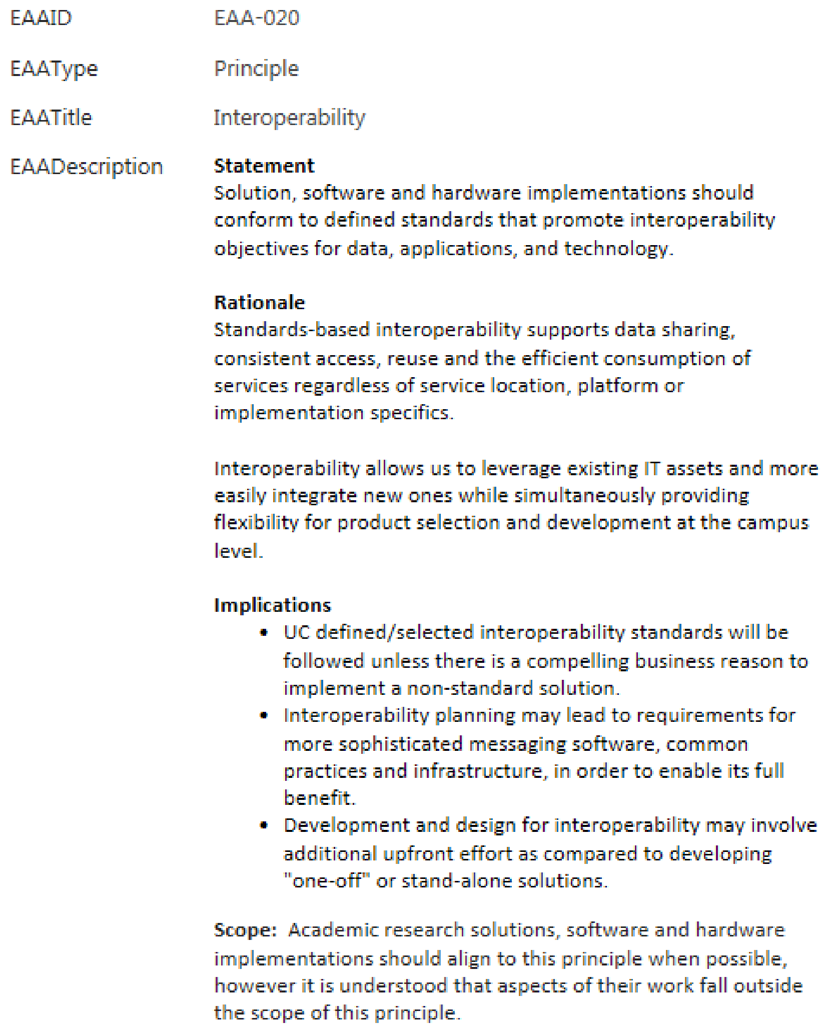
✓	EAAID	EAAType	EAATitle		EAADescription
	EAA-006	Standard	Federated authentication protocols (Cross-campus Applications)	•••	**Requirement:** Web-based applications authenticating users from multiple campuses will use SAML 2.0 to authenticate and present information interactively to applications. • SAML Assertions must always be signed. • SAML Assertions must be encrypted. SAML Resource Providers should be able to interact with multiple Identity Providers (i.e., provide discovery services to allow users to select their home campus)
	EAA-007	Standard	User Identification Attributes	•••	**Requirement:** Applications will identify users by leveraging UCTrust attributes intended for this purpose. This includes both attributes that identify users individually (e.g., "unique IDs") and those that identify users by categories (e.g., "Faculty/Staff")

