OPERATION VULCAN LOGIC (OVL)

Cyber Risk Assessor (CRA) Level 1 Playbook

V1.0

Jun 2023

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 Jun 2023	V1.0	Initial Version	ARLO-Solutions

TABLE OF CONTENTS

1. TERMINOLOGY

This section covers:

- General Terminology.
- Documents and Deliverables.
- Changes and Updates in Terminology.

2. GENERAL TERMINOLOGY

Assessment Plan: The objectives for the security and privacy risk assessments and a detailed roadmap of how to conduct such assessments.

Assessor: The individual, group, or organization responsible for conducting a security assessment.

Authorization Boundary: All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.

Continuous Monitoring: Maintaining ongoing awareness to support organizational risk decisions.

Risk Assessment: Identification of the risks and assessment of the residual risk level for the system.

Risk Management: The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Security Categorization: The process of determining the security category for information or a system.

Systems Engineering: An engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and all other stakeholder needs are satisfied in a high-quality, trustworthy, cost-efficient, and schedule-compliant manner throughout a system's entire life cycle.

System Development Lifecycle (SDLC): Federal information systems such as operational systems, systems under development, and systems undergoing modification or upgrade are in some phase of an SDLC.

- National Institute of Standards and Technology (NIST) identifies five phases of a general SDLC:
  - Initiation.
  - Acquisition/Development.
  - Implementation/Assessment.
  - Operations/Maintenance.
  - Disposition/Sunset.

System Owner or Program Manager: Official responsible for the overall procurement, development, integration, modification, operation, and maintenance of a system.

3. Documents and Deliverables

The document deliverables include the finalization of the Authorization Package, boundaries, requirements, diagrams, assessment reports, final acceptance test plan, and all documents required during implementation such as boundaries, proposed schedule, testing results, and training materials.

4. Changes in Terminology

The old terminology is previously associated with the information assurance process formerly referred to as Certification and Accreditation. This new terminology is adopted under the Risk Management Framework (RMF).

Key Concepts:

Old Terminology	New Terminology
Accreditation	Authorization
Certification	Assessment or Cyber Risk Assessment
Certification and Accreditation (C&A) Process	RMF
Certification Test and Evaluation (CT&E)/Security Test and Evaluation (ST&E) Report	Security Assessment Report (SAR)

Guest Systems	External Information System
Interim Approval to Operate (IATO)	Authorization to Operate with Conditions (ATO-c)
Level of Concern	Impact Level
Protection Levels (PL) • PL1/PL2. PL3/PL4/PL5.	Accessibility • Baseline. Baseline + Appropriate Overlay (e.g., Cross Domain Solution (CDS) Overlay).
CONOPs	AO Determination Brief

Roles:

Old Terminology	New Terminology
Certifier, Certification Authority, Service Certifying Organization (SCO), Security Control Assessor	Cyber Risk Assessor (CRA)
	Information System Security Engineer (ISSE)/Information Assurance Systems Architect and Engineer (IASAE)
	Authorizing Official (AO)/AO Designated Representative (AODR)
Government Contracting Authority (GCA), Customer, etc.	Information System Owner (ISO)

5. CYBERSECURITY: ROLES

This section covers:

- Support/Oversight Roles.
- Decision Authorities.
- Assessors and Owners.
- Implementers.

6. Supporting Roles

Program Security Officer (PSO):

- Verifies configuration management policies and procedures for hardware and software on an IS.
- With ISSM coordination, provides written approval for entry of IS into the facility as appropriate.
- Has authority to appoint the ISSM.
- Report's data spillage incidents to Director of Security and/or Cognizant Authority Coordinating Office (CA).
- Authorizes all digital media and the use of such media.
- Reviews media sanitization procedures and equipment.
- Issues specific guidance regarding TEMPEST requirements.

Government Security Officer (GSSO)/Contractor Program Security Officer (CPSO):

- Creates a secure environment for development and execution.
- With ISSM coordination, provides written approval for entry and removal as appropriate.
- Facilitates several control families essential to securing IS.
- Reports incidents regarding information spillage to the PSO via secure communications.
- Coordinates on the Incident Response Plan.
- Develops media sanitization and removal procedures for PSO/Authorizing Official (AO) approval.

7. Decision Authorities

Element Head/(Service/Agency) (must be Government):

- **Primary Responsibility:** Authorizing Official.
- **Supporting Task:** 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.
    - Bears ultimate responsibility for mission accomplishment, execution of business functions, and all decisions made on his/her behalf.
    - Responsible for adequately mitigating risks to the organization, individuals, and the Nation.
    - Designates an Authorizing Official to make authorization decisions on behalf of the Element Head.

