



DOD/CDAO OVL

Operation Vulcan Logic (OVL) Guide
AO Determination Brief
V2.1
October 2024

Point of Contact for this document:
osd.ncr.cdao.mbx.ovl@mail.mil

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 annually.

Date	Version	Change Type	Modified By
18 Dec 2023	V1.0	Initial Version	Arlo Solutions
11 July 2024	V2.0	Updated for CDAO	Arlo Solutions
31 Oct 2024	V2.1	Updated for CDAO	Arlo Solutions

TABLE OF CONTENTS

Version History.....	1
Table of Contents.....	2
1. Risk Assessment Process Overview.....	4
1.1 Introduction.....	4
1.2 Objective.....	4
1.3 Applicability and Scope.....	4
1.4 AO Confidence Levels.....	5
2. Assessments.....	6
2.1 Threat Assessment	6
2.2 Vulnerability Assessment	6
2.3 Risk Assessment	6
3. AO Determination Briefing.....	7
3.1 Slide Instructions	7
3.2 Title Slide.....	8
3.3 Program and AO Team	9
3.4 Bottom Line Up Front (BLUF).....	10
3.5 Mission and System Description	12
3.6 Cybersecurity and Resilience Enablers.....	13
3.7 Supply Chain Risks.....	14
3.8 System Architecture.....	16
3.9 Interconnections and Interfaces	17
3.10 Authorization Boundary.....	18
3.11 Authorization Boundary Continued.....	19
3.12 Mission Partners.....	20
3.13 Cyber Tech Order and Continuous Monitoring	21
3.14 CDAO ORTB.....	22
3.15 CDAO ORTB – AI View.....	23
3.16 CDAO ORTB Controls.....	25
3.17 Risk Assessment Model.....	26

3.18	Assessment Approach	28
3.19	Cyber Test Schedule	31
3.20	PenTest Schedule	32
3.21	Risk Scale Summary	33
3.22	Risk Analysis Report	34
3.23	Mitigating Factors	35
3.24	Summary	36
3.25	Backup Slides.....	37
3.26	Impact Level Comparison.....	38
3.27	Cloud System Architecture	39
3.28	Cloud Data Flow Diagram	40
3.29	Cloud Authorization Boundary	41
3.30	Cybersecurity Service Provider (CSSP) or Equivalent Services	42
3.31	Equivalent CSSP Services	43
3.32	OVL Authorization Package	44
3.33	SAP Protection Levels	45
3.34	SAP Body of Evidence	47
3.35	SAP Connection Package Required Documentation	48
3.36	SAP ORTB.....	49
3.37	SAP ORTB (Continued)	51
4.	Additional DAF Back-Up Slides.....	53
4.1	eMASS Guidance AFI 17-101	53
4.2	OVL AO eMASS Guidance.....	55
4.3	Authorization Package	56
4.4	Authorization Determination Table	57

1. RISK ASSESSMENT PROCESS OVERVIEW

1.1 Introduction

The Authorizing Official (AO) has been appointed to issue determinations information technology (IT), including information systems (IS); Platform IT (PIT); IT services; IT products; IT applications; Research, Development, Test, and Evaluation (RDT&E); Cloud IS services; and products requiring agile acquisition. The AO issues determinations based on the confidence in the actual risk levels and information presented. Program Management Offices (PMOs) are expected to conduct assessments of the IT within their purview, document results in a determination briefing, and present the information to the AO so a risk determination can be made and an operational determination issued.

1.2 Objective

The objective of this guide is to assist program personnel in understanding what the AO expects to make an informed risk determination. This includes but is not limited to the PMO recognizing threats, identifying internal and external vulnerabilities, understanding the impact of vulnerabilities being exploited, likelihood of occurrence, the identification of risks, remediation actions to eliminate risk, and mitigation strategies to lower risk to an acceptable level.

Program Managers (PMs) are fully expected to own the Assessment and Authorization (A&A) process for the systems within their purview. The AO requests that PMs present the determination briefing when requesting an authorization determination. All artifacts, test results, and related documentations are expected to be thoroughly reviewed and understood by the PM, and any vulnerabilities or items requiring any sort of mitigation must be included in an updated Plan of Action and Milestones (POA&M) prior to briefing the AO.

1.3 Applicability and Scope

This guide is applicable to organizations that develop and/or maintain information systems, Cloud information systems, PIT, IT applications, products, services, RDT&E, and agile acquisition. The scope of this guide is limited to providing guidance for developing determination briefings to receive authorization determination.

This guide is intended for an audience familiar with *NIST 800-series Special Publications*; experienced with threat/vulnerability pairing, conducting risk and vulnerability assessments, and understanding the output of such assessments; and experienced with implementing remediation actions and/or mitigation strategies.

1.4 AO Confidence Levels

The AO expects to be fully informed of a program's security posture and will make risk determinations based on the confidence in the information presented. A typical program would have completed the assessments in *Section 2* below, had independent assessments conducted (including but not limited to penetration and/or vulnerability testing, verification testing, developmental/operational testing, Control Risk Assessor (CRA) assessments, etc.), and documented the results in the determination briefing prior to requesting the AO make a risk-based determination. The higher level of involvement by the PM and the more assessments conducted to truly understand the security posture will lead to a higher level of confidence in the determination made by the AO, typically resulting in a longer authorization period.

The Risk Scale Summary is expected to be used to determine a residual risk based on available artifacts, documentation, and completed actions. The completed Risk Analysis report will be made available to the AO as part of the determination briefing. The AO reserves the right to determine the final risk based on evidence presented. Note: Evidence will result in an overall LOW confidence level if it is not presented, completed, and/or inaccurate, and the conclusion may be determined as HIGH Risk.

2. ASSESSMENTS

2.1 Threat Assessment

Threat assessment is the practice of determining the credibility and seriousness of a potential threat as well as the probability that the threat will become a reality. A threat assessment is the process of identifying and formally evaluating the degree of threats to information technology and describing the nature of the threat.

