DOD/CDAO

Operation Vulcan Logic (OVL)

Cyber Risk Assessor (CRA) Objectives

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 June 2023	V1.0	Initial Version	ARLO-Solutions

TABLE OF CONTENTS

1. INTRODUCTION

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.

A "Risk of Use" is the probability of exposure or loss resulting from a cyber-attack or data breach of an organization, system, or capabilities. In other words, it is the potential loss or harm related to the technical infrastructure, use of technology, or reputation of an organization due to exposure.

To further outline, the CRA is the individual appointed (or representative) in writing by the AO to act on his or her behalf to conduct an "independent" security analysis of the information system, hardware and or software application. The CRA is responsible for conducting a comprehensive analysis of the management, operational, and technical security requirements employed within or inherited by an IS to determine the overall effectiveness (i.e., the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or the environment). CRAs provide a risk analysis of the severity of vulnerabilities, weaknesses, or deficiencies discovered in the IS and its environment of operation as well as recommend corrective actions to address identified vulnerabilities. The CRA's accountability is to the AO, but the CRA or Authorizing Official Designated Representative (AODR), on behalf of the AO will inform the Information System Owner (ISO) whether an outcome is satisfactory and whether the system is being maintained at an acceptable level of risk. This coordination provides the ISO and the Information System Security Manager (ISSM) with "periodic" views of the system as well as provides assurance to the CRA that safeguards are implemented appropriately, and the system is being maintained. Throughout the entire OVL Ecosystem Agile Authorization process, the evidence from the analysis documents the results of the security analysis and provides the AO with the essential information anticipated to make a risk-based determination on whether to authorize the operation of an IS or a determined set of common controls. Unless specifically determined otherwise by the AO, the ISO or common control provider is responsible for the assembly, compilation, and submission of the evidence. The ISO or common control provider obtains input from the CRA, AODR and the AO.

The security documentation and supporting evidence is to be sustained and maintained throughout a system's lifecycle and is further introduced in the CRA Onboarding Process. The Security Authorization Package (SAP) consists of the AO Determination Brief, AO Authorization Memo, CRA Risk Recommendation Letter, IT Categorization Security Checklist (ITCSC), Plan of Action and Milestones (POA&M) and the DevSecOps CONOPs (DSOP) if applicable. The Supporting Evidence (not limited to) consists of the Security Assessment Plan

(SAP), Risk Analysis Report (RAR), Security Assessment Report (SAR), Hardware and Software List, System Security Plan (SSP), Security Controls Traceability Matrix (SCTM), ACAS Scans, ConMon, Incident Response and Contingency Plans.

2. CYBER RISK ASSESSOR RESPONSIBILITIES

The CRA is an AO appointed role, with the authority and responsibility for the analysis of all ISs and PIT systems governed by a Department of Defense (DoD) Component Cybersecurity Program. CRA's evaluate the cybersecurity capabilities and services of DoD IS and PIT system and make recommendations to the AO. This recommendation accompanies the supporting evidence and serves as the primary basis for the AO's authorization determination. The CRA continuously works with the program to analyze and guide the quality and completeness of activities. The Component SISO either performs the CRA functions or formally appoints CRA Representatives to do so for all governed ISs and PIT systems.

The AO and the ISO rely on the technical expertise and judgment of assessors to:

- Develop, review, and document a plan to assess the security requirements.
- Assess the requirements employed within or inherited by the information system using procedures specified in the security assessment plan.
- Provide specific recommendations on how to correct weaknesses or deficiencies and reduce or eliminate identified vulnerabilities.
- Conduct initial remediation actions on the findings and recommendations of the security assessment report and reassess remediated mitigations, as appropriate.
- Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.
- Prepare the final authorization package, create, and submit the Risk Assessment Report and Risk Recommendation Letter and submit to and obtain the AO's signature on the authorization determination document(s), transmitting the authorization package to appropriate officials.
- Make certain determinations about the planning and resourcing of the security authorization process, approval of the security plan, approval, and monitoring of the implementation of plans of action and milestones, and the assessment and/or determination of risk.

The findings are an unbiased, factual reporting of the weaknesses and deficiencies discovered during the analysis. The organization ensures assessors have access to:

- The information system and environment of operation.
- The appropriate documentation, records, artifacts, test results, and other materials needed to assess the requirements.

3. OBJECTIVES

3.1. Simplified Authorizations

- **Phase 1**: Systems/Systems Security Engineering, Evidentiary Data and Analysis.
  - Output: Standard Acquisition Systems Engineering Data.
- **Phase 2**: Collaboration with the AO/CRA.
  - Output: Scope of the assessment criteria and outcomes.
- **Phase 3**: Continually Execute Risk Assessment.
  - Output: Providing of the Determination Briefing to the AO.