Authorizing Official (AO) (Designated in writing by Service/Agency; must be Government):

- **Primary Responsibility:** AO.

- **Supporting Task:** 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.
    - Has a broad and strategic understanding of the environment, his/her organization, and its place/role in the overall system.
    - Accountable to the Element Head for system authorization and associated risk management decisions.
    - Senior official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk.

Authorizing Official Designated Representative (AODR) (Appointed in writing by Service/Agency AO):

- **Primary Responsibility:** AO Designated Representative.
- **Supporting Task:** Represents the AO in all matters as outlined by the AO.
    - Acts on behalf of the AO.
    - Carries out and coordinates the required activities associated with security authorization.
    - Cannot authorize high impact-level systems.

8. Assessors and Owners

- **Cyber Risk Assessor (CRA)** (Appointed in writing by Service/Agency AO):
- **Primary Responsibility:** AO Designated Representative.
- **Supporting Task:** Represents the AO in all matters as outlined by the AO.
    - Designated by AO.
    - Acts on his or her behalf to conduct security assessments.
    - Responsible for conducting a comprehensive assessment of the management, operational, and technical security requirements employed within or inherited by an IS to determine the overall effectiveness of the requirements.
    - Responsible for determining the degree to which it meets its security requirements.

Information Owner/Steward (STWD) (Service/Agency; must be Government):

- **Primary Responsibility:** System Operational Owner.
- **Supporting Task:** Responsible for system requirements definition, funding advocacy, system acceptance, system employment, and operations.
    - Has statutory or operational authority for specified information and responsibility for establishing requirements for its generation, classification, collection, processing, dissemination, and disposal.
    - Typically, in the case of Stewards of classified information, this role is also the appointed Original Classification Authority (OCA) for that information.

- Development and maintenance of AO Determinations in accordance with security requirements.
- Appoints the ISSM.

9. IMPLEMENTORS

Information System Owner (ISO) (Government or Contract PM):

- **Primary Responsibility:** System Operational Owner.
- **Supporting Task:** Responsible for system requirements definition, funding advocacy, system acceptance, system employment, and operations.
  - Responsible for overall procurement, development, integration, modification, or operation, maintenance, and disposal of an IS.
  - Responsible for the development and maintenance of the AO Determination Brief and every other document required for security ATO.
  - Ensures the system is deployed and operated in accordance with the agreed-upon security requirements.
  - Appoints the program ISSM and ISSE (may be the same person).

Information System Security Manager (ISSM):

- **Primary Responsibility:** Program/Capability Cyber Lead.
- **Supporting Task:** 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.
- Principal advisor on all matters, technical and otherwise, involving the security of information systems under his/her purview.
  - Responsible for the day-to-day security posture and continuous monitoring
  - Responsible for the overall information assurance of a program, organization, system, or enclave.
  - Responsibilities also include physical and environmental protection, personnel security, incident handling, and security training and awareness.
  - May be identified and appointed in writing to fulfill the role of ISSE.
  - ISSM responsibilities should not be assigned as collateral duties.

Information System Security Engineer (ISSE):

- **Primary Responsibility:** Developer.
- **Supporting Task:** An ISSE/IASAE ensures that information-security requirements are effectively implemented throughout the security architecting, design, development, configuration, and implementation processes. The ISSE coordinates his/her security-related activities with ISOs and ISSOs/ISSMs.
  - An individual or group responsible for conducting information system security engineering activities.
  - An integral part of the development team, designing and developing organizational information systems or upgrading legacy systems.

- Ensures the information system is designed, developed, and implemented with required security features and safeguards.
- Appointed in writing by the ISO.

10. SUPPORTING TASKS

OVL	RMF
Phase 1: Systems/Systems Security Engineering, Evidentiary Data, and Analysis	Step 0: Prepare
	Step 1: Categorize
	Step 2: Select Security Controls
	Step 3: Implementation of the Security Controls
Phase 2: Collaboration with AO/CRA	Step 4: Assess Controls
	Step 5: Authorize System
Phase 3: Continually Execute Risk Assessment	Step 6: Monitor Controls

1.1. 10.1 Element 1: Categorize System

Supporting Task 1.1:

- **Supporting Task:** Categorize the information system and document the results in the AO Determination Brief.
- **Primary Responsibility:** ISO/Mission Owners
- **Stakeholders:** AO/AODR/ISSM/PM/SM/SISO
- **Output(s):** Draft AO Determination Brief with system categorization determined.