2.2 Vulnerability Assessment

A vulnerability assessment is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system. It is a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

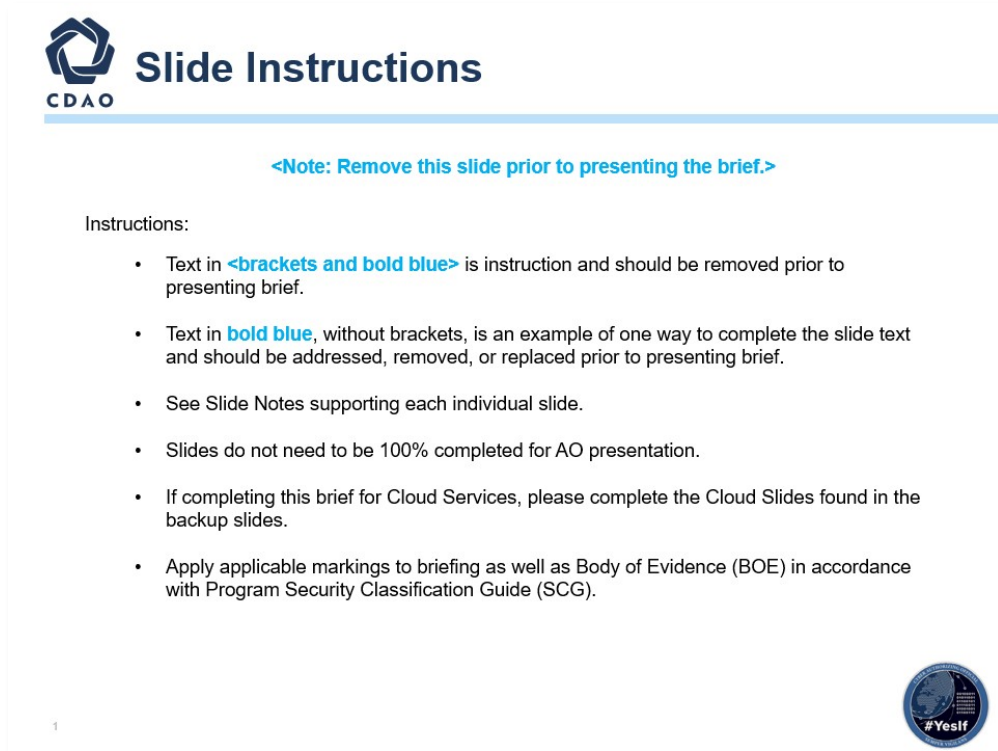
2.3 Risk Assessment

A risk assessment is a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking. It is the process of identifying and prioritizing risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation of information technology. It also incorporates threat and vulnerability analyses and considers mitigations provided by security requirements either planned or in place.

For the purposes of this guide, the risk assessment is recognizing threats, identifying vulnerabilities, making the threat/vulnerability pairs (threat + vulnerability = risk), and determining what the risk level is to inform the AO and decide what will be done to reduce or remediate risk. The determination briefing should capture the output of the risk assessment so the AO can make a well-informed determination.

3. AO DETERMINATION BRIEFING

3.1 Slide Instructions



The slide is titled "Slide Instructions" and features the CDAO logo in the top left corner. A blue horizontal bar is positioned below the title. A note in blue text reads: "<Note: Remove this slide prior to presenting the brief.>". Below this, the word "Instructions:" is followed by a bulleted list of seven items. The first item mentions "<brackets and bold blue>" as text to be removed. The second item mentions "bold blue" as an example of text to be addressed. The third item refers to "Slide Notes". The fourth item states that slides do not need to be 100% completed. The fifth item refers to "Cloud Slides" in the backup slides. The sixth item refers to the "Body of Evidence (BOE)" and the "Program Security Classification Guide (SCG)". In the bottom right corner, there is a circular seal with the text "#YesIf" and a small number "1" in the bottom left corner.


Slide Instructions

<Note: Remove this slide prior to presenting the brief.>

Instructions:

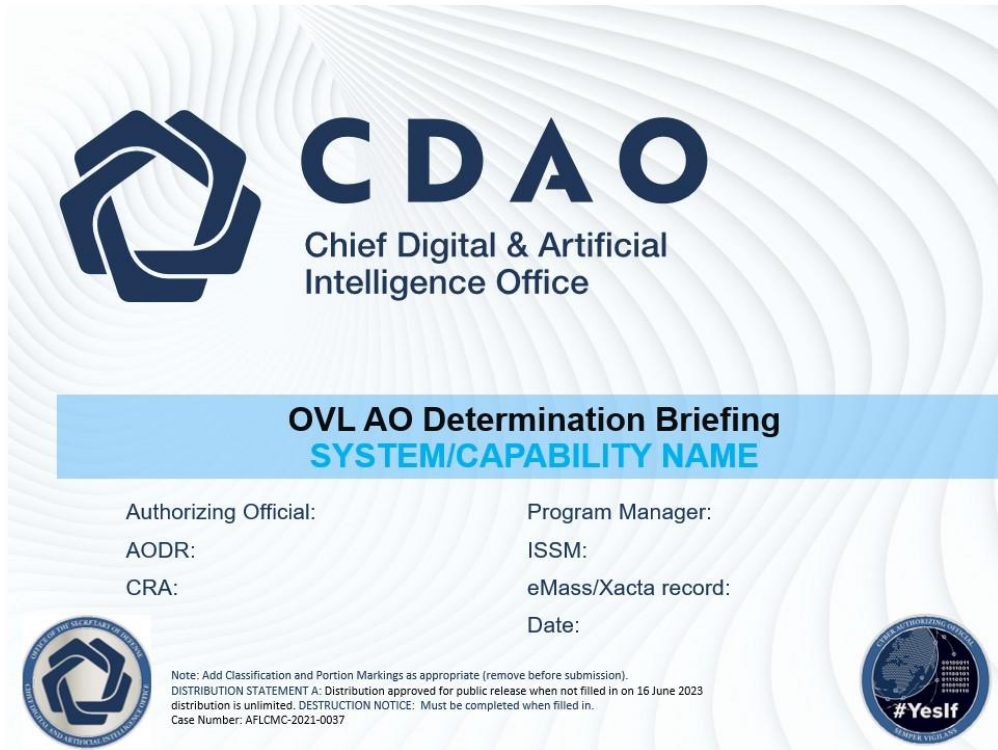
- Text in **<brackets and bold blue>** is instruction and should be removed prior to presenting brief.
- Text in **bold blue**, without brackets, is an example of one way to complete the slide text and should be addressed, removed, or replaced prior to presenting brief.
- See Slide Notes supporting each individual slide.
- Slides do not need to be 100% completed for AO presentation.
- If completing this brief for Cloud Services, please complete the Cloud Slides found in the backup slides.
- Apply applicable markings to briefing as well as Body of Evidence (BOE) in accordance with Program Security Classification Guide (SCG).

