CDAO

Chief Digital & Artificial Intelligence Office

Agile Risk Management – Enabling the Adoption of Data, Analytics and AI

September 24, 2024

Daniel C. Holtzman, SL, CES
Chief Information Officer (CIO);
Principle Deputy, Acquisitions & Assurance;
Authorizing Official (AO) &
Senior Component Official for Privacy (SCOP)

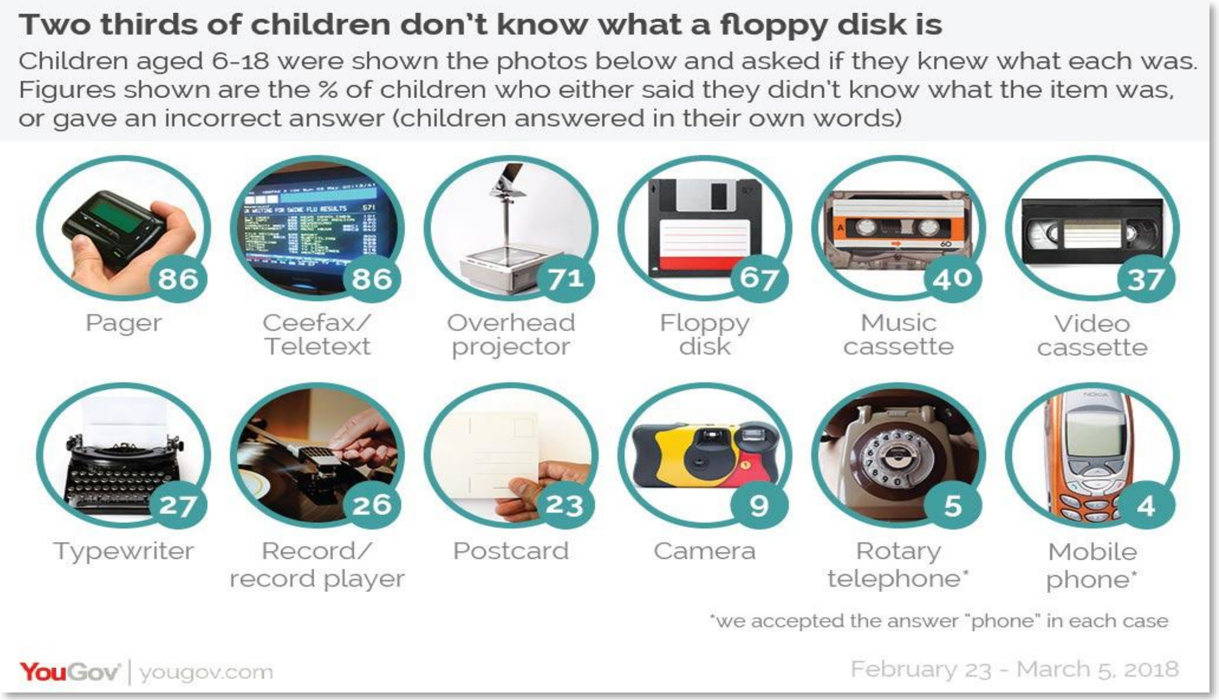
Authorizing Official for:
DoD CDAO
JSF F-35 ALIS

Decision Advantage From the Battlefield to the Boardroom
Acceleration of the DoD's Adoption of Data, Analytics, and AI

osd.cdao.ovl@mail.mil

Culture Change Challenge: *Unperceived Bias*

> *Cool, you 3D printed the save icon!*



Two thirds of children don't know what a floppy disk is

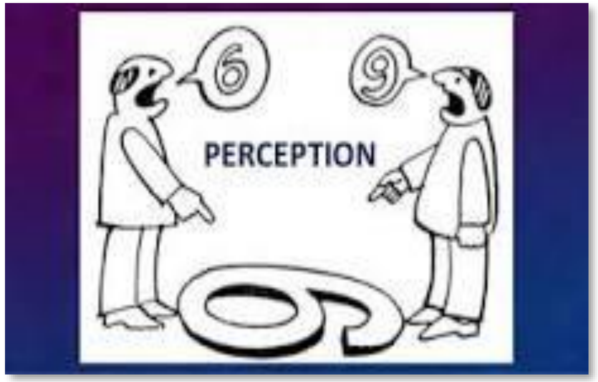
Children aged 6-18 were shown the photos below and asked if they knew what each was. Figures shown are the % of children who either said they didn't know what the item was, or gave an incorrect answer (children answered in their own words)

Item	%
Pager	86
Ceefax/ Teletext	86
Overhead projector	71
Floppy disk	67
Music cassette	40
Video cassette	37
Typewriter	27
Record/ record player	26
Postcard	23
Camera	9
Rotary telephone*	5
Mobile phone*	4

*we accepted the answer "phone" in each case

YouGov | yougov.com

February 23 - March 5, 2018



Do you know the answers to these?

Do you realize your own bias?

<u>Communication is key to culture change</u>

***"Change your thoughts and change your world."* – Norman Peale**

Agenda

- **Chief Digital & Artificial Intelligence Office (CDAO)**
- **Operation Vulcan Logic – Agile Risk Management**
- **Deep Thoughts**
- **Back-up info on Operation Vulcan Logic**

> *Cybersecurity and resiliency is a journey; not a destination.*
>
> — D.C. Holtzman

CDAO - Mission and Functions

Mission:

Accelerate DoD’s adoption of data, analytics, and AI to generate decision advantage from the boardroom to the battlefield.

Functions:

1. **Lead and oversee** DoD' s strategy development and policy formulation for data, analytics, and AI.
2. **Break down barriers** to data and AI adoption within DoD institutional processes (serve as a “demanding customer”).
3. **Create enabling digital infrastructure and services** that support Components' development and deployment of data, analytics, AI, and digital-enabled solutions.
4. **Selectively scale** proven digital and AI-enabled solutions for enterprise and joint use cases.
5. **Surge digital services** for rapid response to crises and emergent challenges.

Enable …… Scale …… Speed

CDAO

Data, Data, Data – Its all about the DATA

1

DATA AS A PRODUCT

Data has value when producers make promises to customers

2

DATA DOMAIN OWNERSHIP

Functional leaders responsible for driving enterprise data products

3

FEDERATED COMPUTATIONAL GOVERNANCE

Sharing and use must be increasingly automated

4

SELF SERVICE PLATFORMS

Users at echelon to create value using the ecosystem of distributed platforms

Moving beyond Network Centric….. Toward DATA Centric !

The Sea is our DATA – All Boats can use the Sea

The CDAO Mission

Accelerate DoD’s adoption of data, analytics, and AI to generate **decision advantage**, from the boardroom to the battlefield

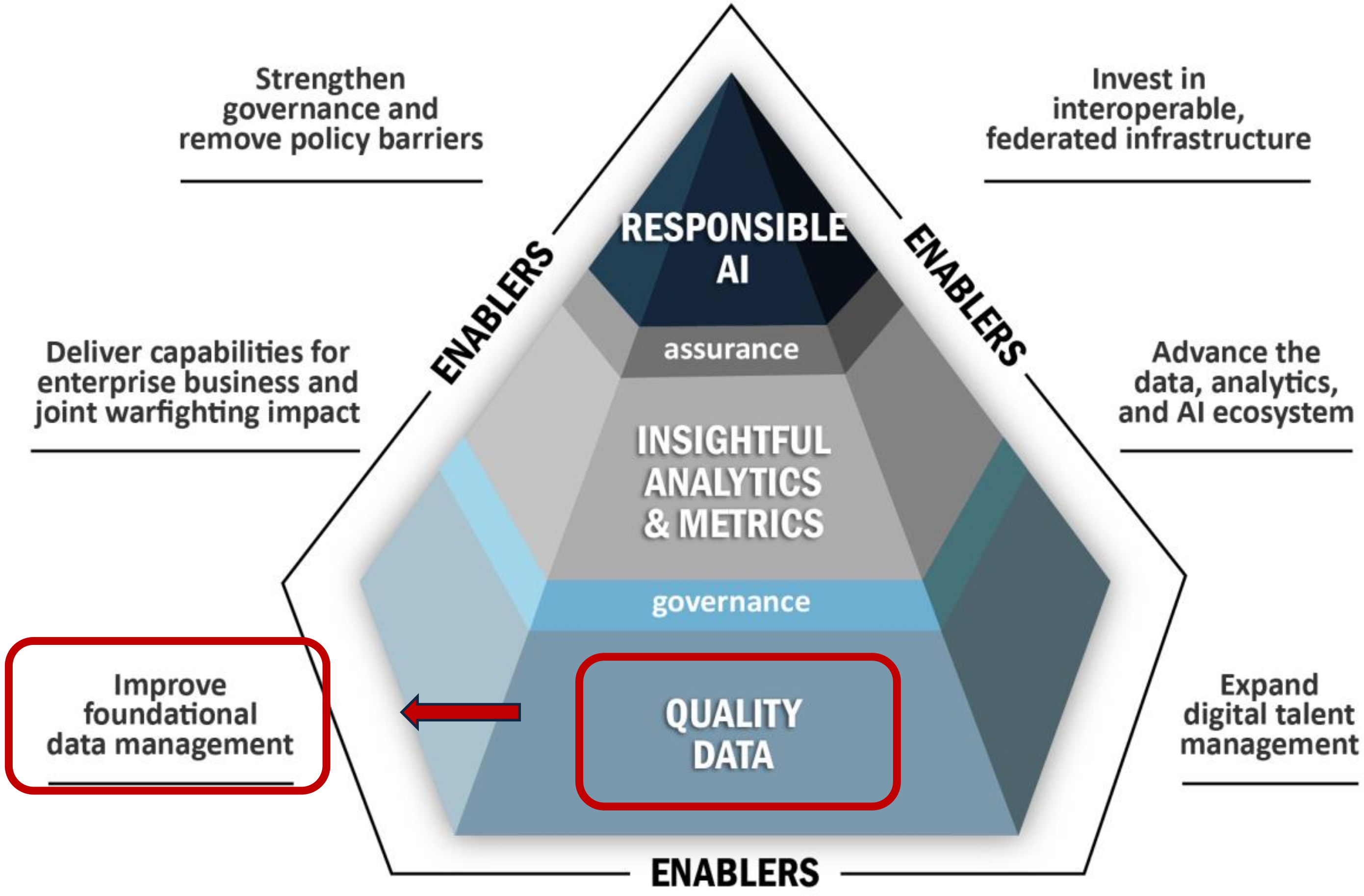
The DoD OATSD(PCLT) Mission

Implement the Department of Defense’s Privacy, Civil Liberties, and Freedom of Information programs.