EABoK Screen Shots – EAA types



✓	EAAID	EAAType	EAATitle		EAASubmittedBy	EAAStatus
▷ **EAAType : Anti-pattern** (2)						
▷ **EAAType : Guideline** (7)						
▷ **EAAType : Principle** (22)						
▷ **EAAType : Reference Architecture** (4)						
◢ **EAAType : Standard** (13)						
	EAA-006	Standard	Federated authentication protocols (Cross-campus Applications)	•••	UCOP - Eric Goodman	Current
	EAA-007	Standard	User Identification Attributes	•••	UCOP - Eric Goodman	Current
	EAA-008	Standard	Web Service standard for Restricted Information	•••	UCLA - Lakshmi Dasari	Current
	EAA-009	Standard	Two-way SSL (Mutual Authentication)	•••	UCOP - Stephen Dean	Current
	EAA-011	Standard	WS-Security 1.1	•••	UCOP - Stephen Dean	Current
	EAA-013	Standard	SSH File Transfer Protocol Key (SFTP)	•••	UCOP - Stan Lee	Current
	EAA-018	Standard	"Last Mile" security for Web Services	•••	UCLA - Shan Kandaswamy	Current
	EAA-032	Standard	Account Owner Uniqueness	•••	UCOP - Eric Goodman	Current
	EAA-033	Standard	Password Complexity and Online Guessing Resistance	•••	UCOP - Eric Goodman	Current
	EAA-035	Standard	Password Storage	•••	UCOP - Eric Goodman	Current
	EAA-039	Standard	PGP Encryption for files	•••	UCOP - Jerome McEvoy	Current
	EAA-052	Standard	web Service Contracts	•••	UCLA - Lakshmi Dasari	Current
	EAA-053	Standard	Test Data Protection	•••	UCOP - Bo Pitsker	Submitted

EABoK Screen Shots – EAA detail



EAAID	EAA-020
EAAType	Principle
EAATitle	Interoperability

EAADescription

Statement
Solution, software and hardware implementations should conform to defined standards that promote interoperability objectives for data, applications, and technology.

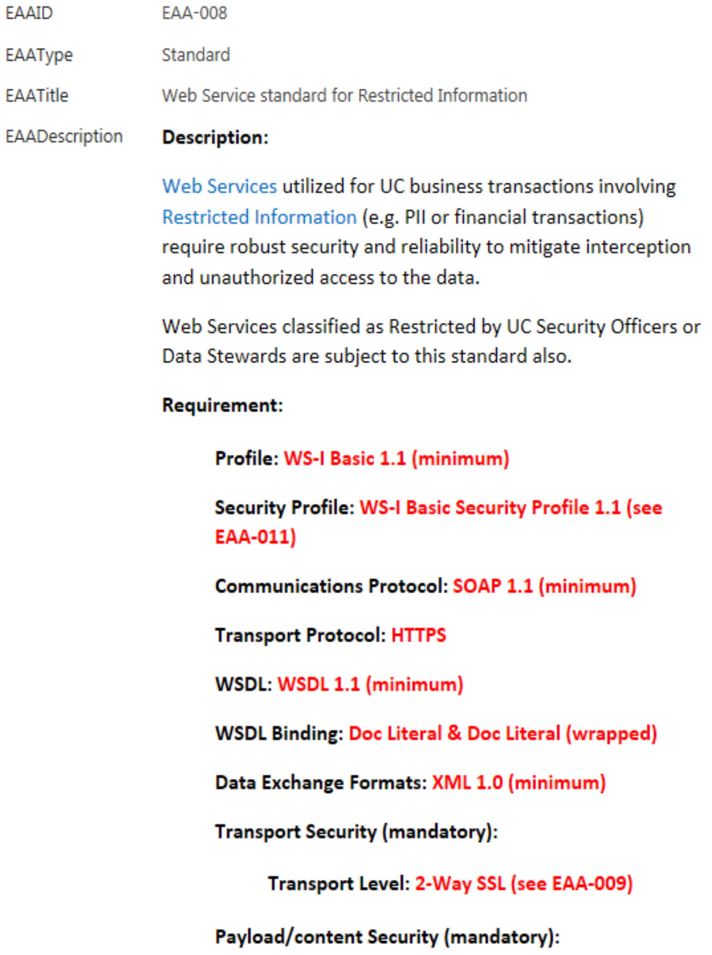
Rationale
Standards-based interoperability supports data sharing, consistent access, reuse and the efficient consumption of services regardless of service location, platform or implementation specifics.

Interoperability allows us to leverage existing IT assets and more easily integrate new ones while simultaneously providing flexibility for product selection and development at the campus level.

Implications

- UC defined/selected interoperability standards will be followed unless there is a compelling business reason to implement a non-standard solution.
- Interoperability planning may lead to requirements for more sophisticated messaging software, common practices and infrastructure, in order to enable its full benefit.
- Development and design for interoperability may involve additional upfront effort as compared to developing "one-off" or stand-alone solutions.