1



- Deck instructions.
- Complete this slide to incorporate your organization's Communications Listing.
- It is up to the individual completing this slide deck to determine if their environment is Cloud-related. If it is, there are some Cloud-specific slides that need to be completed. If not, they can remove or hide all the identified Cloud slides.


3.2 Title Slide



The title slide features a blue and white wavy background. At the top left is the CDAO logo, a stylized blue hexagon. To its right, the text 'CDAO' is written in large, bold, blue letters, followed by 'Chief Digital & Artificial Intelligence Office' in a smaller, black font. Below this, a light blue horizontal bar contains the text 'OVL AO Determination Briefing' in bold black font, and 'SYSTEM/CAPABILITY NAME' in blue font. Underneath the bar, there are two columns of text for 'Authorizing Official:' and 'Program Manager:', each followed by 'AODR:', 'ISSM:', 'CRA:', 'eMass/Xacta record:', and 'Date:'. At the bottom left is a circular seal for the Department of the Secretary of Defense, Office of the Chief Digital & Artificial Intelligence Officer. At the bottom right is a circular seal for the Department of the Secretary of Defense, Office of the Chief Digital & Artificial Intelligence Officer, with the hashtag #YesIf. In the center, there is a note: 'Note: Add Classification and Portion Markings as appropriate (remove before submission). DISTRIBUTION STATEMENT A: Distribution approved for public release when not filled in on 16 June 2023 distribution is unlimited. DESTRUCTION NOTICE: Must be completed when filled in. Case Number: AFLCMC-2021-0037'.

- The title slide identifies who the program owner is, the name of the program, program type (PIT, Enterprise, Software, Rapid Cyber, product, service, component, Cloud, etc.), and the name(s) of the personnel that will be briefing.
- Please add system name, PM, and date
- This is a joint briefing between the program/system/capability ISSM and the CRA. It is the Executive Summary to the Authorizing Official of the request for a determination. It documents the point in time that the authorization determination is made.
- It is part of the Authorization Package that is documented.
- This briefing provides an overview of the system/capability, the architectures, the data flows, the CONOPS, the technologies, the supply chain, the Risk analysis, the mitigated risk areas, the unmitigated risk areas, the POA&M, the COMMON, and the IR.
- It outlines the system/capability, the risk posture, the agreed-too conditions between the PM and the AO, and the items that will be addressed per the Authorization conditions.
- This AO Determination Briefing forms the basis for communicating the Risk posture of the System/Capability to other stakeholders and to other AOs, for aiding reciprocity, and for informing others of the risk-of-use posture of the system/capability.

3.3 Program and AO Team




<Program> and AO Team

Program Team

- PM, Name, Organization
- ISO, Name, Organization
- ISSM, Name, Organization
- ISSE, Name, Organization
- Pen Test Lead, Name, Organization
- Program Support, Name, Organization


AO Team

- AO, Mr. Daniel Holtzman, CDAO
- AODR, Name, Organization
- CRA, Name, Organization




The diagram shows two overlapping circles labeled 'Program' and 'Assess and Authorize'. These circles are contained within a larger oval labeled 'Cyber' at the top and 'Team Sport' at the bottom.

Team of Teams Concept: Teams collaborate, but assessors must be independent.



- Complete this slide to identify the individual and team roles.


3.4 Bottom Line Up Front (BLUF)



Bottom Line Up Front (BLUF)

- Obtain an authorization determination for **<System Name>**
 - **<Outline mission need and strategic agenda>**
 - *Seeking an IATT to support the “XXX” training exercise scheduled for “day month year” through “day month year”*
 - **<Provide projected schedule>**
 - **<Describe Assumptions and Constraints>**
 - *Industry Partners/Services, Foreign Partners/Customers*
 - *Authorized interconnection between “XXX” and “YYY”*
 - *Network/Boundary Limitations*
 - **<Provide scope/boundary of assessment>**
 - *PIT System, Type Accreditation, Stand Alone, Enterprise, etc.*
- Current Status: **<List current or last approval, other circumstances>**
 - **Approval and Expiration, under testing (IATT), etc.**
- The overall level of residual risk of **<System Name>** is assessed to be **<L,M,H>**

The CRA recommends AO **<Concur/Non-concur>** **<recommendation>** to support deployment of **<System Name>** through **<Authorization Termination Date (ATD)>**.