Supporting Task 1.2:

- **Supporting Task:** Describe the information system (including system boundary) and document the description in the AO Determination Brief.
- **Primary Responsibility:** ISO/Mission Owners
- **Stakeholders:** AO/AODR/ISSM/PM/SM/SISO
- **Output(s):** Updated AO Determination Brief.

Supporting Task 1.3:

- **Supporting Tasks:** Register the IS with the appropriate organizational program management offices.
- **Primary Responsibility:** ISO/PM/SM
- **Stakeholders:** ISSM
- **Output(s):** Document or enter in the IT registry with the official system name, system owner, and categorization.

Supporting Task 1.4:

- **Supporting Tasks:** Assign qualified personnel to the OVL roles
- **Primary Responsibility:** ISO/PM/SM
- **Stakeholders:** ISSM
- **Output(s):** Document or enter in the IT registry with the official system name, system owner, and categorization.

1.2. 10.2 Element 1: Select Security Requirements

Supporting Task 2.1:

- **Supporting Task:** Identify the security requirements provided by the organization as common requirements for organizational IS and document the requirements in the AO Determination Brief.
- **Primary Responsibility:** ISO/ISSM/ISSE/CRA
- **Stakeholders**: AO/AODR/ISO/Risk Executive (Function)
- **Output(s):** Document the common requirements in the AO Determination Brief.

Supporting Task 2.2:

- **Supporting Task:** Select the security requirements for the IS (i.e., baseline, overlays, tailoring) and document the requirements in the AO Determination Brief.
- **Primary Responsibility:** ISO; PM/SM/ISSE
- **Stakeholders**: AO/AODR/IO/ISSM
- **Output(s):** Document the selected requirements in the AO Determination Brief.

Supporting Task 2.3:

- **Supporting Task:** Develop a system-level continuous monitoring strategy
- **Primary Responsibility:** ISO; ISSM/CRA/PM/SM
- **Stakeholders**: AO/AODR/CIO/IO/Risk Executive (Function)/SISO
- **Output(s):** Documented Continuous Monitoring (ConMon) Plan/Strategy including frequency of monitoring for each requirement.

Supporting Task 2.4:

- **Supporting Task:** Review the AO Determination Brief and Continuous Monitoring Strategy.
- **Primary Responsibility:** AO or AODR; CRA/ISSM (pre-submission)
- **Stakeholders**: CIO/IO/Risk Executive (Function)/SISO
- **Output(s):** Documented AO Determination Brief and Continuous Monitoring Strategy.

Supporting Task 2.5:

- **Supporting Task:** Apply Overlays and tailor
- **Primary Responsibility:** ISO; PM/SM/ISSE
- **Stakeholders**: AO/AODR/IO/ISSM
- **Output(s):** Updated AO Determination Brief.

1.3. 10.3 Element 1: Implement Security Requirements

Supporting Task 3.1:

- **Supporting Task:** Implement the security requirements specified in the AO Determination Brief.
- **Primary Responsibility:** ISO; PM/SM/ISSE
- **Stakeholders:** IO/ISSM
- **Output(s):** Document Continuous Monitoring (ConMon) Plan/Strategy including frequency of monitoring for each requirement.

Supporting Task 3.2:

- **Supporting Task:** Document the implementation as appropriate in the AO Determination Brief, providing a functional description of the implementation.
- **Primary Responsibility:** ISO; PM/SM/ISSM/ISSE
- **Stakeholders:** IO
- **Output(s):** Update the AO Determination Brief with information describing how security requirements are being implemented.

1.4. 10.4 Element 2: Assess Security Requirements

Supporting Task 4.1:

- **Supporting Task:** Provide Assessment Criteria and review a plan to assess the security requirements.
- **Primary Responsibility:** AO/AODR; CRA
- **Stakeholders:** IO/ISO/ISSM/PM/SM/SISO
- **Output(s):** Security Assessment Plan (SAP)

Supporting Task 4.2:

- **Supporting Task:** Assess the security requirements in accordance with the assessment procedures defined in the Security Assessment Plan.
- **Primary Responsibility:** CRA.
- **Stakeholders:** IO/ISO/ISSM
- **Output(s):** Individual test results for each test or matrix for all tests.

Supporting Task 4.3:

- **Supporting Task:** Prepare the Security Assessment Report (SAR)
- **Primary Responsibility:** CRA.
- **Stakeholders:** ISO/ISSM
- **Output(s):** Security Assessment Report documenting the issues, findings, and recommendations from the assessment.

