Enterprise Security Architecture isn't just for enterprises

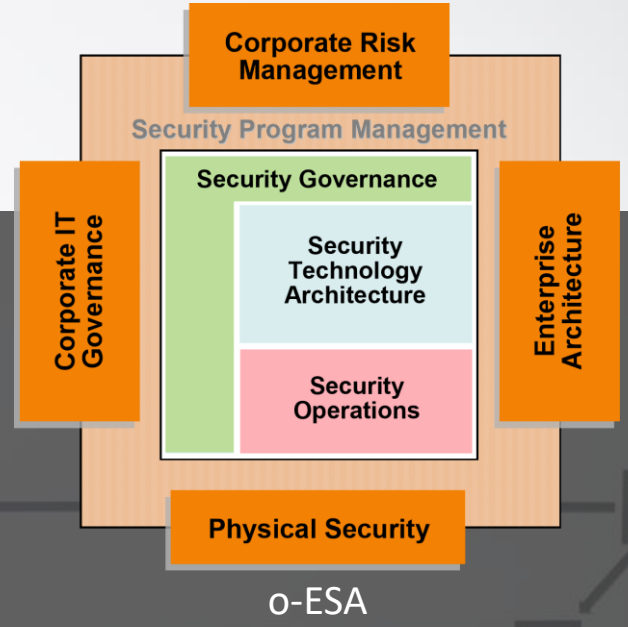
What is this talk about?

- In this talk, Architecture = Governance
- If you're expecting a talk where architecture = design documentation, then I can show you how to make that design documentation even more actionable
- If governance = ewww, run.

```
PS > Get-User | Select Name, Alias, Location, *Company, Role

Name                                : Hudson Bush
Alias                               : @HomeBrewedSec
Location                            : Chattanooga, TN
Company                             : Dragos
Role                                : Principal Security Engineer
SpeakingOnBehalfOfCompany           : FALSE
```

Enterprise Architecture?



o-ESA

- Integrations and relationships between people, systems, processes
- Frameworks for repeatable systems and outcomes

Policies / Standards -> What

Resource Plans -> Who

Project Plans -> When

Procedures / Work Instructions -> How

Architecture -> Why

Why Tailor a Security Architecture?

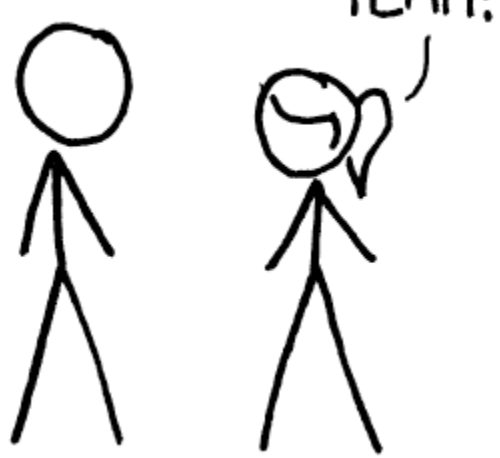
- Most Architecture Frameworks are old models that haven't necessarily aged well
- Designed from a business, not a technology perspective
- Usually used by HUGE organizations with a whole department devoted to architecture

HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.



SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

Architecture Frameworks

TOGAF

o-ESA

SABSA

Zachman

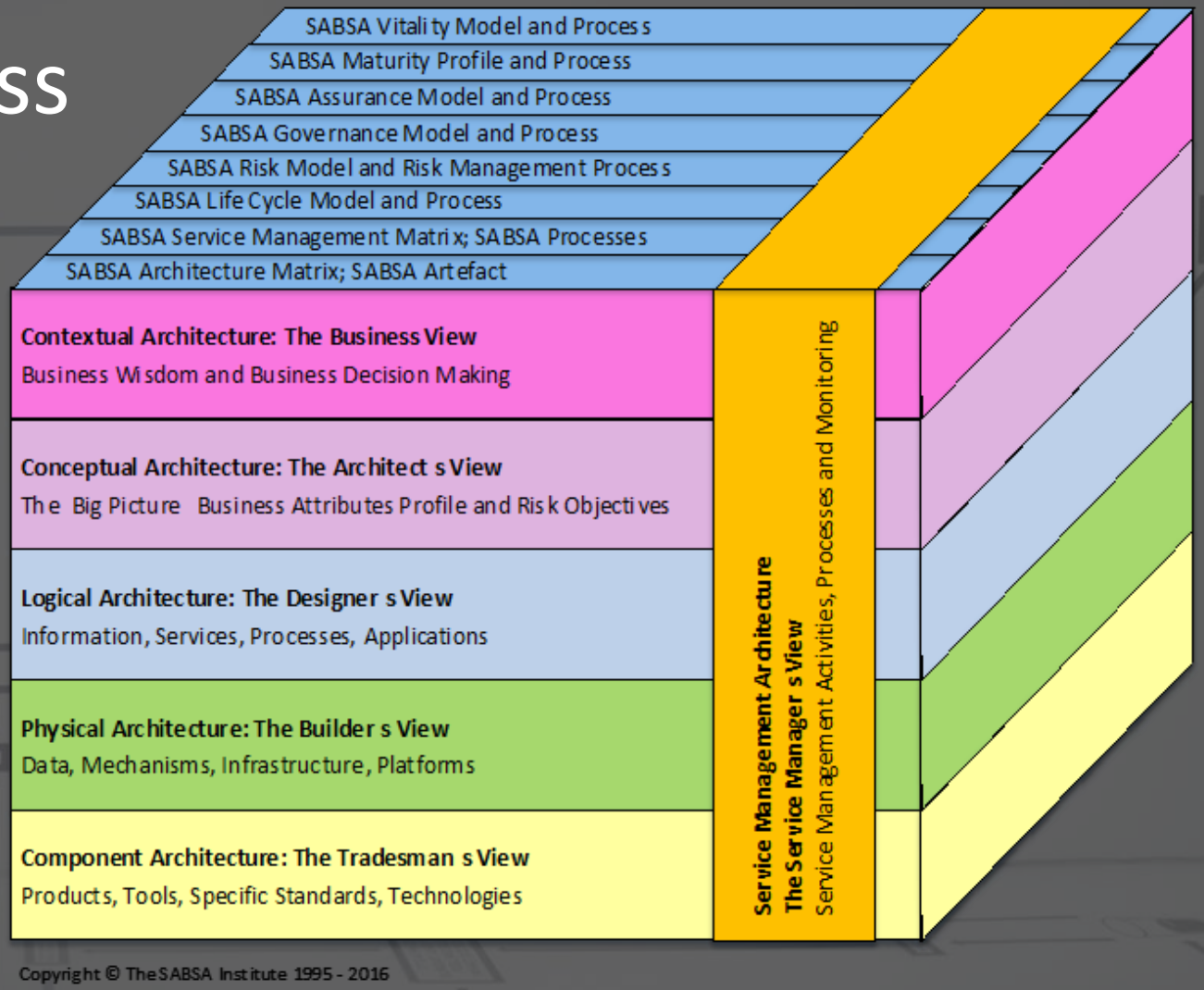
Proprietary (DoDAF, FEAF, EABOK, etc.)