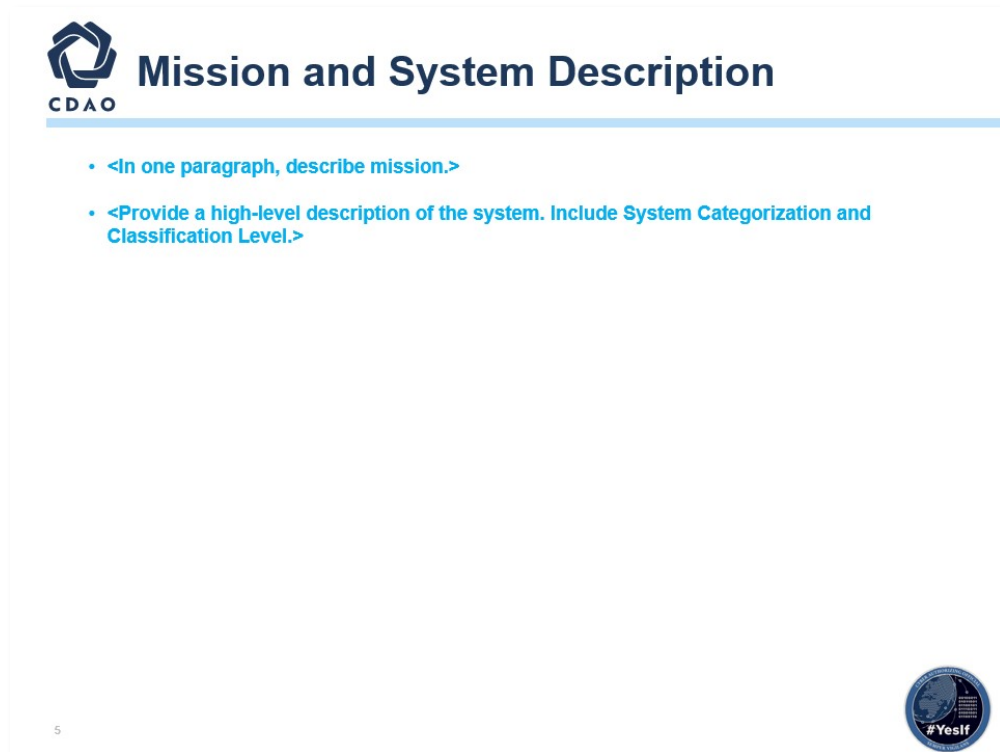


- Bottom Line Up Front: Identify the name of the system, the reason for the requested determination and timeframe the determination is expected, any pertinent information, scope of the assessment, and the current authorization status.
- **Reference *NIST SP 8510.01* and *NIST SP 800-37*.**
- Describe the intention of the briefing. Why are we here, and what do you want from the AO? Use simple statements, direct and to the point. The determination can be either for ATO, ATO with conditions, IATT, or DATO.
- The line “This is a Type Authorization under Reciprocity” is necessary if it applies, and any other pertinent information needs to be identified up front.
- The current situation should describe previous authorizations and dates or confirm that it is an initial (new) assessment and need date. The AO and CRA need these details up front to understand and assist.
- The Cyber Risk Assessor (CRA) is the official with the authority and responsibility for the assessment of all ISs and PIT systems governed by a DoD Component Cybersecurity Program. The CRA evaluates the cybersecurity capabilities and services of a DoD IS and PIT system and makes a recommendation for risk acceptance or denial to the AO.
- This recommendation accompanies the RMF security authorization package and serves as the primary basis for the AO’s authorization determination. The CRA continuously assesses and guides the quality and completeness of RMF activities and tasks and the

resulting artifacts. The DoD Component SISO either performs the CRA functions or formally appoints CRA Representatives to do so for all governed ISs and PIT systems.


- Specific duties include (taken from *NIST SP 800-37*):
 - Develop, review, and approve a plan to assess the risk.
 - Assess the security risks in accordance with the assessment procedures defined in the security assessment plan.
 - Prepare the security assessment report, documenting the issues, findings, and recommendations from the security risk assessment.
 - Conduct initial remediation actions on security risks based on the findings and recommendations of the security assessment report and reassess remediated risk(s) as appropriate.
 - Assess a selected subset of the technical, managerial, and operational security risks employed within and inherited by the information system in accordance with the Organization-Defined Monitoring Strategy.

3.5 Mission and System Description



- **EXECUTIVE-LEVEL CHART ONLY**; focusing on program capabilities.
- Mission Description: In one paragraph, describe the mission. Provide a concise overview of the mission's purpose, objectives, and key outcomes. Highlight the significance and impact of the mission in clear and compelling language.
- Need to describe from a high-level overview (1 paragraph or less) your mission objective (MVP) supporting this need and what the system will intel.
- System Overview: Provide a high-level description of the system, including system categorization and classification level. Briefly outline the system's function, its role within the organization, and its categorization (Confidentiality, Integrity, Availability) (e.g., CCS) and classification level (e.g., CUI, Secret, Top Secret). Ensure clarity and relevance for the intended audience.
- What details did you provide in the CCS?
- You will need to describe from a high-level overview in a generalized viewpoint both the mission and information system requirements driving the need for a new information system authorization.

3.6 Cybersecurity and Resilience Enablers




Cyber Security and Resiliency Enablers

The items below should be conveyed to the AO within this briefing; these slides are NOT to be filled out. Please remove this slide prior to submission.

1. <What is the System? What does it do? CONOPS? Missions?>
2. <What is the System Architecture? Weapon System (e.g., Aircraft, Ground Systems, Maintenance Systems, Training Systems, etc.)>
3. <List of Hardware (LRU), Software and providence of each (e.g., supply chain); identification of Critical Program Information (CPI), Critical Components (CC); Technical Orders, Operational Procedures. Identification of technologies being used.>
4. <Identification of all external communications access points.>
5. <How does data flow into, through, and out of the system? What type of data is it? How is it protected? Where does it come from? Where does it go? What is it used for?>
6. <What threat/intel information is available?>

This is the set of Enablers that should be addressed during the rest of the briefing
This chart can be moved to back up. it can be a pointer to the charts in the briefing that
address the areas.
IT IS A TEMPLATE CHART – THE BRIEFING SHOULD ADDRESS THESE AREAS



- **Reference *NIST Special Publication 800-161*.**
- **System Overview:** Describe what the system is designed to do, how it operates within its operational concept (CONOPS), and the specific mission it supports.
- **System Architecture:** Outline the structural design and components of the system, emphasizing its role and categorization within the broader context of the capability.
- **Hardware, Software, and Critical Information:** Provide a detailed inventory of hardware and software components, their sources, criticality, and any pertinent technical and operational documentation. Mention the technologies integrated into the system.
- **External Communications Access Points:** List and describe the external interfaces and communication channels used by the system to interact with external entities or networks.
- **Data Flow and Protection:** Detail the data handling processes within the system, including data types, security measures, origins, destinations, and utilization purposes.
- **Threat/Intel Information:** Summarize the current threat landscape and available intelligence pertinent to the system's operations and security posture.

3.7 Supply Chain Risks



Supply Chain Risks

The items below should be conveyed to the AO within this briefing; these slides are NOT to be filled out. Please remove this slide prior to submission.

1. <Bill of Materials (BOM) - As part of the systems engineering (SE) process, especially in a legacy system, programs already know all parts (hardware and software).>
2. <Existing supplier management process identifies supplier source, End of Life (EOL) analysis, and alternate part analysis. (Document "As-Is")>
3. <Existing criteria being used by primes and flowed down to subs, on purchasing of parts is known?>
4. <What is the supply chain mapping? Does one exist already?>
 - <With the data collected from items 1-4 above, review the potential risks of the supply chain>
 - <Provide available intel/threat info that can be applied against the list of parts or suppliers identified (or technologies)>
 - <Provide an assessment of risk of the current supply chain>
 - <Provide a graphical representation of the supply chain>

This is the set of Enablers that should be addressed during the rest of the briefing
 This chart can be moved to back up. It can be a pointer to the charts in the briefing that address the areas.