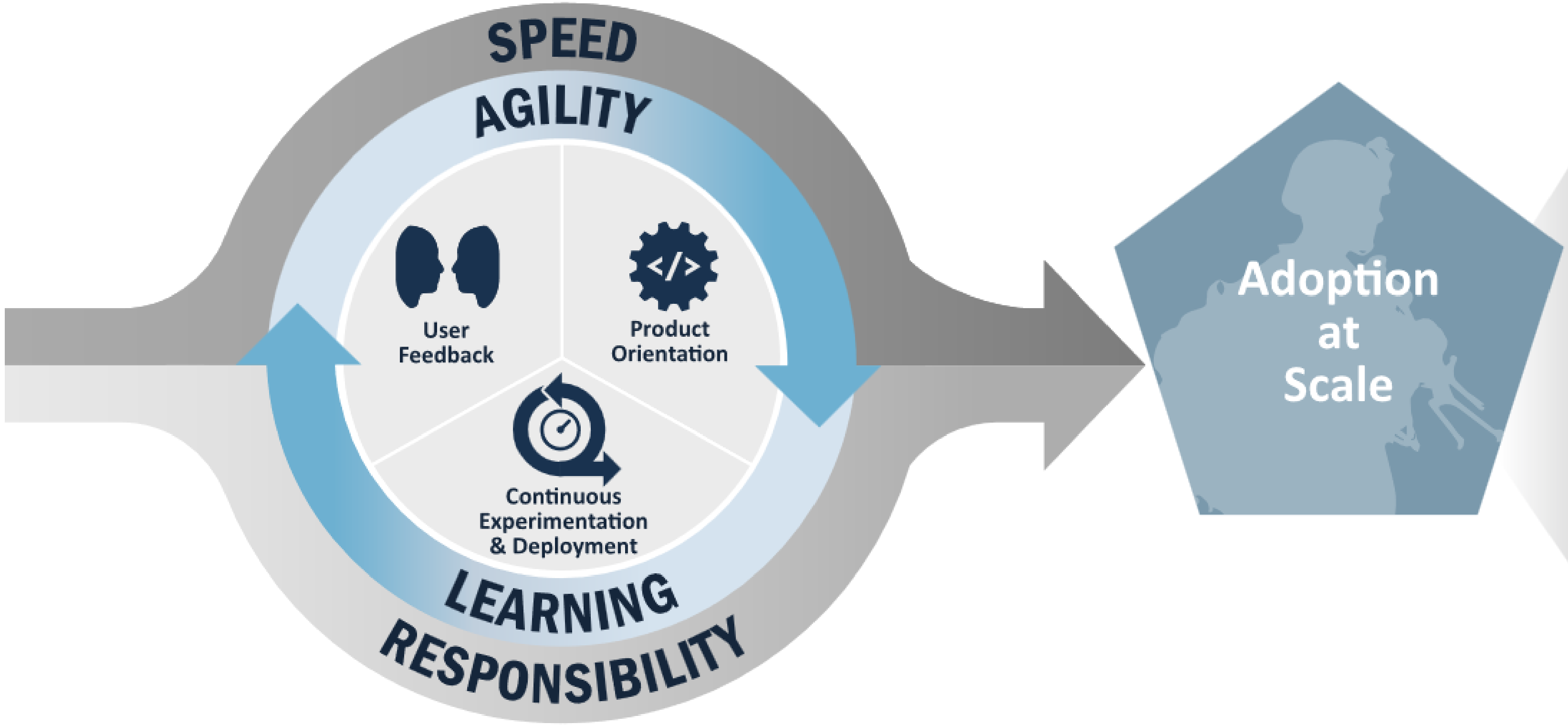
Reciprocity – Collaboration & Partnerships

AI Hierarchy of Needs

The goals outlined in the Strategy advance the Department’s technical maturity to support analytics and AI/ML at scale


Strengthen governance and remove policy barriers
Invest in interoperable, federated infrastructure
Deliver capabilities for enterprise business and joint warfighting impact
Advance the data, analytics, and AI ecosystem
Improve foundational data management
Expand digital talent management
ENABLERS
ENABLERS
ENABLERS
RESPONSIBLE AI
assurance
INSIGHTFUL ANALYTICS & METRICS
governance
QUALITY DATA

Employing an Agile Approach to Adoption



DECISION ADVANTAGE OUTCOMES

1. Superior battlespace awareness and understanding
2. Adaptive force planning and application
3. Fast, precise, and resilient kill chains
4. Resilient sustainment support
5. Efficient enterprise business operations

Enable …… Scale …… Speed

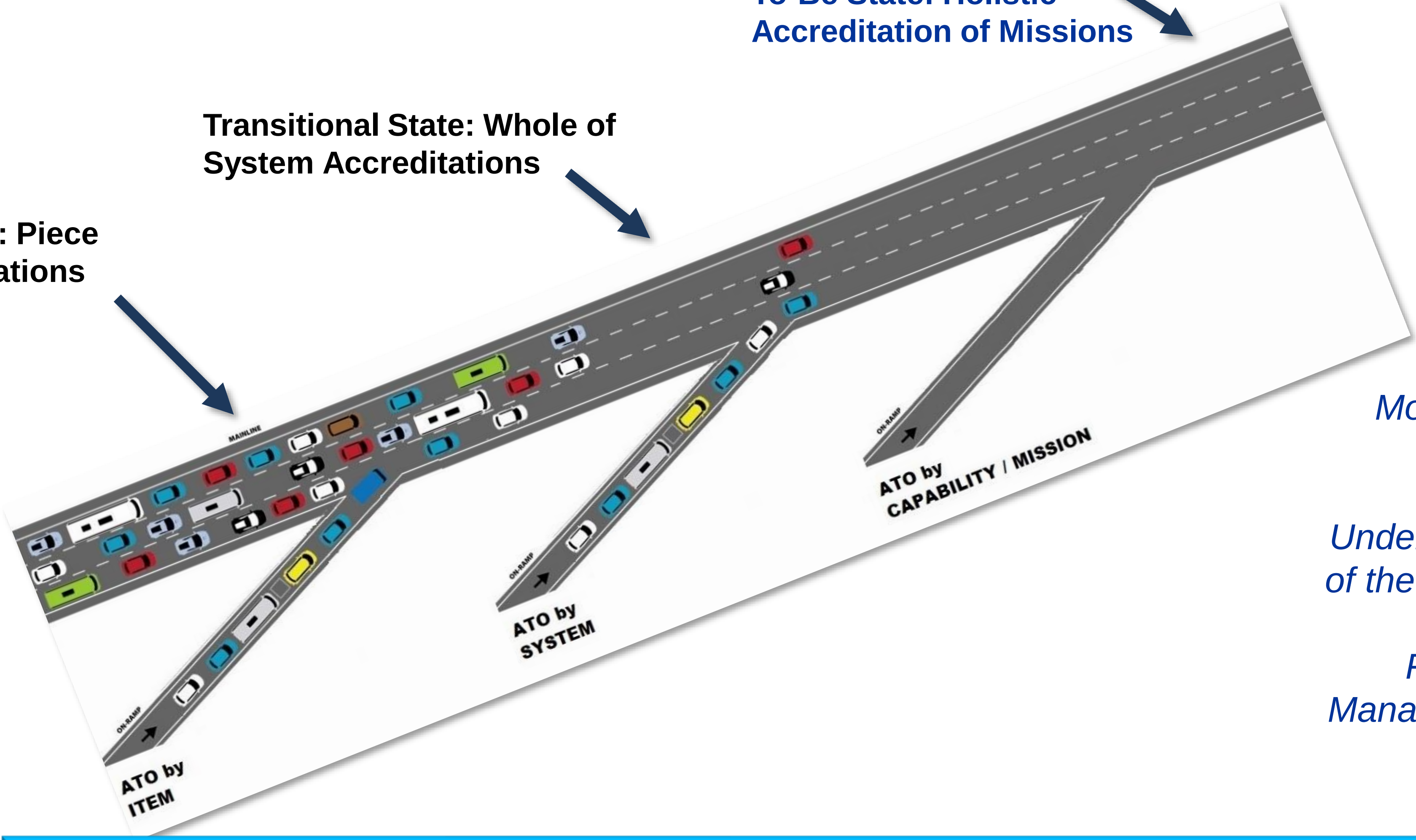
Agenda

- **Chief Digital & Artificial Intelligence Office (CDAO)**
- **Operation Vulcan Logic – Agile Risk Management**
- **Deep Thoughts**
- **Back-up info on Operation Vulcan Logic**

> *The most dangerous phrase in language is:*
>
> ***We've always done it this way***
>
> — Admiral Grace Hopper, USN

CDAO

Highway to Resilient Capabilities



To-Be State: Holistic Accreditation of Missions

Transitional State: Whole of System Accreditations

Current State: Piece Part Accreditations

Moving Towards Agile Authorizations.

Understand the Risk of Use of the system in the context.

Focus on the Risk Management in Operational Context.

Traditional Boundary Configuration Management is no longer sufficient in a software-defined, ubiquitous, connected environment.

Agenda

Challenge:

The Cyber Security (ATO) execution process in general, to date, has been very compliance focused, resource and time intensive.

While the ATO approval process is an important contributor to implementing cybersecurity and managing risk, delays in fielding new systems and capabilities can bring their own risks by extending the use of legacy (often less secure) capabilities.

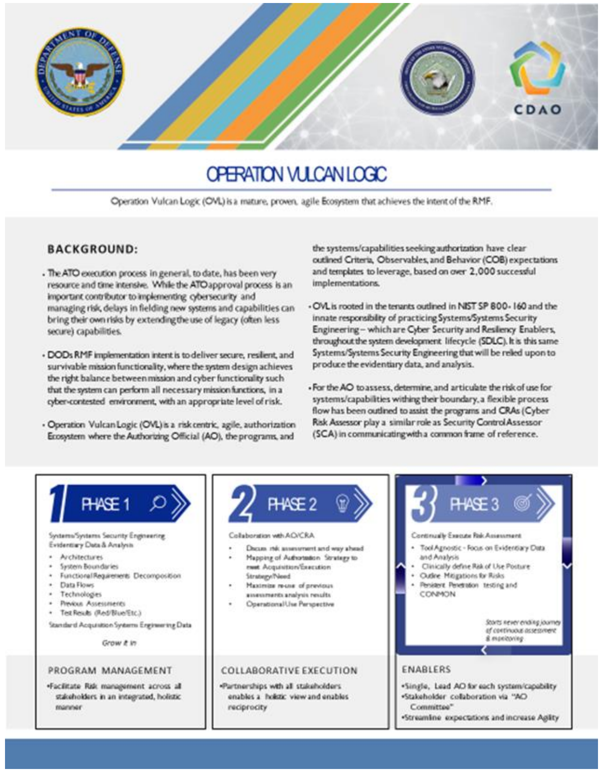
DODs RMF implementation intent is to deliver secure, resilient, and survivable mission functionality, where the system design achieves the right balance between mission and cyber functionality such that the system can perform all necessary mission functions, in a cyber-contested environment, with an appropriate level of risk

Way Forward:

<u>Operation Vulcan Logic (OVL)</u> is a risk-centric, agile, authorization Ecosystem

Where the Authorizing Official (AO), the programs/capability developers, and the systems/capabilities seeking authorization have clear outlined Criteria, Observables and Behavior (COB) expectations

Templates/exemplars to leverage, based on the proven analytics of over 2,000 successful implementations.



OPERATION VULCAN LOGIC

Operation Vulcan Logic (OVL) is a mature, proven, agile Ecosystem that achieves the intent of the RMF.

