Enhanced Consistency and Interoperability: Defense Standards at OMG

March 18, 2025

MATT WILSON (SIMVENTIONS), MIKE ABRAMSON (ASMG)
CO-CHAIRS, C4I (DEFENSE AND MILITARY) DTF

Enhanced Consistency and Interoperability: Defense Standards at OMG

Agenda

- Forging the Future: Synergy in Standards Development
  - Paul Gustavson – SISO
- DevSecOps and MOSA EE Working Groups – update/status
  - Matt Wilson – SimVentions / OMG C4I Defense and Military DTF

Break 3:00 – 3:15

- Data Centric Security
  - Mike Abramson ASMG - / OMG C4I Defense and Military DTF
- Overview of C4I DM DTF Specifications and Current efforts
  - Matt Wilson and Mike Abramson - OMG C4I Defense and Military DTF Co-Chairs
- Intelligence Community - Data Reference Architecture
  - Jasmin Leveille – Office of the Intelligence Community – Chief Data Officer
- Discussion / Next Steps

OMG Standards Development Organization

FORGING THE FUTURE: SYNERGY BETWEEN OMG & SISO IN STANDARDS DEVELOPMENT

PAUL GUSTAVSON - SISO

Forging the Future: Synergy Between OMG & SISO in Standards Development

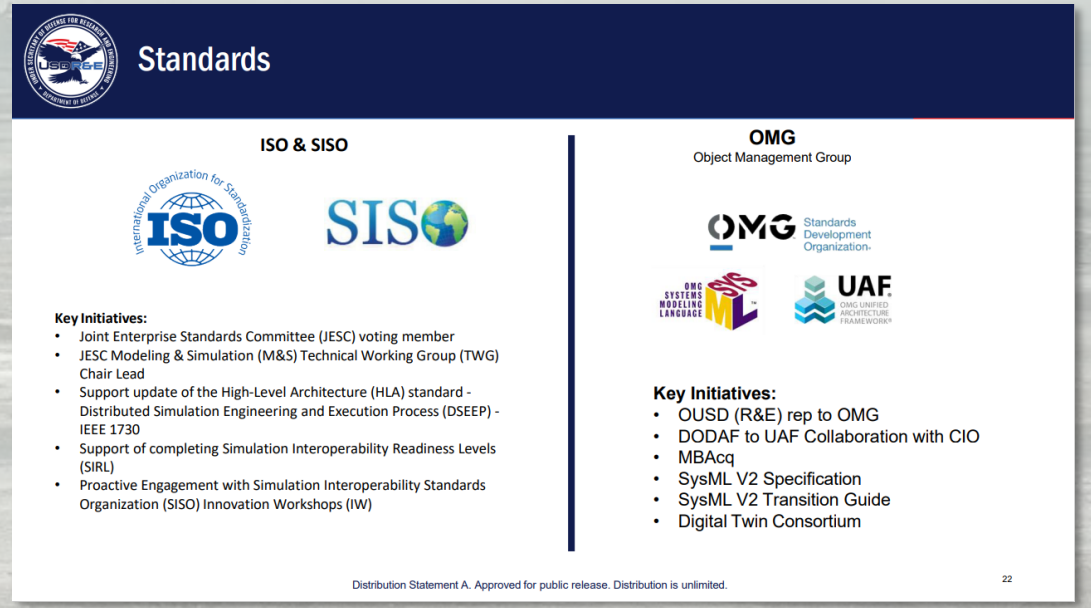
Strengthening Interoperability & Innovation for the Defense Community

Presented by: Paul Gustavson, SISO Representative
Conference: OMG Defense Standards Forum

The Challenge

The Power of Standards

- **Why Standards Matter:**
  - Drive **interoperability** across systems and domains
  - Reduce **costs** and integration **risks**
  - Enable **rapid innovation and scalability**
  - Ensure **longevity and adaptability** of solutions



- **Shared Mission:** OMG and SISO both champion standards to accelerate progress and improve interoperability in complex systems.

Recognizing OMG's Impact

- **OMG's Contributions to Standards Development:**
  - Unified Modeling Language (UML)
  - System Modeling Language (SysML)
  - Data Distribution Service (DDS)
  - Unified Architecture Framework (UAF)
  - Business Process Modeling (BPMN)
  - Common Object Request Broker Architecture (CORBA)
- **OMG's Influence:** Decades of impact in commercial and defense sectors, shaping industry-wide best practices.

Introducing SISO

- **Who We Are:**
  - The Simulation Interoperability Standards Organization (SISO) is a leader in modeling and simulation (M&S) standards.
- **What We Do:**
  - Advance **modeling and simulation (M&S) interoperability and reuse** through internationally recognized standards.
  - Develop and maintain **interoperability standards** for live, virtual, and constructive (LVC) simulation.
  - **Support and connect** M&S developers, procurers, and users worldwide.
  - **Foster collaboration** between government, industry, and academia.
  - Serve as a **key technical resource** for M&S interoperability.
- **Our Connection to OMG:**
  - Shared vision for system-of-systems integration and digital transformation.

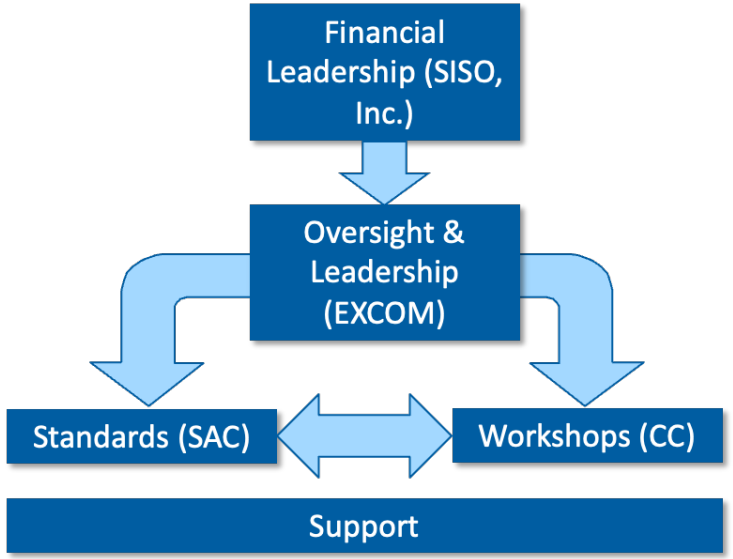


Image: SISO Structure

SISO's Key Standards & Initiatives

- **SISO's Contributions to Standards Development:**
  - Distributed Interactive Simulation (DIS) / High-Level Architecture (HLA)
  - Distributed Simulation Engineering and Execution Process (DSEEP)
  - Distributed Modeling & Simulation Architecture and Ontology (DMAO)
  - Cyber Data Exchange Model (CyberDEM)
  - Real-time Platform Reference (RPR) FOM / Space Reference Federation Object Model (SpaceFOM)
  - Base Object Models (BOMs)
  - Simulation Readiness Level (SRL)
  - Common Image Interface (CIGI)
  - Simulation Reference Markup Language (SRML)

- **Emerging Focus Areas:**
  - Digital Engineering & Digital Twins
  - AI and Data-Driven Simulation
  - XR (Extended Reality) for Defense Applications

SISO Affiliations

NATO Modelling & Simulation Group (NMSG)

- SISO signed a Technical Cooperation Agreement (TCA) with the NMSG in 2007.
  - *The two organizations signed a revised TCA during I/ITSEC 2019.*
- SISO and NMSG work closely together with close coordination through NATO M&S Groups aligned with SISO standards.

SISO has working relationships and/or MOUs with other organizations, including:

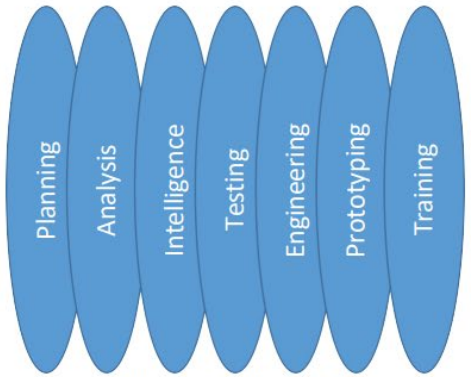
- IEEE - Institute of Electrical and Electronics Engineer
- NTSA - National Training & Simulation Association
- ETSA - European Training & Simulation Association
- IT^{2}EC - International Training Technology Exhibition & Conference
- NATO M&S Center of Excellence
- OGC - Open Geospatial Consortium
- DSET - Defence Simulation Education & Training
- *More to come*

The Synergy Between OMG & SISO

- **Where We Align:**
  - Model-Based Engineering and Digital Twins
  - System-of-Systems Interoperability
  - Standards for Defense, Aerospace, and Industry
- **Potential Collaborative Opportunities:**
  - Joint working groups on M&S and MBSE integration.
  - Harmonizing interoperability frameworks across OMG and SISO standards.
  - Expanding participation and cross-pollination between communities.

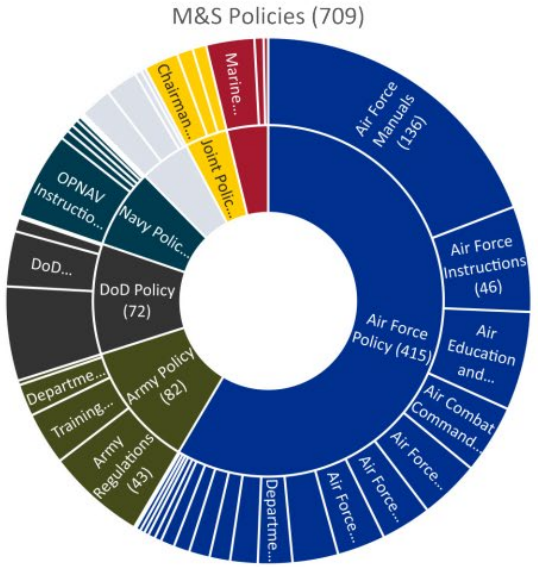
The Opportunity

What do we Mean by Saying "M&S"



"Seven Surfboards"

Modeling Levels



The Opportunity

"Everyone thinks their job in the Silo is the most important.

Mine actually is." — *Juliette Nichols*

A Call to Action – Shaping the Future Together

> "Everyone thinks their job in the Silo is the most important.
>
> Mine actually is." — *Juliette Nichols*

- **The Challenge:** Future mission success depends on interoperability, adaptability, and alignment across digital and physical domains.
- **The Opportunity:** By working together, OMG and SISO can accelerate innovation, enhance interoperability, and future-proof standards for evolving defense and industry needs.
- **Join the Conversation:**
  - Engage with SISO Working Groups
  - Explore Cross-Industry Collaboration
  - Influence the Next Generation of Standards

Closing & Contact Information

> "Everyone thinks their job in the Silo is the most important.
>
> Mine actually is." — *Juliette Nichols*

- **Final Thought:** "The future of standards is not just about compliance—it's about shaping a smarter, more connected world."
- **How to Get Involved:**
  - **Visit** *www.sisostandards.org*
  - **Attend** SISO Conferences & Workshops
  - **Present** White Papers
  - **Connect** with OMG & SISO Communities
  - **Share** about your Silo with SISO

- **Contact:** Paul Gustavson, paulgustavson@simventions.com

Background slides

SISO Mission

The Simulation Interoperability Standards Organization (SISO) is an organization :

- Dedicated to the promotion of modeling and simulation (M&S) interoperability and reuse
- Internationally recognized M&S standards development and support organization
- Benefits diverse modeling and simulation communities, including developers, procurers, and users, worldwide

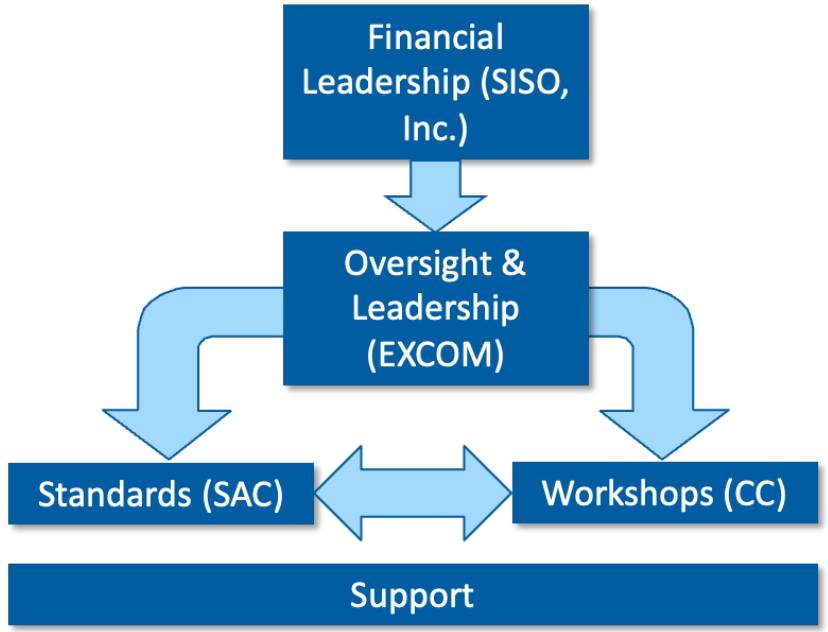


Image: SISO Structure

SISO Overview

Formation of SISO

- Distributed Interactive Simulation (DIS) Workshops in the 1990s led to the formation of SISO.
- The U.S. DoD Defense Modeling and Simulation Office sponsored the establishment of SISO.
- SISO was formed in 1997 as a Non-Profit Corporation.

SISO Membership

- SISO currently has approximately 400 individual members.

SISO Sponsorship

- SISO currently has approximately 17 organizational sponsors/members.

Simulation Innovation Workshop (SIW)

- SISO holds an annual workshop (SIW) every February in Orlando, FL.

SIMposium

- SISO also holds a two-day virtual event every September.

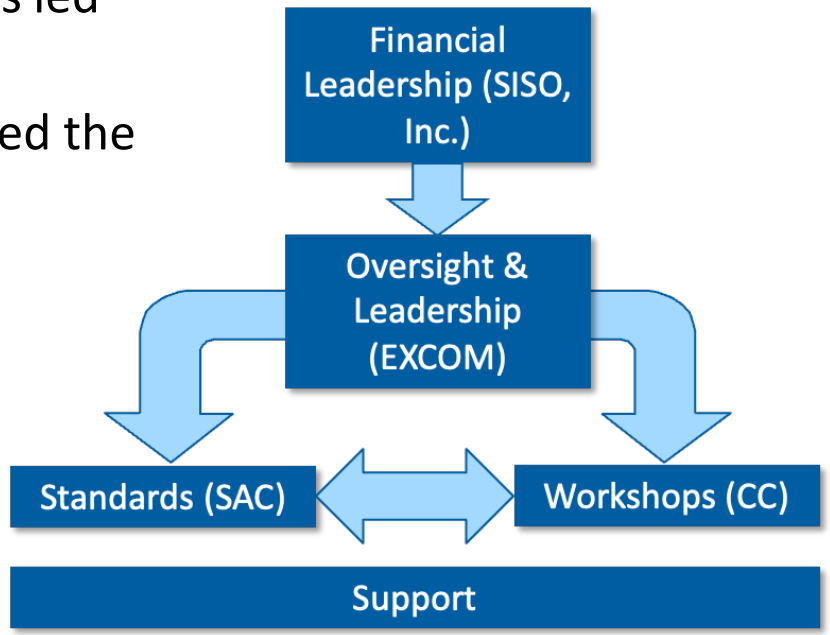


Image: SISO Structure

SISO Products

SISO has published an array of:

- Standards Products
- Guidance Products
- Reference Products
- Associated data files, schemas, and templates

IEEE recognizes the SISO Standards Activity Committee (SAC) as the IEEE Computer / Simulation Interoperability (C/SI) Standards Committee. The C/SI sponsors three series of IEEE Standards:

- IEEE Std 1278™ — Distributed Interactive Simulation (DIS)
- IEEE Std 1516™ — High Level Architecture for M&S (HLA)
- IEEE Std 1730™ — Distributed Simulation Engineering and Execution Process (DSEEP)

Enhanced Consistency and Interoperability: Defense Standards at OMG

March 18, 2025

MATT WILSON (SIMVENTIONS), MIKE ABRAMSON (ASMG)
CO-CHAIRS, C4I (DEFENSE AND MILITARY) DTF

Enhanced Consistency and Interoperability: Defense Standards at OMG

Agenda

- Forging the Future: Synergy in Standards Development
  - Paul Gustavson – SISO
- DevSecOps and MOSA EE Working Groups – update/status
  - Matt Wilson – SimVentions / OMG C4I Defense and Military DTF

Break 3:00 – 3:15

- Data Centric Security
  - Mike Abramson ASMG - / OMG C4I Defense and Military DTF
- Overview of C4I DM DTF Specifications and Current efforts
  - Matt Wilson and Mike Abramson - OMG C4I Defense and Military DTF Co-Chairs
- Intelligence Community - Data Reference Architecture
  - Jasmin Leveille – Office of the Intelligence Community – Chief Data Officer
- Discussion / Next Steps

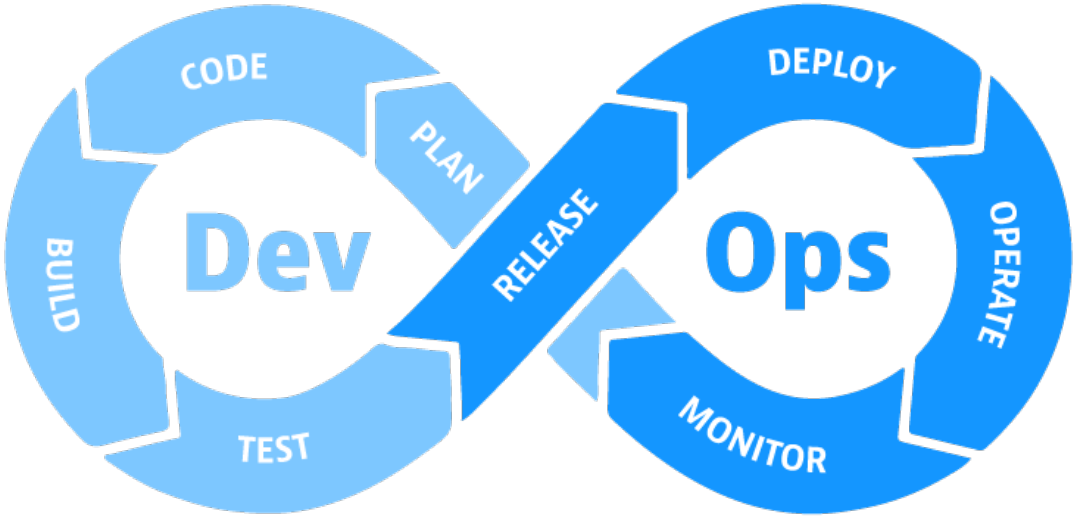
OMG Standards Development Organization

DevSecOps and MOSA EE Working Groups – update/status

MATT WILSON – SIMVENTIONS / C4I DM DTF CO-CHAIR

❑ What is DevOps? https://software.af.mil/training/devops/

- **DevOps** is a software engineering culture and practice that aims at unifying software development (Dev) and software operation (Ops). The main characteristic of the DevOps movement is to strongly advocate automation and monitoring at all steps of software construction, from integration, testing, releasing to deployment and infrastructure management. DevOps aims at shorter development cycles, increased deployment frequency, and more dependable releases, in close alignment with business objectives.
- **DevOps is NOT ENOUGH!**



OMG Standards Development Organization

But why is DevOps not enough?