Scope: Academic research solutions, software and hardware implementations should align to this principle when possible, however it is understood that aspects of their work fall outside the scope of this principle.



EAAID	EAA-008
EAAType	Standard
EAATitle	Web Service standard for Restricted Information

EAADescription

Description:

Web Services utilized for UC business transactions involving Restricted Information (e.g. PII or financial transactions) require robust security and reliability to mitigate interception and unauthorized access to the data.

Web Services classified as Restricted by UC Security Officers or Data Stewards are subject to this standard also.

Requirement:

Profile: **WS-I Basic 1.1 (minimum)**

Security Profile: **WS-I Basic Security Profile 1.1 (see EAA-011)**

Communications Protocol: **SOAP 1.1 (minimum)**

Transport Protocol: **HTTPS**

WSDL: **WSDL 1.1 (minimum)**

WSDL Binding: **Doc Literal & Doc Literal (wrapped)**

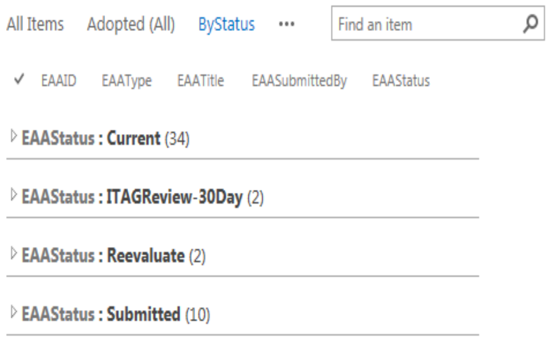
Data Exchange Formats: **XML 1.0 (minimum)**

Transport Security (mandatory):

Transport Level: **2-Way SSL (see EAA-009)**

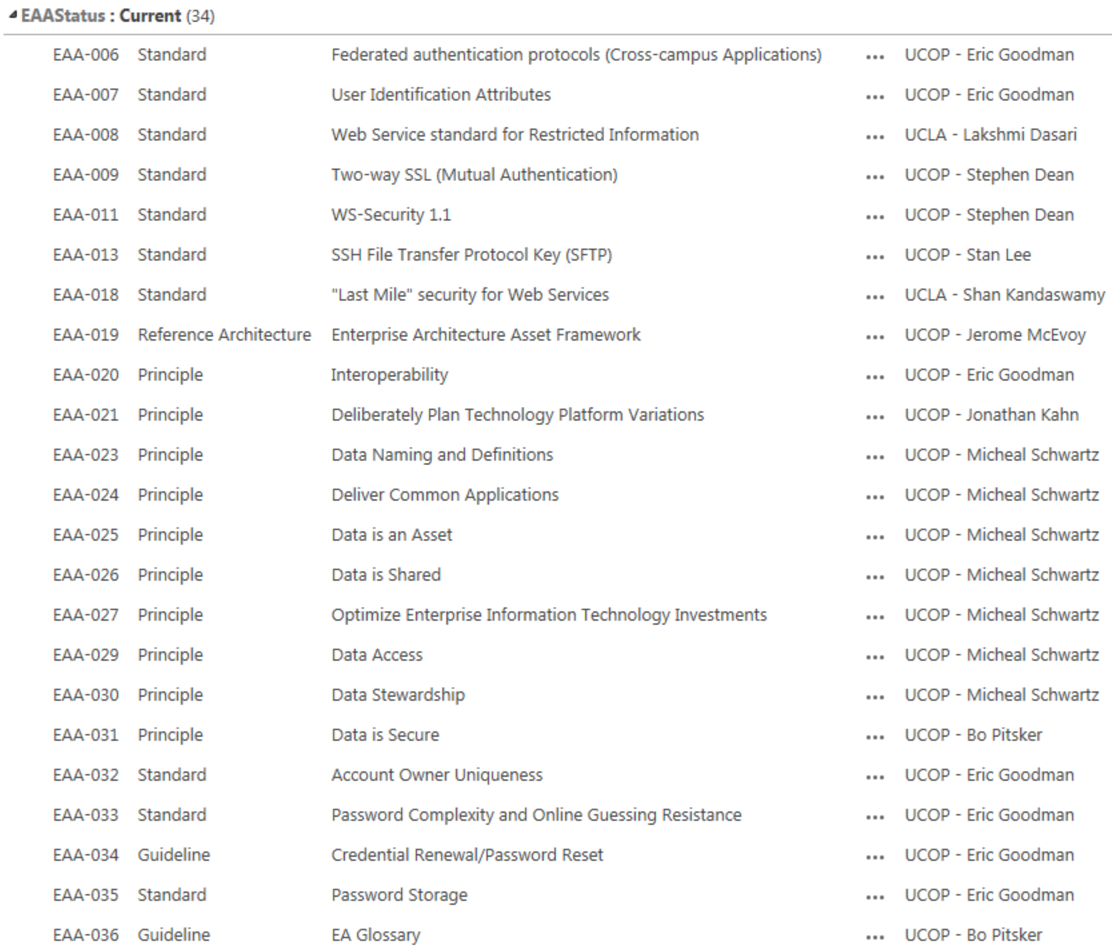
Payload/content Security (mandatory):