BACKGROUND:

- The ATO execution process in general, to date, has been very resource and time intensive. While the ATO approval process is an important contributor to implementing cybersecurity and managing risk, delays in fielding new systems and capabilities can bring their own risks by extending the use of legacy (often less secure) capabilities.
- DODs RMF implementation intent is to deliver secure, resilient, and survivable mission functionality, where the system design achieves the right balance between mission and cyber functionality such that the system can perform all necessary mission functions, in a cyber-contested environment, with an appropriate level of risk.
- Operation Vulcan Logic (OVL) is a risk centric, agile, authorization Ecosystem where the Authorizing Official (AO), the programs, and the systems/capabilities seeking authorization have clear outlined Criteria, Observables, and Behavior (COB) expectations and templates to leverage, based on over 2,000 successful implementations.
- OVL is rooted in the tenants outlined in NIST SP 800-160 and the innate responsibility of practicing Systems/Systems Security Engineering – which are Cyber Security and Resiliency Enablers, throughout the system development lifecycle (SDLC). It is this same Systems/Systems Security Engineering that will be relied upon to produce the evidentiary data, and analysis.
- For the AO to assess, determine, and articulate the risk of use for systems/capabilities withing their boundary, a flexible process flow has been outlined to assist the programs and CRAs (Cyber Risk Assessor play a similar role as Security Control Assessor (SCA) in communicating with a common frame of reference.

1 PHASE 1

Systems/Systems Security Engineering Evidentiary Data & Analysis

- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)

Standard Acquisition Systems Engineering Data

Grow it in

PROGRAM MANAGEMENT

- Facilitate Risk management across all stakeholders in an integrated, holistic manner

2 PHASE 2

Collaboration with AO/CRA

- Discuss risk assessment and way ahead
- Mapping of Authorization Strategy to meet Acquisition/Execution Strategy/Need
- Maximize re-use of previous assessments analysis results
- Operational/Use Perspective

COLLABORATIVE EXECUTION

- Partnerships with all stakeholders enables a holistic view and enables reciprocity

3 PHASE 3

Continually Execute Risk Assessment

- Tool Agnostic - Focus on Evidentiary Data and Analysis
- Clinically define Risk of Use Posture
- Outline Mitigations for Risks
- Persistent Penetration testing and CONMON

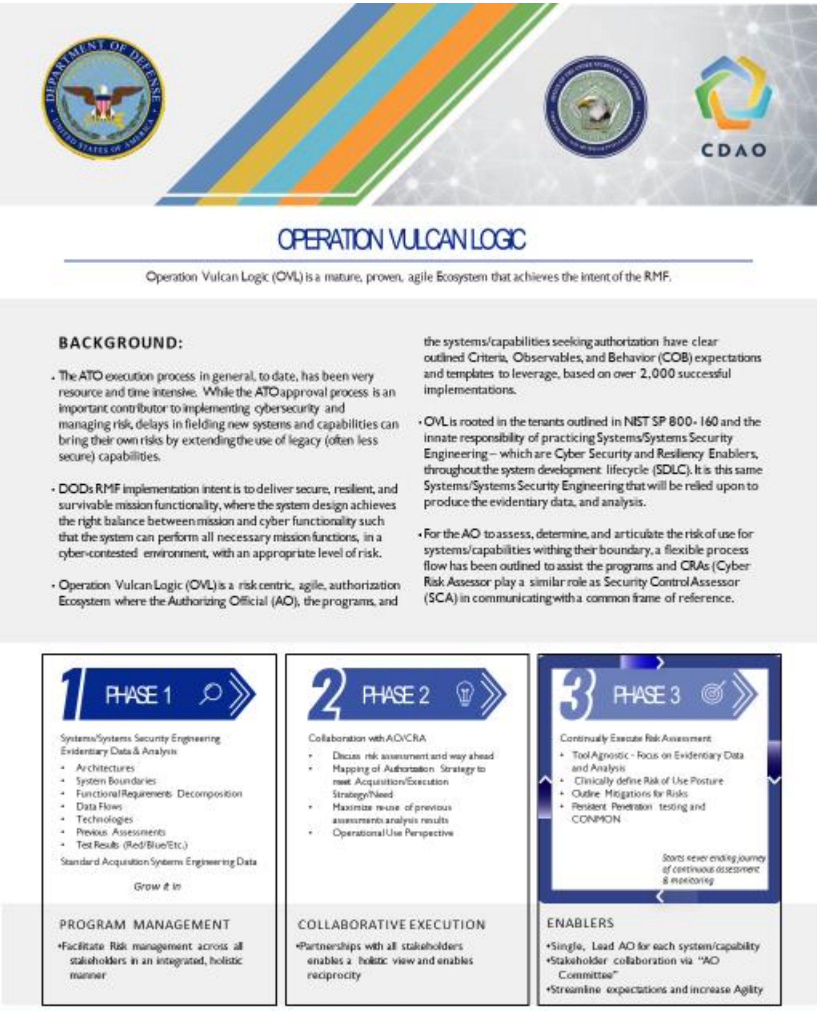
Starts never ending journey of continuous assessment & monitoring

ENABLERS

- Single, Lead AO for each system/capability
- Stakeholder collaboration via "AO Committee"
- Streamline expectations and increase Agility

Operation Vulcan Logic (OVL): *BLUF*

See Handout →



OPERATION VULCAN LOGIC

Operation Vulcan Logic (OVL) is a mature, proven, agile Ecosystem that achieves the intent of the RMF.

BACKGROUND:

- The ATO execution process in general, to date, has been very resource and time intensive. While the ATO approval process is an important contributor to implementing cybersecurity and managing risk, delays in fielding new systems and capabilities can bring their own risks by extending the use of legacy (often less secure) capabilities.
- DODs RMF implementation intent is to deliver secure, resilient, and survivable mission functionality, where the system design achieves the right balance between mission and cyber functionality such that the system can perform all necessary mission functions, in a cyber-contested environment, with an appropriate level of risk.
- Operation Vulcan Logic (OVL) is a risk centric, agile, authorization Ecosystem where the Authorizing Official (AO), the programs, and the systems/capabilities seeking authorization have clear outlined Criteria, Observables, and Behavior (COB) expectations and templates to leverage, based on over 2,000 successful implementations.
- OVL is rooted in the tenants outlined in NIST SP 800-160 and the innate responsibility of practicing Systems/Systems Security Engineering – which are Cyber Security and Resiliency Enablers, throughout the system development lifecycle (SDLC). It is this same Systems/Systems Security Engineering that will be relied upon to produce the evidentiary data, and analysis.
- For the AO to assess, determine, and articulate the risk of use for systems/capabilities withing their boundary, a flexible process flow has been outlined to assist the programs and CRAs (Cyber Risk Assessor play a similar role as Security Control Assessor (SCA) in communicating with a common frame of reference.

1 PHASE 1

Systems/Systems Security Engineering Evidentiary Data & Analysis

- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)

Standard Acquisition Systems Engineering Data

Grow it in

PROGRAM MANAGEMENT

- Facilitate Risk management across all stakeholders in an integrated, holistic manner

2 PHASE 2

Collaboration with AO/CRA

- Discuss risk assessment and way ahead
- Mapping of Authorization Strategy to meet Acquisition/Execution Strategy/Need
- Maximize re-use of previous assessments analysis results
- Operational Use Perspective

COLLABORATIVE EXECUTION

- Partnerships with all stakeholders enables a holistic view and enables reciprocity

3 PHASE 3

Continually Execute Risk Assessment

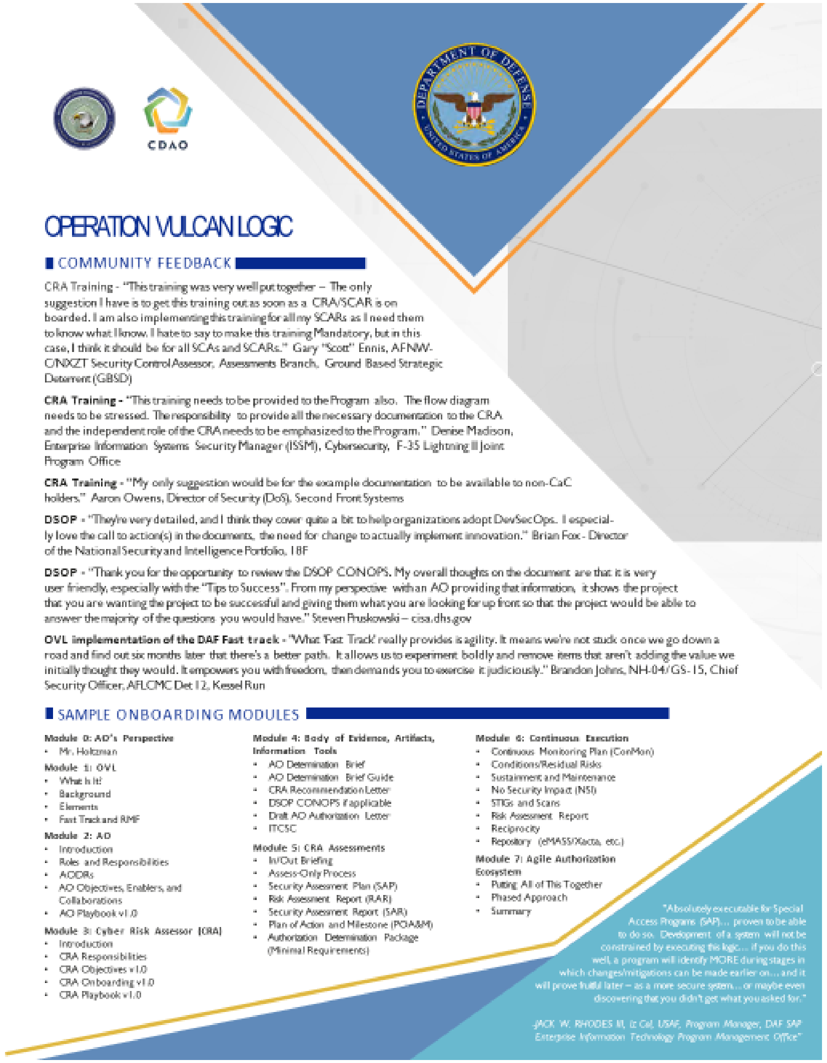
- Tool Agnostic - Focus on Evidentiary Data and Analysis
- Clinically define Risk of Use Posture
- Outline Mitigations for Risks
- Persistent Penetration testing and CONMON

Starts never ending journey of continuous assessment & monitoring

ENABLERS

- Single, Lead AO for each system/capability
- Stakeholder collaboration via "AO Committee"
- Streamline expectations and increase Agility

https://arlo-solutions.com/ovl



OPERATION VULCAN LOGIC

COMMUNITY FEEDBACK

CRA Training - "This training was very well put together – The only suggestion I have is to get this training out as soon as a CRA/SCAR is on boarded. I am also implementing this training for all my SCARs as I need them to know what I know. I hate to say to make this training Mandatory, but in this case, I think it should be for all SCAs and SCARs." Gary "Scott" Ennis, AFNWC/NXZT Security Control Assessor, Assessments Branch, Ground Based Strategic Deterrent (GBSD)

CRA Training - "This training needs to be provided to the Program also. The flow diagram needs to be stressed. The responsibility to provide all the necessary documentation to the CRA and the independent role of the CRA needs to be emphasized to the Program." Denise Madison, Enterprise Information Systems Security Manager (ISSM), Cybersecurity, F-35 Lightning II Joint Program Office

CRA Training - "My only suggestion would be for the example documentation to be available to non-CaC holders." Aaron Owens, Director of Security (DoS), Second Front Systems

DSOP - "They're very detailed, and I think they cover quite a bit to help organizations adopt DevSecOps. I especially love the call to action(s) in the documents, the need for change to actually implement innovation." Brian Fox - Director of the National Security and Intelligence Portfolio, 18F