- National Security Systems
- Weapons Systems
- Banking
- Healthcare
- Space
- Transportation
- Power Grid / Production
- PII / Customer Data
- Others

Setting the stage

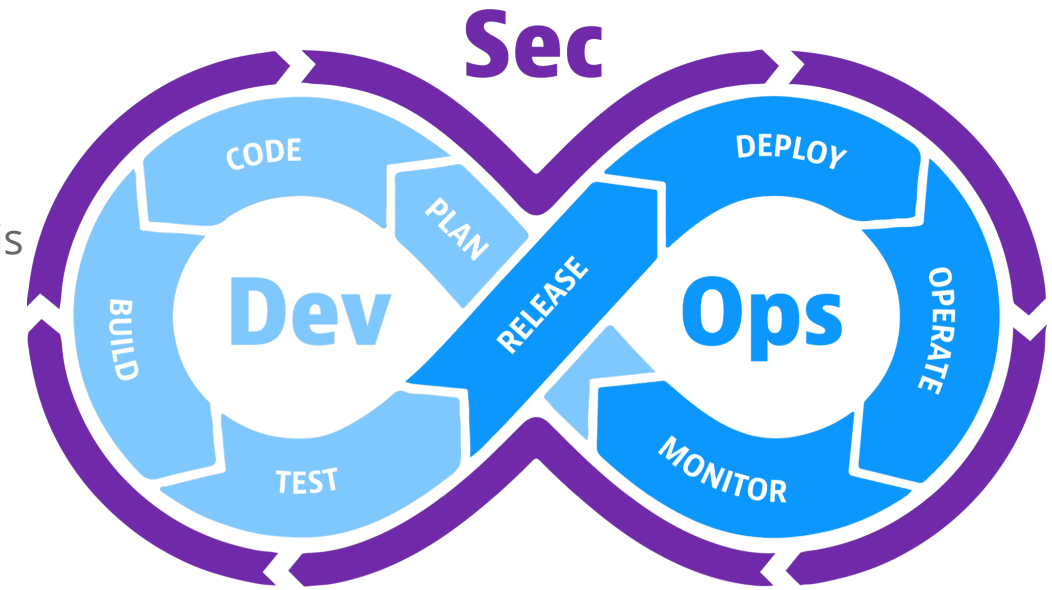
❑ But What is DevSecOps?

https://software.af.mil/training/devops/

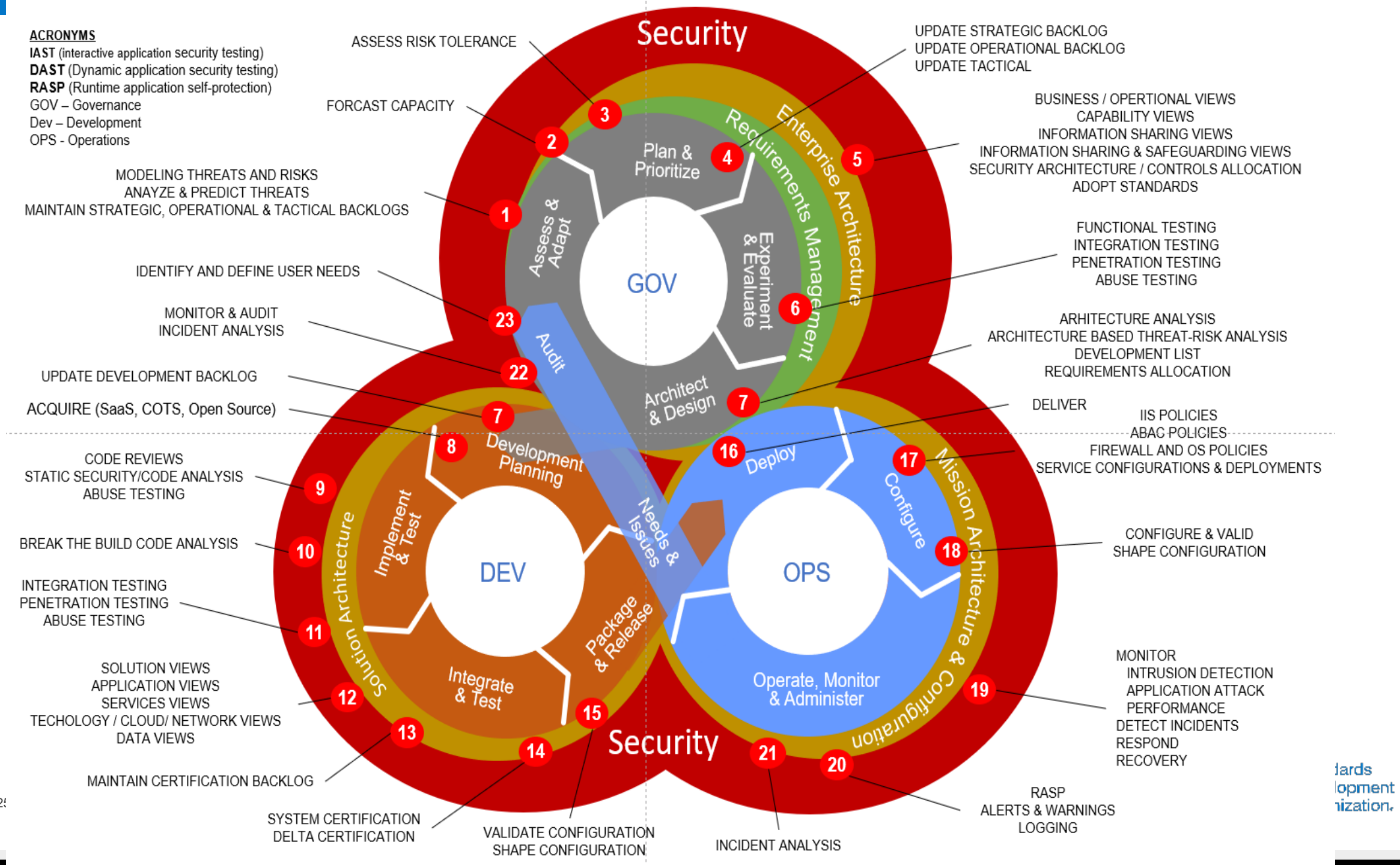
- ➢ DevSecOps is what must be implemented with the cybersecurity stack built-in into the DevOps pipeline.

❑ DevSecOps Metrics

- Ability to detect and prevent security flaws and injections
- Ability to perform fuzzing and static/dynamic source code analysis
- Ability to monitor container security including container base images and libraries



OMG Standards Development Organization


ACRONYMS
IAST (interactive application security testing)
DAST (Dynamic application security testing)
RASP (Runtime application self-protection)
GOV – Governance
Dev – Development
OPS - Operations
Security
ASSESS RISK TOLERANCE
FORCAST CAPACITY
MODELING THREATS AND RISKS
ANAYZE & PREDICT THREATS
MAINTAIN STRATEGIC, OPERATIONAL & TACTICAL BACKLOGS
IDENTIFY AND DEFINE USER NEEDS
MONITOR & AUDIT
INCIDENT ANALYSIS
UPDATE DEVELOPMENT BACKLOG
ACQUIRE (SaaS, COTS, Open Source)
CODE REVIEWS
STATIC SECURITY/CODE ANALYSIS
ABUSE TESTING
BREAK THE BUILD CODE ANALYSIS
INTEGRATION TESTING
PENETRATION TESTING
ABUSE TESTING
SOLUTION VIEWS
APPLICATION VIEWS
SERVICES VIEWS
TECHOLOGY / CLOUD/ NETWORK VIEWS
DATA VIEWS
MAINTAIN CERTIFICATION BACKLOG
SYSTEM CERTIFICATION
DELTA CERTIFICATION
VALIDATE CONFIGURATION
SHAPE CONFIGURATION
INCIDENT ANALYSIS
RASP
ALERTS & WARNINGS
LOGGING
MONITOR
INTRUSION DETECTION
APPLICATION ATTACK
PERFORMANCE
DETECT INCIDENTS
RESPOND
RECOVERY
CONFIGURE & VALID
SHAPE CONFIGURATION
DELIVER
IIS POLICIES
ABAC POLICIES
FIREWALL AND OS POLICIES
SERVICE CONFIGURATIONS & DEPLOYMENTS
ARHITECTURE ANALYSIS
ARCHITECTURE BASED THREAT-RISK ANALYSIS
DEVELOPMENT LIST
REQUIREMENTS ALLOCATION
FUNCTIONAL TESTING
INTEGRATION TESTING
PENETRATION TESTING
ABUSE TESTING
BUSINESS / OPERTIONAL VIEWS
CAPABILITY VIEWS
INFORMATION SHARING VIEWS
INFORMATION SHARING & SAFEGUARDING VIEWS
SECURITY ARCHITECTURE / CONTROLS ALLOCATION
ADOPT STANDARDS
UPDATE STRATEGIC BACKLOG
UPDATE OPERATIONAL BACKLOG
UPDATE TACTICAL
Plan & Prioritize
Requirements Management
Enterprise Architecture
Assess & Adapt
Experiment & Evaluate
GOV
Audit
Architect & Design
Development Planning
Implement & Test
Integrate & Test
Package & Release
Solution Architecture
DEV
Needs & Issues
Deploy
Configure
Operate, Monitor & Administer
Mission Architecture & Configuration
OPS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

What are we doing here?

Continuing a Conversation among…

- Customers / Buyers of technology products
- Systems Implementors / Users of DevSecOps to create systems
- Mainstream DevOps/DevSecOps Pipeline Vendors
- Niche technology providers

Why the OMG?

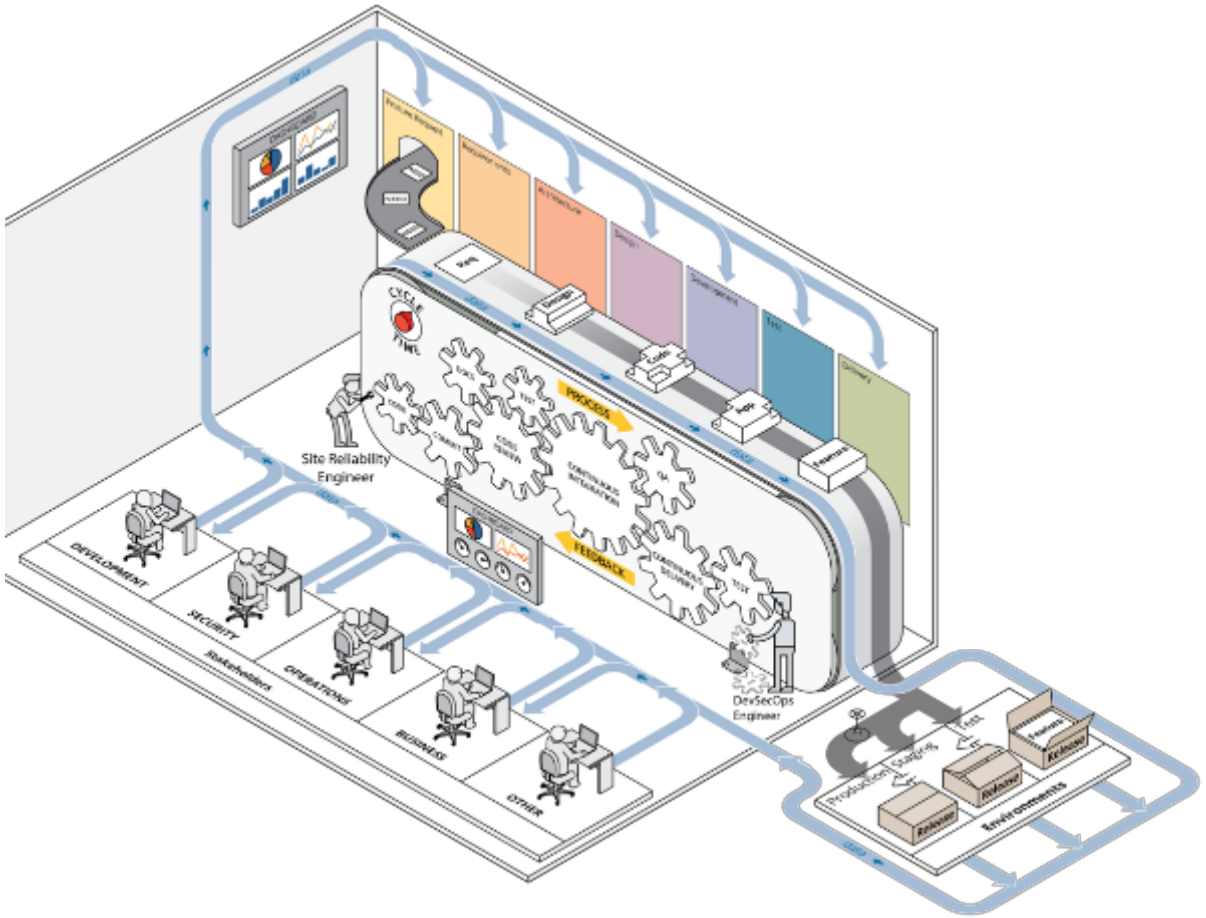
- Provides a public, open, transparent, and neutral forum for the establishment of standards
- Industry, Academia, Government bring expertise to collaborate on solutions for all
- Technical Specifications are initiated, pursued, and created by the voluntary participation of members
- OMG is an established and proven place where technology experts and companies can gather and collaborate to effectively establish standards to their mutual benefit
- Multiple relevant domain task forces and expertise already at OMG

OMG Efforts / Progress to date

- **March 2023**
  - DevSecOps Standards Information Day
- **June 2023**
  - Establish DevSecOps/DevXOps Working Group
- **June – December 2023**
  - Discussed needs / priorities / roadmap for potential standards
- **December 2023**
  - Began Draft RFP for “DevSecOps Core Processes, Elements, and Terms”
- **March 2024**
  - Special Event – Advancing Essential System Development and Security through DevSecOps Standards (this event here)
- **June – December 2024**
  - Discussion, editing, and completion of RFP for DevSecOps Reference Architecture
- **December 2024 / March 2025**
  - Finalize / Publish RFP for DevSecOps Reference Architecture