Supporting Task 4.4:

- **Supporting Tasks:** Conduct initial remedial actions based on findings and reassess remediated risk(s) as appropriate.
- **Primary Responsibility:** ISO/CRA; ISSM
- **Stakeholders:** AO/AODR/CIO/IO
- **Output(s):** Updated SAR, AO Determination Brief (Risk Analysis Report (RAR)).

1.5. 10.5 Element 2: Authorize System

Supporting Task 5.1:

- **Supporting Task:** Prepare the Plan of Action and Milestones (POA&M) based on the findings and recommendations from the SAR, include any remediation actions taken.
- **Primary Responsibility:** ISO/PM/SM; ISSM
- **Stakeholders:** AO/AODR/IO/SISO
- **Output(s):** POA&M.

Supporting Task 5.2:

- **Supporting Task:** Assemble and submit the Security Authorization Package (SAP) to the CRA. References are not part of the Security Authorization Package but must documented and made available. Classified artifacts are not to be submitted as part of the SAP but must be highlighted.
- **Primary Responsibility:** ISO/ISSM; CRA
- **Stakeholders:** AO/AODR
- **Output(s):** SAP; AO Determination Brief, AO Authorization Letter, CRA Risk Recommendation Letter, Categorization Letter, and POA&M (if unclassified).

Supporting Task 5.3:

- **Supporting Task:** AO Determines final risk
- **Primary Responsibility:** AO or AODR
- **Stakeholders:** Risk Executive (Function)/SISO
- **Output(s):** Documented Continuous Monitoring (ConMon) Plan/Strategy including frequency of monitoring for each risk.

Supporting Task 5.4:

- **Supporting Task:** AO makes authorization determination
- **Primary Responsibility:** AO.
- **Stakeholders:** AODR/ISO/PM/SM/Risk Executive (Function)/SISO
- **Output(s):** Authorization decision document (ATO, DATO, or IATT).

1.6. 10.6 Element 3: Monitor Security Requirements

Supporting Task 6.1:

- **Supporting Task:** Determine the security impact of proposed or actual changes to the IS and its environment of operation.
- **Primary Responsibility:** ISO; ISSM.
- **Stakeholders:** CRA/AO/AODR/IO/Risk Executive (Function)/SISO
- **Output(s):** Change Request.

Supporting Task 6.2:

- **Supporting Task:** Assess a selected subset of security requirements employed within and inherited by the IS in accordance with the organization-defined monitoring strategy.
- **Primary Responsibility:** CRA; ISSM.
- **Stakeholders:** AO/AODR/IO/ISO/SISO/ISSE
- **Output(s):** Periodic Continuous Monitoring Report.

Supporting Task 6.3:

- **Supporting Task:** Conduct remediation actions based on the results of ongoing monitoring activities, assessment or risk, and outstanding items in the POA&M.
- **Primary Responsibility:** ISO; ISSM.
- **Stakeholders:** AO/AODR/IO/ISSE/ISSM/CRA
- **Output(s):** Documented evidence of correction such as scan results, registry "dumps," etc.

Supporting Task 6.4:

- **Supporting Task:** Update AO Determination Brief, SAR, and POA&M based on the results of the continuous monitoring process.
- **Primary Responsibility:** ISO; PM/SM; ISSM.
- **Stakeholders:** AO/AODR/IO/CRA
- **Output(s):** Updated AO Determination Brief, SAR, RAR and POA&M.

Supporting Task 6.5:

- **Supporting Task:** Report the security status of the IS (including the effectiveness of security requirements employed within and inherited by the IS) to the AO and other appropriate organizational officials on an ongoing basis and in accordance with the continuous monitoring strategy.
- **Primary Responsibility:** ISO; ISSM.
- **Stakeholders:** AO/AODR/ISO/PM/SM/CRA
- **Output(s):** Periodic Continuous Monitoring Report.

Supporting Task 6.6:

- **Supporting Task:** Review the reported security status of the IS (including the effectiveness of security requirements employed within and inherited by the IS) on an ongoing basis and in accordance with the continuous monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.
- **Primary Responsibility:** AO.
- **Stakeholders:** ISSM/PM/SM/Risk Executive (Function)/CRA/SISO
- **Output(s):** ATO.

Supporting Task 6.7:

- **Supporting Task:** Implement an IS Decommissioning Strategy when needed which executes required actions when a system is removed from service.
- **Primary Responsibility**: ISO; PM/SM.
- **Stakeholders:** AO/AODR/IO/ISSM/SISO/ISSE
- **Output(s):** Updated tracking, management, and inventory system. The AO shall formally decommission the IS by issuing a Decommission letter.