DSOP - "Thank you for the opportunity to review the DSOP CONOPS. My overall thoughts on the document are that it is very user friendly, especially with the "Tips to Success". From my perspective with an AO providing that information, it shows the project that you are wanting the project to be successful and giving them what you are looking for up front so that the project would be able to answer the majority of the questions you would have." Steven Pruskowski – cisa.dhs.gov

OVL implementation of the DAF Fast track - "What 'Fast Track' really provides is agility. It means we're not stuck once we go down a road and find out six months later that there's a better path. It allows us to experiment boldly and remove items that aren't adding the value we initially thought they would. It empowers you with freedom, then demands you to exercise it judiciously." Brandon Johns, NH-04/GS-15, Chief Security Officer, AFLCMC Det 12, Kessel Run

SAMPLE ONBOARDING MODULES

Module 0: AO's Perspective
- Mr. Holtzman

Module 1: OVL
- What is it!
- Background
- Elements
- Fast Track and RMF

Module 2: AO
- Introduction
- Roles and Responsibilities
- AODRs
- AO Objectives, Enablers, and Collaborations
- AO Playbook v1.0

Module 3: Cyber Risk Assessor (CRA)
- Introduction
- CRA Responsibilities
- CRA Objectives v1.0
- CRA Onboarding v1.0
- CRA Playbook v1.0

Module 4: Body of Evidence, Artifacts, Information Tools
- AO Determination Brief
- AO Determination Brief Guide
- CRA Recommendation Letter
- DSOP CONOPS if applicable
- Draft AO Authorization Letter
- ITCSC

Module 5: CRA Assessments
- In/Out Briefing
- Assess-Only Process
- Security Assessment Plan (SAP)
- Risk Assessment Report (RAR)
- Security Assessment Report (SAR)
- Plan of Action and Milestone (POA&M)
- Authorization Determination Package (Minimal Requirements)

Module 6: Continuous Execution
- Continuous Monitoring Plan (ConMon)
- Conditions/Residual Risks
- Sustainment and Maintenance
- No Security Impact (NSI)
- STIGs and Scans
- Risk Assessment Report
- Reciprocity
- Repository (eMASS/Xacta, etc.)

Module 7: Agile Authorization Ecosystem
- Putting All of This Together
- Phased Approach
- Summary

"Absolutely executable for Special Access Programs (SAP)… proven to be able to do so. Development of a system will not be constrained by executing this logic… if you do this well, a program will identify MORE during stages in which changes/mitigations can be made earlier on… and it will prove fruitful later – as a more secure system… or maybe even discovering that you didn't get what you asked for."

-JACK W. RHODES III, Lt Col, USAF, Program Manager, DAF SAP Enterprise Information Technology Program Management Office"

Proven Risk-based Ecosystem

Over 2,000 Authorizations

Across domains

Achieved Reciprocity

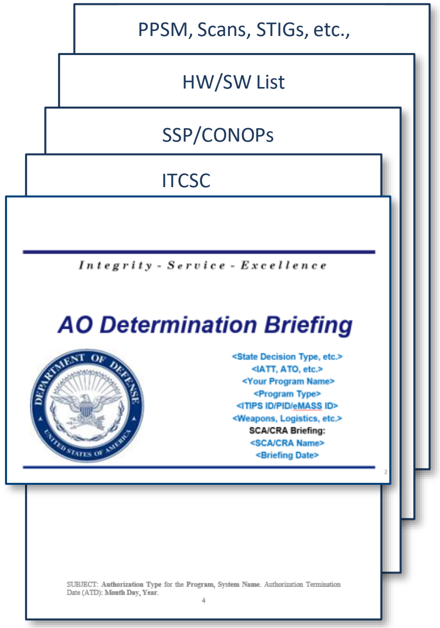
Agility in execution

Continuous updating

Collaboration with Industry via NDIA

Operation Vulcan Logic (OVL) Authorization Templates
Simple, Effective, Agile

AO Determination Briefing and Supporting Evidence



Integrity - Service - Excellence

AO Determination Briefing

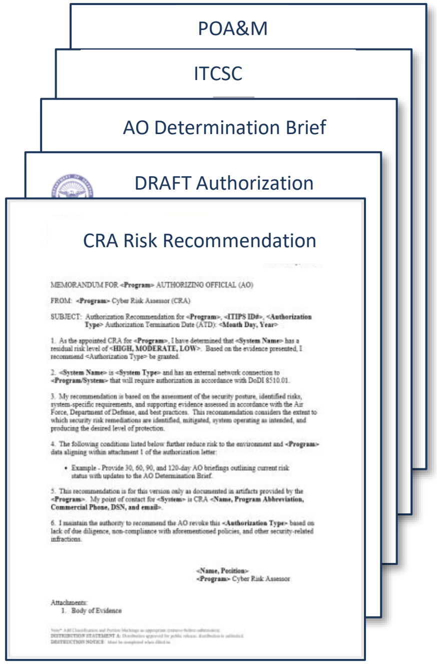
<State Decision Type, etc.>
<IATT, ATO, etc.>
<Your Program Name>
<Program Type>
<ITIPS ID/PID/eMASS ID>
<Weapons, Logistics, etc.>
SCA/CRA Briefing:
<SCA/CRA Name>
<Briefing Date>

2

SUBJECT: **Authorization Type** for the **Program, System Name**. Authorization Termination Date (ATD): **Month Day, Year**.

4

CRA Risk Recommendation



MEMORANDUM FOR **<Program>** AUTHORIZING OFFICIAL (AO)

FROM: **<Program>** Cyber Risk Assessor (CRA)

SUBJECT: Authorization Recommendation for **<Program>**, **<ITIPS ID#>**, **<Authorization Type>** Authorization Termination Date (ATD): **<Month Day, Year>**

1. As the appointed CRA for **<Program>**, I have determined that **<System Name>** has a residual risk level of **<HIGH, MODERATE, LOW>**. Based on the evidence presented, I recommend <Authorization Type> be granted.

2. **<System Name>** is **<System Type>** and has an external network connection to **<Program/System>** that will require authorization in accordance with DoDI 8510.01.

3. My recommendation is based on the assessment of the security posture, identified risks, system-specific requirements, and supporting evidence assessed in accordance with the Air Force, Department of Defense, and best practices. This recommendation considers the extent to which security risk remediations are identified, mitigated, system operating as intended, and producing the desired level of protection.

4. The following conditions listed below further reduce risk to the environment and **<Program>** data aligning within attachment 1 of the authorization letter:

- Example - Provide 30, 60, 90, and 120-day AO briefings outlining current risk status with updates to the AO Determination Brief.

5. This recommendation is for this version only as documented in artifacts provided by the **<Program>**. My point of contact for **<System>** is CRA **<Name, Program Abbreviation, Commercial Phone, DSN, and email>**.

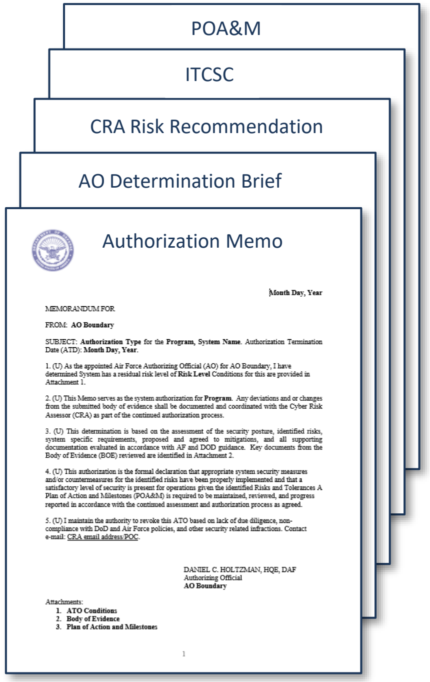
6. I maintain the authority to recommend the AO revoke this **<Authorization Type>** based on lack of due diligence, non-compliance with aforementioned policies, and other security-related infractions.

<Name, Position>
<Program> Cyber Risk Assessor

Attachments:
1. Body of Evidence

Note*: Add Classification and Portion Markings as appropriate (remove before submission).
DISTRIBUTION STATEMENT A: Distribution approved for public release; distribution is unlimited.
DESTRUCTION NOTICE: Must be completed when filled in.

Authorization Package



Month Day, Year

MEMORANDUM FOR

FROM: **AO Boundary**

SUBJECT: **Authorization Type** for the **Program, System Name**. Authorization Termination Date (ATD): **Month Day, Year**.

1. (U) As the appointed Air Force Authorizing Official (AO) for AO Boundary, I have determined System has a residual risk level of **Risk Level** Conditions for this are provided in Attachment 1.

2. (U) This Memo serves as the system authorization for **Program**. Any deviations and or changes from the submitted body of evidence shall be documented and coordinated with the Cyber Risk Assessor (CRA) as part of the continued authorization process.

3. (U) This determination is based on the assessment of the security posture, identified risks, system specific requirements, proposed and agreed to mitigations, and all supporting documentation evaluated in accordance with AF and DOD guidance. Key documents from the Body of Evidence (BOE) reviewed are identified in Attachment 2.

4. (U) This authorization is the formal declaration that appropriate system security measures and/or countermeasures for the identified risks have been properly implemented and that a satisfactory level of security is present for operations given the identified Risks and Tolerances A Plan of Action and Milestones (POA&M) is required to be maintained, reviewed, and progress reported in accordance with the continued assessment and authorization process as agreed.

5. (U) I maintain the authority to revoke this ATO based on lack of due diligence, non-compliance with DoD and Air Force policies, and other security related infractions. Contact e-mail: CRA email address/POC.

DANIEL C. HOLTZMAN, HQE, DAF
Authorizing Official
AO Boundary

Attachments:
1. **ATO Conditions**
2. **Body of Evidence**
3. **Plan of Action and Milestones**

1

Meets all DoDI 8510 and DAF policy requirements for RMF

Authorization Memo has list of BOE that was used to increase reciprocity

Not a workflow or set of "artifacts'

Risk Analysis informed by threat/intel, stakeholder tolerance and operational mission parameters