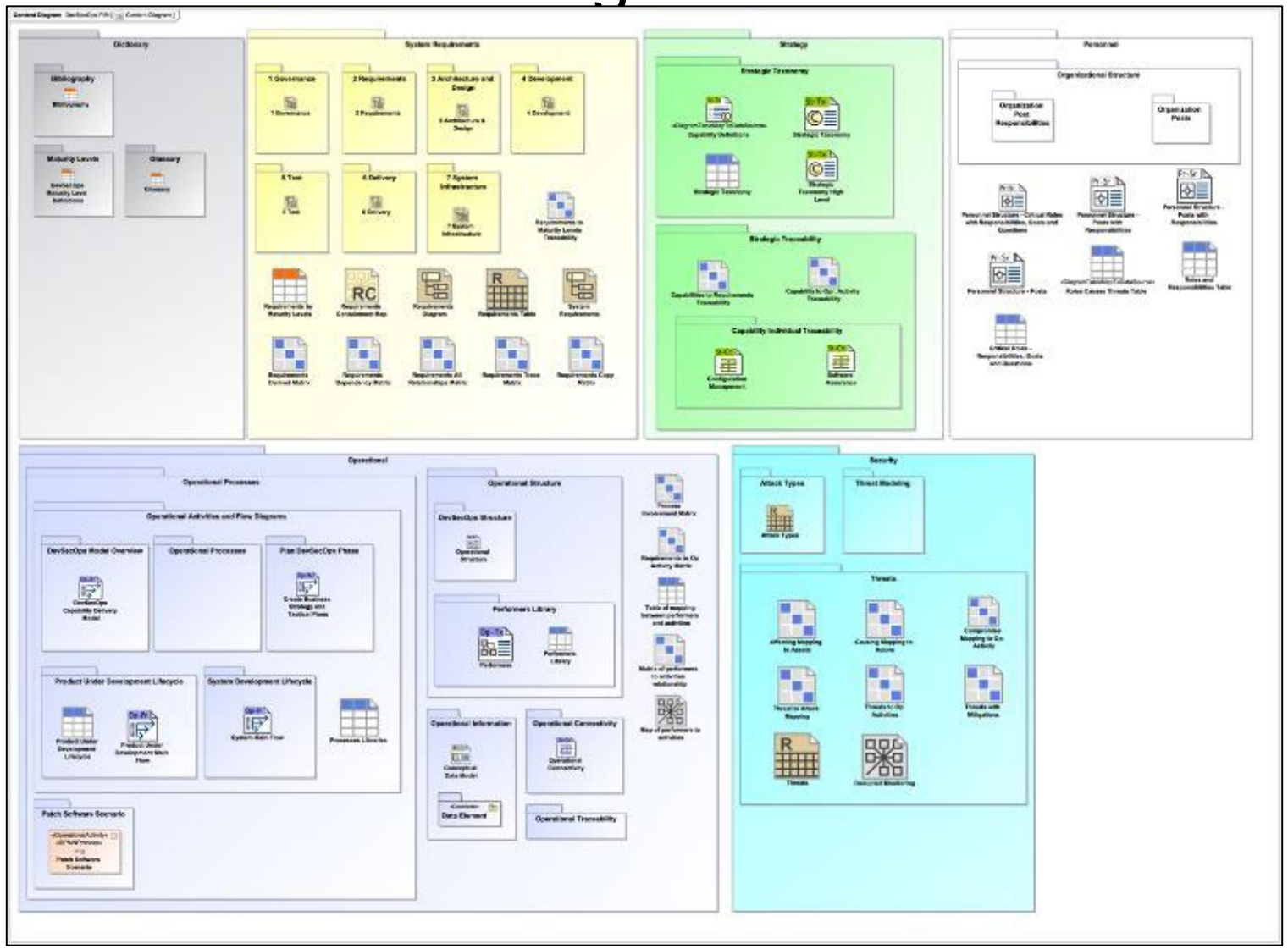
OMG Standards Development Organization

DevSecOps Platform Independent Model (PIM)



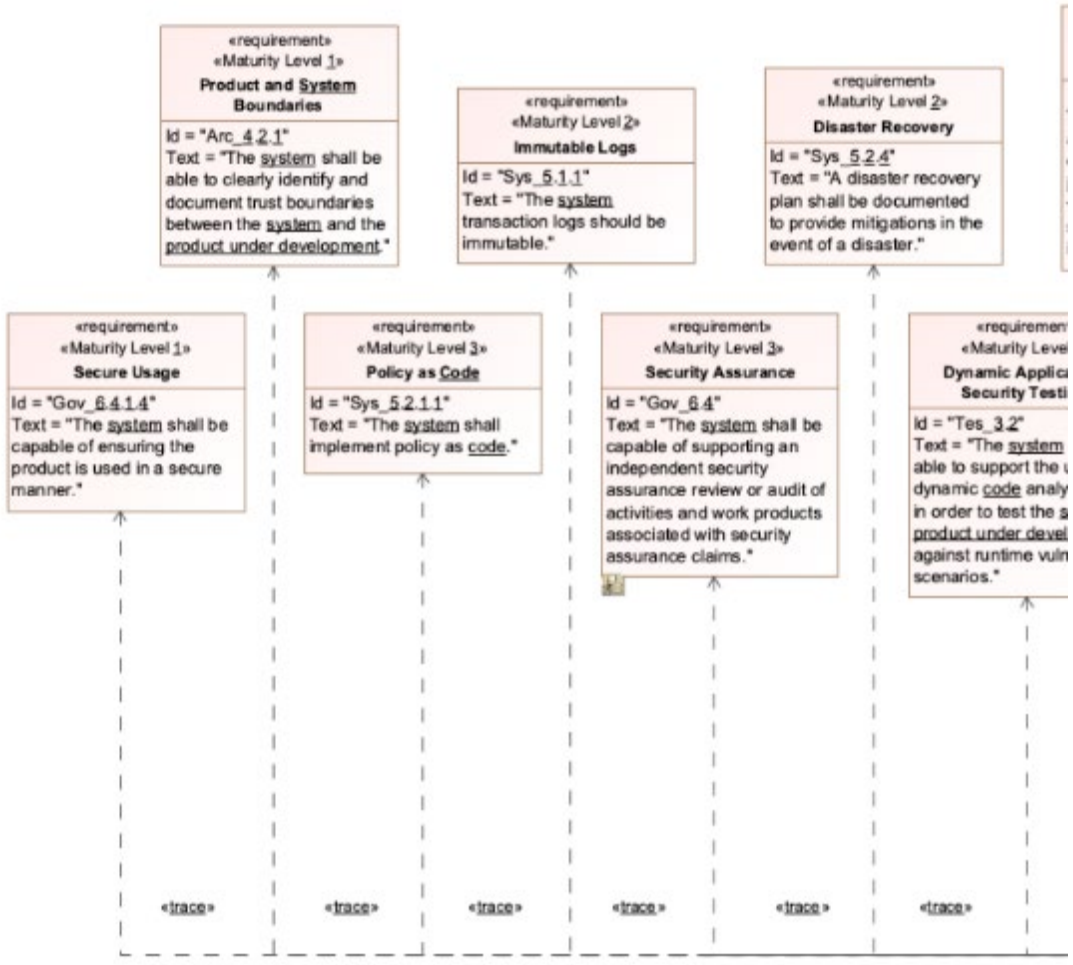
- is an authoritative reference to fully design and execute an integrated Agile and DevSecOps strategy in which all stakeholder needs are addressed
- enables organizations to implement DevSecOps in a secure, safe, and sustainable way to fully reap the benefits of flexibility and speed available from implementing DevSecOps principles, practices, and tools
- was developed to outline the activities necessary to consciously and predictably evolve the pipeline, while providing a formal approach and methodology to building a secure pipeline tailored to an organization's specific requirements

DevSecOps PIM - Content Diagram



https://cmu-sei.github.io/DevSecOps-Model/

DevSecOps Requirements



Example of Requirements Representation in Diagrams from PIM

All requirements are organized into categories based on logical and functional groupings:

- Governance
- Requirements
- Architecture and Design
- Development
- Test
- Delivery
- System Infrastructure

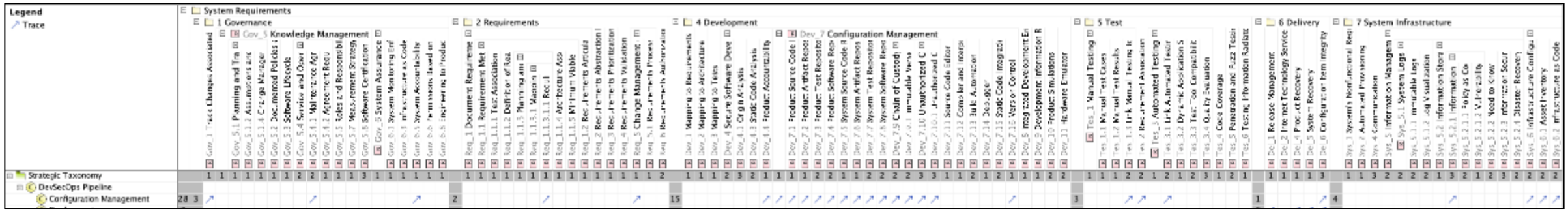
Requirements Table Link

DevSecOps Capability/Strategic Viewpoint

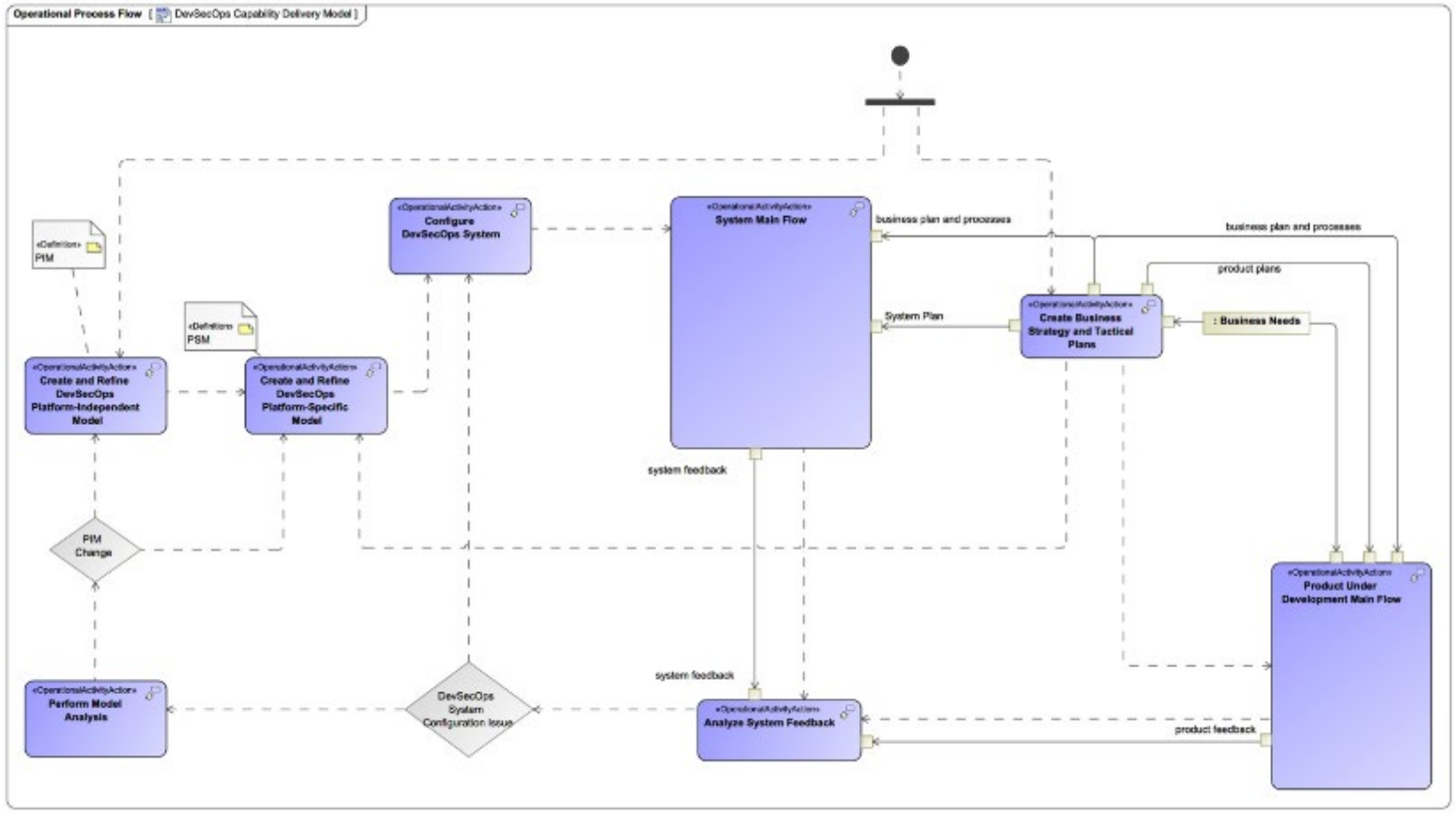
A capability is a high-level concept that describes the ability of a system to achieve or perform a task or a mission.

All requirements in the DevSecOps PIM were allocated to corresponding capabilities.

- Capability to Requirements Traceability Link
- Capability to Operational Activity Traceability Link
- Capability Definitions Link
- Strategic Taxonomy High Level



DevSecOps Operational Viewpoints



- DevSecOps Capability Delivery Model Link

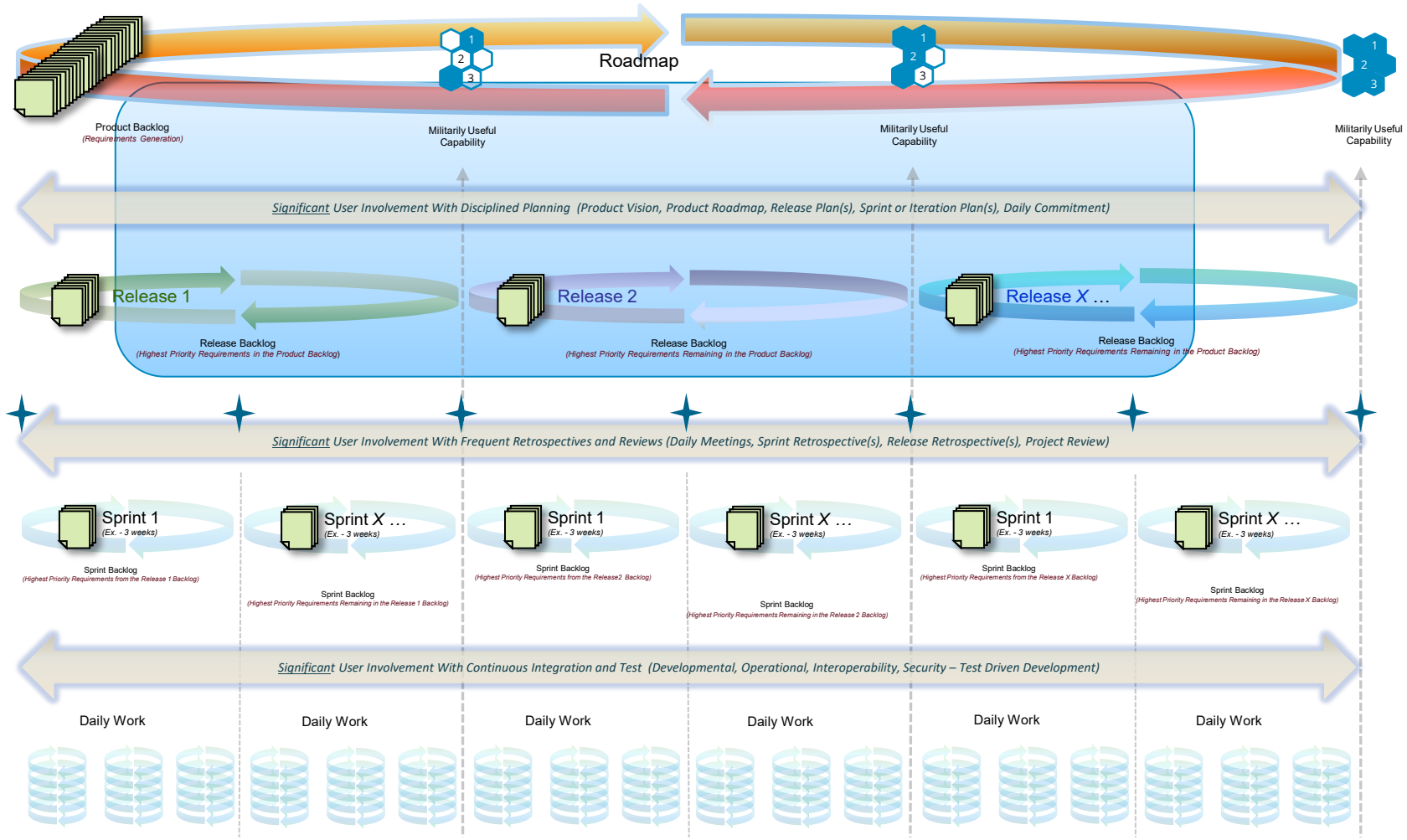
An operational model for a system describes behavior of the system to conduct enterprise operations.

The main operational processes for DevSecOps includes development process for the product, as well as the DevSecOps process itself.

Not a Myth: Agile *is* likely to fail if it's "only the development team" that adopts the new practices

Frequent failure mode: Business and/or operations doesn't keep up with what the development teams can deliver.

Why?
Shift to Agile-based requirements definition and management is more of a change than practices of development alone.