TOGAF

- **T**he **O**pen **G**roup **A**rchitecture **F**ramework
- Orig. 1995, Updated 2019
- Not security focused
- Also published o-ESA (Open Enterprise Security Architecture) – last updated in 2011

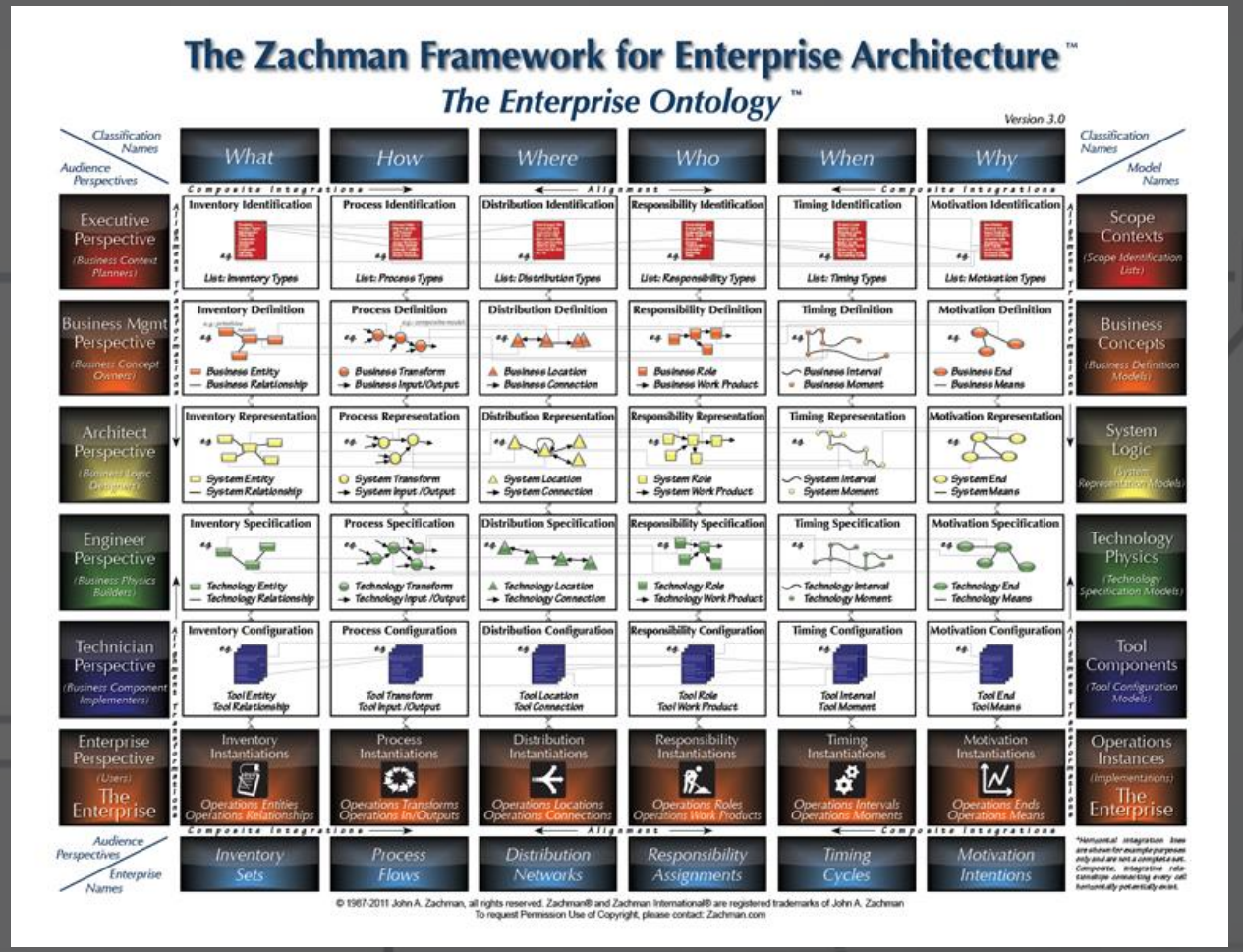
SABSA

- **S**herwood **A**pplied **B**usiness **S**ecurity **A**rchitecture
- Orig. 1995, Updated 2016
- Risk driven
- Similar to Zachman



Zachman

- Created by John Zachman at IBM
- Orig. 1987, Updated 2011
- Described as a “ontology” or a “schema” rather than a methodology



This Thing

(Cloud Security Alliance TCI Reference Architecture)

Business Operation Support Services (BOSS)

Compliance
- Audit Planning
- Contract Authority Maintenance
- Independent Audits
- Third-Party Audits
- Internal Audits
- Info. System Regulatory Mapping
- Intellectual Property Protection

Operational Risk Management
- Operational Risk Committee
- Crisis Management
- Business Impact Analysis
- Key Risk Indicator
- Business Continuity
  - Planning
  - Testing
- Risk Management Framework
  - Business Assessment
  - Technical Assessment
- Independent Risk Management

Human Resources Security
- Employee Termination
- Employment Agreements
- Background Screening
- Job Description
- Rules and Responsibilities
- Employee Awareness
- Employee Code of Conduct

Data Governance
- Data Owner/ Stewardship
- Data Classification
- Handling/Labeling/Security
- Secure Disposal of Data
- Clear Desk Policy
- Rules for Information Leakage Preventions
- Rules for Data Retention

Security Monitoring Services
- SIEM Platform
- Event Mining
- Database Monitoring
- Application Monitoring
- Honey Pot
- End Point Monitoring
- Event Correlation
- Cloud Monitoring
- E-mailing Journaling
- Market Threat Intelligence
- Counter Threat Management
- SOC Portal
- Managed Security Services
- Knowledge Base
- Branding Protection
- Anti-Phishing
- Real-time internetwork defense (SCAP)
- User Behavior and Profile Patterns

Legal Services
- Contracts
- E-Discovery
- Incident Response Legal Preparation

Internal Investigation
- Forensic Analysis
- E-mail Journaling

Information Technology Operations & Support (ITOS)

IT Operation
- Disaster Recovery Plan
  - Plan Management
  - Test Management
- IT Governance
  - Architecture & Governance
  - Standards & Guidance
- Resource Management
  - Segregation of Duties
  - Contractors
- PMO
  - Program Management
  - Project Management
  - Remediation
- Portfolio Management
  - Maturity Model
  - Roadmap
  - Strategy Alignment

Service Delivery
- Service Level Management
  - Objectives
  - Internal SLAs
  - OLAs
  - External SLAs
  - Vendor Management
  - Service Dashboard
- Information Technology Resiliency
  - Availability Management
  - Resiliency Analysis
  - Capacity Planning
- Application Performance Monitoring
- Asset Management
  - Service Costing
  - Operational Budgeting
  - Charge Back
  - Investment Budgeting