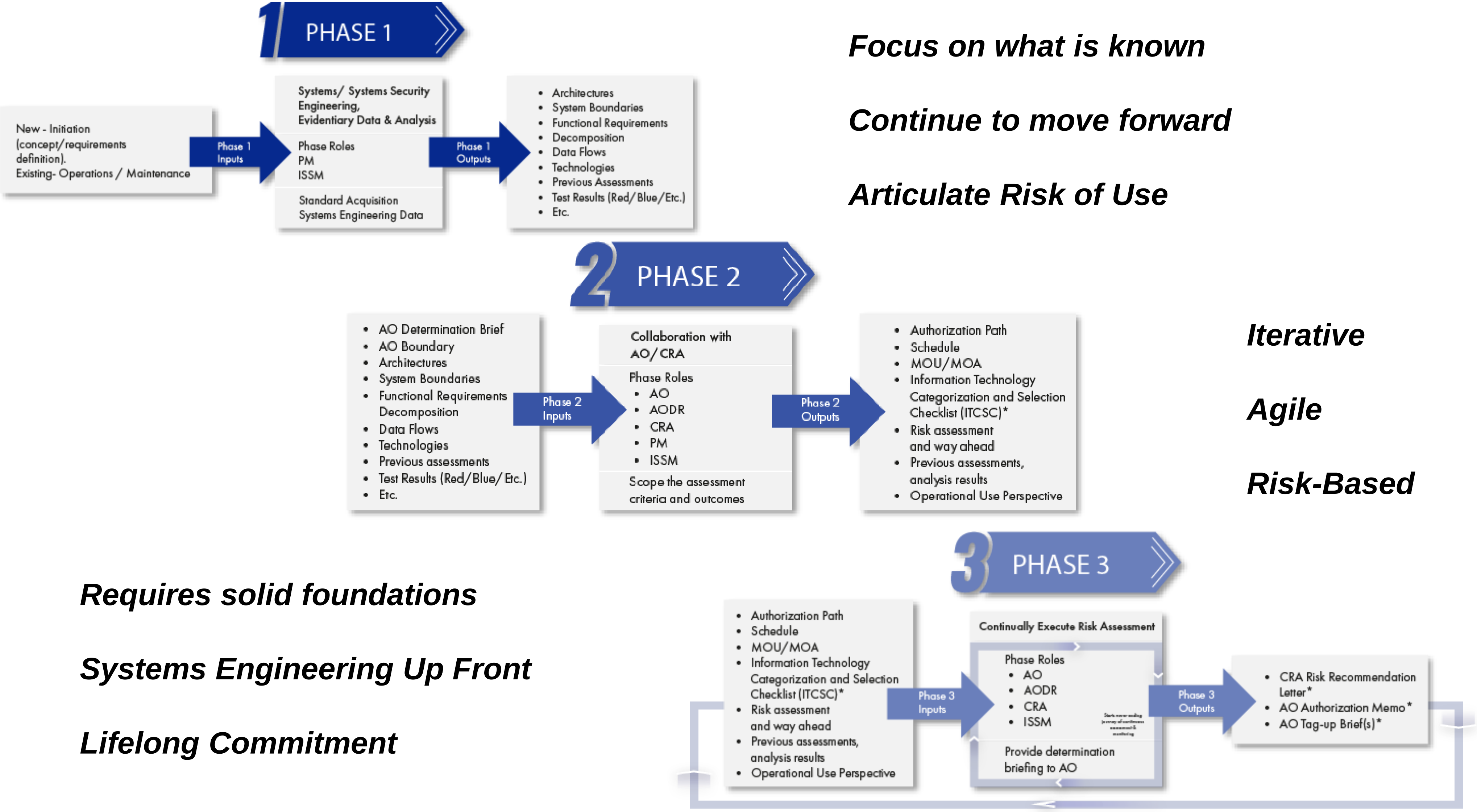
Provides the AO with an independent Assessment

Not a one-time product, developed over time working hand in hand

Authorization starts the lifelong commitment to improving cyber every day

Standardization is Flexible for Authorization Packages; No One-Size-Fits-All Approach

Agile Authorizations:
Enabled by Disciplined Systems Engineering



PHASE 1

New - Initiation (concept/requirements definition).
Existing- Operations / Maintenance

Phase 1 Inputs

Systems/ Systems Security Engineering, Evidentiary Data & Analysis

Phase Roles
PM
ISSM

Standard Acquisition Systems Engineering Data

Phase 1 Outputs

- Architectures
- System Boundaries
- Functional Requirements
- Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)
- Etc.

PHASE 2

- AO Determination Brief
- AO Boundary
- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous assessments
- Test Results (Red/Blue/Etc.)
- Etc.

Phase 2 Inputs

Collaboration with AO/CRA

Phase Roles
- AO
- AODR
- CRA
- PM
- ISSM

Scope the assessment criteria and outcomes

Phase 2 Outputs

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

PHASE 3

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

Phase 3 Inputs

Continually Execute Risk Assessment

Phase Roles
- AO
- AODR
- CRA
- ISSM

Starts never ending journey of continuous assessment & monitoring

Provide determination briefing to AO

Phase 3 Outputs

- CRA Risk Recommendation Letter*
- AO Authorization Memo*
- AO Tag-up Brief(s)*

Focus on what is known

Continue to move forward

Articulate Risk of Use

Iterative

Agile

Risk-Based

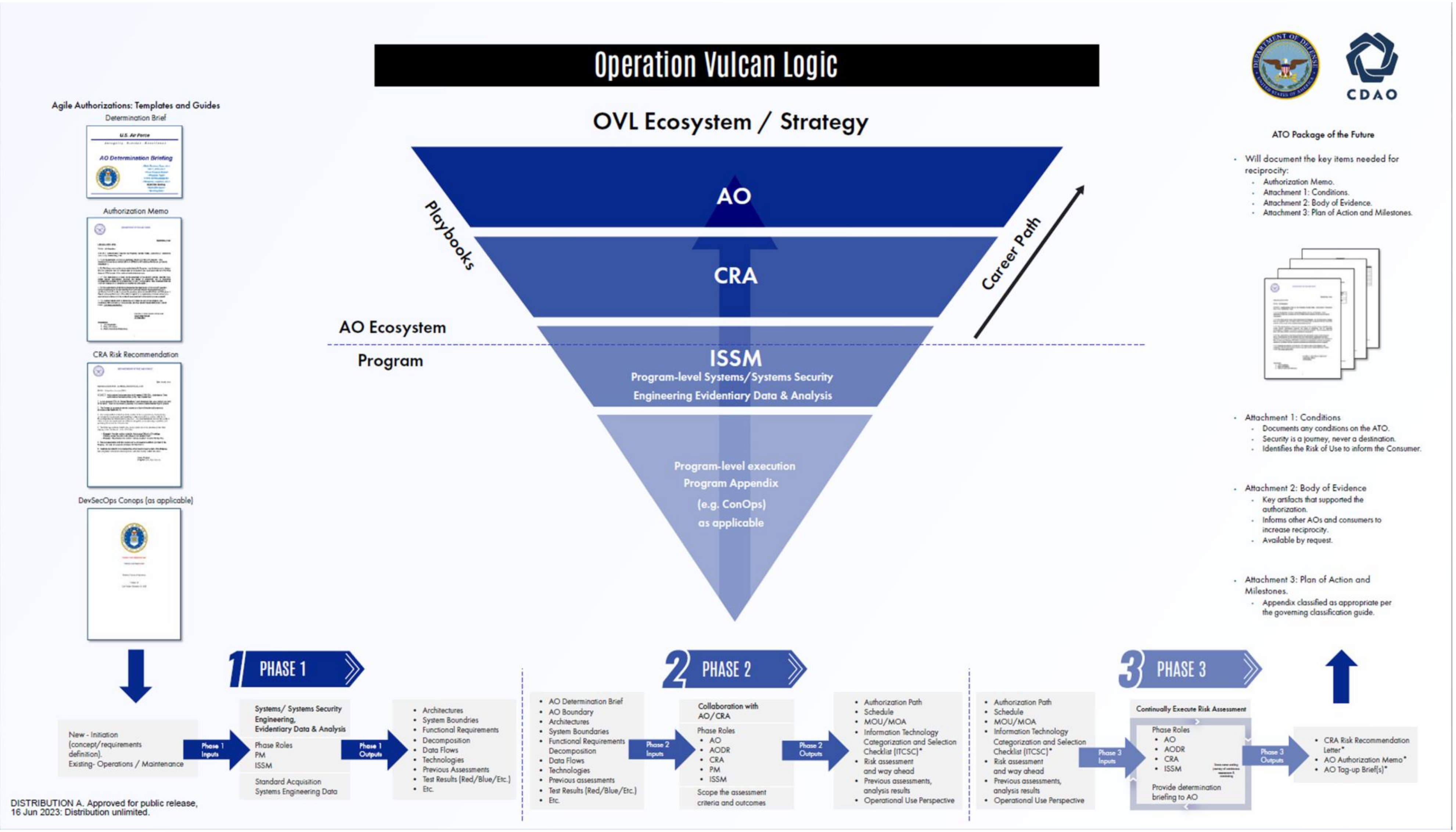
Requires solid foundations

Systems Engineering Up Front

Lifelong Commitment

DISTRIBUTION A. Approved for public release: Distribution unlimited

Operation Vulcan Logic (OVL) Ecosystem:
Systems Engineering-Based – Go Slow to Go Fast



Operation Vulcan Logic

OVL Ecosystem / Strategy

Agile Authorizations: Templates and Guides

Determination Brief

U.S. Air Force

AO Determination Briefing

Authorization Memo

CRA Risk Recommendation

DevSecOps Conops (as applicable)

ATO Package of the Future

- Will document the key items needed for reciprocity:
  - Authorization Memo.
  - Attachment 1: Conditions.
  - Attachment 2: Body of Evidence.
  - Attachment 3: Plan of Action and Milestones.

- Attachment 1: Conditions
  - Documents any conditions on the ATO.
  - Security is a journey, never a destination.
  - Identifies the Risk of Use to inform the Consumer.

- Attachment 2: Body of Evidence
  - Key artifacts that supported the authorization.
  - Informs other AOs and consumers to increase reciprocity.
  - Available by request.

- Attachment 3: Plan of Action and Milestones.
  - Appendix classified as appropriate per the governing classification guide.

1 PHASE 1

New - Initiation (concept/requirements definition).
Existing- Operations / Maintenance

Phase 1 Inputs

Systems/ Systems Security Engineering, Evidentiary Data & Analysis

Phase Roles
PM
ISSM

Standard Acquisition Systems Engineering Data

Phase 1 Outputs

- Architectures
- System Boundries
- Functional Requirements
- Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)
- Etc.

2 PHASE 2

- AO Determination Brief
- AO Boundary
- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous assessments
- Test Results (Red/Blue/Etc.)
- Etc.

Phase 2 Inputs

Collaboration with AO/CRA

Phase Roles
- AO
- AODR
- CRA
- PM
- ISSM

Scope the assessment criteria and outcomes

Phase 2 Outputs

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

3 PHASE 3

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

Phase 3 Inputs

Continually Execute Risk Assessment

Phase Roles
- AO
- AODR
- CRA
- ISSM

Provide determination briefing to AO

Phase 3 Outputs

- CRA Risk Recommendation Letter*
- AO Authorization Memo*
- AO Tag-up Brief(s)*

DISTRIBUTION A. Approved for public release, 16 Jun 2023: Distribution unlimited.

CDAO

CDAO Organizational Risk Tolerance Baseline (ORTB): *Foundational Areas of Risk – Analytics based impact*

1. Account Management (Aligns to ORTB: AC-2)

Monitor and Enforce user and group account creation/deletion

2. Administrative Privileged Accounts (Aligns to ORTB: AC-6)

Privileged user/service accounts are only authorized to perform security relevant functions. Review and approve annually.

3. Audit Review, Analysis, and Reporting (Aligns to ORTB: AU-6)

Review and analyze Information System (IS) audit logs for indications of inappropriate or unusual activity and reports findings to designated personnel IAW IRP

4. Boundary Protection (Aligns to ORTB: SC-7)

Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system

5. Continuous Monitoring (Aligns to ORTB: CA-7)

System level monitoring metrics, including control monitoring frequencies, are defined by the organization and approved by the AO

6. Data Integrity (Aligns to ORTB: SI-7)

Employ automated tools to report system (hw/sw/fw) and information (data) integrity violations. Ensure automatic integrity validation of all electronically transmitted software and data

7. External Connections (Aligns to ORTB: CA-3)

Agreement/authorization used to approve external connections and manage the exchange of information should be defined (ATC, ISA, CSA, ICD, etc.) and reviewed annually

8. External Media (Aligns to ORTB: AC-4, MP-7)

If authorized, place configuration control process on all external media including auditing. Institute external media whitelisting. Implement processes to monitor logs and audit usages.

