Operation Vulcan Logic (OVL)

CRA Onboarding Process

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
15 June 2023	V1.0	Initial Version	ARLO-Solutions

TABLE OF CONTENTS

1.0 INTRODUCTION

As part of the onboarding process, we have annotated the key areas that will assist you in moving through the Operation Vulcan Logic (OVL) Fast-Track Agile Authorization process. The tools and guidance referenced in this document will support you in not just having a restored appreciation for the overall workflow but provide a perceptive transformed approach in meeting the same goals and outcomes as the Risk Management Framework (RMF) intent, but from a different perspective.

2.0 CYBER RISK ASSESSOR

The Cyber Risk Assessor (CRA) is an AO appointed role, responsible for providing an independent "*Cyber Risk Analysis*" and acceptable "*Risk of Use*" recommendation for the systems or capabilities throughout the entire Agile Authorization process. The CRA is not much unlike that of a Security Control Assessor (SCA), the one variance is that the CRA focuses on overall risk verse a controls checklist of compliance.

3.0 AUTHORIZING OFFICIAL

The AO is responsible for determining the overall risk of use for an Information System (IS) or capability and informing the IS/capability stakeholders while focusing on criteria, observables, and overall behaviors. Provides authorization determinations with specific conditions, guardrails, assumptions, constraints, and an acceptable risk tolerance level. Relies on the CRA's to fully understand an IS/capability along with providing their written recommendation.

4.0 APPOINTMENT

DODI 8500.01 directs the appointment of an AO and Security Control Assessor (SCA) for DOD information systems (ISs) and platform information technology (PIT) systems to ensure all DOD IS and PIT systems under their purview are analyzed and authorized in accordance with DODI 8510.01. If selected as an Authorizing Official Designated Representative (AODR) or CRA under the OVL Ecosystem, an appointment letter will be provided by the AO.

5.0 CYBER ROLES AND RESPONSIBILITIES

FUNCTION	TITLE	ROLE	RESPONSIBILITIES (AO DEFINED)
System Owners	Program Executive Officer (PEO)	Senior Acquisition Official	Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system/capability.
	Information System Owner (ISO)	System Operational Owner	Responsible for system requirements definition, funding advocacy, system acceptance, system employment & operations.
Assess & Authorize	Authorizing Official (AO)	Authorizing Official	Responsible for assessing and determining the Risk of Use for the system or capability and informing the system/Capability stakeholders. Provides Authorizations to Operate with specific guardrails, assumptions, constraints, and acceptable risk tolerance.
	Authorizing Official Designated Representative (AODR)	AO Designated Representative	Represents the AO in all matters as outlined by the AO.
	Cyber Risk Assessors (CRA)	Independent Risk Assessor	Responsible for providing the AO with an independent Cyber Risk Analysis and acceptable Risk of Use for the System or Capability.
Acquisition Program	Information System Security Manager (ISSM)	Program/Capability Cyber Lead	Responsible for integration of cybersecurity into, and throughout the lifecycle of the system or capability as the cybersecurity technical advisor to the PM and or the ISO.
	Program Manager (PM)	Program/Capability Manager	Responsible for the system/capability development and delivery. Responsible for registering system/capability in the ITIPS, eMASS, or similar authorization tracker and for obtaining an Authorization to Operate from an AO.
System Responsibilities	DevSecOps Pipeline Engineers	Developer	Responsible the design and development of the Continuous Integration/Continuous Development (CI/CD) pipeline to meet AF/DoD standards.
	Software Developers	Developer	Responsible for engineering and developing secure and resilient code that will be utilized within the environment, while meeting DoD standards.
	System Operators	End User	Authorized individuals that operate and/or consume information from the system/capability to access information.