EABoK Screen Shots – EAA status



✓ EAAID EAAType EAATitle EAASubmittedBy EAAStatus

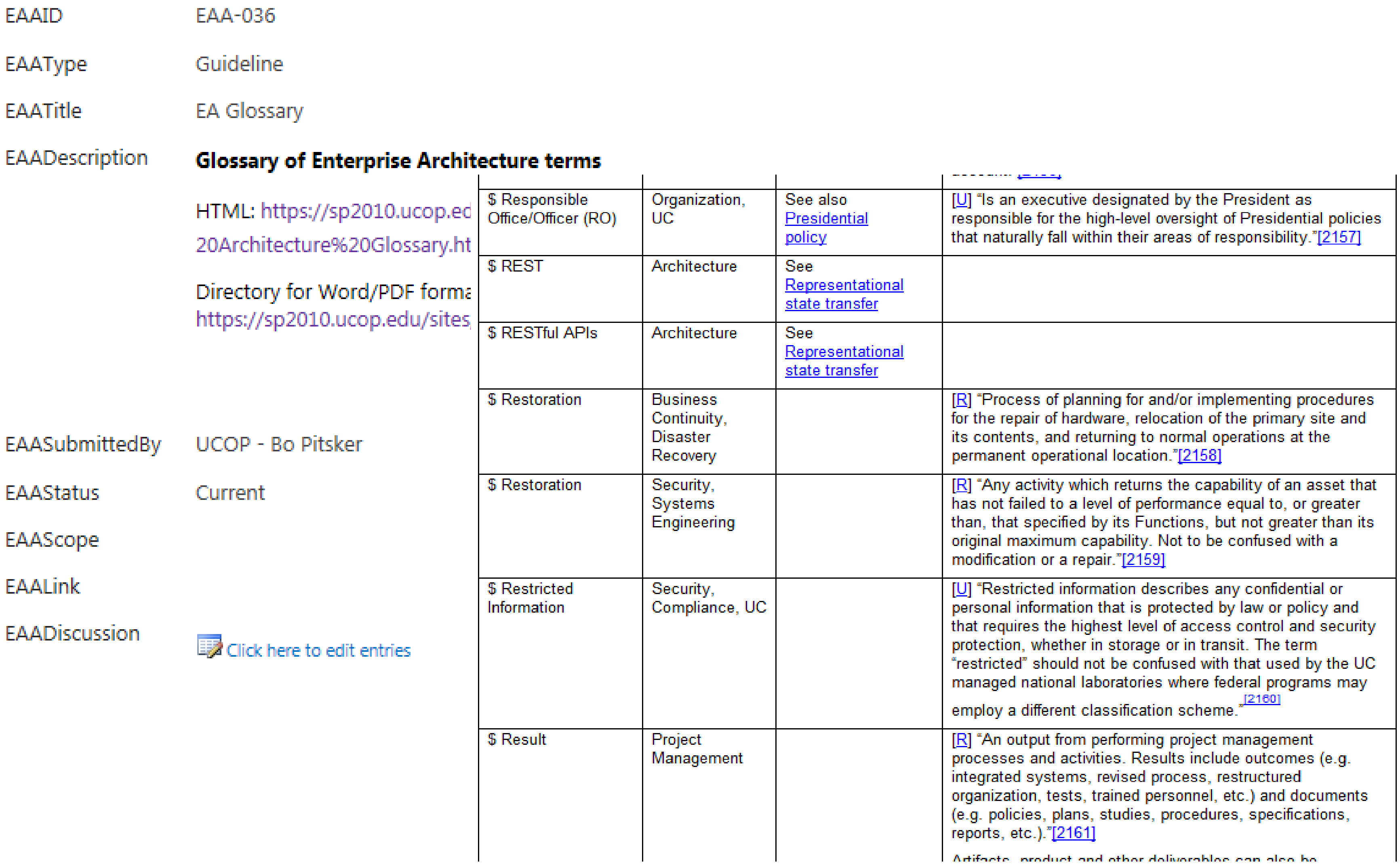
- EAAStatus : Current (34)
- EAAStatus : ITAGReview-30Day (2)
- EAAStatus : Reevaluate (2)
- EAAStatus : Submitted (10)