Service Support
- Configuration Management
  - Capacity Building
  - Software Management
  - Physical Inventory
  - Automated Asset Discovery
  - Configuration Management
- Knowledge Management
  - Best Practices
  - Trend Analysis
  - Benchmarking
  - Security Job Aids
  - Security FAQ
- Change Management
  - Service Provisioning
  - Approval Workflow
  - Change Review Board
  - Planned Changes
    - Project Changes
    - Operational Changes
  - Emergency Changes
- Incident Management
  - Security Incident Response
  - Automated Ticketing
  - Self-Service
  - Ticketing
  - Cross Cloud Security Incident Response
- Problem Management
  - Event Classification
  - Root Cause Analysis
  - Trend Analysis
  - Problem Resolution
  - Orphan Incident Management
- Release Management
  - Scheduling
  - Testing
  - Build
  - Version Control
  - Source Code Management

Technology Solution Services (TSS)

Presentation Services

Presentation Modality
- Consumer Service Platform
  - Social Media
  - Collaboration
  - Search
  - E-Readers
  - E-mail
- Enterprise Service Platform
  - B2E
  - B2M
  - B2B
  - B2C
  - P2P

Speech Recognition (IVR)

Presentation Platform
- End-Points
  - Mobile Devices
    - Mobile Device Management
  - Portable Devices
  - Fixed Devices
  - Medical Devices
  - Desk Top
    - Company Owned
    - Third Party
    - Public Kiosk
  - Smart Appliances
  - Secure Sandbox

Handwriting (ICR)

Application Services

Programming Interfaces
- Input Validation

Security Knowledge Lifecycle
- Security Design Pattern
- Security Application Framework
- Code Samples
- Attack Patterns

Intergration Middleware

Connectivity & Delivery

Abstraction

Development Process
- Self-Service
  - Security Code Review
  - Application Vulnerability Scanning
  - Stress and Volume Testing
- Software Quality Assurance

Information Services

Service Delivery
- Service Catalog
- SLAs
- OLAs
- Contracts
- Recovery Plans

Data Governance
- Risk Assessments
- Non-production Data
- Information Leakage Metadata
- Data Segregation

Reporting Services
- Dashboards
- Data Mining
- Business Intelligence
- Reporting Tools

BOSS
- Risk Assessments
- Data Classification
- Process Ownership
- Audit Findings
- HR Data (Employees & Contractors)
- Business Strategy

ITOS
- PMO
- Strategy
- Road map
- Problem Management
- Incident Management
- CMDB
- Knowledge Management
- Service Management
- Change Management

Risk Management
- GRC
- RA
- BIA
- DR & BC Plans
- VRA
- TVM (Threat Vulnerability Management)

Service Support
- Configuration Rules (Metadata)
- Service Events
- Configuration Management Database
- Knowledge Repository
- Change Logs

User Directory Service
- Active Directory Services
- Registry Services
- LDAP Repositories
- Location Services
- X.500 Repositories
- Federated Services
- DBMS Repositories
- Virtual Directory Services
- Meta Directory Services

Security Monitoring
- Session Events
- Authorization Events
- Authentication Events
- Application Events
- Network Events
- Computer Events
- Privilege Usage Events
- eDiscovery Events
- DLP Events
- NIPS Events
- Compliance Monitoring
- CRLs
- ACLs
- Database Events
- HIDS-HIPS
- Transformation Services

Infrastructure Services

Internal Infrastructure
- Facility Security
  - Controlled Physical Access
    - Barriers
    - Electronic Surveillance
    - Security Patrols
    - Physical Authentication
  - Asset Handling
    - Data
    - Storage
    - Hardware
  - Environmental Risk Management
    - Physical Security
    - Equipment Location
    - Power Redundancy
- Availability Services
- Patch Management
  - Compliance Monitoring
  - Service Discovery
- Servers
  - Secure Build
  - Image Management
- Equipment Maintenance
- Network Services
  - Network Segmentation
  - Authoritative Time Source
- Storage Services

Virtual Infrastructure
- Desktop "Client" Virtualization
  - Local
  - Remote
    - Session-based
    - VM-Based (VDI)
- Application Virtualization
  - Client-Application Streaming
  - Server-Application Streaming
- Virtual Workspaces
  - Vertical Isolation
- Server Virtualization
  - Virtual Machines (Host-Based)
    - Full
    - Paravirtualization
    - Hardware-assisted
  - OS Virtualization
  - TPM Virtualization
  - Virtual Memory
- Storage Virtualization
  - Block-Based Virtualization
    - Host-Based
      - LDM
      - LVM
      - LUN
    - Storage Device-Based
    - Network-Based
      - Appliance
      - Switched
  - File-Based Virtualization
- Network Virtualization
  - Network Address Space
    - IPv4
    - IPv6
  - External (VLAN)
  - Internal (VNIC)
- Database Virtualization
- Mobile Device Virtualization
- Smartcard Virtualization

Security and Risk Management

Governance Risk & Compliance
- Compliance Management
- Policy Management
  - Exceptions
  - Self-Assessment
- Vendor Management
- Audit Management
- IT Risk Management
- Technical Awareness & Training

InfoSec Management
- Capability Mapping
- Maturity Model
- Risk Portfolio Management
- Risk Dashboard
- Residual Risk Management

Privilege Management Infrastructure
- Identity Management
  - Domain Unique Identifier
  - Federated IDM
  - Identity Provisioning
  - Attribute Provisioning
- Authentication Services
  - SAML Token
  - Risk-Based Authentication
  - Multi-Factor Authentication
  - OTP
  - Smart Card
  - Password Management
  - Biometrics
  - Network Authentication
  - Single Sign On
  - WS-Security
  - Middleware Authentication
  - Identity Verification
  - Out of the Box (OTB) Authentication
- Authorization Services
  - Entitlement Review
  - Policy Enforcement
  - Policy Definition
  - Policy Management
  - Principal Data Management
  - Resource Data Management
  - XACML
  - Obligation
  - Out of the Box (OTB) Authorization
- Privilege Usage Management
  - Keystroke / Session Logging
  - Password Vaulting
  - Privilege Usage Gateway
  - Resource Protection
  - Hypervisor Compliance and Governance

Threat & Vulnerability Management
- Compliance Testing
  - Databases (DBs)
  - Servers
  - Networks
- Vulnerability Management
  - Application
  - Infrastructure
  - DB
- Penetration Testing
  - Internal
  - External
- Threat Management
  - Source Code Scanning
  - Risk Taxonomy

Infrastructure Protection Services
- Server
  - Behavioral Malware Prevention
  - White Listing
  - Sensitive File Protection
  - HIPS / HIDS
  - Anti-Virus
  - Host Firewall
- Endpoint
  - Anti-Virus, Anti-Spam, Anti-Malware
  - HIPS / HIDS
  - Host Firewall
  - Media Lockdown
  - Hardware-Based Trusted Assets
  - Behavioral Malware Prevention
  - Inventory Control
  - Content Filtering
  - Forensic Tools
  - White Listing
- Network
  - Behavioral Malware Prevention
  - Firewall
  - Content Filtering
  - DPI
  - NIPS / NIDS
  - Wireless Protection
  - Link Layer Network Security
  - Black Listing Filtering
- Application
  - XML Appliance
  - Secure Messaging
  - Application Firewall
  - Secure Collaboration
  - Real Time Filtering