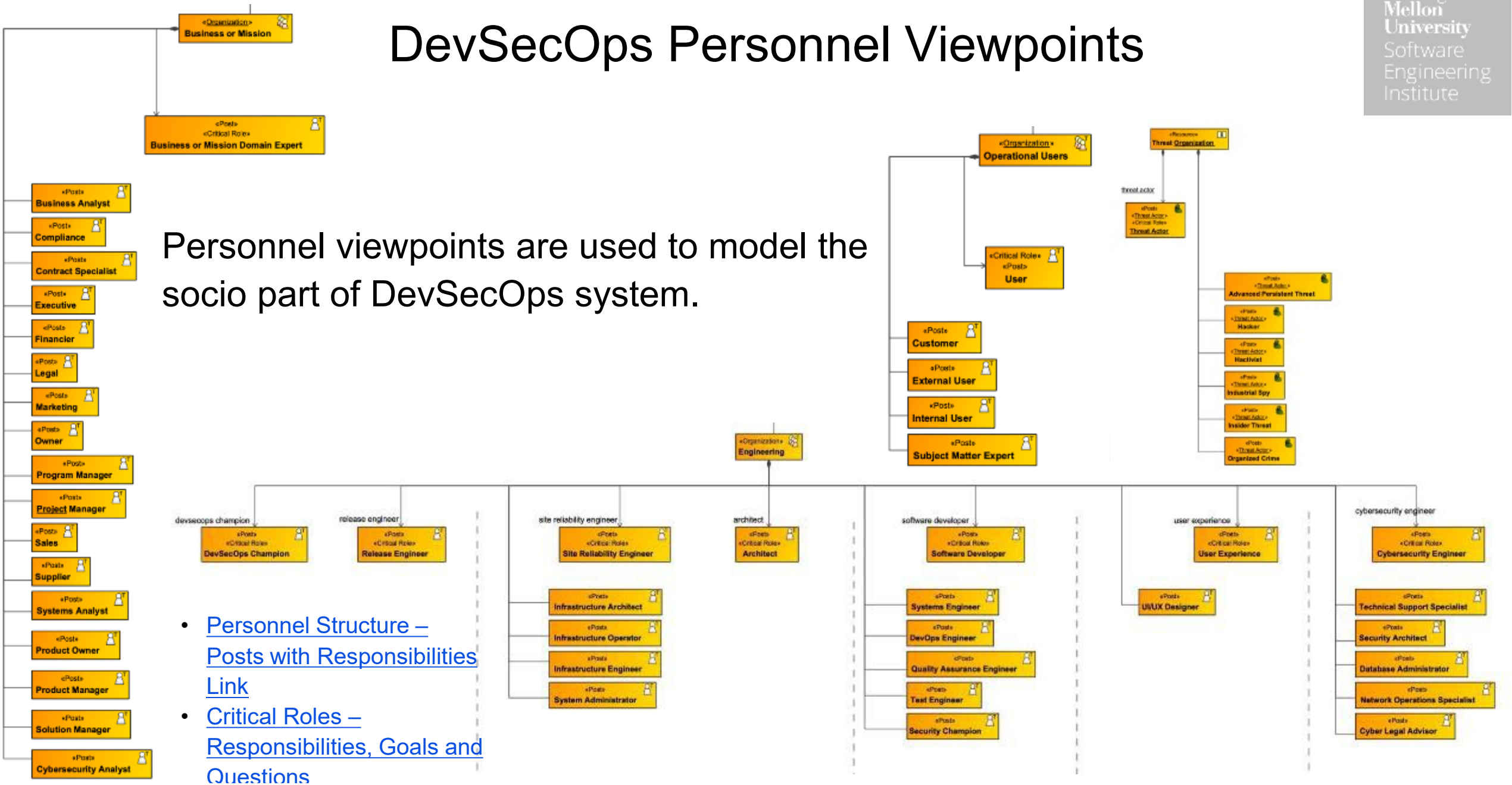


Graphic Source: Figure 4, *Parallel Worlds: Differences in Agile and Waterfall Differences & Similarities,* S. Palmquist et al, SEI-2013-TN-021, October 2013.

DevSecOps Personnel Viewpoints

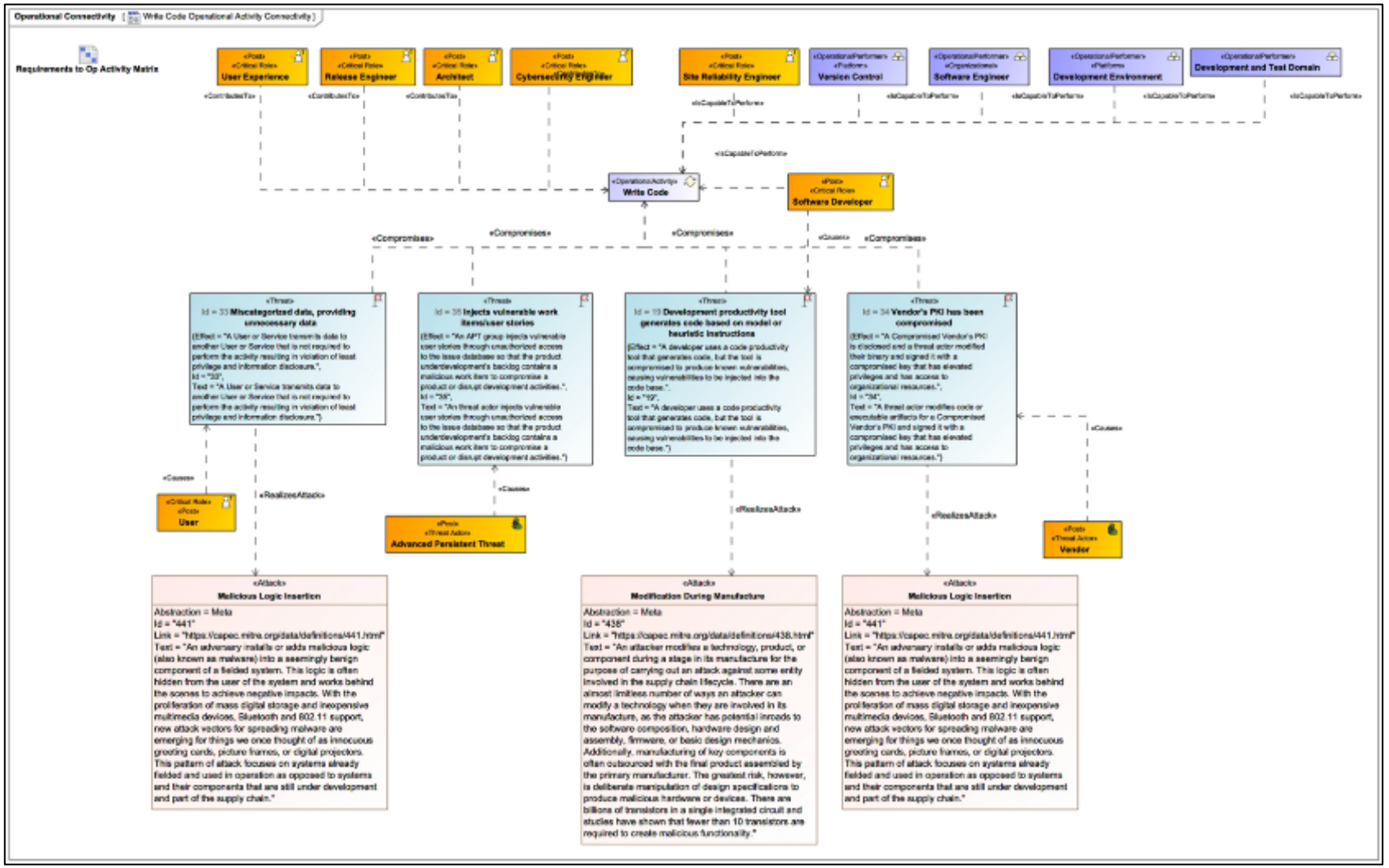
Carnegie Mellon University Software Engineering Institute

Personnel viewpoints are used to model the socio part of DevSecOps system.



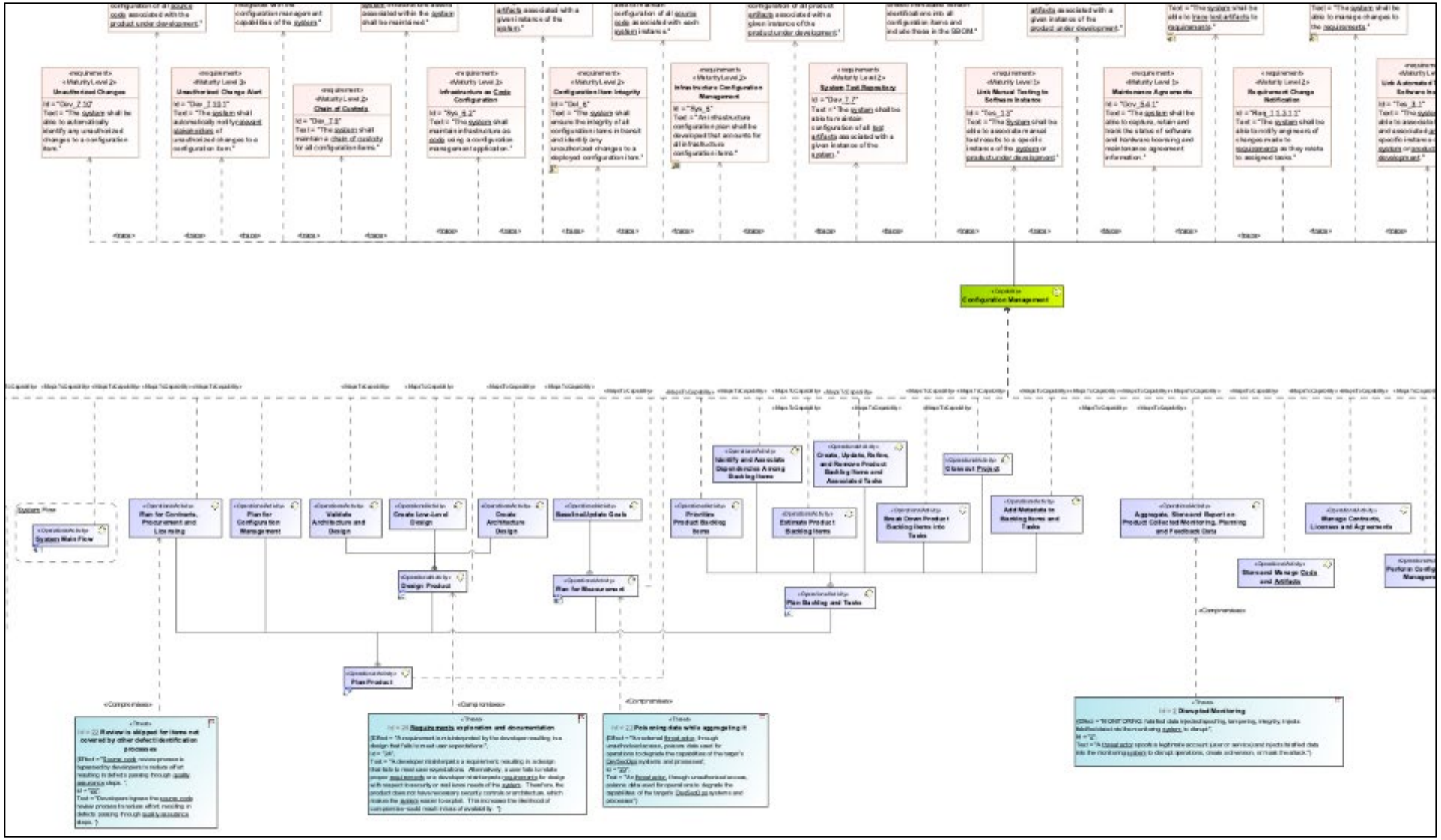
- Personnel Structure – Posts with Responsibilities Link
- Critical Roles – Responsibilities, Goals and Questions

Example Threat Modeling Diagram for Write Code Operational Activity



[Write Code Operational Activity Connectivity Link]

Capturing the Complexity of the DevSecOps System



Example of Threats Traced to Capabilities via Operational Activities

[Configuration Management Complexity Link]

Current RFP

❑DevSecOps Reference Architecture

❑High Level Scope

- This request for proposals seeks a reference architecture platform-independent model (PIM) expressed in OMG based architecture language(s) (UAF) for DevSecOps that will provide a common definition of capabilities, utilization patterns, and means to describe, assess, and improve the maturity, reliability, integrity and security of DevSecOps implementations.

❑Get Involved

- ❑ **Respond to the RFP**
  - ➢ Provide an initial submission with as much as you want to cover
  - ➢ Collaborate and contribute with the other submitters on the final submission
- ❑ **Bring others to help / Submit / Write**
  - ➢ Pipeline Vendors
  - ➢ Practitioners
  - ➢ Academics
- ❑ **DevSecOps Working Group –**
  - ➢ under the C4I Defense and Military Domain Task Force at the OMG SDO
  - ➢ C4IDM_DevXXOps_WG@omg.org – email distro group
    - ▪ self-register to the distro group online through your OMG Member Page

OMG Standards Development Organization

MOSA EE

LOU EYERMANN

THE MOSA ENABLING ENVIRONMENT

March 2025

Louis J Eyermann, Cory Casanave and Nadine Geier,
Co-Chairs MOSA EE WG

MOSA ENABLING ENVIRONMENT (EE)

- What is it?; What it's not! and … How it interrelates to the five MOSA Pillars.
- The five pillars of MOSA are: (1) An Enabling Environment (EE); (2) Employ Modular Design; (3) Designate Key Interfaces; (4) Select Open Standards; and (5) Certify Conformance.
- Is the EE is the most Critical Pillar of MOSA? Could it be the Foundation which MOSA Pillars stand on? Why?
- How do OMG standards play the key and pivotal role in selecting open standards, improving MOSA interoperability, requirements, architecture, use cases, and guiding the development of a MOSA EE.

FIVE MOSA PILLARS

•Establish Enabling Environment

•Integration of Development & Operations

•Phased Technology Insertion by Module

•Cloud Data Sharing

•Employ Modular Design

•Cohesive, encapsulated, self-contained, highly binned

•Designate Key Interfaces

•Published Key Interfaces

•Select Open Standards

•Well defined, mature, widely used, readily available

•Certify Conformance

•Published Conformance Criteria

•Automatic Testing & Certification

The Purpose of the OMG MOSA EE WG

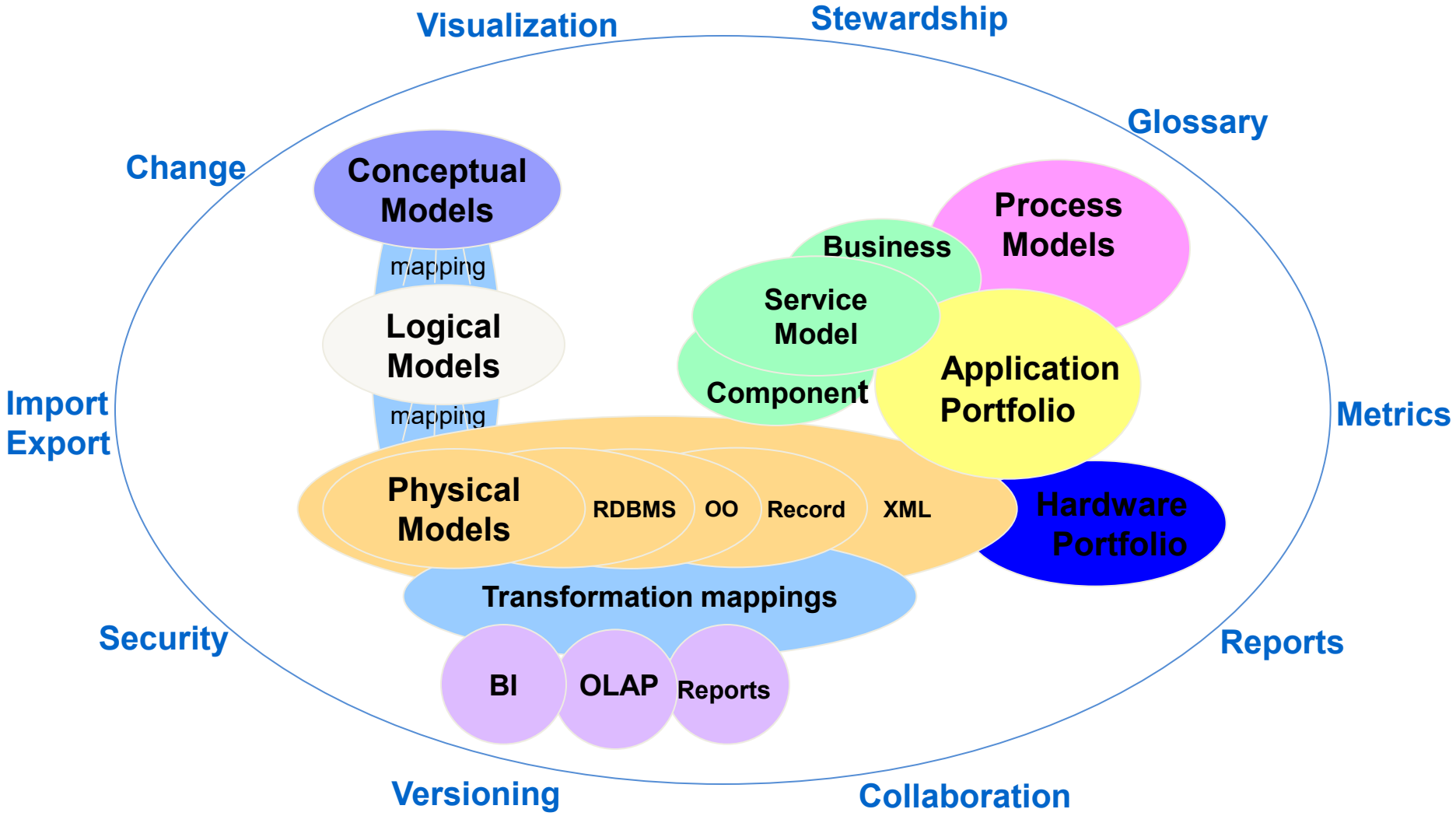
MOSA ENABLING ENVIRONMENT (EE)