6.0 KEY WEBSITE AND ARTIFACTS

- Operation Vulcan Logic

  - **Security Authorization Package**

1. AF Authorizing Official (AO) Determination Brief + Risk Analysis Report (RAR)
2. AF Authorization Memo Template
3. AF CRA Risk Recommendation Letter
4. Information technology Categorization and Selection Checklist (ITCSC)

  - **Supporting Evidence** (not limited to)

1. System Security Plan (SSP)
2. Concept Of Operations (CONOPs)
3. Plan of Action and Milestones (POA&M)
4. Security Controls Traceability Matrix (SCTM)
5. STIG's/ACAS Scans
6. Security Assessment Plan (SAP) and Security Assessment Report (SAR)
7. ConMon Plan, Incident Response Plan, Contingency Plan etc.,

7.0 SUPPORTING PROGRAMS

- The CRA acts as the main point of contact (POC) between the program and the AO/AODR for the completion of the following documents and activities:
  - IT Categorization and Selection Checklist(s)
  - Assessment activities (In-brief, Out-brief, SAP, schedule, coordinate resources)
  - Assessment Reports (RAR, SAR)
  - CRA Recommendation Letter
  - AO Authorization Letter
  - Continuous Monitoring Plan (i.e., POA&M, Conditions),
  - Coordinate with the ISSM and PM on all CM Changes – verify a repeatable review process and ensure changes are vetted through the organizations Change Control Board (CCB)).
  - AO Briefings (Weekly, monthly, quarterly)

- Obtain contact Information – POCs (PM, CRA, ISSM, staff/stakeholders that will communicate with the AO), phone numbers, email, program website links, site location or physical address.
- Validate current or establish new meetings (DoD Microsoft Team Meetings, Google Meet, WebEx).
- AO Tag-Up Brief (Quarterly, monthly, weekly – program-defined).

8.0 SIMPLIFIED AUTHORIZATIONS

- 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.)
    - **Output - Standard Acquisition Systems Engineering Data**

- Phase 2: Collaboration with AO/CRA
    - Discuss risk assessment and way ahead
    - Previous assessments, analysis results
    - Operational Use
    - Perspective
    - **Output - Scope the assessment criteria and outcomes**

- Phase 3: Execute Risk Assessment
    - Tool Agnostic – Focus on Evidentiary Data and Analysis
    - Clinically define Risk of Use Posture
    - Outline Mitigations for Risks
    - **Output: AO Determination Brief**