Note: *See CRA Onboarding Process for specific details.*

3.2. Develop and Document a Security Assessment Plan

The CRA develops the Security Assessment Plan, and the AO or their representative reviews the plan. The purpose of the security assessment plan is to establish the appropriate expectations for the assessment and bind the level of effort.

Preparing for an assessment includes the following key activities:

- Ensuring appropriate policies covering assessments are in place and understood by all stakeholders.
- Ensuring all steps prior to the assessment step have been successfully completed and received appropriate management oversight.
- Ensuring the requirements identified as common (and the common portion of hybrid requirements) have been assigned to appropriate entities (such as common control providers) for development and implementation.
- Establishing the objective and scope of the assessment, the purpose of the assessment, and what is being assessed.

3.3. Security Requirements

Proper analysis determines the extent to which the requirements are implemented correctly, operate as intended, and produce the desired outcome. Assessments occur as early as practical in the System Development Lifecycle (SDLC), preferably during the development phase of the information system. Related activities may include design and code reviews, application scanning, and regression testing.

Organizations should consider both the technical expertise and level of independence required in selecting security assessors. Ensure security assessors possess the required skills and technical expertise to successfully carry out assessments of all aspects, to include system-specific, hybrid, and common requirements.

3.4. Security Analysis

An documented security assessment plan helps to ensure an appropriate level of resources are applied toward determining mitigation effectiveness. When security requirements are provided to an organization by an external provider (such as through contracts, licensing agreements, etc.), obtain a security assessment plan from the provider.

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

- Determine which security requirements and enhancements are to be included in the assessment based upon the contents of the supporting evidence and the scope of the assessment.
- Select the appropriate assessment procedures to be used during the assessment based on the security requirements and enhancements to be included in the assessment.
- If required, tailor the selected assessment procedures. For example, select appropriate assessment methods and objects, assign depth, and cover attribute values.
- Optimize the assessment procedures to reduce duplication of effort. For example, sequence, consolidate assessment procedures, and reuse Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) test results.
- Provide cost-effective assessment solutions.
- Finalize the assessment plan and obtain the necessary approvals to execute the plan.

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 their representative documents 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 of the security requirements.

3.5. Assessment Results

The Security Requirements Guide (SRG) and Security Technical Information Guide's (STIG) compliance results will be documented and used as part of the overall supporting evidence. The RMF Knowledge Service is the authoritative source for assessment procedures. Findings are recorded in the Security Assessment Report (SAR) and the Plan of Action and Milestones (POA&M) updated along with any artifacts produced during the assessment (for example, output

from automated test tools or screen shots depicting aspects of system configuration). Final risk should be annotated within the Risk Analysis Report. To make the risk management process as timely and cost-effective as possible, the reuse of previous assessment results, when reasonable and appropriate, is strongly recommended. Assessment results are reused to support reciprocity wherever possible. For inherited security requirements, assessment test results and supporting documentation are maintained by the providing system and are made available to CRAs of receiving systems when requested. For common requirements inherited from the enterprise, instructions for documenting compliance are provided on the RMF Knowledge Service. CRAs will maximize the reuse of existing assessment and T&E documentation in their assessment of the system.

4. RISK ANALYSIS REPORT

Risk Assessment Reports (RAR) contain information organizations can use to communicate the results of risk assessments. Risk assessment reports provide decision makers with an understanding of the information security risk to organizational operations and assets, individuals, other organizations, or the Nation deriving from the operation and use of organizational information systems and the environments in which those systems operate.

The RAR is focused on "risk of use" of non-mitigated requirements and addresses vulnerabilities and weaknesses presented in the SAR after the assessment has been completed by the CRA. The individual risk levels are then used to inform the CRA's recommendation to the AO on acceptance of the cybersecurity risk of operating the system. The essential elements of information in a risk assessment can be described in three sections of the risk assessment report: (i) an executive summary, (ii) the main body containing detailed risk assessment results, and (iii) supporting appendices. Each step is divided into a set of tasks. For each task, supplemental guidance provides additional information for conducting risk assessments. Figure 1 illustrates the basic steps in the risk assessment process and highlights the specific tasks for conducting the assessment.