- The Intersection of Technology, OMG and Other Open Standards & Structure (MOF repository), an Integrated Environment
- An Enterprise-wide Platform built on an Architecture and Requirements
- Repository complements and can integrate with all Relational Databases and query to external endpoints
- Core Repository with MOF capabilities beyond tool vendor server capabilities that promote technical and business information and interoperability for vertical and horizontal data linage
- Must support both Systems and Digital Engineering

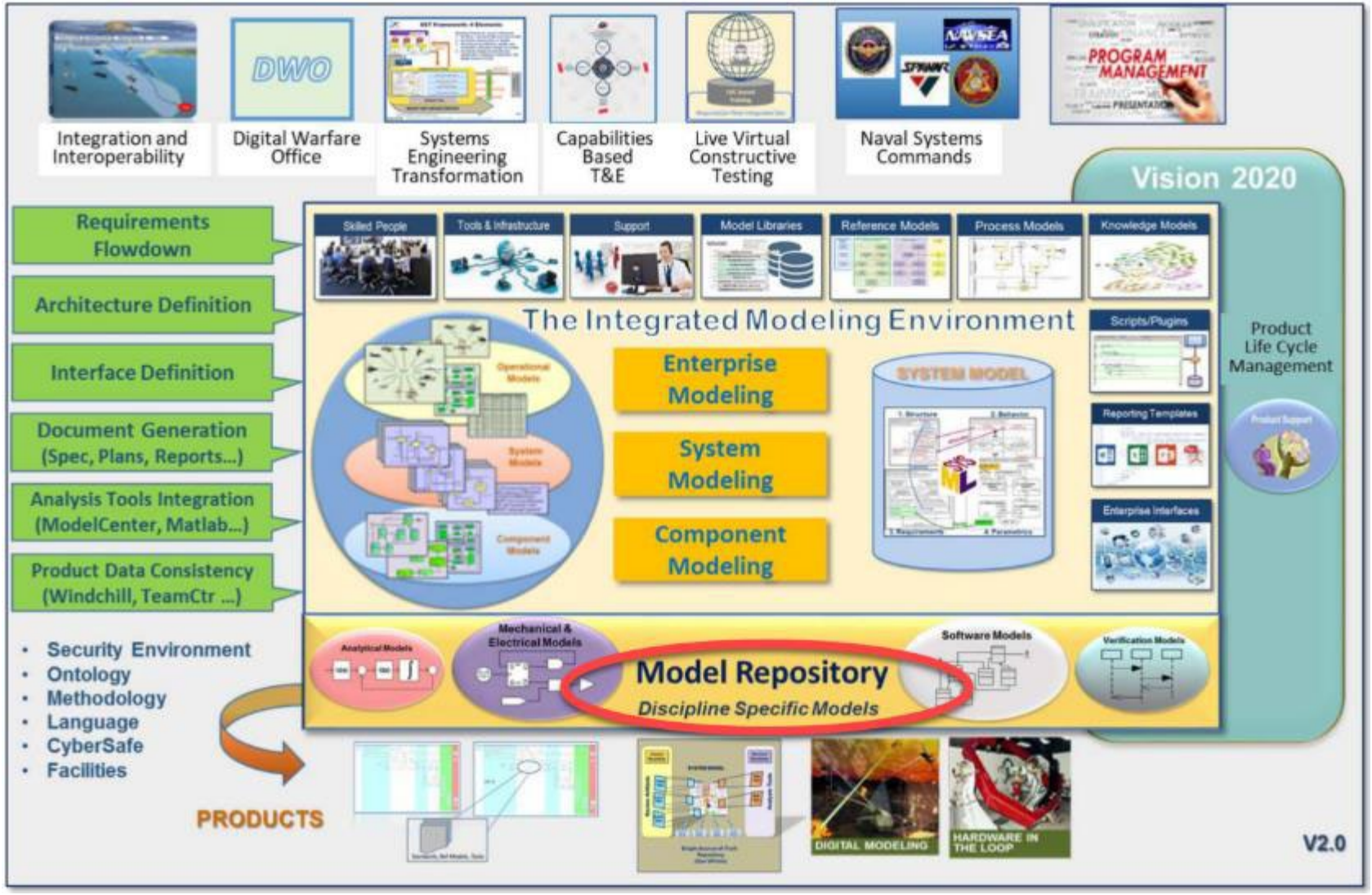
MOSA ENABLING ENVIRONMENT (EE) (CONTINUED)

- Must support and allow connections to client applications and a variety of tools
- Must create an authoritative source for MBSE Intellectual Property, facilitate reuse of components and interfaces for systems engineers and their business colleagues
- Initial MOSA EE Repositories for each Service selectively linked to current databases are federated across DOD

Model Integration / Horizontal & Vertical Data Linage



STRATEGIC ARCHITECTURE
MULTIPLE TOOLS ENABLED BY REPOSITORY



Naval Enterprise Integrated Modeling Environment From US Naval DSET Strategy, 2020

SUMMARY, CURRENT STATUS & NEXT STEPS

SUMMARY: The EE is an Enterprise Wide Platform with an OMG Standards-based (MOF) Repository for MBSE

Core based MOF repository platform metamodel driven, complements current repositories (vendor tool servers and file based)

Frontend Client applications such as Data, Semantic/Link Open Data (LOD), product and product line management, life cycle management, BI Clients, acquisitions, supply chain, etc.

Back end tools supporting systems and digital engineering, and other business needs

STATUS: Initial MOSA EE WG Charter completed and working minor Charter revision and requirements & architecture

NEXT STEPS: Finish initial requirements, architecture development, examine “mega” use cases, refine requirements and conduct pilot(s)

CURRENT STATUS

- **September 2023**
  - Charter MOSA EE Working Group under C4I Defense and Military DTF
- **December 2023 – September 2025**
  - Discussion, authoring, and completion of discussion paper on MOSA EE Digital Framework
- **December 2025**
  - Approved release of MOSA EE Digital Framework Discussion Papaer
- **March 2025 -> Future**
  - Develop requirements for a MOSA EE Reference Architecture

Quarter	Deliverable
Q1 2025	• Standards Needs Assessment: Perform an initial assessment of existing standards and emerging OMG standards and identify alignments and gaps to achieving a MOSA EE. • Document Set of Use Cases: revise existing use-cases and document new ones as needed
Q2 2025	• Implementation Guidance Outline: Create an outline for integration of the MOSA EE DF with broader MOSA guidance documents. • Preliminary MOSA EE DF Reference Architecture Document
Q3 2025	• Update Implementation Guidance: Update and distribute the first draft of the implementation guidance.
Q4 2025	• First Full Draft of MOSA DF Reference Architecture

Enhanced Consistency and Interoperability: Defense Standards at OMG

March 18, 2025 - BREAK until 3:15

MATT WILSON (SIMVENTIONS), MIKE ABRAMSON (ASMG)
CO-CHAIRS, C4I (DEFENSE AND MILITARY) DTF

Enhanced Consistency and Interoperability: Defense Standards at OMG

Agenda

- Forging the Future: Synergy in Standards Development
  - Paul Gustavson – SISO
- DevSecOps and MOSA EE Working Groups – update/status
  - Matt Wilson – SimVentions / OMG C4I Defense and Military DTF

Break 3:00 – 3:15

- Data Centric Security
  - Mike Abramson ASMG - / OMG C4I Defense and Military DTF
- Overview of C4I DM DTF Specifications and Current efforts
  - Matt Wilson and Mike Abramson - OMG C4I Defense and Military DTF Co-Chairs
- Intelligence Community - Data Reference Architecture
  - Jasmin Leveille – Office of the Intelligence Community – Chief Data Officer
- Discussion / Next Steps

OMG Standards Development Organization

Delivering Data Centricity with Data Centric Security

MICHAEL ABRAMSON: PRESIDENT ASMG

ASMG
ADVANCED SYSTEMS MANAGEMENT GROUP

Delivering Data Centricity with Data Centric Security

March 2025

Michael Abramson: President ASMG

Stockmayer's rule:
If it looks easy, it's tough. If it looks tough, it's damn near impossible.

AN OMG STANDARD IEF™ Information Exchange Framework™
AN OMG STANDARD IEPPV™ Information Exchange Packaging Policy Vocabulary™
DDS
OMG Standards Development Organization

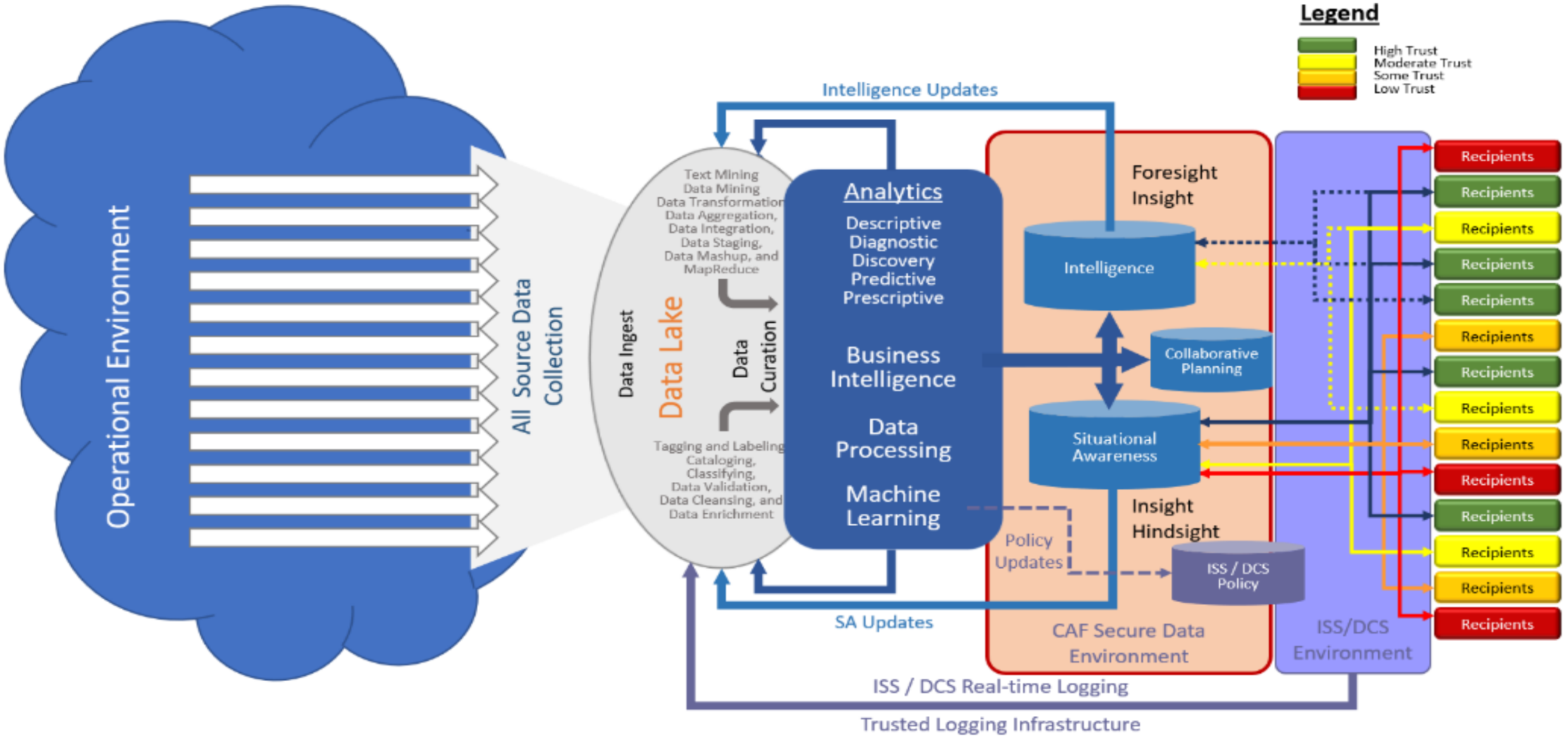
Data Management Objectives

Right Information – Right Place – Right Time

Maximize the Availability of Quality Data to Authorized Users
While Protecting Sensitive (Private, Confidential, Legally Significant and Classified)
Information From Unauthorized Access, Use, Manipulation, Deletion or Appropriation

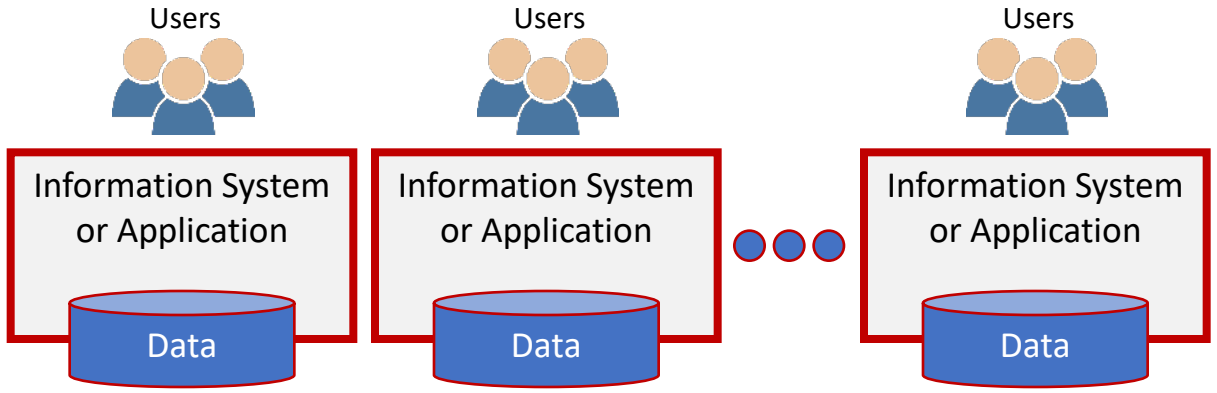
Treat Data as a Valuable and Versatile Asset Instead of a Piece of an Information System

Data Management Objectives on a Slide

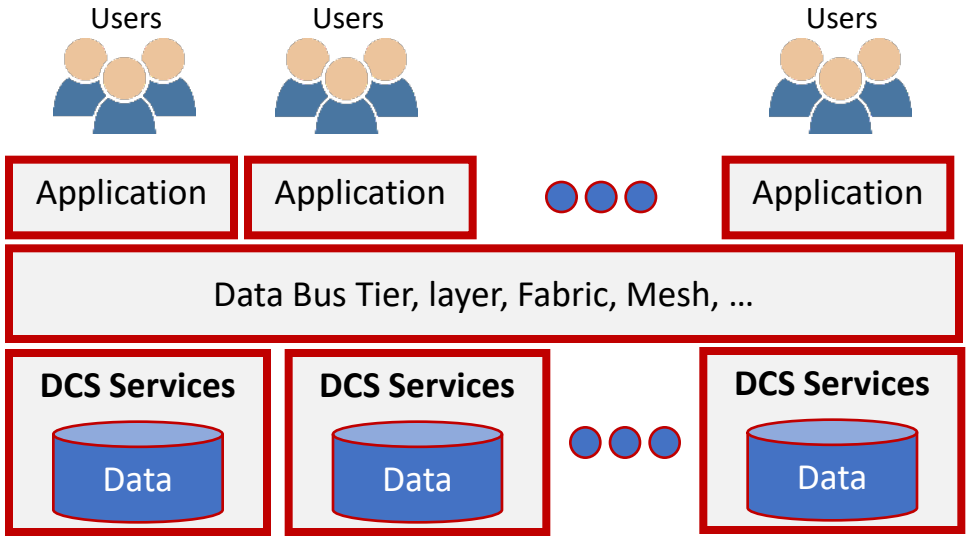


Data Driven - Application Centric or Data Centric

Traditional System Deployment



Digital Transformation Target



Application Centric

- Siloed Data
- Data is Bound to the system or application
- Based on Network, Platform and Application based security
- High lifecycle cost and high risk

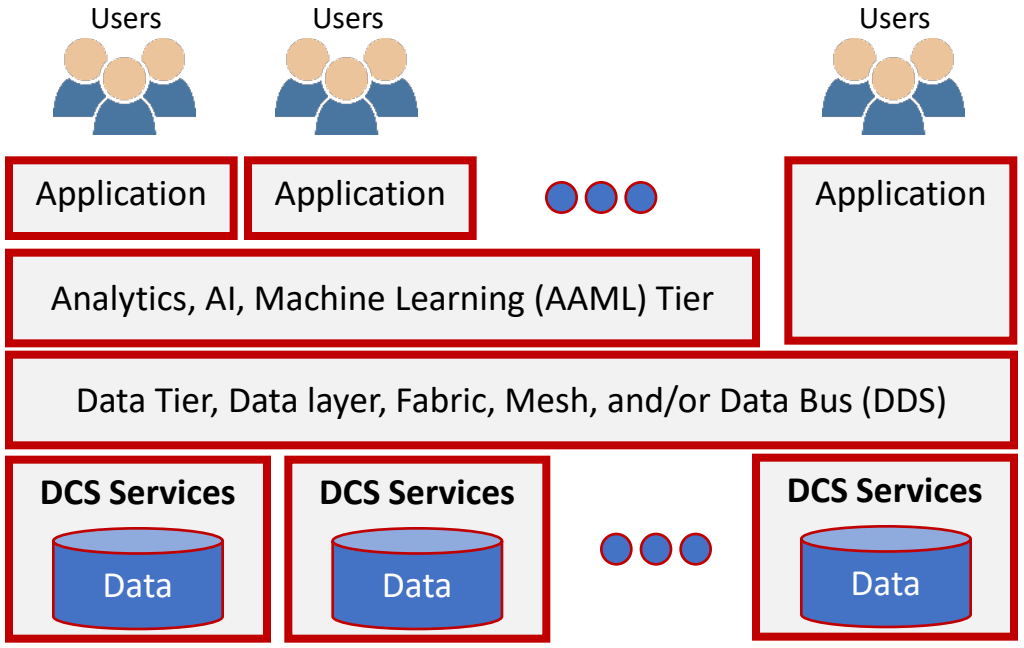
Data Centric

- Data managed as an independent resources (/assets)
- Security applied to the data based on its sensitivity and value
- Data shared based on the needs and authorisations of user
- Policy driven Data Centric Interoperability
- Single sources of truth