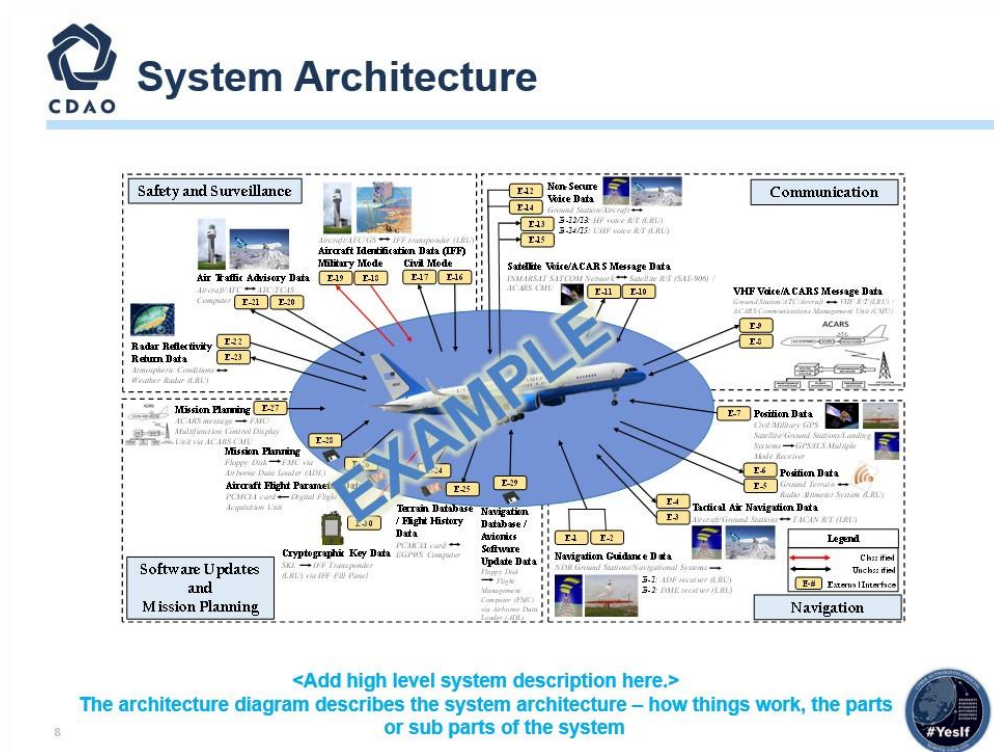
IT IS A TEMPLATE CHART – THE BRIEFING SHOULD ADDRESS THESE AREAS



- Identify your program’s supply chain risks for the information system.
- Bill of Materials (BOM): Include a detailed BOM outlining all components of the system, categorized by hardware and software, as per the existing knowledge base.
- Supplier Management Process: Describe how suppliers are currently managed, including processes for identifying sources, conducting EOL and alternate part analyses, and any documentation reflecting the current state (“As-Is”).
- Criteria for Purchasing Parts: Outline the established criteria and guidelines used in the procurement process for parts, detailing requirements imposed by prime contractors and how these are communicated to subcontractors.
- Supply Chain Mapping: Assess the presence and detail of an existing supply chain map, if available, outlining the relationships and dependencies among suppliers, manufacturers, and distributors involved in the supply chain.
- Supply Chain Risks: Analyze and present potential risks such as supplier dependencies, part availability issues, and vulnerabilities identified through the BOM, supplier management processes, purchasing criteria, and supply chain mapping.
- Intel/Threat Information: Summarize any pertinent intelligence or threat data that could impact the identified parts, suppliers, or technologies within the supply chain.
- Assessment of Supply Chain Risk: Present an assessment of the identified risks, providing insights into the overall risk posture of the current supply chain environment.

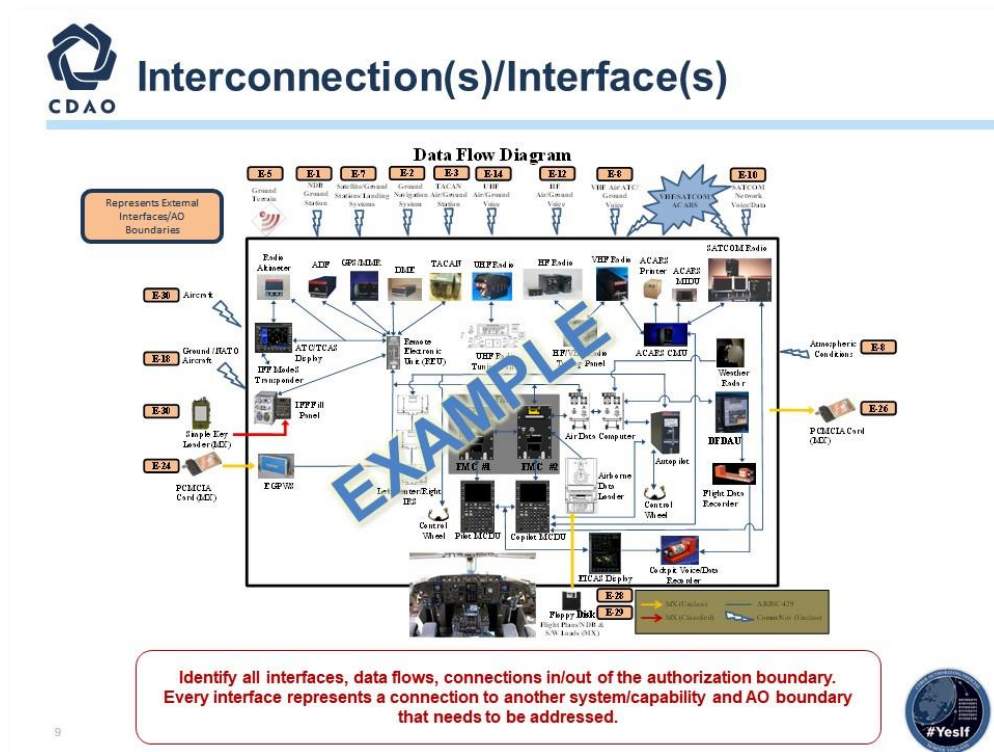
- Graphical Representation of Supply Chain: Create a visual diagram illustrating the relationships and flow within the supply chain, highlighting key suppliers, manufacturers, distributors, and dependencies.

