OPERATION VULCAN LOGIC (OVL)

AO Level 1 Playbook

V1.0

June 2023

DISTRIBUTION STATEMENT:

VERSION HISTORY

REVISION AND HISTORY PAGE: Revisions and version changes to this document are recorded within the following table. New versions are published when changes to the document equate to 10 percent or greater of the document's content or if a change requires immediate implementation. This record is maintained throughout the life of the document.

This document will be reviewed at a minimum of annually.

Date	Version	Change Type	Modified By
23 May 2023	V0.1	Initial Version	ARLO-Solutions

TABLE OF CONTENTS

1. Introduction

Operation Vulcan Logic (OVL), AO Playbook Level I, is a high-level guide on the Criteria, Observables, and Behavior (COB) expectations and templates used when interacting with the Authorizing Official for authorization determinations. A more in-depth "implementation" of this process flow will be highlighted in the Operation Vulcan Logic (OVL), AO Playbook Level II.

2. AO Objectives

The AO's objective is to address, assess, and determine risk of a system. In doing so, a risk determination will be made based on the risk assessments conducted by the CRA and the CRA's risk recommendations to the AO. The AO has specific criteria and objectives for his team to aid in reaching a risk determination. Below are key tenets for the AO, AO team, and system owners' success:

Objectives:

- Make Determinations Faster: Transparent, foster reciprocity.
- Facilitate Risk Management: Acquisition, operations, and sustainment.
- Enable Program Managers: Advance cybersecurity and cyber resiliency.

Enablers:

- Set Clear Requirements: Sample determination briefing (template not compliance).
- Standard System Engineering: Evidentiary analysis and data based.
- Focus on Risks That Matter: Operationally focused with enterprise view.

Collaborative Execution:

- Cyber Risk Assessors (CRA, formerly SCA): Focused on assessing risks.
- Authorizing Official: Informs enterprise determination makers on Cyber Risks.
- Partnerships PEO's, DOEs, PMs, Users, Sustainers: Enable holistic view.

3. Operation Vulcan Logic (OVL) Agile Authorization Process

For the AO to assess, determine, and articulate the risk of use for systems/capabilities within his or her boundary, a standard process flow has been outlined to assist the programs and CRAs in communicating with a common frame of reference.

The Authorizing Official defined a standard set of information needed to inform a holistic risk assessment and determination. This information is already part of the standard acquisition systems engineering and systems security engineering (SSE) evidentiary analysis and data.

The process needed to collect, analyze, and provide a risk-based recommendation for the AO to consider, and ultimately issue an authorizing determination, is accomplished through the 3-Phase Agile Authorization Process Flow shown in Figure 1.

The following sections outline the OVL process flow areas and provide insight into the inputs and outputs for each phase. Reference or template elements have been identified with an asterisk. Their definition can be found in the "Quick Guide" section of this guide.