Data Centricity – Flexible, Agile and Adaptive

- Data is the persistent element
- New capabilities and services can be continuously added and integrated to each layer without disrupting operations
- Building Security (ZTA) into all Tiers Building Security (DCS/ZTA) into the data services and data ties
- The architecture enables continuous development, test, integration, approval and deployment
- Based on Modular Open System/Capability Architecture

Maximise the availability of quality information to authorised users



Protect Sensitive (private, confidential, legally-significant and classified) data and metadata from unauthorized access, release, manipulation, deletion and appropriation

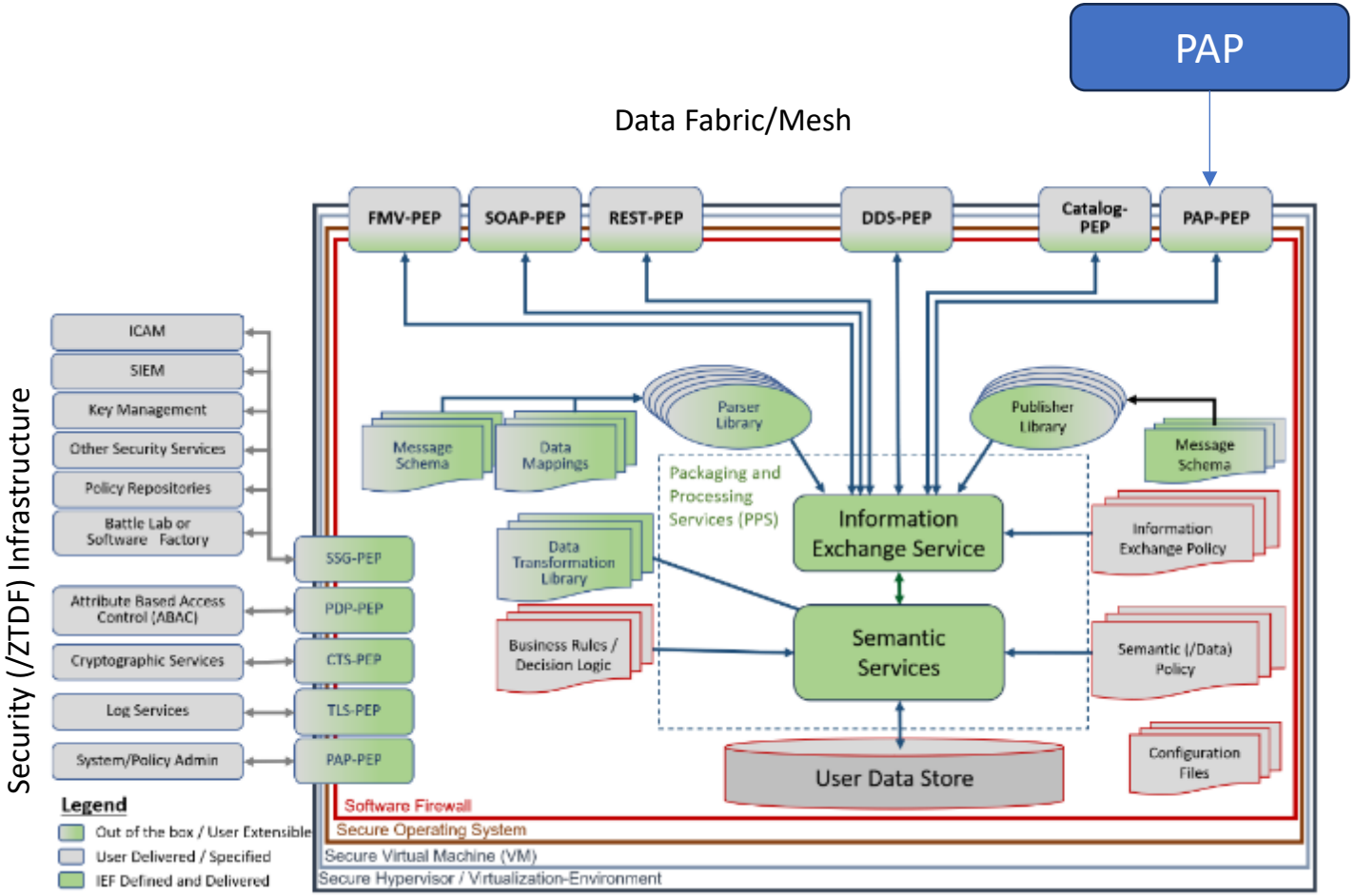
Data Centricity Principles

Provision users with the ability to:

1. **Understand the data** – Maintain institutional knowledge and memory of the semantics, structure, syntax, state, status and location of data and information elements
2. **Control the Data** – Administer receipt, processing, storage, discovery and release of data and information.
3. **Share the data** – Provision users with the data and information needed to inform decisions.
4. **Protect the data** – Safeguard data from unauthorised access, use, manipulation and appropriation.
5. **Govern the data** – Ensure that data is collected, used, shared (/released), and disposed of per legislation, regulation and policy.

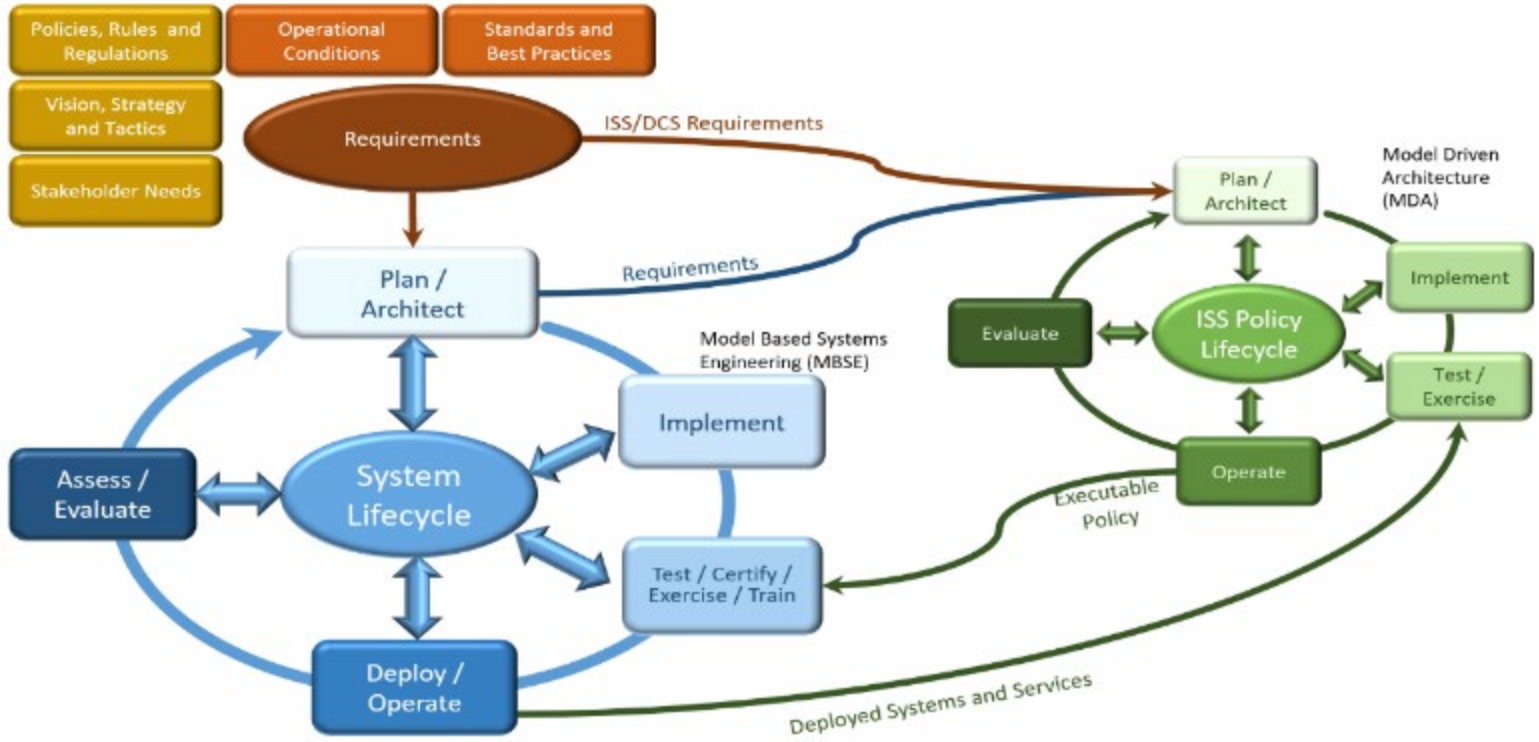
Wrap Data in its Own Security

- Focus on Data Centricity
  - Provision data based on recipient needs and authorisations
  - Security travels with the data
- Microservice Based Architecture
  - Configurable at runtime
- Policy Driven
  - Policy separated from enforcing services
  - Enterprise policies →operation
- Role of the PEPs
  - Access Controls
  - Integration into the User's Security Environment
- Standards based



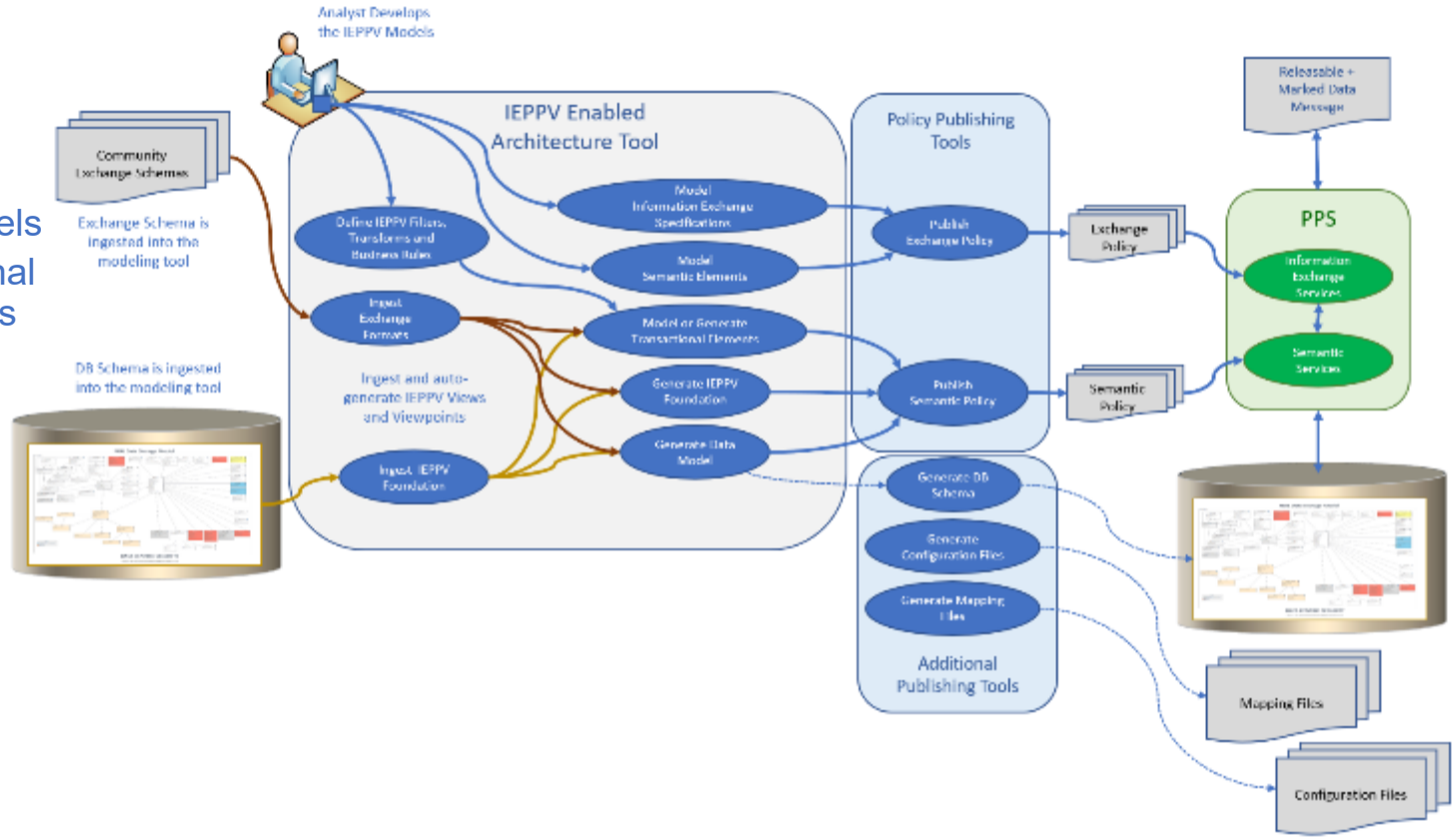
Agile Development – Two Lifecycles

- Separate development lifecycles for:
  - Information Sharing and Safeguarding (ISS) Policies
  - Software Services
- Addresses the need to implement ISS policies at the speed of operations
- Standards based – enables best of breed implementations and policy portability

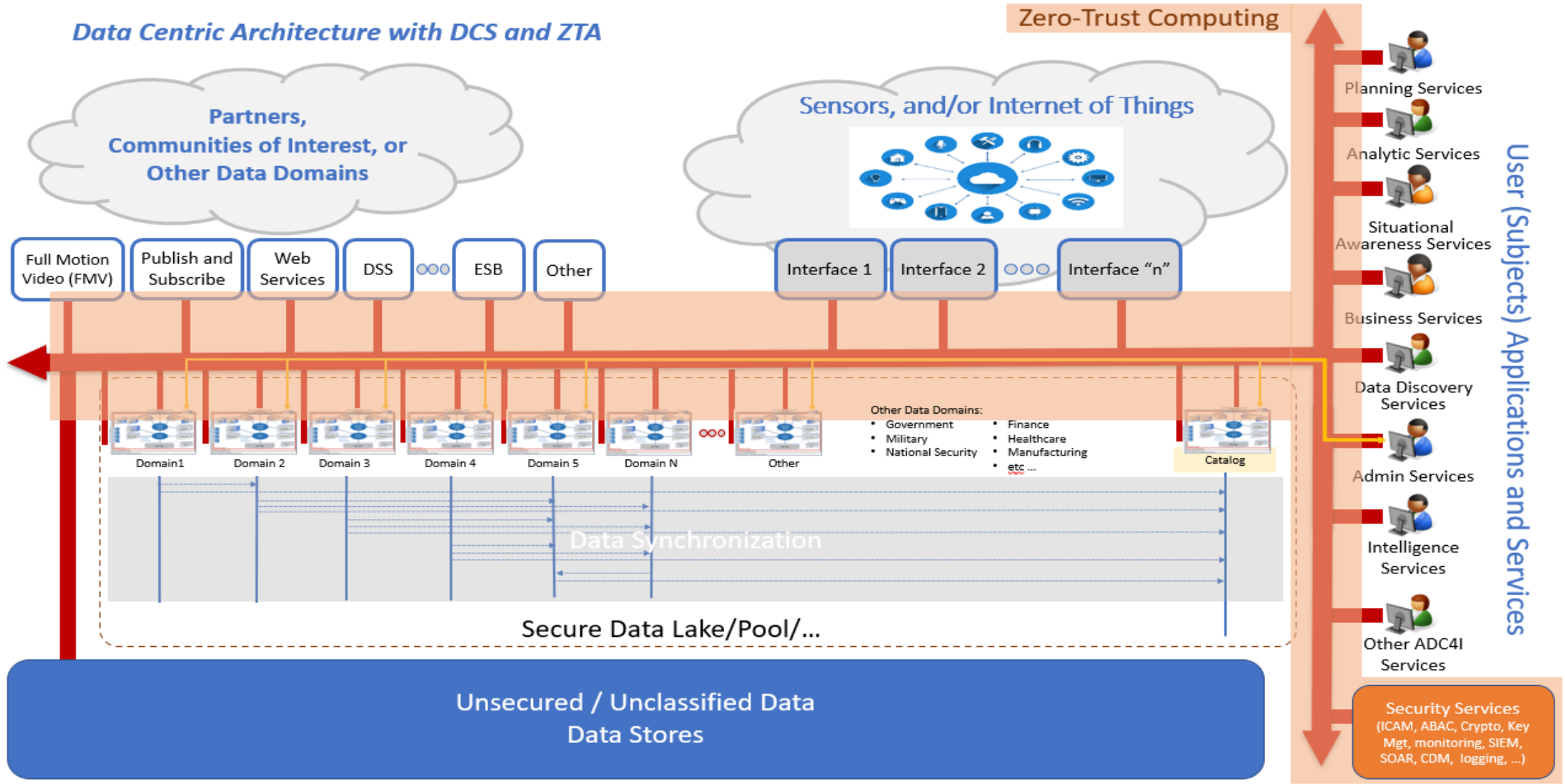


Architecture Driven Approach

- Data View of Enterprise Architecture Modeling
  - Data Exchange Semantics
  - Data Exchange Specifications
  - Data Processing and Packaging Specification
  - Data Storage Semantics
- MDA and MBSE:
  - Import user data storage and exchange models
  - Generates IEPPV foundation and transactional models based on the semantics and business rule from the users' environment
  - Transform the IEPPV models into:
    - Executable Exchange Policies
    - Executable Semantic Models
    - Configuration Files
    - Mapping Files
    - Other runtime elements
- Yielding flexible, agile and adaptive data environment



Data Centric Architecture



Questions and Answers

Michael (Mike) Abramson (Consultant)

President ASMG Ltd.
Co-Chair Military and Defence (C4I) Task Force at the Object Management Group
Chair IEF Working Group at the Object Management Group
Email: MICHAEL.ABRAMSON@forces.gc.ca
Or ABRAMSON@asmg-ltd.com
Phone: (613) 797-8167 (cell)

Finagle's Fourth Law:
Once a job is fouled up, anything done to improve it only makes it worse.