3.8 System Architecture



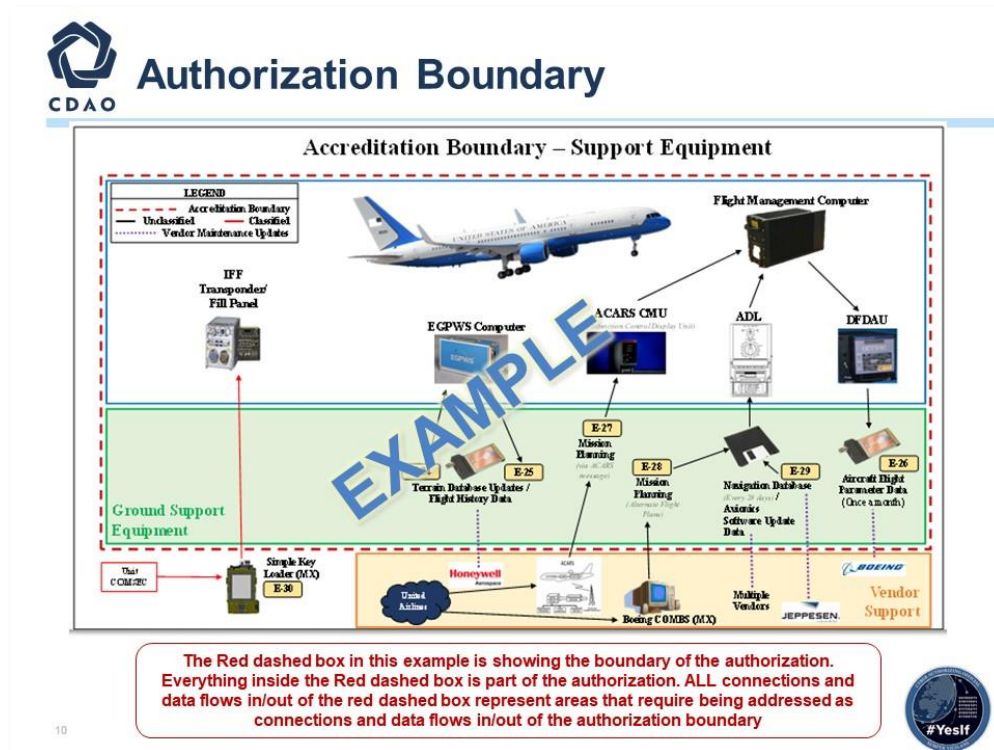
- **Reference only; replace architecture.**
- The system architecture should show the AO what the architecture is, its physical location, encryption, interfaces and protocols, physical and technical protection mechanisms, vendor access, etc.
- A system architecture is the conceptual model that defines the structure and behavior and supplies more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. Identify the architecture, locations, encryption, interfaces, protocols, physical and technical protection measures, vendor access, etc.

3.9 Interconnections and Interfaces



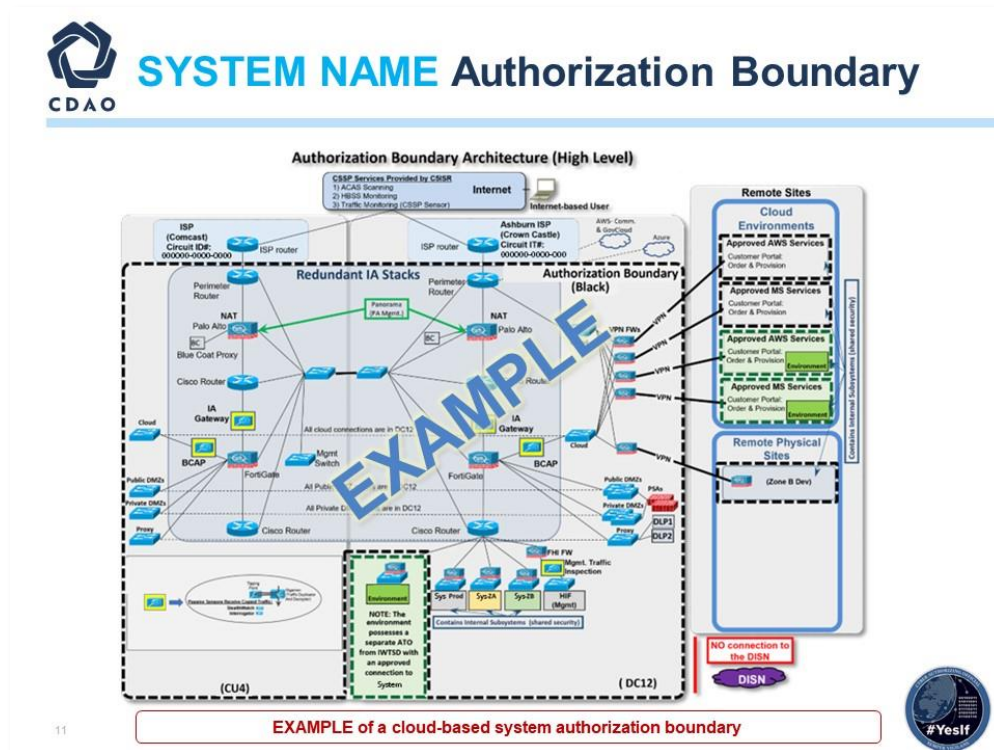
- **Reference only; replace architecture.**
- Describe the interconnections/data flows this system has with any external systems or networks. Describe what the external connections are: PITIs, other external connections, standalone system, etc.