9. Information Flow Enforcement (Aligns to ORTB: AC-4)

The information system enforces approved connections for controlling the flow of information within the system and between interconnected systems

10. Least Privilege (Aligns to ORTB: AC-6)

Reviews, at least annually, the privileges assigned to privileged user accounts including Designated Transfer Agent and Trusted Cloud Credential Manager roles

11. Operational Change Management (Aligns to ORTB: CM-8, CM-8(3), SI-7)

Automated mechanisms shall be used to detect the presence of unauthorized hardware/software/firmware within the system. One or more of the following action shall be taken upon discovery of unauthorized components: disable network access by unauthorized components; isolate unauthorized components; notify designated personnel identified in IRP

12. Proposed Equipment (Aligns to ORTB: SA-22–applies to C.I.A. impact High on non-SAP systems, CM-3)

Lock down all mission support systems and migrate off unsupported operating systems. Review support agreements (hw/sw/fw) annually

13. Protection of Information at Rest (Aligns to ORTB: SC-28, SC-28(1))

Encryption is implemented to complement protection of information at rest, using approved cryptographic methods for data encryption

14. Secure Baseline Configuration (Aligns to ORTB: CM-2, CM-6)

This Information System's secure configuration includes DoD Security Technical Implementation Guides or industry best practices and verified conformance prior to introduction into production or operational environments

15. Security Categorization (Aligns to ORTB: RA-2)

Enforce proper security categorization and review annually

16. Separation of Duties (Aligns to ORTB: AC-5)

Separates defined duties of individuals and documents separation of duties of individuals

17. Vulnerability / Anti-Virus Scanning (Aligns to ORTB: RA-5)

Conduct routine anti-virus scans on traditional IT systems and hosted applications. Institute continuous monitoring protection on all IT systems to include maintenance and testing support systems

*Red font indicates specific JSIG, Non-Tailorable controls

CDAO Organizational Risk Tolerance Baseline (ORTB): *Draft AI-Specific Areas*

AI Foundation (Aligns to CDAO ORTB: 4/5/6/13/17)

- Encrypt any stored AI-related data and models
- Regularly patch AI components (hardware and software) on known vulnerabilities and update threat definitions
- Account for vetting of AI supply chain

Data Integrity (Aligns to CDAO ORTB: 4/6/9/11/17)

- Depict provenance and lineage of datasets used for training models
- Implement mechanisms that ensures the integrity and authenticity of ingested data against adversarial attacks.
- Ensure privacy of personal data, anonymizing information where necessary
- Establish data retention and disposal mechanisms

Model Management (Aligns to CDAO ORTB: 3/4/11/17)

- Depict architecture, justification, and rationale for the selection of a specific model
- Establish regular evaluation and validation procedures of training models
- Ensure rollback mechanism for models, configurations, and training data

Operational Resilience (Aligns to CDAO ORTB: 3/5/14/17)

- Regularly employ red teaming testing methodologies and maintain logs of outcomes
- Continuously monitor system performance metrics against predefined benchmarks or thresholds for validation

User Interaction (Aligns to CDAO ORTB: 1/2/10/16)

- Incorporate mechanisms for users or other stakeholders to provide feedback on model output
- Implement oversight on user interactions, including data input, queries, and code base changes

Responsible Accountability (Aligns to CDAO ORTB: NEW)

- Implement tools and/or methodologies that can elucidate model decisions
- Implement DoD Responsible AI (RAI) principles

Seeking Collaboration to experiment, flush out, path find, validate

*Draft AI-Specific Cyber Risk Areas are derived from—and aligned to—CDAO ORTB Foundational Areas of Risk

Operation Vulcan Logic (OVL) – Applicability (#YESIF)

CRC

- ShOC-N
- Wide-Area Surveillance
- RADSIL
- BACN
- ACBN
- C2IMERA

- Advana
- SUNet
- LongBow

- MAVEN
- Hack-a-Thon's
- JADC2

- EITaaS
- SEITaaS
- RDT&E DREN

- NGAD
- Commercial UAS
- TORCC

cUAS

TAC-P

- PRC2
- WaRTAK
- GCCS / DCGS
- Pocket-J
- TBMCS
- Mission Planning
- Special Programs

E-3

- JADC2/ABMS
- Kessel Run/AOC
- Cloud One/Platform One
- E3 AWACS and JSTARS
- F-35 ALIS
- F-35 Cloud and DevSecOps
- GBSD Cloud and DevSecOps

AOC

Over 2,000 Authorizations

Proven Risk-based Ecosystem

Over 2,000 Authorizations

Across domains

Achieved Reciprocity

Agility in execution

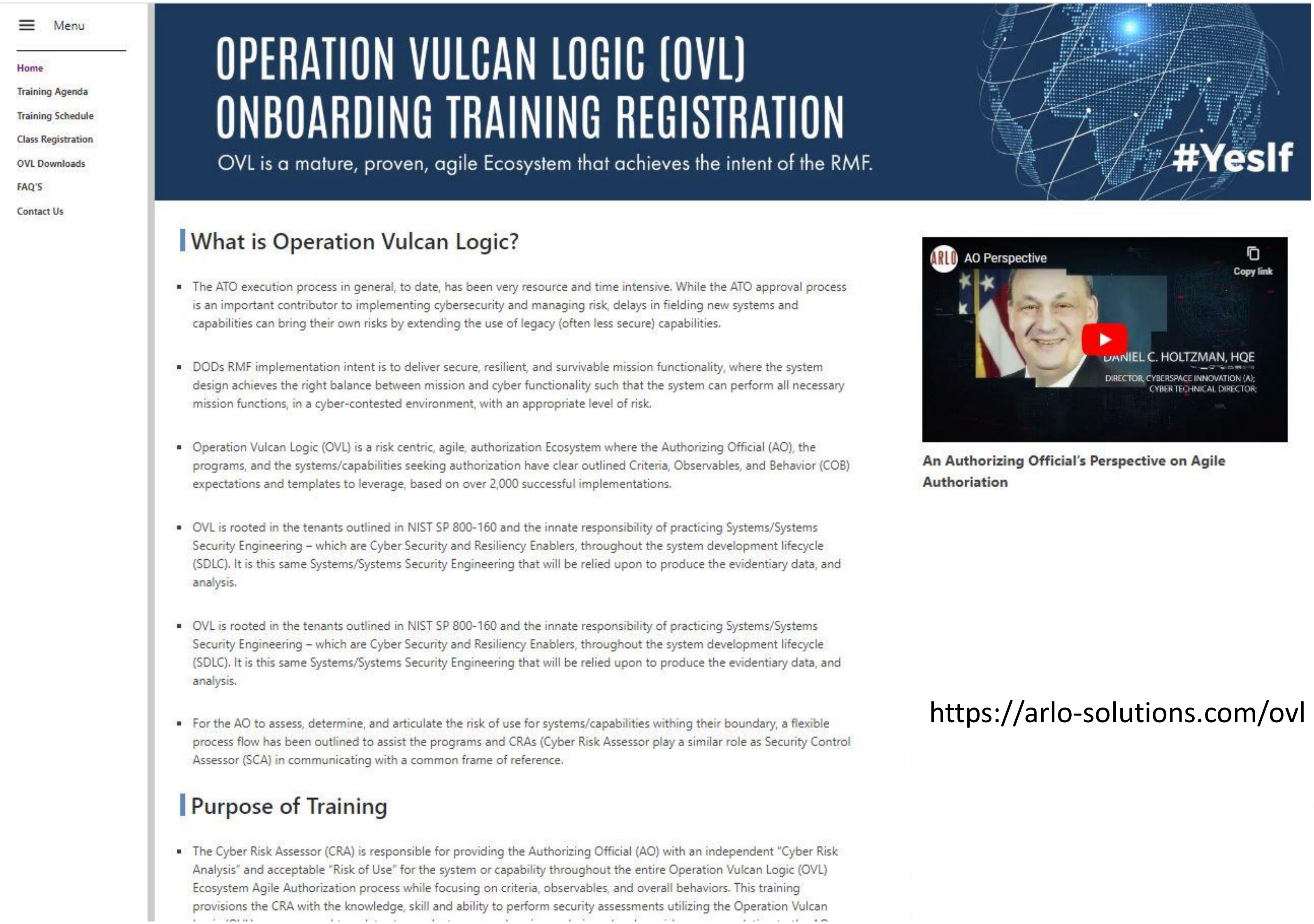
Continuous updating

CDAO

DISTRIBUTION A. Approved for public release: Distribution unlimited

Operation Vulcan Logic (OVL)
Enabling the Ecosytem

- Cyber Security is a Team Sport
- Partnerships, collaboration and sharing are key to success
- Everyone is under attack
- CDAO On boarding is available to all
- Future Round tables are planned
  - Sharing best practices
  - Learning from each other
  - Increased awareness of environment
- The Cyber Threat impacts us all!



OPERATION VULCAN LOGIC (OVL)
ONBOARDING TRAINING REGISTRATION

OVL is a mature, proven, agile Ecosystem that achieves the intent of the RMF.

What is Operation Vulcan Logic?

- The ATO execution process in general, to date, has been very resource and time intensive. While the ATO approval process is an important contributor to implementing cybersecurity and managing risk, delays in fielding new systems and capabilities can bring their own risks by extending the use of legacy (often less secure) capabilities.
- DODs RMF implementation intent is to deliver secure, resilient, and survivable mission functionality, where the system design achieves the right balance between mission and cyber functionality such that the system can perform all necessary mission functions, in a cyber-contested environment, with an appropriate level of risk.
- Operation Vulcan Logic (OVL) is a risk centric, agile, authorization Ecosystem where the Authorizing Official (AO), the programs, and the systems/capabilities seeking authorization have clear outlined Criteria, Observables, and Behavior (COB) expectations and templates to leverage, based on over 2,000 successful implementations.
- OVL is rooted in the tenants outlined in NIST SP 800-160 and the innate responsibility of practicing Systems/Systems Security Engineering – which are Cyber Security and Resiliency Enablers, throughout the system development lifecycle (SDLC). It is this same Systems/Systems Security Engineering that will be relied upon to produce the evidentiary data, and analysis.
- OVL is rooted in the tenants outlined in NIST SP 800-160 and the innate responsibility of practicing Systems/Systems Security Engineering – which are Cyber Security and Resiliency Enablers, throughout the system development lifecycle (SDLC). It is this same Systems/Systems Security Engineering that will be relied upon to produce the evidentiary data, and analysis.
- For the AO to assess, determine, and articulate the risk of use for systems/capabilities withing their boundary, a flexible process flow has been outlined to assist the programs and CRAs (Cyber Risk Assessor play a similar role as Security Control Assessor (SCA) in communicating with a common frame of reference.