IEF/DCS Videos

1. Introduction to IEF 4Node Demo – https://vimeo.com/678451494
2. 4 Node Demonstration – https://vimeo.com/678454136
3. Introduction to PPS - https://vimeo.com/684731310
4. Intro to IES Configuration Parameters (3-headed) - https://vimeo.com/688112603
5. IES Parameter Demo - https://vimeo.com/689767647
6. Introduction to Information Sharing and Safeguarding - https://vimeo.com/696111602

7. 2023 CWIX (Video Processing) Testing: https://vimeo.com/841375922

IEF Objectives

- Capabilities
  - Data Centricity
  - Data (/Information) Sharing and Safeguarding
  - Data Centric Security
  - Data Interoperability
  - Architecture Driven Data Centric Sharing and Safeguarding

- Benefits
  - Retention of Institutional Memory
  - Enhanced Data Management
  - Enhanced Data Governance
  - Reduced Lifecycle risk and cost

Why is it so Challenging?

Simply: There is a Lot to Remember!

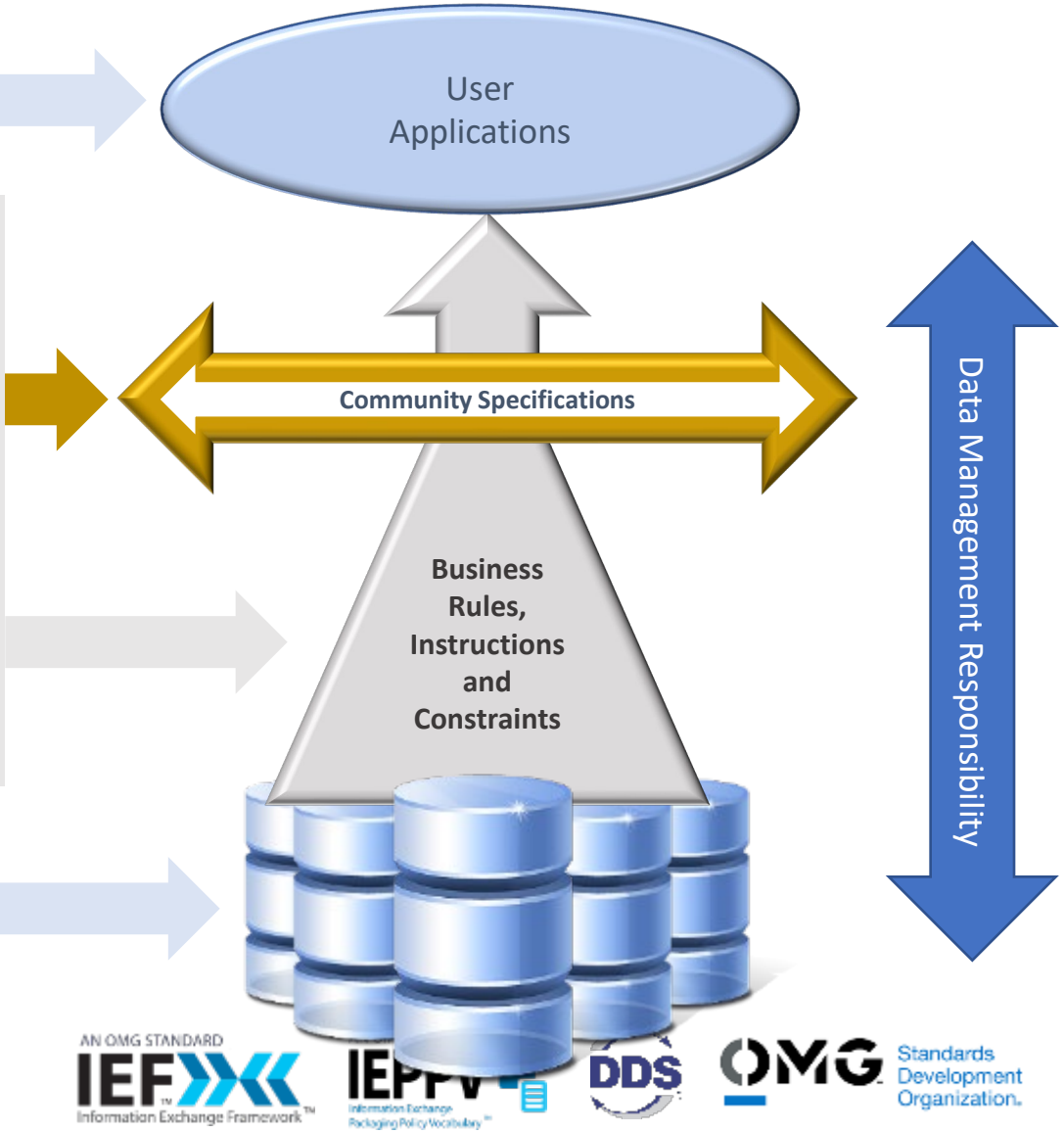
Application Semantics
Application Interface Specification

Information Sharing and Safeguarding Policy

Community Exchange and Service Level Agreements
Community Interface Specifications
Community Exchange Semantics
Community Messaging Protocols
Community Networking and Community Specifications

Data and Information (Semantic) Patterns
- Aggregation, Parsing/Marshalling
- Data Filters (Security, Privacy, QoS, …)
- Data Transformations
- Data and Information Tags (Metadata)
- Business Rules (e.g., Labelling)

Storage Semantic
Storage Business Rules
Store attributes and domains
Meta tags and labels
Data and information Relationships
GUIDs / DB Keys



Overview of C4I Defense and Military Specs

C4I DM DTF CO-CHAIRS

OMG Defense Standards

OFFBOARD PLATFORMS

IEPPV Policy

TEX

IEF

HQ

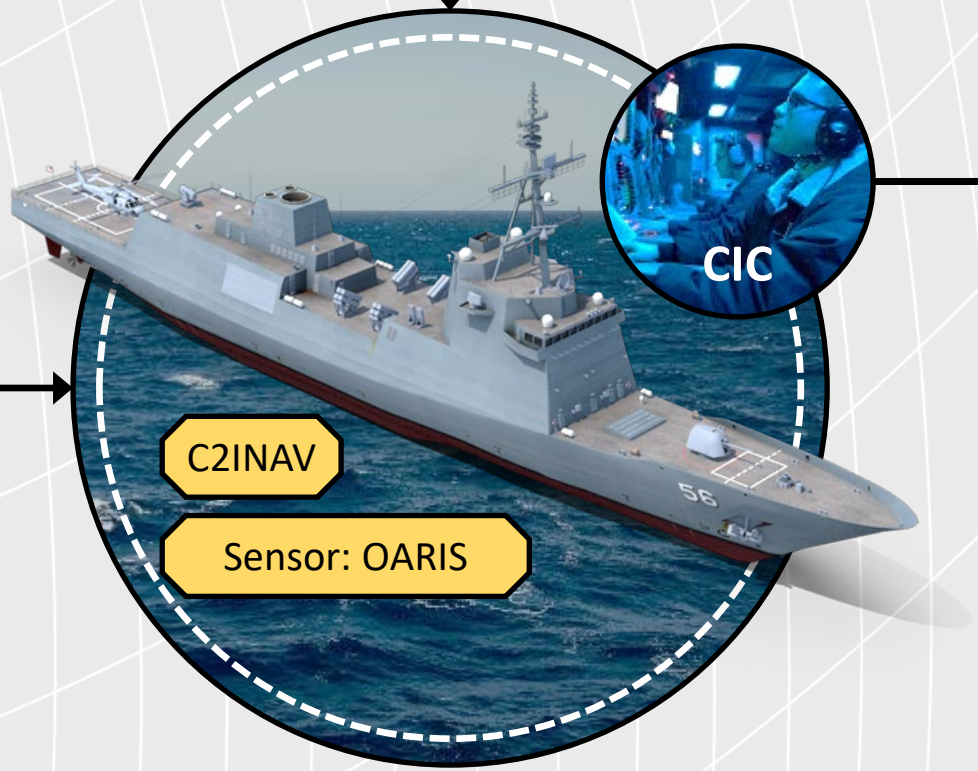
IEPPV Policy

IEF

IEF

IEPPV Policy

PARTNERS



COMBAT PLATFORM

TDAI

TCI

TEX

ALMAS

DDS
CORBA
UAF
TestIF
ReqIF
Application Instr
FACE UML Profile
DevSecOps
DDS Monitoring
MOSA EE

Definitions / Acronyms / etc.

❑ TEX – TACSIT data EXchange	V 1.1 – RTF for 1.2
❑ IEF – Information Exchange Framework	V 1.0 – V 2 RFC Submitted
❑ IEPPV – Information Exchange Packaging Policy Vocabulary	V 1.0
❑ C2INav – Command and Control Interface to Navigation Systems	V 1.2 – RTF for 1.3
❑ OARIS – Open Architecture Radar Interface Standard	V 1.2, 2.0, 3.0 – RTF for 3.1
❑ TDAI – Tactical Decision Aid Interface	V 1.0 – RFT for 1.1
❑ TCI – TACSIT Controller Interface	V 1.0 – RFT for 1.1
❑ ALMAS – Alert Management Services	V 1.4 – RFT for 1.5
❑ DDS – Data Distribution Service	
❑ UAF – Unified Architecture Framework	
❑ TestIF – Test Data Interchange Format	
❑ ReqIF – Requirements Interchange Format	
❑ App Instr – Application Instrumentation	
❑ FACE Profile – Future Airborne Capability Environment – UAF Profile	

OMG Standards Development Organization

OMG & MANAGED PROGRAMS

The Object Management Group (OMG) mission is to develop technology standards that provide real-world value for dozens of vertical industries. OMG is dedicated to bringing together its international membership of end-users, vendors, government agencies, universities and research institutions to develop and revise these standards as technologies change throughout the years.

35 Years of Excellence

Standards Development Organization

The OMG SDO is organized with many groups and teams focused on specific areas.

Domain Technical Committee (DTC)
Vertical market segment needs

Domain Task Force(s) - DTF

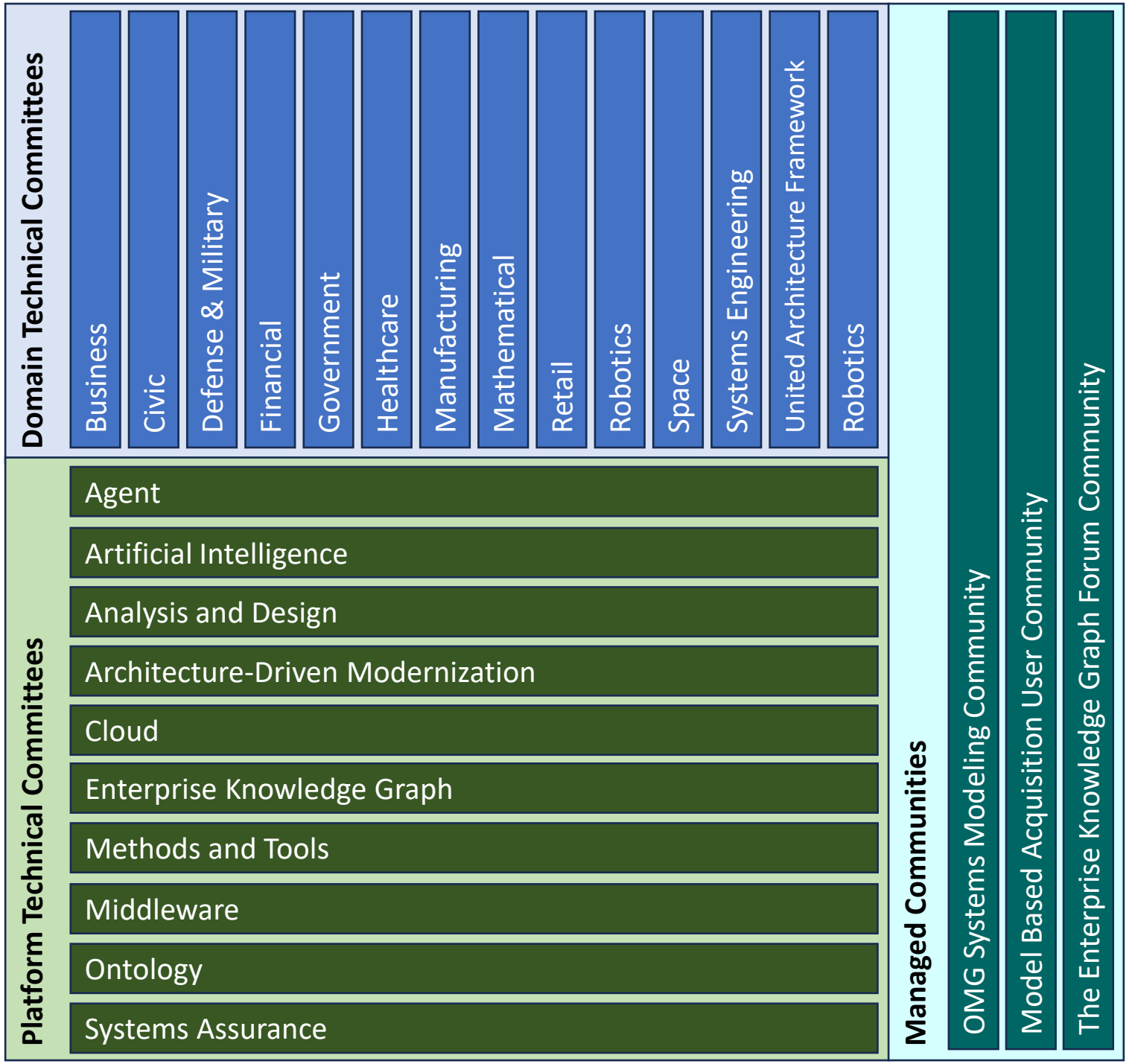
Platform Technical Committee (PTC)
Horizontal cross-market needs

Platform Task Force(s) - PTF

Managed Communities (MC)
Focus on specific communities across both

Many efforts, topics, and specifications are being developed independently in each Task Force.

Many of these efforts compliment, overlap, and/or relate to the work in other DTFs, PTFs, MCs.

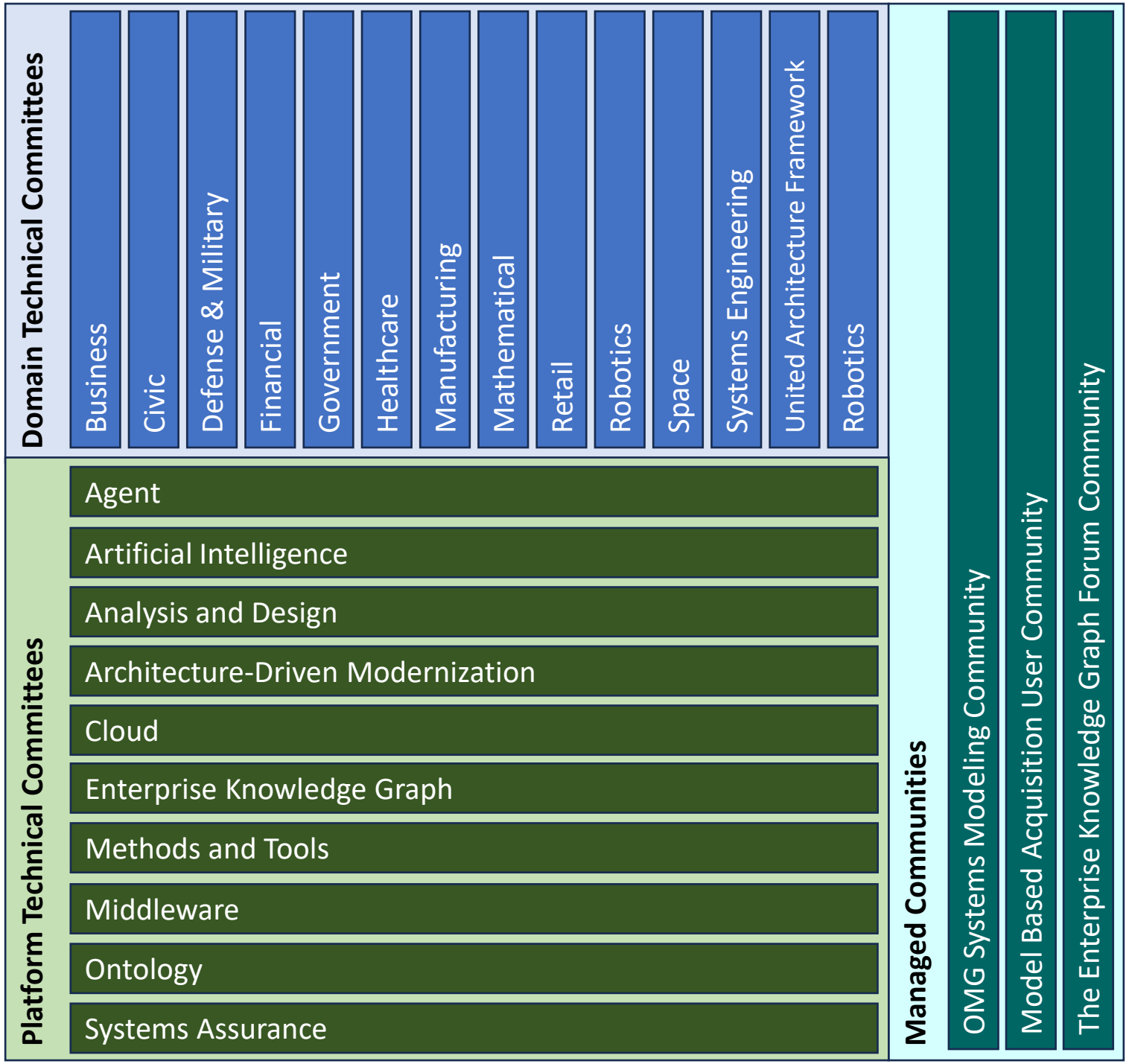


Standards Development Organization

In 2023, the leaders of certain teams across (DTF, PTF, MC) started a forum at every other quarterly Technical Meeting to increase awareness of work being done related to Digital Engineering Model Interchange, Interoperability, and Integration (DEMI3).

