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 on 09 May 2025:
Distribution unlimited. Case Number: 25-T-2015

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"