3.10 Authorization Boundary



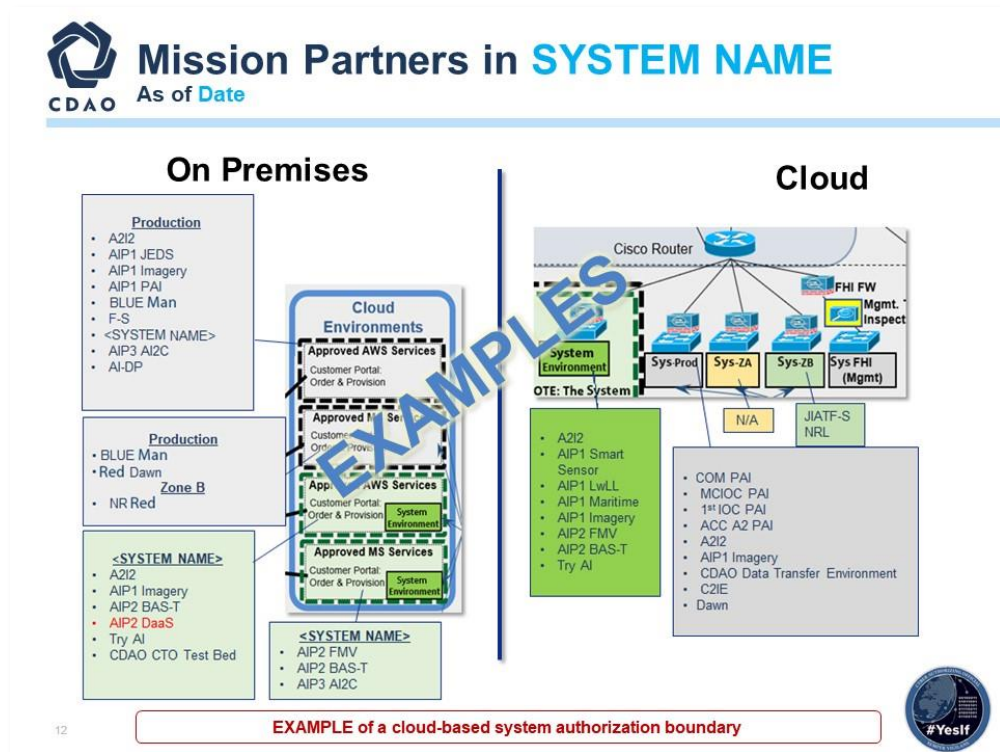
- **Reference only; replace architecture.**
- The authorization boundary diagram must specifically identify what is included in the boundary. The AO risk acceptance determination will be strictly based on threat/vulnerability pairs identified within the specific boundary.
- The main purpose of this chart is an example of WHAT is in the boundary of the Authorization that the AO is being asked to assess and make a determination on, as shown by the RED dashed line (see the legend). What is IN the boundary of the authorization, and what is EXTERNAL to the boundary of the authorization?
- This chart is an example of an “Airplane Weapon System” boundary.

3.11 Authorization Boundary Continued




- **Reference only; replace with your capability's authorization boundary diagram.**
- This shows what is authorized. It should have a legend and be standard across all Tag Up Briefings. For example, this chart shows TWO authorizations, one in black dashes and one in green dashes. This should show the AO what is under their authorization. It should have a very clear line or box around the area that is within the ATO.
- Illustrates what the AO is responsible for with a key on the chart so that it is easily understood. This chart should be the same in the AO determination briefing (or should be at that point in time, and then we monitor change from that point forward).

3.12 Mission Partners



- **Reference only; replace with your capabilities mission partner chart.**
- In this case, this program shows a second chart to outline the workloads within the system.
 1. Note that this is a second authorization boundary chart with more detail.
 2. It is the Operational View of how the capability is being used and the 18 different workloads inside the capability.
 3. It shows the various cloud zones of the capability (e.g., prod, ZA, ZB, etc.). This gives the AO and team an understanding of “how” the capability is being authorized and is being used.

3.13 Cyber Tech Order and Continuous Monitoring



Cyber Tech Order and Continuous Monitoring

Provide the status and location of the items listed in the table to the right.

Cyber Tech Order:

- Communicate the “How” to maintain systems for Secure Resiliency.
- Provide clear operating instructions for users and maintainers.
- Educate, enable, and execute.

Continuous Monitoring:


- Recognize that change is constant.
 - New vulnerabilities and threats appear every day.
 - Technology changes.
 - Mitigation effectiveness degrades over time.

Outline ALL cyber related process for the system/capability.
These represent the set of instructions/process that are used to sustain the system authorization, to have the COMMON and insight into the system risk posture.

1. Executive Abstract	(1 to 2 explanatory pages for roles & 2 pages max)
<ul style="list-style-type: none"> Secure and Resilient System Design Overview Secure and Resilient Operations Overview Secure and Resilient System Sustainment Overview 	
1. ATO Compliant Execution	(3 paras no more than 1 page + 1 para docx reference table)
<ul style="list-style-type: none"> Managing Operations in Accordance with the System Security Plan Actions or behaviors that can impact the ATO Reference Documentation 	
1. Training & Awareness	(Will engage SSR for applicable training references)
3.1 - Statement that Unit level (SSM/SSO/ Security Officer/ COMSEC Officer) responsible for ensuring training and awareness of entire unit.	
3.2 - Conducting Periodic System/network Operations Secure Practices Training	(Typically an introductory file or two referencing any mandated policy followed by practical tips guiding implementation. Will utilization of Top level instruction and guidance for outlining the unit's responsibility... same format for remaining sections)
4.1 - Maintaining Configuration Baselines	
4.2 - Updating for Malicious Code Protection virus/malware: code patches, GPOs, TCNOs, TCTOs, etc.)	(anti-)
4.3 - Performing Configuration and Change Management	
1. Monitoring Identity and Access	
<p>(Top level Statement with Unit level Security Officer/SSM/ Info Owners having first step of responsibility with Physical/Data SAAR access)</p>	
5.1 - Limiting Access to Authenticated Entities	
5.2 - Controlling System Access Requirements	
5.3 - Controlling Internal & Remote System Access	
5.4 - Controlling and Limiting Physical & Remote Data Access	
5.5 - Controlling and Limiting Data Access to only Authorized Users and Processes	
6. Maintaining Information	
6.1 - Controlling Communications at System Boundaries (PPS / HOSC / etc.)	
6.2 - Protecting Auditing/Monitoring Information	
6.3 - Managing Backups	
6.4 - Identifying and Marking Media	
6.5 - Protecting and Controlling Media Storage and Transport	
6.6 - Sanitizing & Destroying Media	
7. Continuous Improvement	
7.1 - Auditing/Monitoring Requirements	
7.2 - Configuring Auditing/Monitoring for Systems and Networks	
7.3 - Cyber Health Auditing/Monitoring	
7.4 - Reviewing and Managing Auditing Logs and Monitoring Tools	
7.5 - Monitoring Threats	
8. Incident Response and Reporting	
8.1 - The NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)	
8.2 - Conducting Incident Response Training Exercises	
8.3 - Identifying Risks and Protecting Capabilities and Services	
8.4 - Detecting and Responding to Incident and Events	
8.5 - Reporting a Potential or Declared Incident or Event	
8.6 - Recovering from an Incident or Event	
8.7 - Performing Post Incident/Event Reviews	