EAAStatus : Current (34)

EAA-006	Standard	Federated authentication protocols (Cross-campus Applications)	•••	UCOP - Eric Goodman
EAA-007	Standard	User Identification Attributes	•••	UCOP - Eric Goodman
EAA-008	Standard	Web Service standard for Restricted Information	•••	UCLA - Lakshmi Dasari
EAA-009	Standard	Two-way SSL (Mutual Authentication)	•••	UCOP - Stephen Dean
EAA-011	Standard	WS-Security 1.1	•••	UCOP - Stephen Dean
EAA-013	Standard	SSH File Transfer Protocol Key (SFTP)	•••	UCOP - Stan Lee
EAA-018	Standard	"Last Mile" security for Web Services	•••	UCLA - Shan Kandaswamy
EAA-019	Reference Architecture	Enterprise Architecture Asset Framework	•••	UCOP - Jerome McEvoy
EAA-020	Principle	Interoperability	•••	UCOP - Eric Goodman
EAA-021	Principle	Deliberately Plan Technology Platform Variations	•••	UCOP - Jonathan Kahn
EAA-023	Principle	Data Naming and Definitions	•••	UCOP - Micheal Schwartz
EAA-024	Principle	Deliver Common Applications	•••	UCOP - Micheal Schwartz
EAA-025	Principle	Data is an Asset	•••	UCOP - Micheal Schwartz
EAA-026	Principle	Data is Shared	•••	UCOP - Micheal Schwartz
EAA-027	Principle	Optimize Enterprise Information Technology Investments	•••	UCOP - Micheal Schwartz
EAA-029	Principle	Data Access	•••	UCOP - Micheal Schwartz
EAA-030	Principle	Data Stewardship	•••	UCOP - Micheal Schwartz
EAA-031	Principle	Data is Secure	•••	UCOP - Bo Pitsker
EAA-032	Standard	Account Owner Uniqueness	•••	UCOP - Eric Goodman
EAA-033	Standard	Password Complexity and Online Guessing Resistance	•••	UCOP - Eric Goodman
EAA-034	Guideline	Credential Renewal/Password Reset	•••	UCOP - Eric Goodman
EAA-035	Standard	Password Storage	•••	UCOP - Eric Goodman
EAA-036	Guideline	EA Glossary	•••	UCOP - Bo Pitsker

EABoK Screen Shots – EA Glossary (EAA-036)



EAAID	EAA-036
EAAType	Guideline
EAATitle	EA Glossary
EAADescription	**Glossary of Enterprise Architecture terms** HTML: https://sp2010.ucop.ed 20Architecture%20Glossary.ht Directory for Word/PDF forma https://sp2010.ucop.edu/sites
EAASubmittedBy	UCOP - Bo Pitsker
EAAStatus	Current
EAAScope	
EAALink	
EAADiscussion	Click here to edit entries