Data Protection
- Data Life Cycle Management
  - Meta Data Control
  - eSignature (Unstructured Data)
  - Data De-Identification
  - Life Cycle Management
  - Data Masking
  - Data Obscuring
  - Data Tagging
  - Data Seeding
- Data Loss Prevention
  - Data Discovery
  - Network (Data in Transit)
  - Endpoint (Data in Use)
  - Server (Data at Rest)
- Intellectual Property Protection
  - Intellectual Property
  - Digital Rights Management
- Cryptographic Services
  - Key Management
    - Symmetric Keys
    - Asymmetric Keys
  - PKI
  - Signature Services
  - Data in Use Encryption (Memory)
  - Data in Transit Encryption (Transitory, Fixed)
  - Data at Rest Encryption (DB, File, SAN, Desktop, Mobile)

Policies & Standards
- Operational Security Baselines
- Job Aid Guidelines
- Role Based Awareness
- Information Security Policies
- Technical Security Standards
- Data / Asset Classification
- Best Practices & Regulatory Correlation

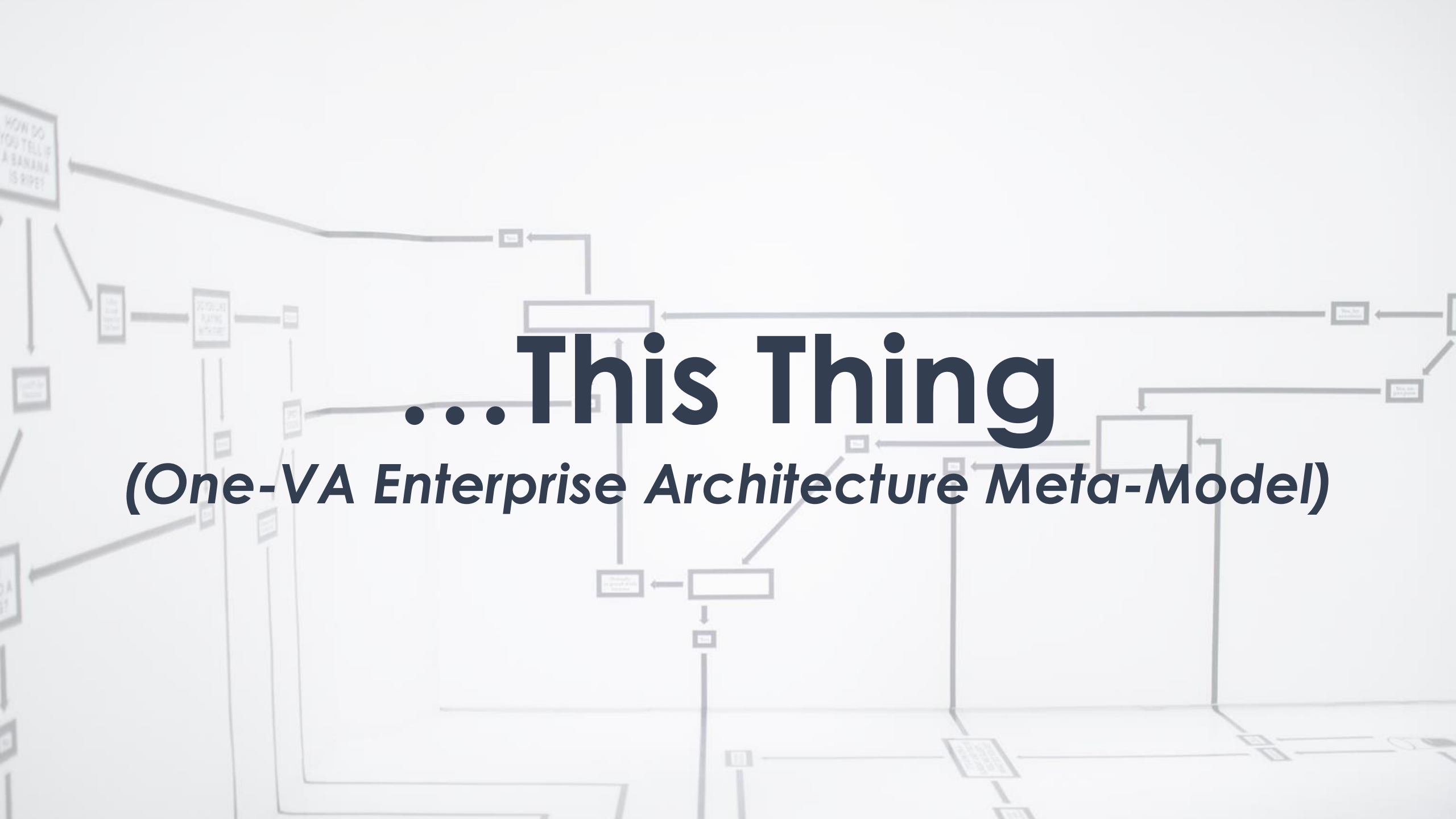
Enterprise Architecture / Trusted Cloud Initiative Reference Mapping Classifications

- Key Domain
- Solution Domains
- Domains
- Component Groups
- Component Sub Groups
- Controls