An Authorizing Official's Perspective on Agile Authoriation

Purpose of Training

- The Cyber Risk Assessor (CRA) is responsible for providing the Authorizing Official (AO) with an independent "Cyber Risk Analysis" and acceptable "Risk of Use" for the system or capability throughout the entire Operation Vulcan Logic (OVL) Ecosystem Agile Authorization process while focusing on criteria, observables, and overall behaviors. This training provisions the CRA with the knowledge, skill and ability to perform security assessments utilizing the Operation Vulcan

https://arlo-solutions.com/ovl

CDAO

Agenda

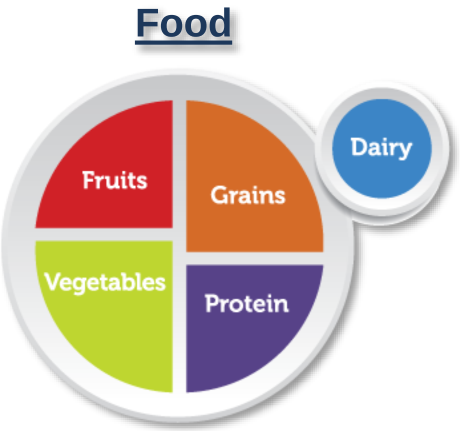
- **Chief Digital & Artificial Intelligence Office (CDAO)**
- **Operation Vulcan Logic – Agile Risk Management**
- **Deep Thoughts**
- **Back-up info on Operation Vulcan Logic**

> *Artificial intelligence is a tool, not a threat*
>
> — Rodney Brooks

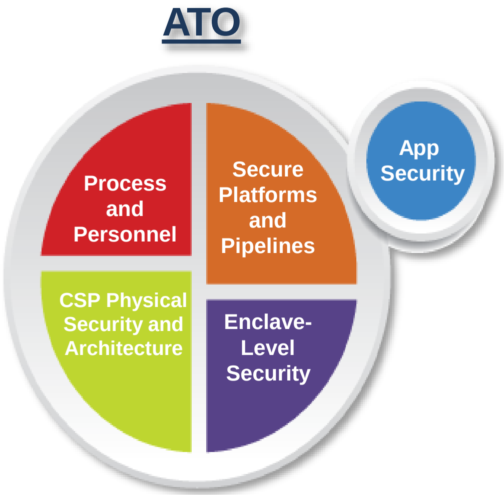
Cyber Risks Facts Label
What if we could?

- **Application Security is NOT just about the security of the application itself:**
  - It is a layered perspective (hosted environment, TTPs, etc.).
  - As one goes lower in an application architecture, the potential for harm increases.

- **An Authority to Operate (ATO) is a risk-based determination and includes many factors:**
  - The technology employed, the execution processes, the hosting environment, the risk tolerance, etc.
  - The ATO is a statement of the “Risk of Use,” informing the consumer.



Just like a well-balanced meal, risk is made up of several ingredients

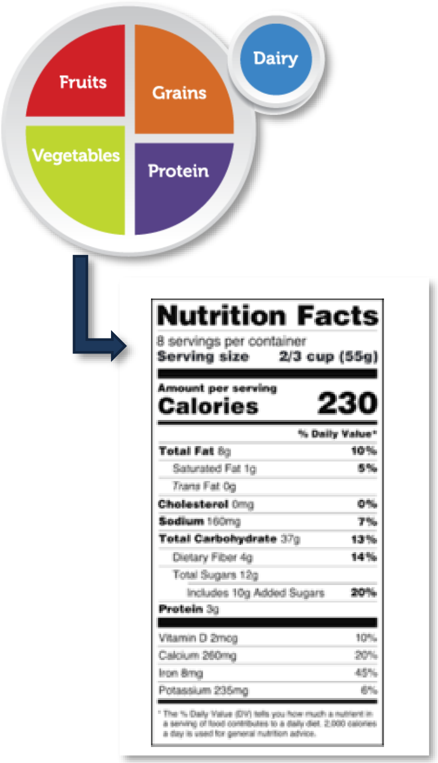


ATO
Process and Personnel
Secure Platforms and Pipelines
App Security
CSP Physical Security and Architecture
Enclave-Level Security

Cyber risk is made up of several ingredients.

DISTRIBUTION A. Approved for public release: Distribution unlimited.

Cyber Risks Facts Label: Allowing for an Informed Consumer



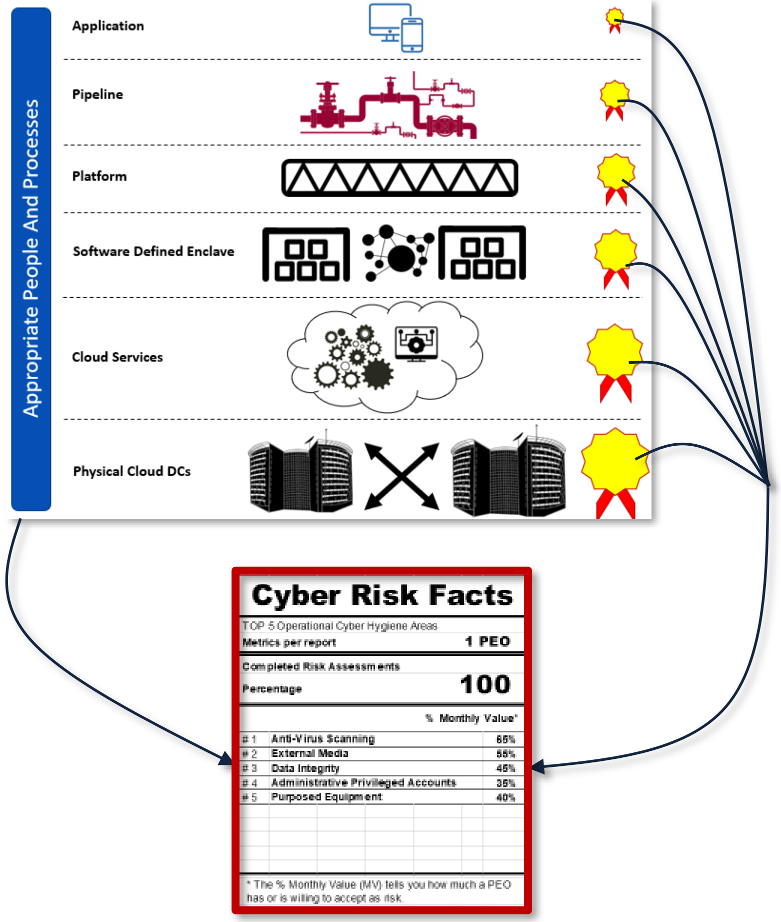
Nutrition Facts

8 servings per container

Serving size	**2/3 cup (55g)**
Amount per serving	
Calories	**230**
	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 1g	**5%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 160mg	**7%**
Total Carbohydrate 37g	**13%**
Dietary Fiber 4g	**14%**
Total Sugars 12g	
Includes 10g Added Sugars	**20%**
Protein 3g	
Vitamin D 2mcg	10%
Calcium 260mg	20%
Iron 8mg	45%
Potassium 235mg	6%

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

- **A Nutrition Facts label shows the consumer WHAT nutrients are in the food based on FDA guidelines.**
- **A Cyber Risk label shows the consumer what the RISK OF USE is for an application based on ATO Guidelines.**



Cyber Risk Facts

TOP 5 Operational Cyber Hygiene Areas

Metrics per report		**1 PEO**
Completed Risk Assessments		
Percentage		**100**
		% Monthly Value*
# 1	**Anti-Virus Scanning**	**65%**
# 2	**External Media**	**55%**
# 3	**Data Integrity**	**45%**
# 4	**Administrative Privileged Accounts**	**35%**
# 5	**Purposed Equipment**	**40%**

* The % Monthly Value (MV) tells you how much a PEO has or is willing to accept as risk.

Cyber Risk label is the foundation to an informed consumer and enables true reciprocity.

CDAO

DISTRIBUTION A. Approved for public release: Distribution unlimited.

Questions / Discussions

This is a work in progress. Need to continue to collaborate.

CDAO

OPERATION VULCAN LOGIC

Operation Vulcan Logic (OVL) is a mature, proven, agile Ecosystem that achieves the intent of the RMF.

BACKGROUND:

- The ATO execution process in general, to date, has been very resource and time intensive. While the ATO approval process is an important contributor to implementing cybersecurity and managing risk, delays in fielding new systems and capabilities can bring their own risks by extending the use of legacy (often less secure) capabilities.

- DODs RMF implementation intent is to deliver secure, resilient, and survivable mission functionality, where the system design achieves the right balance between mission and cyber functionality such that the system can perform all necessary mission functions, in a cyber-contested environment, with an appropriate level of risk.

- Operation Vulcan Logic (OVL) is a risk centric, agile, authorization Ecosystem where the Authorizing Official (AO), the programs, and the systems/capabilities seeking authorization have clear outlined Criteria, Observables, and Behavior (COB) expectations and templates to leverage, based on over 2,000 successful implementations.

- OVL is rooted in the tenants outlined in NIST SP 800-160 and the innate responsibility of practicing Systems/Systems Security Engineering – which are Cyber Security and Resiliency Enablers, throughout the system development lifecycle (SDLC). It is this same Systems/Systems Security Engineering that will be relied upon to produce the evidentiary data, and analysis.

- For the AO to assess, determine, and articulate the risk of use for systems/capabilities withing their boundary, a flexible process flow has been outlined to assist the programs and CRAs (Cyber Risk Assessor play a similar role as Security Control Assessor (SCA) in communicating with a common frame of reference.

1 PHASE 1

Systems/Systems Security Engineering Evidentiary Data & Analysis

- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)

Standard Acquisition Systems Engineering Data

Grow it in

PROGRAM MANAGEMENT

- Facilitate Risk management across all stakeholders in an integrated, holistic manner

2 PHASE 2

Collaboration with AO/CRA

- Discuss risk assessment and way ahead
- Mapping of Authorization Strategy to meet Acquisition/Execution Strategy/Need
- Maximize re-use of previous assessments analysis results
- Operational Use Perspective

COLLABORATIVE EXECUTION

- Partnerships with all stakeholders enables a holistic view and enables reciprocity

3 PHASE 3

Continually Execute Risk Assessment

- Tool Agnostic - Focus on Evidentiary Data and Analysis
- Clinically define Risk of Use Posture
- Outline Mitigations for Risks
- Persistent Penetration testing and CONMON

Starts never ending journey of continuous assessment & monitoring

ENABLERS

- Single, Lead AO for each system/capability
- Stakeholder collaboration via "AO Committee"
- Streamline expectations and increase Agility

DISTRIBUTION A. Approved for public release,
16 Jun 2023: Distribution unlimited.

arlo-solutions.com/ovl/ovl-downloads/ arlo-solutions.com/ovl/contact-us/

CDAO

OPERATION VULCAN LOGIC

COMMUNITY FEEDBACK

CRA Training - "This training was very well put together – The only suggestion I have is to get this training out as soon as a CRA/SCAR is on boarded. I am also implementing this training for all my SCARs as I need them to know what I know. I hate to say to make this training Mandatory, but in this case, I think it should be for all SCAs and SCARs." Gary "Scott" Ennis, AFNW-C/NXZT Security Control Assessor, Assessments Branch, Ground Based Strategic Deterrent (GBSD)

CRA Training - "This training needs to be provided to the Program also. The flow diagram needs to be stressed. The responsibility to provide all the necessary documentation to the CRA and the independent role of the CRA needs to be emphasized to the Program." Denise Madison, Enterprise Information Systems Security Manager (ISSM), Cybersecurity, F-35 Lightning II Joint Program Office

CRA Training - "My only suggestion would be for the example documentation to be available to non-CaC holders." Aaron Owens, Director of Security (DoS), Second Front Systems

DSOP - "They're very detailed, and I think they cover quite a bit to help organizations adopt DevSecOps. I especially love the call to action(s) in the documents, the need for change to actually implement innovation." Brian Fox - Director of the National Security and Intelligence Portfolio, 18F