9.0 DOCUMENTATION ASSESSMENT AND AUTHORIZATION PROCESS (A&A) LIFECYCLE

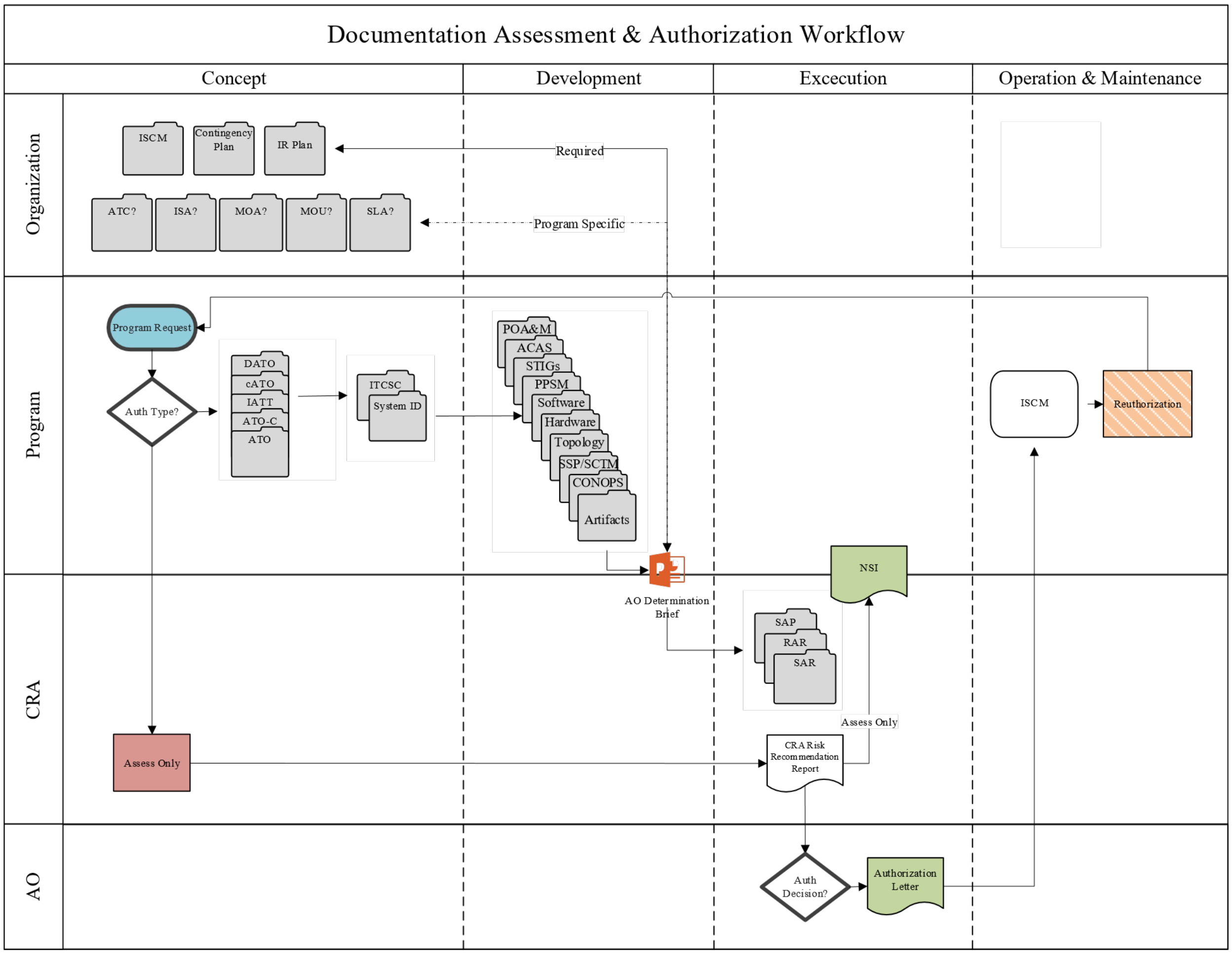

Figure 1. Document Assessment & Authorization Lifecycle

10.0 CRA TOOLS AND DESCRIPTIONS

10.1 IT Categorization and Selection Checklist

ITCSC is the process of determining the security category for information or an information system. This checklist helps in determining impact values: (i) for the information type(s) processed, stored, transmitted, or protected by the information system; and (ii) for the information system and identify overlays that apply to the information system and its operating environment to account for additional factors (beyond impact) that influence the selection of security requirements.

10.2 AO Determination Briefing

- Provides a concept of operations (CONOPS), defines the overall environment, implemented requirements and a path to considering the intent and type of authorization determination (i.e., IATT, ATO w/Conditions, etc.).
- To be completed for every environment and supporting authorization/re-authorization determination.
- CRA is charged with briefing the contents to the AO/AODR.

10.3 Security Assessment Plan (SAP)

The CRA develops the security assessment plan, and the AO or AODR reviews and approves the plan. The purpose of the security assessment plan approval is to establish the appropriate expectations for the security assessment; and to bound the level of effort. An approved security assessment plan helps to ensure that an appropriate level of resources is applied toward determining overall effectiveness. When security requirements are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization obtains a security assessment plan from the provider.

- The security assessment plan identifies objectives for the security assessment, a roadmap describing how to conduct the assessment, and points to the detailed assessment procedures on the RMF KS. The roadmap describing how to conduct the assessment is simply a high-level plan for completing the task of assessing the requirements for the specific system.
    - Consideration should be given to starting assessments early before development and integration of all components is completed; and to leverage the results of testing done by developers and integrators. This allows for early identification and correction of deficiencies and completion of assessments in a timely manner.
- The CRA ensures the plan is consistent with the security objectives of the organization; employs state-of-the-practice tools, techniques, procedures, and automation to support the concept of information security monitoring and near real-time risk management; and is cost-effective about the resources allocated for the assessment.

- The AO or AODR approves the security assessment plan, establishes appropriate expectations for the security assessment, defines the level of effort for the assessment and ensures the appropriate level of resources are applied in determining the effectiveness.

- From the organizational perspective, preparing for a security assessment includes the following key activities:

1. Ensuring that appropriate policies covering security assessments are in place and understood by all affected elements.
2. Ensuring that all steps in the RMF prior to the security assessment step, have been successfully completed and received appropriate management oversight.
3. Ensuring that security requirements identified as common (and the common portion of hybrid requirements) have been assigned to appropriate entities (i.e., common providers) for development and implementation.
4. Establishing the objective and scope of the security assessment (i.e., the purpose of the assessment and what is being assessed).