Lead Authors: Jon-Michael C. Brook, Michael Roza

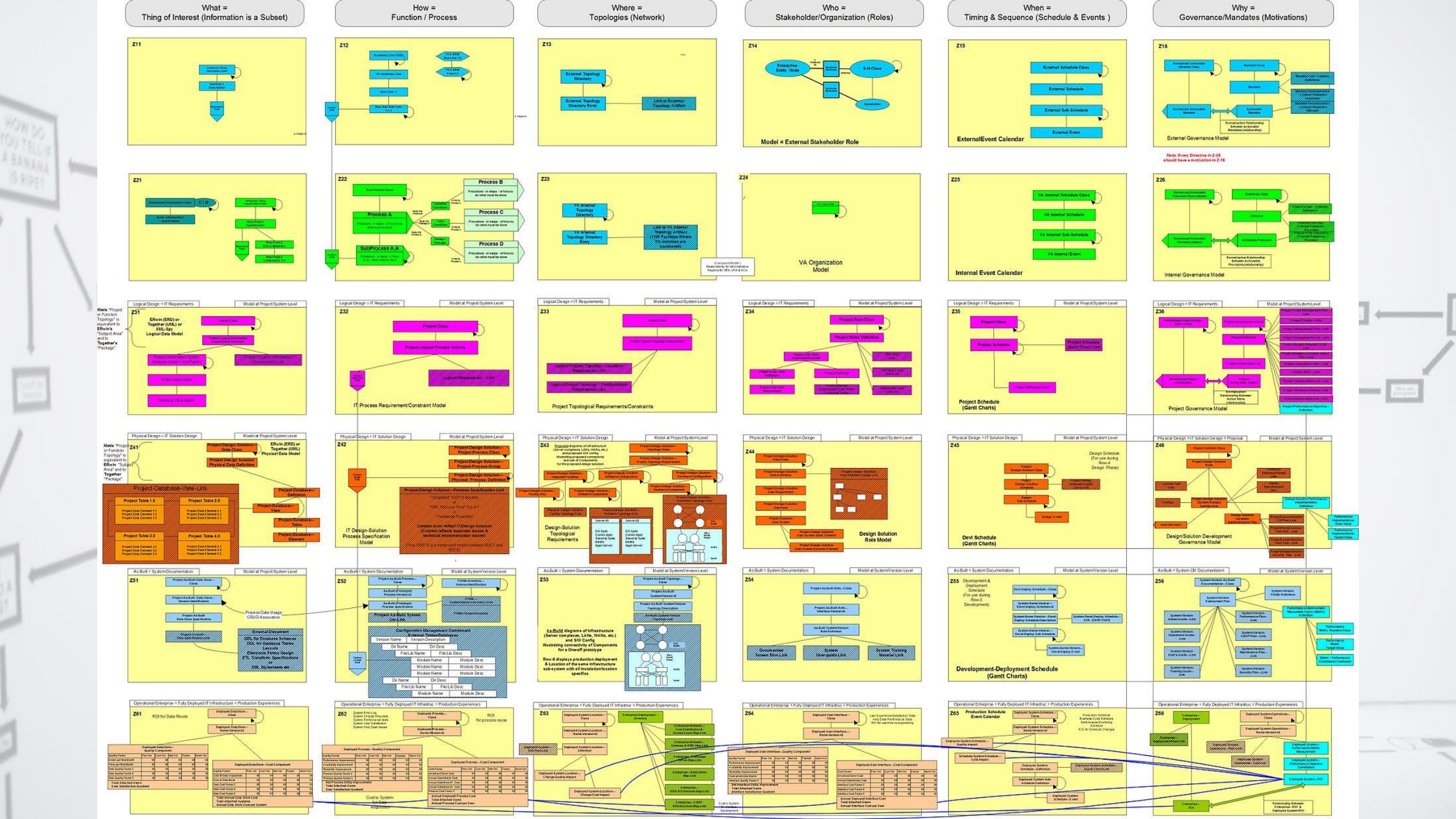
Contributors: Shawn Harris, Sunil Shanthi, Michael Theriault, Rolando Marcelo Vallejos, Ashish Vashishtha, Suri Venkat, Henry Wenchan

CSA Team: Sean Heide, Jim Reavis, AnnMarie Ulskey (Design), John Yeoh



…This Thing

(One-VA Enterprise Architecture Meta-Model)


What =
Thing of Interest (Information is a Subset)
How =
Function / Process
Where =
Topologies (Network)
Who =
Stakeholder/Organization (Roles)
When =
Timing & Sequence (Schedule & Events)
Why =
Governance/Mandates (Motivations)
Z11
Z12
Z13
Z14
Z15
Z16
Model = External Stakeholder Role
ExternalEvent Calendar
External Governance Model
Note: Every Directive in Z-26
should have a motivation in Z-16
Z21
Z22
Z23
Z24
Z25
Z26
VA Organization
Model
Internal Event Calendar
Internal Governance Model
Z31
Z32
Z33
Z34
Z35
Z36
IT Process Requirement/Constraint Model
Project Topological Requirements/Constraints
Project Schedule
(Gantt Charts)
Project Governance Model
Z41
Z42
Z43
Z44
Z45
Z46
IT Design-Solution
Process Specification
Model
Design-Solution
Topological
Requirements
Design Solution
Role Model
Devi Schedule
(Gantt Charts)
Design/Solution Development
Governance Model
Z51
Z52
Z53
Z54
Z55
Z56
Development-Deployment Schedule
(Gantt Charts)
Z61
Z62
Z63
Z64
Z65
Z66

The good

- We can pull out the good features from some of these "legacy" architecture frameworks
- TOGAF
  - Architecture Development model – tailor it down and use it like an architecture lifecycle
  - Deliverables – just don't try to adopt all of it, it's too much

The good (cont.)

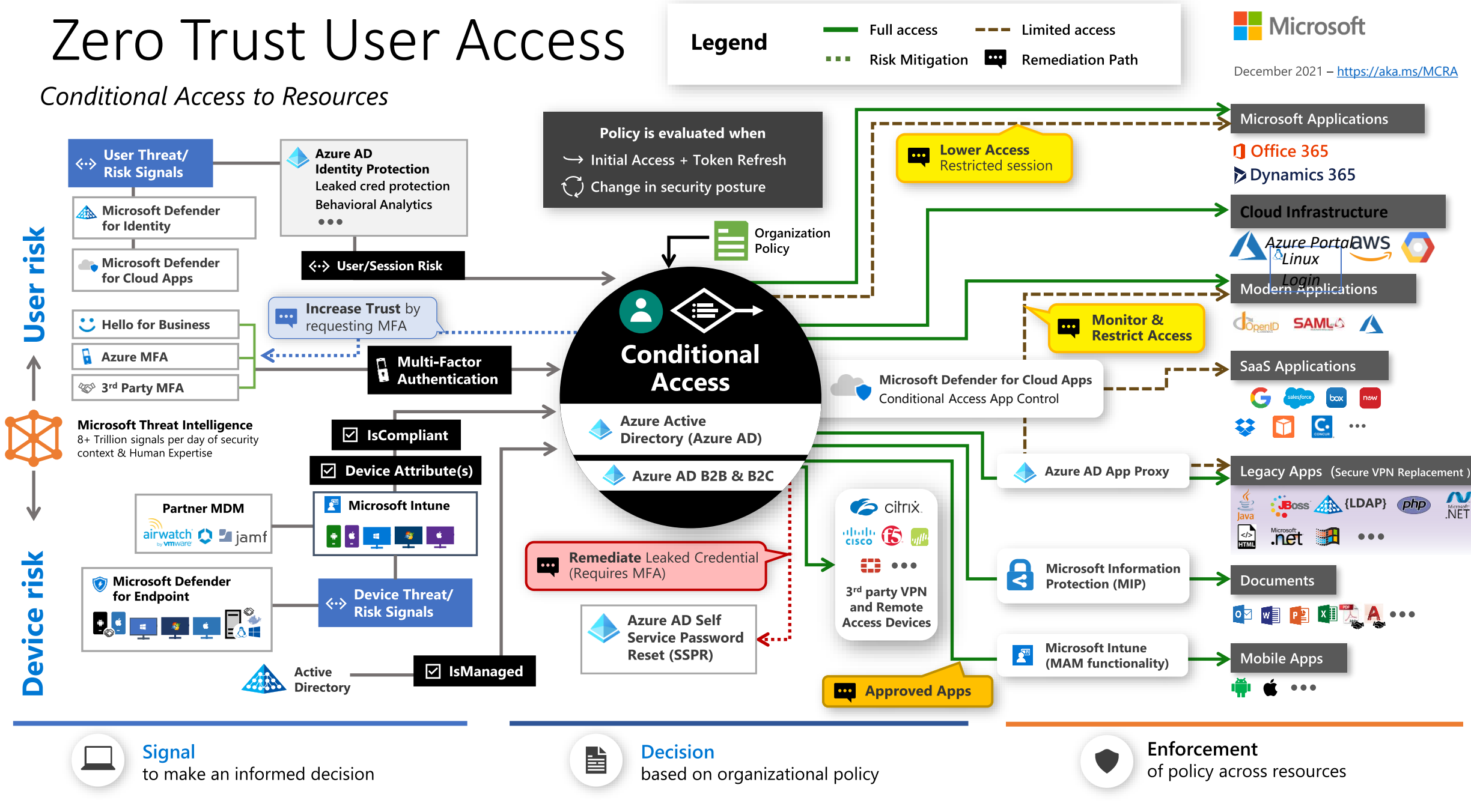
- TOGAF (cont.)
  - Content metamodel – treat it like an “architecture style guide”
- Zachman
  - How to craft meaningful views and viewpoints, how to think from a stakeholder perspective
- SABSA
  - Zachmann, but security