DSOP - "Thank you for the opportunity to review the DSOP CONOPS. My overall thoughts on the document are that it is very user friendly, especially with the "Tips to Success". From my perspective with an AO providing that information, it shows the project that you are wanting the project to be successful and giving them what you are looking for up front so that the project would be able to answer the majority of the questions you would have." Steven Pruskowski – cisa.dhs.gov

OVL implementation of the DAF Fast track - "What 'Fast Track' really provides is agility. It means we're not stuck once we go down a road and find out six months later that there's a better path. It allows us to experiment boldly and remove items that aren't adding the value we initially thought they would. It empowers you with freedom, then demands you to exercise it judiciously." Brandon Johns, NH-04/GS-15, Chief Security Officer, AFLCMC Det 12, Kessel Run

SAMPLE ONBOARDING MODULES

Module 0: AO's Perspective
- Mr. Holtzman

Module 1: OVL
- What Is It?
- Background
- Elements
- Fast Track and RMF

Module 2: AO
- Introduction
- Roles and Responsibilities
- AODRs
- AO Objectives, Enablers, and Collaborations
- AO Playbook v1.0

Module 3: Cyber Risk Assessor (CRA)
- Introduction
- CRA Responsibilities
- CRA Objectives v1.0
- CRA Onboarding v1.0
- CRA Playbook v1.0

Module 4: Body of Evidence, Artifacts, Information Tools
- AO Determination Brief
- AO Determination Brief Guide
- CRA Recommendation Letter
- DSOP CONOPS if applicable
- Draft AO Authorization Letter
- ITCSC

Module 5: CRA Assessments
- In/Out Briefing
- Assess-Only Process
- Security Assessment Plan (SAP)
- Risk Assessment Report (RAR)
- Security Assessment Report (SAR)
- Plan of Action and Milestone (POA&M)
- Authorization Determination Package (Minimal Requirements)

Module 6: Continuous Execution
- Continuous Monitoring Plan (ConMon)
- Conditions/Residual Risks
- Sustainment and Maintenance
- No Security Impact (NSI)
- STIGs and Scans
- Risk Assessment Report
- Reciprocity
- Repository (eMASS/Xacta, etc.)

Module 7: Agile Authorization Ecosystem
- Putting All of This Together
- Phased Approach
- Summary

"Absolutely executable for Special Access Programs (SAP)... proven to be able to do so. Development of a system will not be constrained by executing this logic... if you do this well, a program will identify MORE during stages in which changes/mitigations can be made earlier on... and it will prove fruitful later – as a more secure system... or maybe even discovering that you didn't get what you asked for."

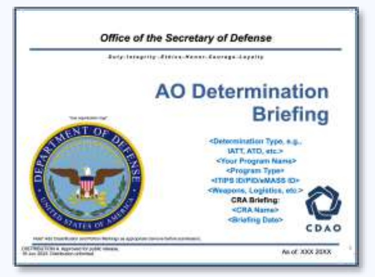
-JACK W. RHODES III, Lt Col, USAF, Program Manager, DAF SAP Enterprise Information Technology Program Management Office"

DISTRIBUTION A. Approved for public release, 16 Jun 2023: Distribution unlimited.

Operation Vulcan Logic

Agile Authorizations: Templates and Guides

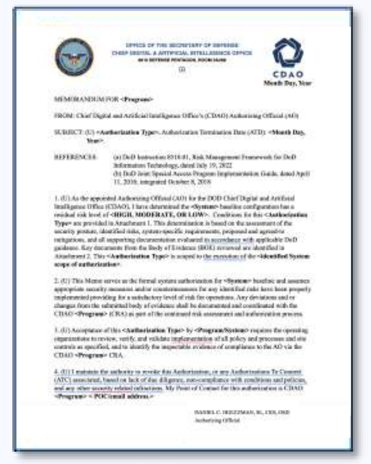
Determination Brief



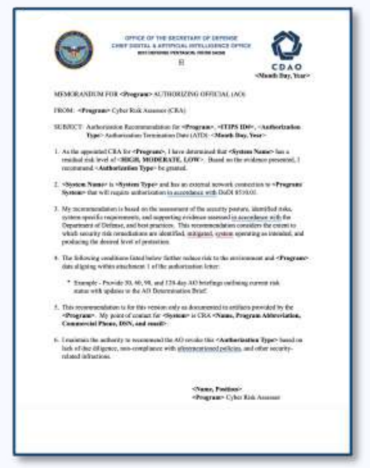
Office of the Secretary of Defense

AO Determination Briefing

Authorization Memo

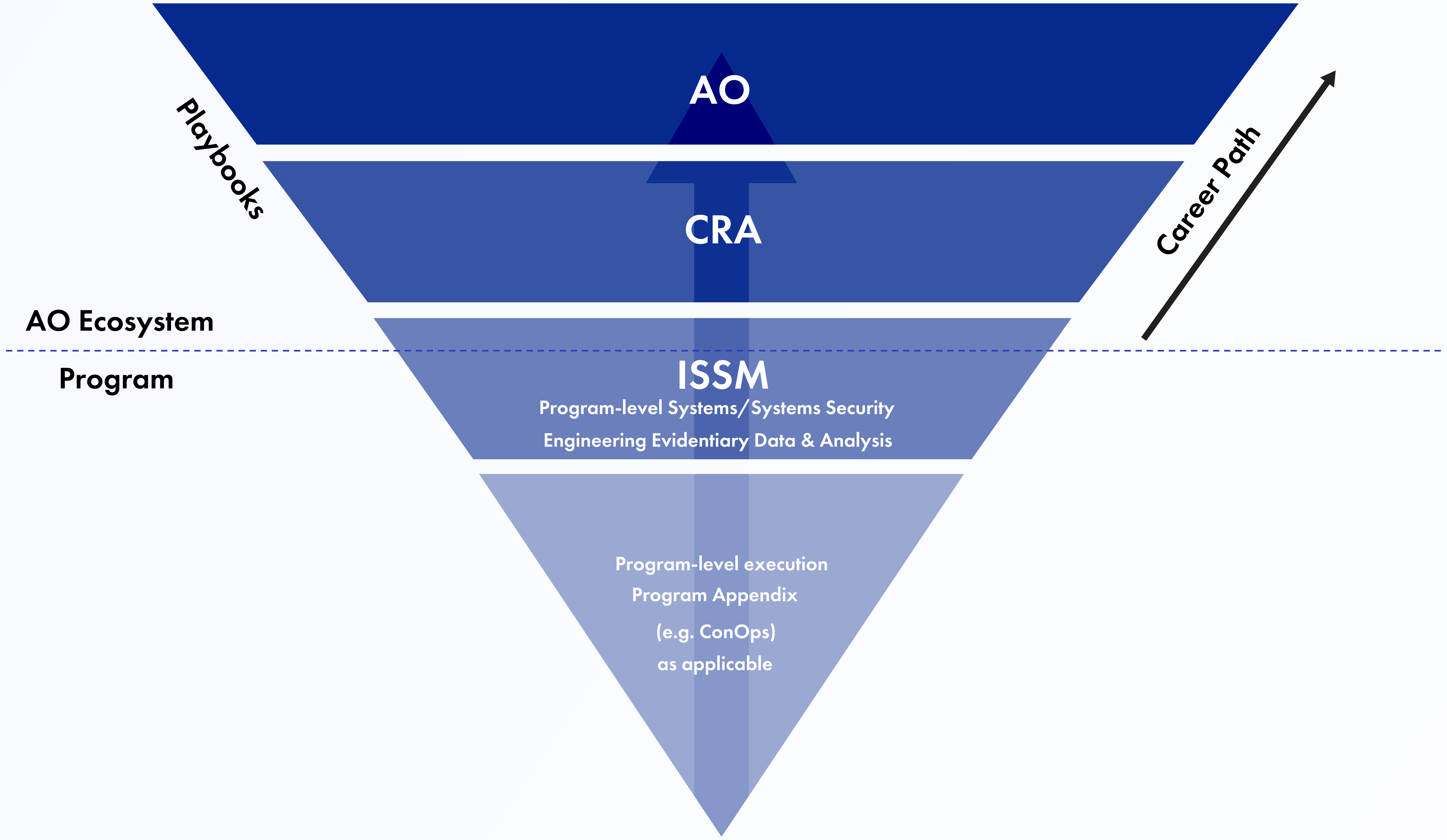


CRA Risk Recommendation



DevSecOps Conops (as applicable)

OVL Ecosystem / Strategy



Playbooks

AO

CRA

Career Path

AO Ecosystem

Program

ISSM

Program-level Systems/Systems Security Engineering Evidentiary Data & Analysis

Program-level execution

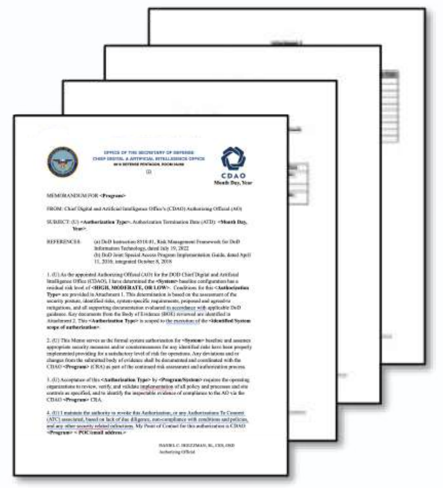
Program Appendix

(e.g. ConOps)

as applicable

ATO Package of the Future

- Will document the key items needed for reciprocity:
  - Authorization Memo.
  - Attachment 1: Conditions.
  - Attachment 2: Body of Evidence.
  - Attachment 3: Plan of Action and Milestones.



- Attachment 1: Conditions
  - Documents any conditions on the ATO.
  - Security is a journey, never a destination.
  - Identifies the Risk of Use to inform the Consumer.

- Attachment 2: Body of Evidence
  - Key artifacts that supported the authorization.
  - Informs other AOs and consumers to increase reciprocity.
  - Available by request.

- Attachment 3: Plan of Action and Milestones.
  - Appendix classified as appropriate per the governing classification guide.

New - Initiation (concept/requirements definition).
Existing- Operations / Maintenance

1 PHASE 1

Phase 1 Inputs

Systems/ Systems Security Engineering, Evidentiary Data & Analysis

Phase Roles
PM
ISSM

Standard Acquisition Systems Engineering Data

Phase 1 Outputs

- Architectures
- System Boundries
- Functional Requirements
- Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)
- Etc.

2 PHASE 2

- AO Determination Brief
- AO Boundary
- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous assessments
- Test Results (Red/Blue/Etc.)
- Etc.

Phase 2 Inputs

Collaboration with AO/CRA

Phase Roles
- AO
- AODR
- CRA
- PM
- ISSM

Scope the assessment criteria and outcomes

Phase 2 Outputs

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

3 PHASE 3

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

Phase 3 Inputs

Continually Execute Risk Assessment

Phase Roles
- AO
- AODR
- CRA
- ISSM

Starts never ending journey of continuous assessment & monitoring

Provide determination briefing to AO

Phase 3 Outputs

- CRA Risk Recommendation Letter*
- AO Authorization Memo*
- AO Tag-up Brief(s)*

DISTRIBUTION A. Approved for public release,
16 Jun 2023: Distribution unlimited.

arlo-solutions.com/ovl/ovl-downloads/

arlo-solutions.com/ovl/contact-us/