- The following steps are considered by assessors in developing plans to assess the security requirements in organizational information systems or inherited by those systems:

1. Determine which security enhancements are to be included in the assessment based upon the contents of the security plan and the purpose/scope of the assessment.
2. Select the appropriate assessment procedures to be used during the assessment based on the security requirements that are to be included in the assessment.
3. If required, tailor the selected assessment procedures (e.g., select appropriate assessment methods and objects, assign depth and coverage attribute values);
4. Optimize the assessment procedures to reduce duplication of effort (e.g., sequencing, consolidating assessment procedures, and reuse of DT&E and OT&E test results) and provide cost-effective assessment solutions; and

- Finalize the assessment plan and obtain the necessary approvals to execute the plan.

- The security assessment plan is a key element throughout the process for IS and PIT systems of the Fast-Track Agile Authorization Process:

- **Assessing Security Requirements**

- The CRA will leverage the SAP to formulate the SAR (which includes documenting the issues, findings, and recommendations from the security assessment).
- Conduct initial remediation actions (based on the findings and recommendations of the SAR and reassess remediated security requirement(s), as appropriate).

- **Authorizing System/ Submitting Body of Evidence (BOE)**
  - Security Authorization Package (SAP) - AO Determination Brief, AO Authorization Letter, CRA Risk Recommendation, ITCSC and POA&M.
  - References – Supporting Evidence: SSP/CONOPs, HW/SW List, PPSM, SCTM, RAR, SAR etc., Note* Highlight classified references

- **Monitor Security Requirements**
  - Assess selected requirements annually (results of the annual assessment must be documented in an SAR).
  - Update the AO Determination Brief, RAR, SAR, CRA Risk Recommendation, and POA&M as applicable.

10.4 Security Assessment Report (SAR)

The results of the security assessment, including recommendations for correcting any vulnerabilities, weaknesses, or deficiencies in the requirements, are documented in the security assessment report (SAR). The SAR includes information from the assessor necessary to determine the effectiveness of the mitigations employed within or inherited by the information system based upon the assessor's findings. The SAR is the primary document used by an authorizing official to determine risk to operations and assets, individuals, other organizations, and the Nation. The SAR documents the CRA's findings with assigned requirements based on actual assessment results. It addresses findings in a non-mitigated status, including existing and planned mitigations. A SAR is always required before an authorization determination. If a compelling mission or business need requires the rapid introduction of a new IS or PIT system, assessment activity and a SAR are still required.

10.5 CRA Risk Recommendation

- Defines the results from the formal Security Assessment, outlining all vulnerability and weaknesses found and defining recommended conditions for the program to follow in correcting each found item.
- CRA to provide official recommendation for authorization determination with the AO. CRA must digitally sign document prior to sending to the AO.

10.6 Risk Analysis Report (RAR)

Risk reports contain valuable information used to communicate the results of the risk assessments. The Risk Analysis report offers decision makers a better understanding of the information security risk to operations, assets, individuals, other organizations, or the Nation that originate from the operations and use of organizational information systems and the environments in which those systems operate. The essential elements of information in a report can be described in three sections: (i) an executive summary; (ii) detailed risk assessment results; and (iii) supporting mitigations and or appendices. This report is focused on the evidence of non-mitigated risks and addresses vulnerabilities and weaknesses exhibited after the assessment has been completed. All non-mitigated risks must be subjected to a risk analysis that considers multiple factors in assigning a residual risk level to each non-mitigated requirement. The individual risk levels are then used to inform the CRA's written recommendation to the AO on acceptance of operating the system.