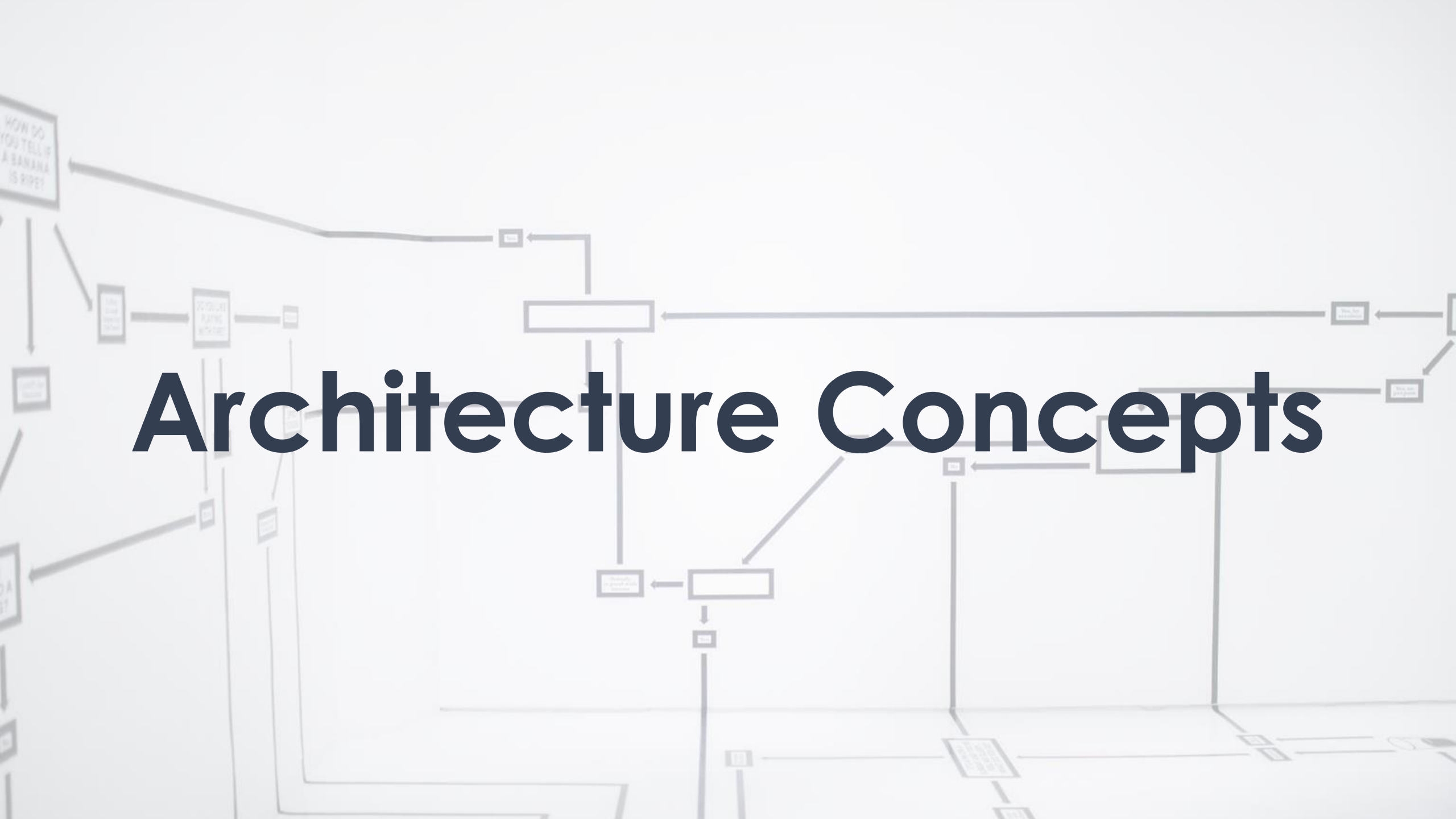
And This Thing

(Microsoft's Zero Trust IAM Reference Architecture)