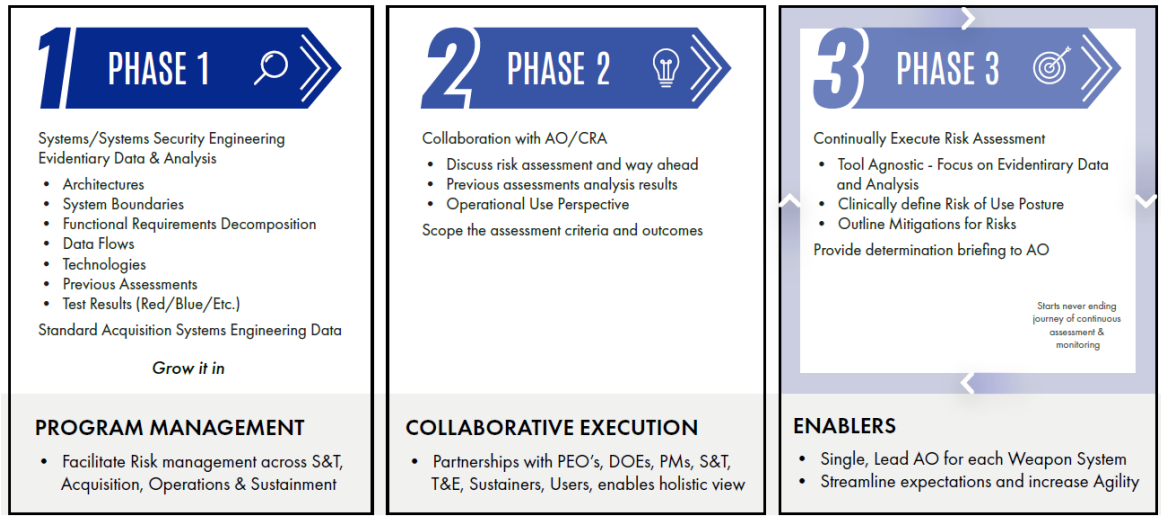
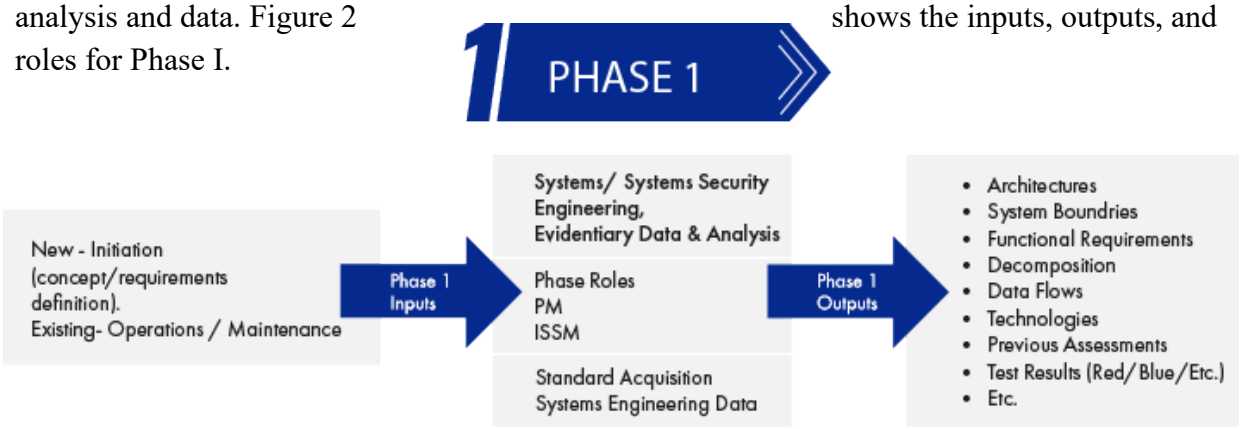


Figure 1: OVL 3-Phase Agile Authorization Process

3.1 Phase I: Systems/Systems Security Engineering, Evidentiary Data, and Analysis

Phase I is focused on collecting the Systems/Systems Security Engineering, Evidentiary Data, and Analysis. This is accomplished by leveraging standard acquisition systems engineering analysis and data. Figure 2 shows the inputs, outputs, and roles for Phase I.



The objective of Phase I is to clearly outline the System/Capability being assessed via standard acquisition systems engineering/systems security engineering-produced information. Examples include but are not limited to:

Figure 2: OVL Phase 1 Input/Output Elements

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

1.1. 3.2 Phase II: Collaboration with AO/CRA

Phase II is focused on the AO and CRA's collaborating with the system stakeholders to develop the scope of the assessment's COB. This is in preparation for conducting the risk assessment in Phase III. Figure 3 shows the inputs, outputs, and roles for Phase II to be effective.