10.7 Plan of Action and Milestones (POA&M)

The purpose of a POA&M is to assist in identifying, assessing, prioritizing, and monitoring security deficiencies found in programs and systems, and to document progress in correcting those deficiencies. OMB requires agencies to prepare POA&Ms for all programs and systems where security deficiencies have been found. The POA&M is designed to be a management tool to assist in closing security performance gaps, assist inspectors general (IGs) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities. POA&Ms are permanent records. Once posted, entries are updated, but not removed even after correction or mitigation actions are completed. Inherited deficiencies are also reflected on the POA&Ms. DoD is responsible for maintaining the confidentiality of POA&Ms because they may contain pre-decisional budget or other sensitive information. After completing the assessment procedures, the CRA initiates a POA&M to document non-mitigated results, if necessary. If the CRA found no vulnerabilities after executing the assessment procedures, then the CRA records the requirements as mitigated in the POA&M. If the assessment finds vulnerabilities, the CRA records the requirements as non-mitigated in the POA&M, with sufficient explanation. The CRA will record requirements determined not technically or procedurally relevant to the system, as determined by the AO, as Not Applicable (N/A) in the POA&M with sufficient justification.

The CRA assigns vulnerability severity values to all non-mitigated requirements as part of the security analysis to indicate the severity associated with the identified vulnerability. CCI level assessments inform vulnerability severity values. If a requirement has a STIG or SRG associated through CCIs, the vulnerabilities identified by STIG or SRG assessments will be used to inform the overall vulnerability severity value. The CRA determines and documents in the SAR a level of risk for every NC security requirement in the system baseline. NC requirements are subjected to a risk assessment process that considers multiple factors in producing the risk level.

10.8   DevSecOps CONOPs

The DevSecOps CONOPs is meant to be used as a template only and can be modified at the program's discretion. It is not meant to be an all-inclusive or conclusive guide to how your DSOP environment should operate. The program is responsible for addressing the "How" details of the DSOP environment (i.e., system functionality, internal processes, procedures, and risk determinations). This CONOPS provides a foundation to address all areas within the DSOP program.

10.9   Authorization Determinations

- AO determination for each requested environment.
- IATT, ATO with Conditions, cATO, ATO, DATO.
- CRA to complete draft with the conditions that the AO agreed upon. To be signed by the AO.

11.0 ADDITIONAL TOOLS

11.1 Non-Security Impact (NSI)

- Joint effort by both the ISSM and CRA.

- CRA will review any and all supporting evidence and provide a certified endorsement based on that evidence to the ISSM.
- If no security impacts exist to the authorized environment, the AO has approved that a determination can be made at the ISSM level.

11.2 AO Tag-Up slides

- It is the responsibility of the program to determine the frequency of these meetings, however, the goal is to provide the AO with program updates on the environments currently authorized, existing, and new efforts.
- Generally initiated after the initial AO Determination Brief has been submitted.
- Provide a minimum of quarterly updates.
- Program and the CRA are responsible in briefing the contents to the AO.

11.3 Authorization to Connect (ATC)

The ATC is a step-by-step internal process that outlines procedures customers (programs) must follow to obtain and retain enclave connections within the AOs boundary. The process consolidates the connection processes for networks and services into one document, helps customers understand connection requirements and timelines, and provides contacts for assistance throughout the process. The ATC focus is on the Connection Approval Process (CAP) and where appropriate point customers to appropriate information services, websites, or offices wherever possible to help guide customers through other related processes.

11.4 Interconnection Security Agreement

Regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection.

11.5 Memorandum of Agreement

A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes specific terms that are agreed to, and a commitment by at least one party to engage in action. It "includes" either a commitment of resources or binds a party to a specific action.

11.6 Memorandum of Understanding

A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes only general understandings between the parties. It "neither includes" a commitment of resources nor binds a party to a specific action.

11.7 Penetration Test Plan

A document that outlines the specific steps that will be performed for a particular test, including the required logistical items, and expected outcome or response for each step.

12.0 SUMMARY

Although the PM/ISO are accountable for all aspects of the information system, from concept to disposal, the ISSM/ISSO, is responsible for the day-to-day security posture and continuous monitoring of the system, addressing and reporting any issues/concerns to the PM/ISO and the AO if applicable. The CRA is appointed by the AO to assess the system and assist addressing issues with the ISSM/ISSO that arise between assessments. The CRA's responsibility is to the AO/AODR, but the CRA (or AO/AODR) will keep apprised the PM/ISO of whether an assessment is satisfactory or not and whether the system is being maintained and sustained at an acceptable level. This provides the PM/ISO with independent views of the system and a reasonable assurance they are on target.