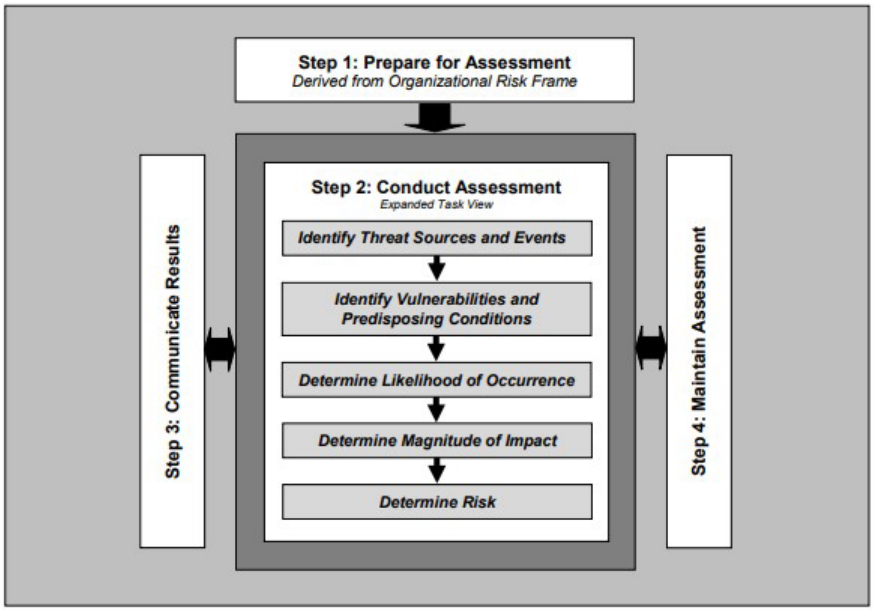

Figure 1: Risk Assessment Process

4.1. Risk Tolerance Level

When assessing risk level:

- Defer to the AO Determination Brief Cyber Hygiene Slides (Cloud, DevSecOps. Weapons, Special Access Program etc.,).
- If no vulnerabilities or weaknesses are found through the process of executing the assessment procedures, the requirement is recorded as satisfactory.
- If vulnerabilities or weaknesses are found, the requirement is recorded with sufficient explanation as High, Moderate, or Low in the SAR and a final risk of use in the Risk Analysis Report.
- If a requirement is found to be not technically or procedurally relevant to the system, an NA for Not Applicable is recorded with sufficient justification in the SAR, however this determination should have been documented when the requirements were initially selected, but circumstances can and do sometimes change
- The CRA Risk Recommendation should provide supporting evidence to the findings and a proposed path forward behind each risk determination.

Not achieving expected results for all assessment procedures does not equate to unacceptable risk. However, all requirements must be assessed for risk and documented in a POA&M with an explanation as to how and when they will be fixed and/or mitigated. Please note that any assessment procedures used that are not in accordance with the procedures outlined by the AO will be documented fully in the SAR.

4.2. Determine Risk Level

The CRA determines and documents in the SAR a risk level of High, Moderate, or Low for each credible risk relative to the system baseline. High risk findings are to be subjected to a risk assessment process that considers multiple factors in producing the risk level and must be coordinated with the AO. As described in the NIST Special Publication 800-30, "Guide for Conducting Risk Assessments," these factors include but are not limited to:

- The CRA's determination that a credible or validated threat source and potential event exists that is capable of and likely to exploit vulnerabilities and weaknesses in the implementation of the requirement.
- Vulnerability severity level and pre-disposing conditions. This includes the CRA's estimate of the adequacy of existing mitigations or compensating to address the vulnerability and mitigations provided by the hosting enclave, Computer Network Defense Service Provider (CNDSP), or other protective measures.
- The cybersecurity attribute (that is confidentiality, integrity, or availability) and associated categorization impact level (high, moderate, and low).
- The CRA's estimate of impact of a successful threat event.

Low	The potential impact is **low** if: the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The potential impact is **moderate** if: the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
High	The potential impact is **high** if: the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The CRA must also determine and document in the SAR an assessment of overall system level of risk. The risk assessment must address all non-mitigated requirements and clearly communicate the CRA's conclusion on system cybersecurity risk along with any recommendations for special instructions to accompany the authorization determination.

4.3. Recording Results

Reasoning for risk and comments can be added to the SAR along with the supporting evidence. The SAR and the RAR contain information the CRA, and the program can use to communicate the results of risk assessment to the AO. Detailed reports provide decision makers with an understanding of the information security risk to organizations, operations and assets, individuals, other organizations, or the Nation that derive from the operation and use of

organizational IS and the environments in which those systems operate. The essential elements of information in a risk assessment can be described in three sections of the risk report: (i) an executive summary; (ii) the main body containing detailed risk results; and (iii) supporting appendices. Programs must identify location for Body of Evidence (BoE).

5. PLAN OF ACTION AND MILESTONES (POA&M)

The purpose of the POA&M is to assist organizations in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses/deficiencies/vulnerabilities found in programs and systems.