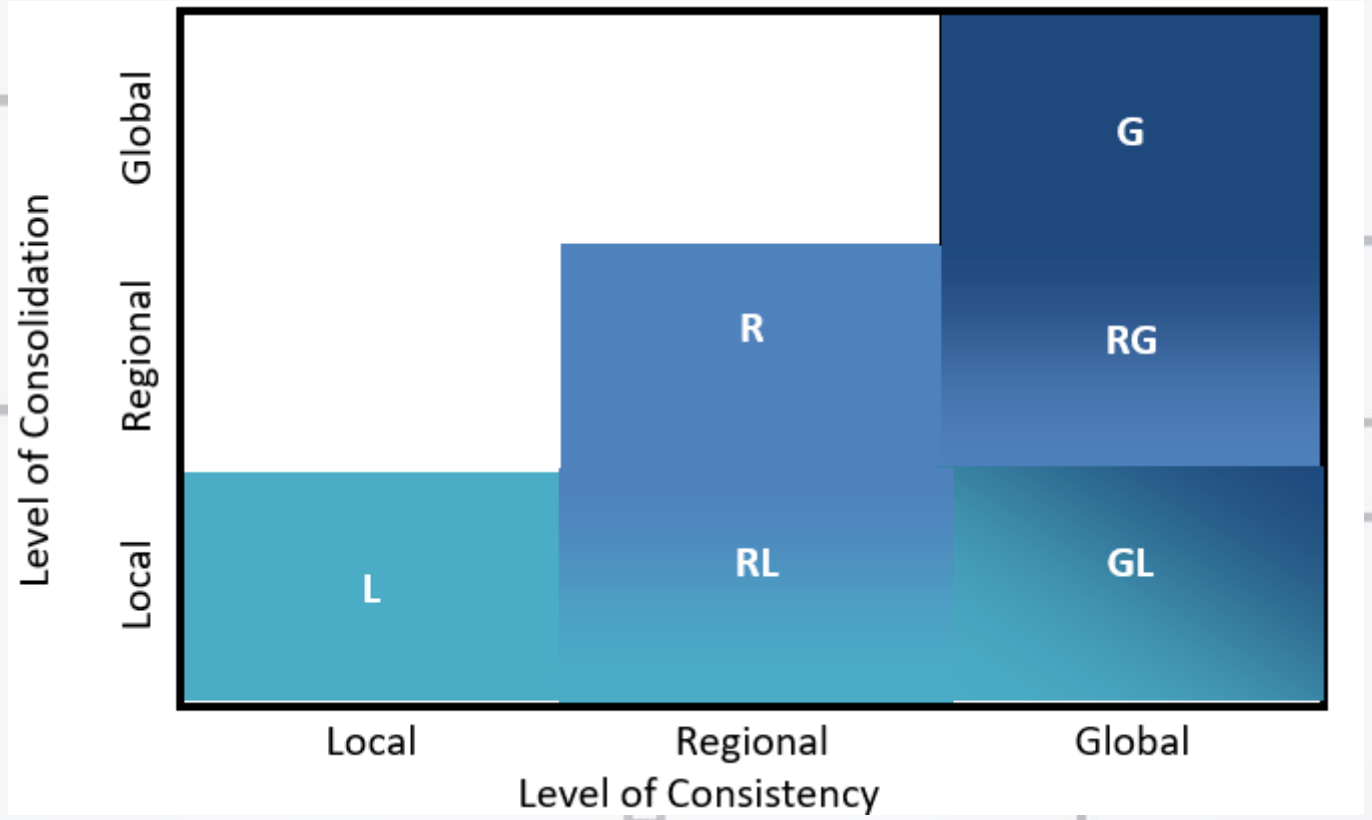
Zero Trust User Access

Conditional Access to Resources

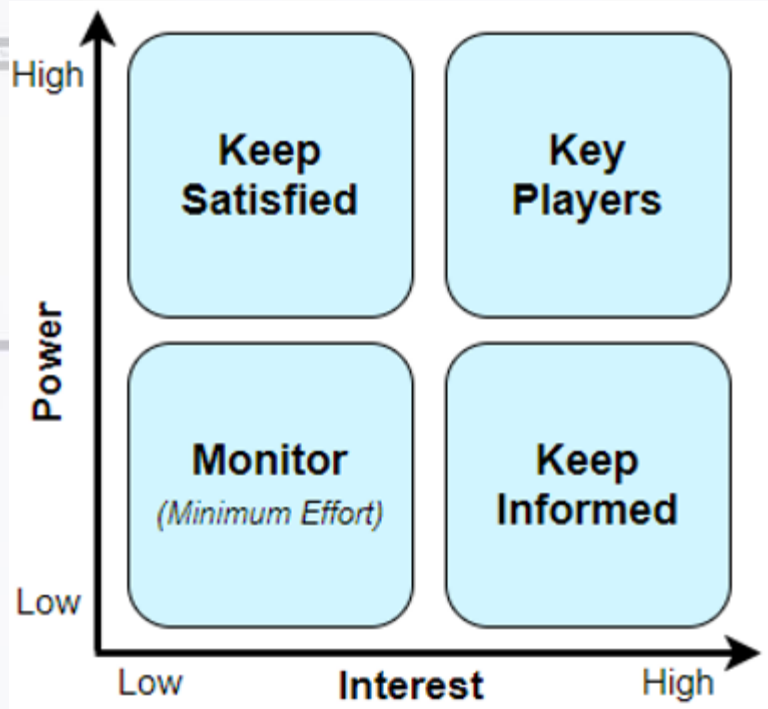




Architecture Concepts



Architecture Commonality



Stakeholder Management

Enterprise Architecture Elements	Enterprise Architecture Levels
Architecture Process	0 - None
Architecture Development	1 - Initial
Business Linkage	2 - Under Development
Senior Management Involvement	3 - Defined
Architecture Communication	4 - Managed
IT Security	5 - Measured
Architecture Governance	
IT Investment and Acquisition Strategy	

Architecture Conformance
0 - Irrelevant
1 - Consistent
2 - Compliant
3 - Conformant
4 - Fully Conformant
5 - Non-Conformant

Architecture Maturity

Architecture Compliance

Architecture Metrics

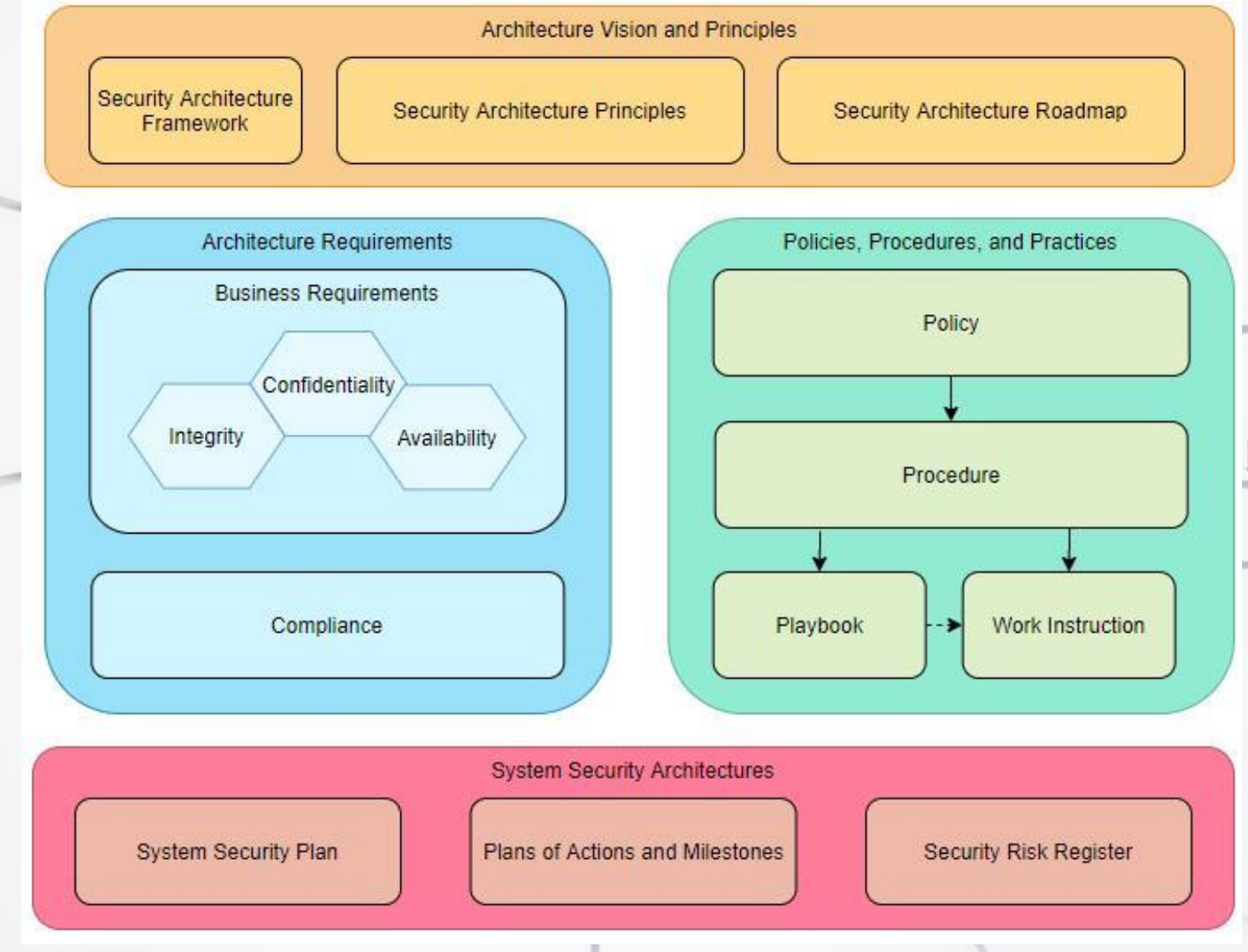
Views / Viewpoints

- Views: Representations of the overall architecture that are meaningful to one or more stakeholders in the system.
  - Generic and can be stored in libraries for reuse
- Viewpoint: The perspective from which a view is taken.
  - Always specific to the architecture for which it is created
- A viewpoint defines how to construct and use a view, the information that should appear in the view, the modelling techniques for expressing and analyzing the information, and a rationale for these choices.