$ Responsible Office/Officer (RO)	Organization, UC	See also Presidential policy	[U] "Is an executive designated by the President as responsible for the high-level oversight of Presidential policies that naturally fall within their areas of responsibility."[2157]
$ REST	Architecture	See Representational state transfer	
$ RESTful APIs	Architecture	See Representational state transfer	
$ Restoration	Business Continuity, Disaster Recovery		[R] "Process of planning for and/or implementing procedures for the repair of hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location."[2158]
$ Restoration	Security, Systems Engineering		[R] "Any activity which returns the capability of an asset that has not failed to a level of performance equal to, or greater than, that specified by its Functions, but not greater than its original maximum capability. Not to be confused with a modification or a repair."[2159]
$ Restricted Information	Security, Compliance, UC		[U] "Restricted information describes any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. The term "restricted" should not be confused with that used by the UC managed national laboratories where federal programs may employ a different classification scheme."[2160]
$ Result	Project Management		[R] "An output from performing project management processes and activities. Results include outcomes (e.g. integrated systems, revised process, restructured organization, tests, trained personnel, etc.) and documents (e.g. policies, plans, studies, procedures, specifications, reports, etc.)."[2161] Artifacts, product and other deliverables can also be

About the EABoK Enterprise Architecture Glossary

- Over 5,000 entries; 1,100 pages
- Subject matter includes:

- Enterprise architecture
- Business architecture
- Technology architecture
- Data architecture
- Change management and organizational development
- Risk, privacy, and compliance
- Security and identity management architecture
- Physical security, operations security, security awareness
- Project management
- Application architecture
- Infrastructure architecture
- Service oriented architecture (SOA)
- Solutions architecture
- Requirements engineering
- Service management
- Record management
- Procurement
- Knowledge management

The EABoK Enterprise Architecture Glossary benefits include:

- Entries have complete citations
- Each entry is tagged with a “quality” indicator
- Extensive cross-references
- Entries are linkable from any MS Office document or from web pages
- UC-specific entries are marked
- The Glossary is available in multiple formats, including Word and PDF

EA Security principles

EAA #	Principle
EAA-031	Data is Secure
EAA-041	Compliance with Law
EAA-042	Business Continuity
EAA-043	Management of enterprise systems
EAA-045	Security compliance with industry standards and best practices

EA Security standards

EAA #	Standard
EAA-006	Federated authentication protocols (Cross-campus Applications)
EAA-007	User Identification Attributes
EAA-008	Web Service standard for Restricted Information
EAA-009	Two-way SSL (Mutual Authentication)
EAA-011	WS-Security 1.1
EAA-013	SSH File Transfer Protocol Key (SFTP)
EAA-018	"Last Mile" security for Web Services
EAA-032	Account Owner Uniqueness
EAA-033	Password Complexity and Online Guessing Resistance
EAA-035	Password Storage
EAA-039	PGP Encryption for files
EAA-047	Don't use MD5 for cryptographic functions
EAA-053	Data Protection for Test Data
EAA-055	RC4 usage is disallowed
EAA-056	REST and Secure REST
EAA-060	SHA-1 usage is disallowed for Cryptographic Functions
EAA-065	Event Logging and Management

EA Security guidelines and references

EAA #	Guideline / Reference Artifact
EAA-010	Provisioning or Generating X.509 Certificates
EAA-012	Secure FTP set-up guidelines for UCPath
EAA-034	Credential Renewal/Password Reset
EAA-036	Enterprise Architecture Glossary
EAA-037	Delegated Access
EAA-050	Data Classification Questionnaire/Checklist
EAA-061	Secure Data Transfer Mechanisms

EA Security reference architectures

EAA #	Reference Architecture
EAA-038	Password Complexity - Fixed Composition and Lockout
EAA-048	Password Complexity - Variable Composition Fixed Lockout

Conclusion

- Security is driven by business needs
- Enterprise architecture provides the basis for security transformation
- Frameworks establish the means to organize and prioritize the work of security
- The UC EA team and ITAC have established a process and a body of work for security
- We are here to help (and we’re not from the IRS!)

Q & A

For more information

Presenter

Bo Pitsker, Enterprise Security Architect

Bo.pitsker@ucop.edu

510-587-6490

UC EABoK

sp.ucop.edu/sites/its/apptech/enterprisearchitecture/EABoK/default.aspx

If unable to access, contact Jerome McEvoy, jerome.mcevoy@ucop.edu

Information Technology Architecture Committee (ITAC)

spaces.ais.ucla.edu/display/ucitag/Home