Current topics include:

- CASCaDE (Collaborative Artifact, Specification, Context and Data Exchange)
- RAS (Reusable Asset Specification)
- SysML V2 and the KerML based approach for model interchange
- Systems Modeling API and Services specification
- MOSA Enabling Environment
- Commons Library Ontology
- MBAcq (Model Based Acquisition)
- Data Products Ontology
- SPDX 3.0
- UAF Roadmap



Enhanced Consistency and Interoperability: Defense Standards at OMG

Agenda

- Forging the Future: Synergy in Standards Development
  - Paul Gustavson – SISO
- DevSecOps and MOSA EE Working Groups – update/status
  - Matt Wilson – SimVentions / OMG C4I Defense and Military DTF

Break 3:00 – 3:15

- Data Centric Security
  - Mike Abramson ASMG - / OMG C4I Defense and Military DTF
- Overview of C4I DM DTF Specifications and Current efforts
  - Matt Wilson and Mike Abramson - OMG C4I Defense and Military DTF Co-Chairs
- Intelligence Community - Data Reference Architecture
  - Jasmin Leveille – Office of the Intelligence Community – Chief Data Officer
- Discussion / Next Steps

Intelligence Community - Data Reference Architecture

JASMIN LEVEILE – OFFICE OF THE INTELLIGENCE COMMUNITY – CHIEF DATA OFFICER

Office of the Director of National Intelligence

OFFICE OF THE INTELLIGENCE COMMUNITY CHIEF DATA OFFICER

(U) Intelligence Community Data Reference Architecture (DRA)

(U) Executive Brief

Office of the IC Chief Data Officer

3/18/2025

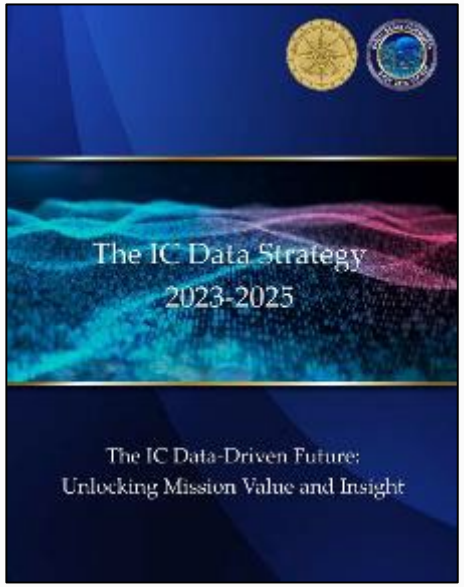
(U) Addressing the Challenges

(U) The IC Data Reference Architecture: The IC CDO and CDO Council proposed an IC DRA to address the IC Data Challenges:

- **A Reference Architecture (RA):** Provides guidance for the design of solution architectures with repeatable technical standards
- **A Data Reference Architecture (DRA):** Provides guidance specific to data components (data security, ingest points, storage, processing and dissemination nodes, etc.)
- The **IC DRA** is a Data Reference Architecture developed using common and tailored principles for the IC, that private sector and other government agencies are using to solve tough data challenges.
  - It addresses IC challenges by providing guidance to increase data discoverability, interoperability and quality
  - It is **not** a solution architecture or an implementation plan or a requirements document
  - It aligns to data mesh principles increasingly adopted in industry

(U) Foundations of the IC DRA

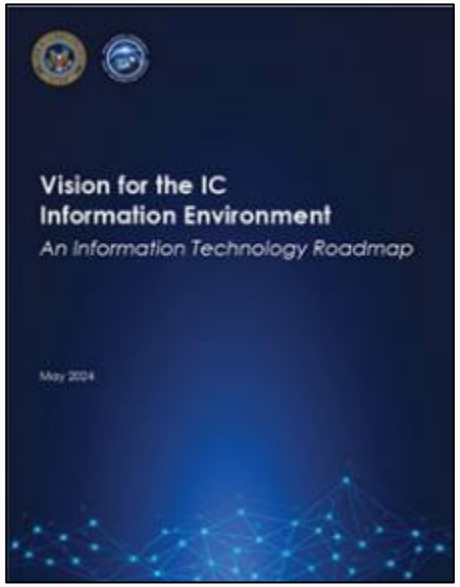
(U) The DRA is a key milestone toward data-centricity and builds upon a strong policy foundation.



2023:

(U) The IC Data Strategy

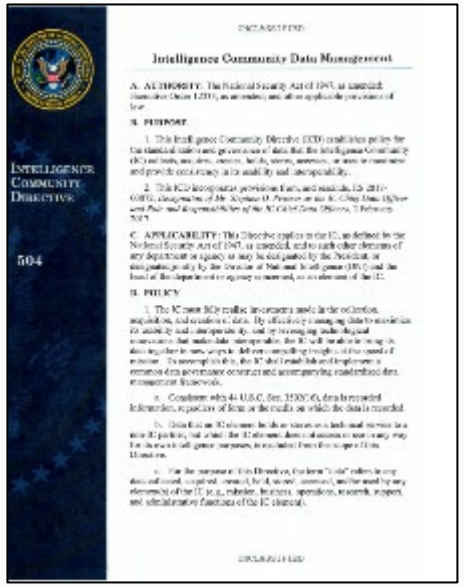
Make data discoverable, securely accessible, scalable, and interoperable across boundaries and domains.



May 2024:

(U) Vision for the IC Information Environment

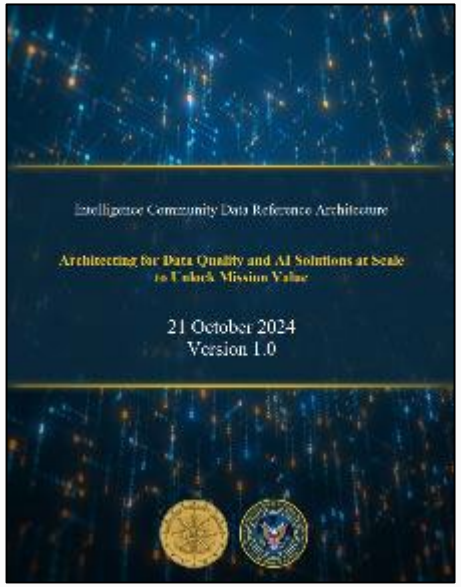
Maximize intelligence value by implementing a data-centric architecture.



June 2024:

(U) Intelligence Community Directive (ICD) 504

Data management policy guidance for standardization and governance, to maximize data usability and interoperability.



October 2024:

(U) IC Data Reference Architecture (DRA)

Increase responsiveness to mission challenges.

Graphic is Unclassified in its entirety

(U) DRA Benefits

- (U) Delivers structural guidance for the IC to transform how it accesses, manages, and shares data across multiple agencies and mission domains
- (U) DRA is used to increase data discoverability, interoperability and quality
- (U) By aligning to data mesh principles that link disparate data sources through federated model for managing sharing and governance guidelines, the IC DRA will increase interoperability, discoverability and decision advantage
- (U) The IC DRA is being used to drive a cultural shift toward a more efficient enterprise data marketplace where higher quality data is available for AI and other uses
- (U) Through close partnership and collaboration, multiple Private Industry leaders have adopted core DRA principles and have used the DRA to embed standards within their platforms to ensure their service offerings are aligned with the IC's future

(U) ZT Data Pillar Alignment

- (U) End-to-End Data Management Plans
- (U) Map Data Flows (especially external interfaces)
- (U) Data Inventory & Cataloging
- (U) Data Loss Monitoring & Prevention
- (U) Data Tagging & Labeling
- (U) Data Protection (e.g., encryption in-transit/at-rest, integrity)
  - Data protection "in-use" at Advanced maturity level
- (U) Dynamic Access based on User, Non-Person Entity (NPE), Environment, and Data Authorization Attributes

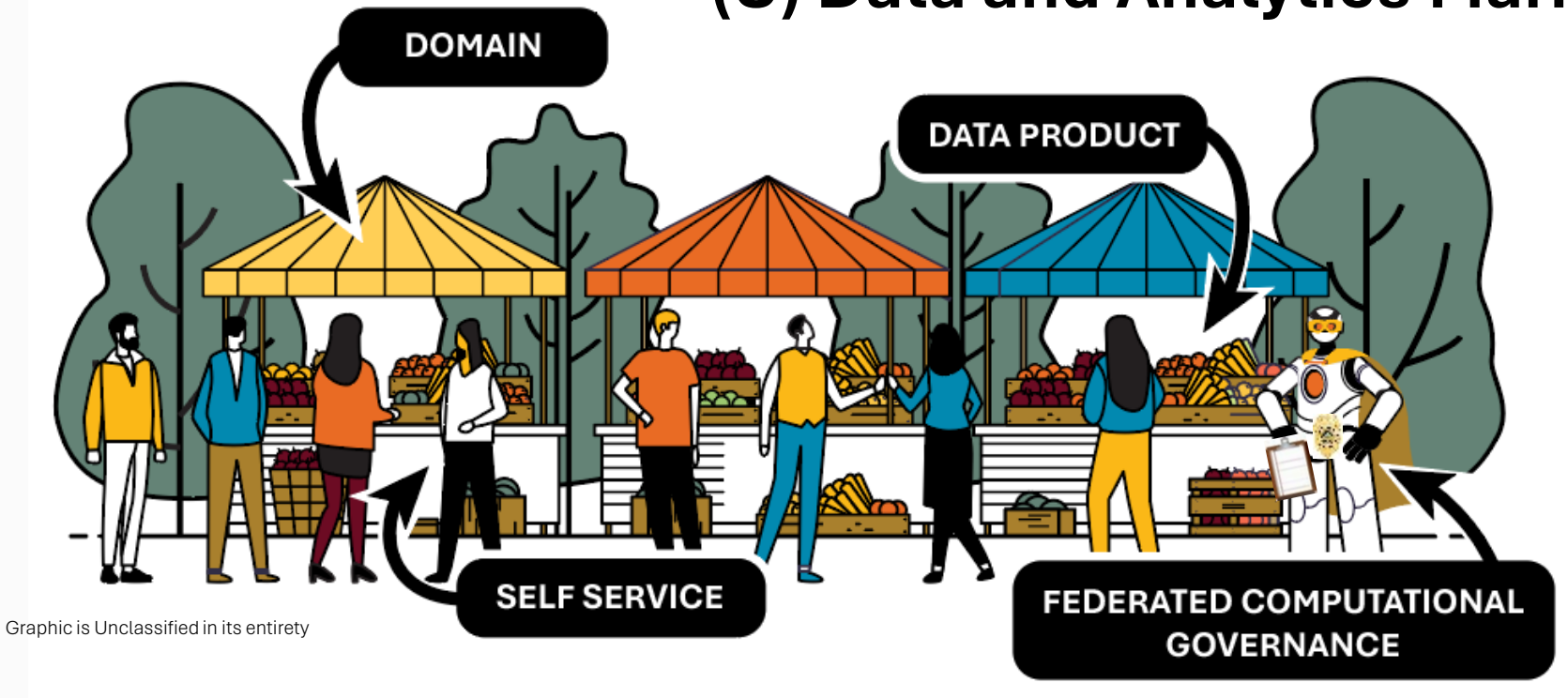
Graphic is U//FOUO in its entirety

(U) Data asset protection and best practices for accurate, least privilege, per-request data access decisions

(U) IC DRA Data Mesh Principles

(U) Domain Ownership (IC Stewardship): Domains are groups of experts within an organization, stewards of specific datasets.

(U) Data and Analytics Marketplace



Graphic is Unclassified in its entirety

(U) Data-as-a-Product: Domains maintain Data Products, and make them available for others on the IC Enterprise Data Marketplace.

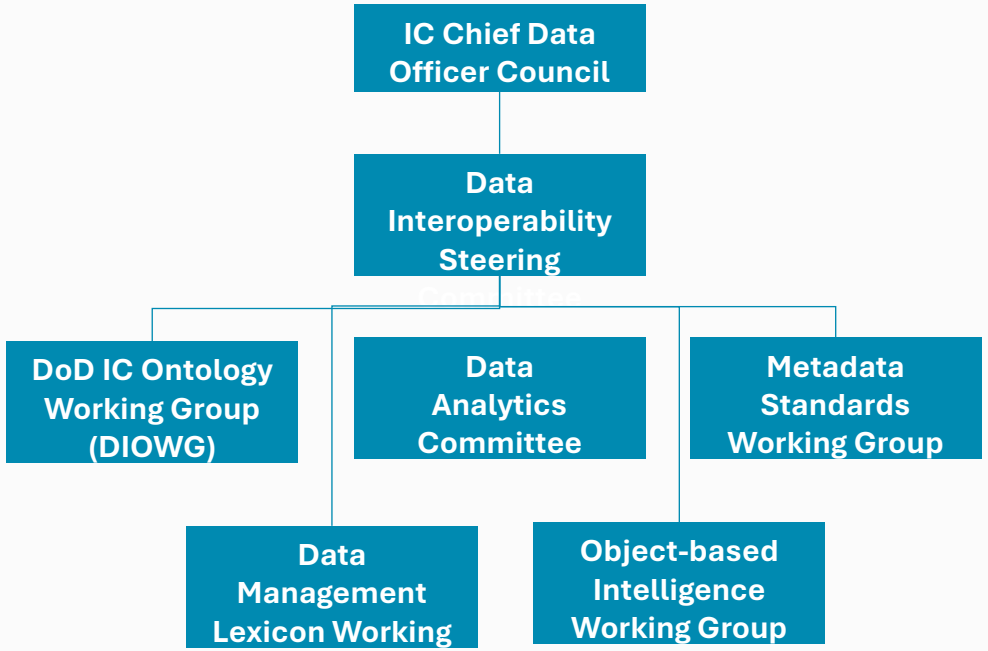
* **(U) Federated Computational Governance:** Data Products are built on common standards, such that handling of legal, policy and technical requirements is automated.

* *Human shown here but this will become automated over time*

(U) Self-service Data Platforms: Data Products are consumed through Self-service Data Platforms.

(U) Implementation Strategy

- (U) Establish an IC Data Interoperability Steering Committee (DISC)
  - Chaired by the IC Chief Data Architect
  - Action arm of the CDO Council
  - Coordinates IC DRA implementation efforts
  - Aligns the activities of Working Groups (WGs) under the CDOC
- (U) Engage with partners on mission sprints
  - Rapid iteration, focus on lessons learned
  - Identify gaps and requirements
- (U) Insert recommendations into future budget requests for solution architecture implementations



Graphic is Unclassified in its entirety

(U) Interest in OMG Standardization

(U) The IC CDO DRA team is actively working on developing the DRA implementation plan.

(U) We are actively engaging with IC and DOD partner organizations to identify 45-90 day pilot projects to help develop the implementation plan.

(U) We believe **Data Product** specifications and **Metadata** specifications will play a critical role as potential candidates for developing standards as part of the implementation plan.

(U) Interest in understanding OMG Data Product Ontology Specifications and how it may inform an IC-wide Data Product Ontology Specification.

(U) Interest in understanding OMG Information Exchange Framework (IEF) and how it may inform Metadata Standards.

(U) Key Take-aways

- (U) The IC DRA is designed to increase data **interoperability, discoverability, and quality.**
- (U) **Delivers guidance and standards** for the implementation of IC data architectures.
- (U) Provides an **approach to increase responsiveness** to IC mission challenges.
- (U) **Key milestone** as the IC transitions to a data-centric environment.
- (U) **Based on data mesh principles** widely-adopted in large and small private sector organizations.
- (U) **Coordinated with all IC components**, IC CIO, DoD, NATO, and private sector (already using IC DRA to align their product offerings), signed in October 2024.
- (U) Now in **implementation phase** through rapid, iterative mission sprints with mission partners.

ODNI

Questions?