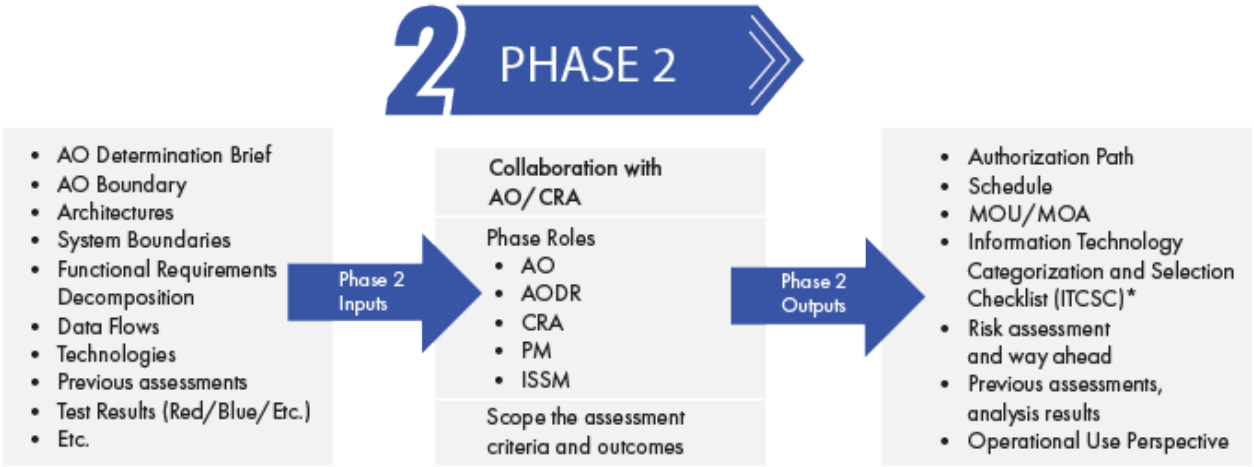


Figure 3: OVL Phase 2 Input/Output Elements

The objective of Phase II is to clearly identify the type of authorization being requested based on system maturity and to schedule an outline of the System/Capability being assessed via standard acquisition systems engineering/systems security engineering-produced information. A key input for Phase II is:

- AO Determination Brief.

During the scoping of the assessment criteria and outcome, outputs for Phase II include but are not limited to:

- Authorization Path.
- Schedule.
- MOU/MOA.
- Information Technology Categorization and Selection Checklist (ITCSC)*.
- Discuss Risk Assessment and Way Ahead.
- Previous Assessments, Analysis Results.
- Operational Use Perspective.

1.2. 3.3 Phase III: Continually Execute Risk Assessment

Phase III is focused on the CRA's conducting a comprehensive assessment of the systems/systems security engineering, evidentiary data, and analysis information as an output from Phase I. The CRA provides the determination briefing to the AO based on the authorization path requested, using the CRA Risk recommendation template. Figure 4 shows the inputs, outputs, and roles required for Phase III to be effective.

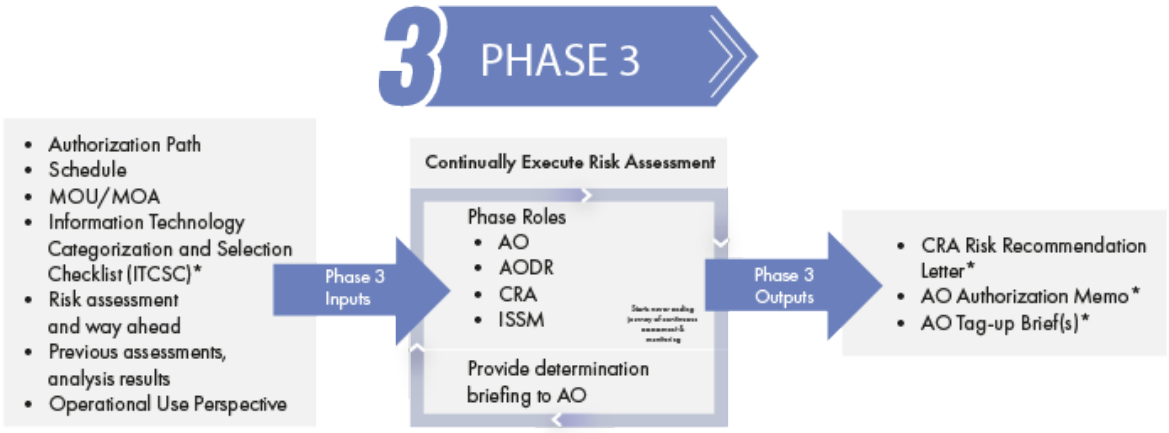


Figure 4: OVL Phase 3 Input/Output Elements

4. AO Playbook Level 1 Quick Guide

These are tools and templates needed to prepare and execute the agile authorization process.

AO Determination Brief Template:

- Brief to assist program personnel in understanding what the Authorizing Official is expecting to see to make an informed risk determination.

AO Determination Brief Guide:

- An AO determination brief guide has also been created to provide guidance on the completion of the above AO determination brief.

Information Technology Categorization and Selection Checklist (ITCSC):

- Form to document the security categorization of the system, including the information processed by the system and represented by the identified information types.

CRA Risk Recommendation Template:

- The document the CRA uses to articulate the risk recommendation once the risk assessment is complete.

AO Authorization Memo Template:

- Leveraged to articulate the authorization determination to stakeholders. After the determination of risk from the operation or use of the information system has been made, this letter is used to inform the System Owner and other stakeholders of the authorization determination along with terms and conditions for the authorization.

AO Tag-up Brief Template:

- Used to provide regular updates on system status to allow the Authorizing Official or Designated Representative to make continuous and on-going, risk-based determinations based on guidance from the Authorizing Official.