Security Architecture Concepts

- Threat Modelling
- Design for Malice
- Bake in Zero Trust / Defense in Depth / etc
- Define CIA (confidentiality, integrity, and availability) goals
- USABILITY IS SECURITY

How a tailored architecture can act as a style guide



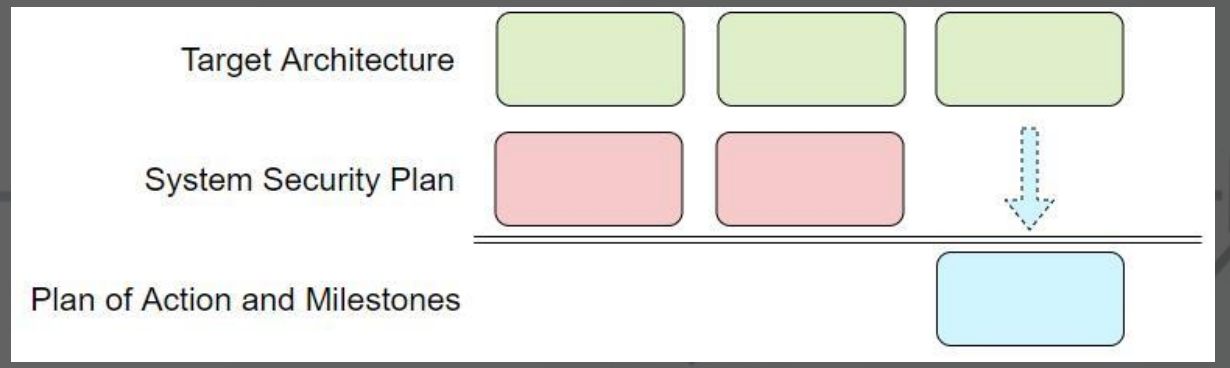
Content MetaModel

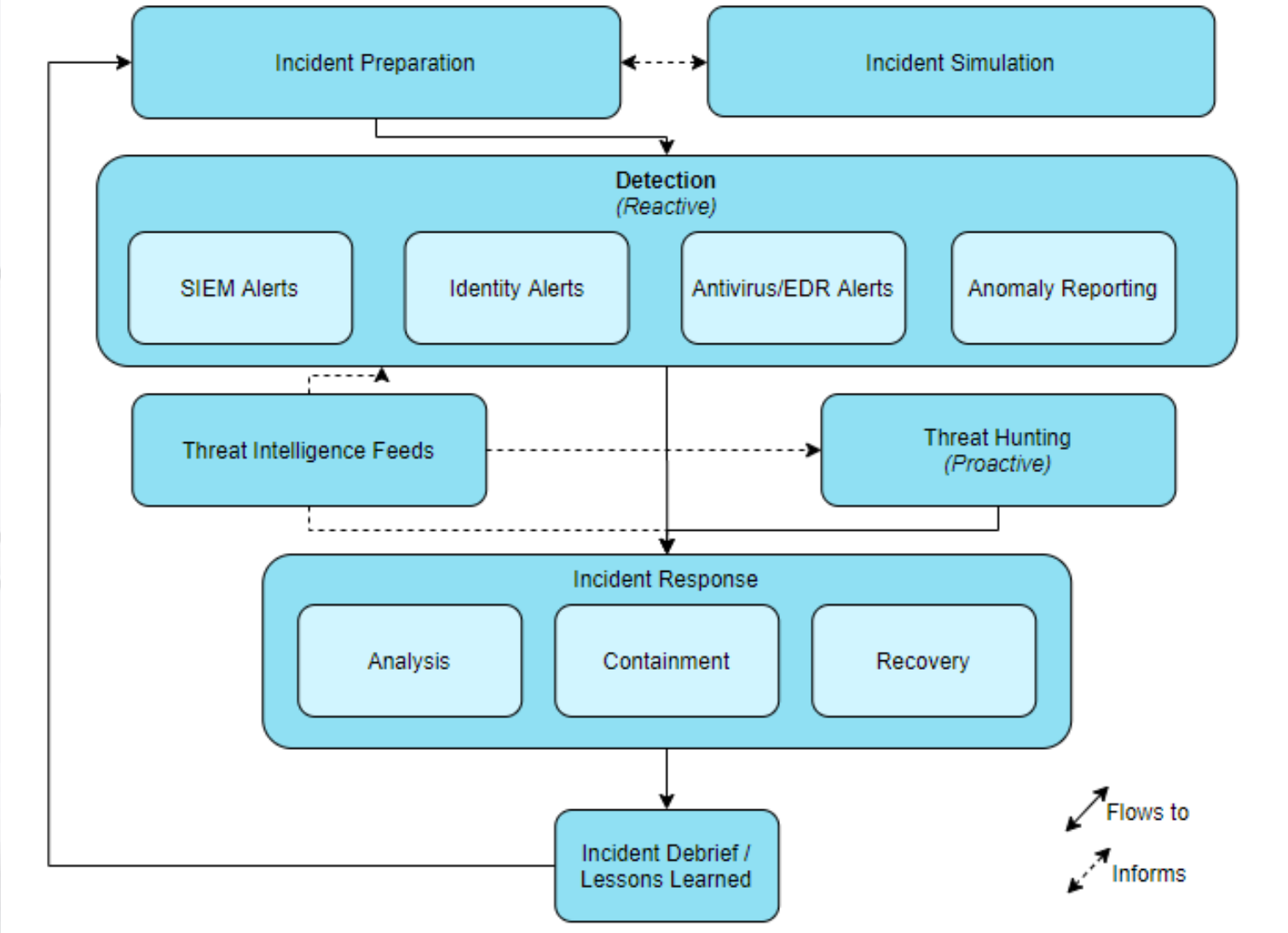
Architecture Content

Architecture Charter
Gap Analysis
System Security Plans
Reference Architecture
Architecture Definitions

Architecture Content

- Charter
- Gap Analysis
- System Security Plans
- Reference Architectures
- Architecture Definitions





Example Reference Architecture:
Incident Detection

Tl;dr

- Enterprise security architecture provides a common language and framework for security implementations
- The existing architecture frameworks are OLD, and/or made for organizations that are HUGE
- You can pick and chose which pieces to implement to create a model that works for your organization

Enterprise Security Architecture isn't just for enterprises

Questions
Twitter: @HomeBrewedSec

Slides
HomeBrewedSec.com/Talks