The POA&M:

- Facilitates a disciplined and structured approach to mitigating risks in accordance with the priorities of the ISO.
- Includes the findings and recommendations of the security assessment report and the continual security assessments.
- Is a living document and to be maintained throughout the life of the system.

All non-mitigated requirements must be documented in the POA&M with an explanation as to how and when they will be fixed and/or mitigated. Information can be added to the POA&M attachment as part of the Security Authorization Package.

5.1. Remediation Preparation

In all cases, organizations should review findings and determine the severity or seriousness of the findings (potential adverse impact) and whether the findings are sufficiently significant to be worthy of further investigation and/or remediation. The SAR helps determine the initial remediation actions and the prioritization of such actions and provides visibility into specific weaknesses and deficiencies in the security requirements used within or inherited by the information system that remain unresolved. The Risk Analysis Report further clarifies the immediate impact (Threat x Vulnerability x Likelihood), area of concern, mechanisms, initial risk, mitigations, and residual risk level. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source. Remediation Actions are intended to fix NM requirements. POA&Ms are used to provide the method and timeline for remediation. Assigned personnel conduct remediation of NM requirements based on findings and recommendations of the SAR, reassessing remediated control(s) as appropriate.

The AO Determination Brief and security plan is to be updated based on the findings of the security control assessment and all remediation actions taken. The updated brief and security plan reflect the actual state of the security requirements after the initial assessment along with any modifications by the ISO or common provider in addressing recommendations for corrective actions.

6. SECURITY ASSESSMENT REPORT

A Security Assessment Report (SAR) is a key artifact within the supporting evidence in an authorization determination, but not in all scenarios and is at the AOs discretion. The SAR documents the issues, findings, and recommendations from a security assessment. It addresses security requirements in a Non-Mitigated (NM) status, including existing and planned mitigations. If a compelling mission or business need requires the rapid introduction of a new information system or Platform IT system, both the assessment activity and a corresponding SAR should be considered. Organizations may choose to develop an executive summary from the detailed findings generated during a security assessment. An executive summary provides the AO with an abbreviated version of the assessment report focusing on the highlights of the assessment, synopses of key findings, and/or recommendations for addressing weaknesses and deficiencies.

7. RISK ANALYSIS REPORT

This report is focused on "risk assessment of non-mitigated risks and addresses vulnerabilities and weaknesses displayed in the SAR after the assessment" has been completed by the CRA. All non-mitigated risks must be subjected to a risk assessment 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 recommendation (i.e., Risk Analysis Report) to the AO on acceptance of the cybersecurity risk of operating the system.

8. CRA RISK RECOMMENDATION

Based off the SAR results, the CRA will complete their CRA Risk Recommendation outlining the findings, risk levels, and conditions to mitigate. This written recommendation is based off the final risk determination, including correcting any weaknesses, deficiencies, or existing and planned mitigations. The recommendation includes information from the assessor necessary to determine the effectiveness of the mitigation employed within or inherited by the IS based upon the assessor's independent review. The RAR, SAR and CRA Risk Recommendation are the primary documents used by an AO to determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

9. AO AUTHORIZATION

The AO will determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The AO considers the current security state of the system (as reflected by the risk assessment, recommendations provided in the SAR and final risk annotated in the Risk Analysis Report) and weighs this against the operational need for the system. The AO must also consider any applicable risk-related guidance from the DoD SISO, PAOs, DoD ISRMC, DSAWG, DoD

Component SISO, or mission owner(s). Weighing these factors, the AO renders a final determination of risk to DoD operations and assets, individuals, other organizations, and the Nation from the operation and use of the system.

An authorization determination applies to a specifically identified IS or PIT system and balances mission need against risk to the mission, the information being processed, the broader information environment, and other missions reliant on the shared information environment. A DoD authorization determination is expressed as an ATO, an ATO with conditions, an IATT, or a DATO. An IS or PIT system is considered unauthorized if an authorization determination has not been made. The product of the final risk determination is the authorization determination document (letter) documenting the AO's determination along with any terms or conditions the AO attaches to the determination. Finally, the AO's signature on the authorization determination document indicates full acceptance of the risks associated with operating the system.

10. TOOLS

Defer to the CRA Onboarding process for associated guidance and links to the following tools and documents:

1. AO Determination Brief
2. AO Determination Brief Guide
3. IT Categorization and Security Checklist
4. DevSecOps CONOPs (DSOP)
5. Security Assessment Plan (SAP)
6. Risk Analysis Report (RAR)
7. Plan of Action and Milestone (POA&M)
8. Security Assessment Report (SAR)
9. CRA Risk Recommendation Letter
10. DRAFT Authorization Letter
11. No Security Impact (NSI)
12. Miscellaneous Templates (ISA, MOA, MOU, NSI)