- Cyber Tech Order Overview: Provide a high-level overview of each component of the Cyber Tech Order, detailing how the organization has implemented and is maintaining alignment with these requirements.
- System Security Plan (SSP): Explain the security measures, controls, policies, and procedures outlined in the SSP to protect the system and its information assets from cybersecurity threats.
- Concept of Operations (CONOPS): Provide an overview of how the system is intended to operate, including roles and responsibilities related to cybersecurity, processes for handling incidents, and interactions with other systems or stakeholders.
- Cybersecurity Strategy: Discuss the overarching approach to cybersecurity, including goals, objectives, risk management strategies, and how these align with organizational objectives and industry best practices.
- Incident Response Plan (IRP): Describe the procedures, roles, and responsibilities for detecting, responding to, mitigating, and recovering from cybersecurity incidents affecting the system.
- Continuous Monitoring: Explain how continuous monitoring activities are conducted to detect and respond to cybersecurity threats in real-time, including monitoring tools, metrics, frequency, and reporting mechanisms.

3.14 CDAO ORTB




CDAO ORTB (1/2)
(Organizational Risk Tolerance Baseline)

1. **Account Management (Aligns to ORTB: AC-2)**
Monitor and Enforce user and group account creation/deletion
2. **Administrative Privileged Accounts (Aligns to ORTB: AC-6)**
Privileged user/service accounts are only authorized to perform security relevant functions. Review and approve annually.
3. **Audit Review, Analysis, and Reporting (Aligns to ORTB: AU-6)**
Review and analyze Information System (IS) audit logs for indications of inappropriate or unusual activity and reports findings to designated personnel IAW IRP
4. **Boundary Protection (Aligns to ORTB: SC-7)**
Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system
5. **Continuous Monitoring (Aligns to ORTB: CA-7)**
System level monitoring metrics, including control monitoring frequencies, are defined by the organization and approved by the AO
6. **Data Integrity (Aligns to ORTB: SI-7)**
Employ automated tools to report system (hw/sw/fw) and information (data) integrity violations. Ensure automatic integrity validation of all electronically transmitted software and data
7. **External Connections (Aligns to ORTB: SC-3)**
Agreement/authorization used to approve external connections and manage the exchange of information should be defined (ATC, ISA, CSA, ICD, etc.) and reviewed annually
8. **External Media (Aligns to ORTB: AC-4, MP-7)**
If authorized, place configuration control process on all external media including auditing. Institute external media whitelisting. Implement processes to monitor logs and audit usages.
9. **Information Flow Enforcement (Aligns to ORTB: AC-4)**
The information system enforces approved connections for controlling the flow of information within the system and between interconnected systems

10. **Least Privilege (Aligns to ORTB: AC-6)**
Reviews, at least annually, the privileges assigned to privileged user accounts including Designated Transfer Agent and Trusted Cloud Credential Manager roles
11. **Operational Change Mgmt (Aligns to ORTB: CM-8, CM-8(3), SI-7)**
Automated mechanisms shall be used to detect the presence of unauthorized hardware/software/firmware within the system. One or more of the following action shall be taken upon discovery of unauthorized components: disable network access by unauthorized components; isolate unauthorized components; notify designated personnel identified in IRP
12. **Proposed Equipment (Aligns to ORTB: SA-22 – applies to C.I.A. impact High on non-SAP systems, CM-3)**
Lock down all mission support systems and migrate off unsupported operating systems. Review support agreements (hw/sw/fw) annually
13. **Protection of Information at Rest (Aligns to ORTB: SC-28, SC-28(1))**
Encryption is implemented to complement protection of information at rest, using approved cryptographic methods for data encryption
14. **Secure Baseline Configuration (Aligns to ORTB: CM-2, CM-6)**
This Information System's secure configuration includes DoD Security Technical Implementation Guides or industry best practices and verified conformance prior to introduction into production or operational environments
15. **Security Categorization (Aligns to ORTB: RA-2)**
Enforce proper security categorization and review annually
16. **Separation of Duties (Aligns to ORTB: AC-5)**
Separates defined duties of individuals and documents separation of duties of individuals
17. **Vulnerability / Anti-Virus Scanning (Aligns to ORTB: RA-5)**
Conduct routine anti-virus scans on traditional IT systems and hosted applications. Institute continuous monitoring protection on all IT systems to include maintenance and testing support systems


*Red font indicates specific JSIG, Non-Tailorable controls

Foundational ORTB



- ORTB Overview: Provide an overview of the approach taken to assess and address each identified security control, including whether they have been Implemented, Partially Implemented, Not Implemented, or are Not Applicable.
- It is recommended that you break each control into their own slide to break down whether that control has been satisfied and how.
- Be sure to generate a legend showing the colors used to determine implementation status (e.g., green for Implemented, yellow for Partially Implemented, red for Not Implemented, purple for Not Applicable).

3.15 CDAO ORTB – AI View



CDAO ORTB – AI View (2/2)

(Organizational Risk Tolerance Baseline)

Cyber risks for AI are not new. AI risks are inherently covered by the CDAO ORTB. Each of the AI-Specific Views below tie back to multiple ORTB risks numbers noted on slide 1 of 2.

AI Foundation (Aligns to CDAO ORTB: 4/5/6/13/17)

- Encrypt any stored AI-related data and models
- Regularly patch AI components (hardware and software) on known vulnerabilities and update threat definitions
- Account for vetting of AI supply chain

Data Integrity (Aligns to CDAO ORTB: 4/6/9/11/17)

- Depict provenance and lineage of datasets used for training models
- Implement mechanisms that ensures the integrity and authenticity of ingested data against adversarial attacks.
- Ensure privacy of personal data, anonymizing information where necessary
- Establish data retention and disposal mechanisms

Model Management (Aligns to CDAO ORTB: 3/4/11/17)

- Depict architecture, justification, and rationale for the selection of a specific model
- Establish regular evaluation and validation procedures of training models
- Ensure rollback mechanism for models, configurations, and training data

Operational Resilience (Aligns to CDAO ORTB: 3/5/14/17)

- Regularly employ red teaming testing methodologies and maintain logs of outcomes
- Continuously monitor system performance metrics against predefined benchmarks or thresholds for validation

User Interaction (Aligns to CDAO ORTB: 1/2/10/16)


- Incorporate mechanisms for users or other stakeholders to provide feedback on model output
- Implement oversight on user interactions, including data input, queries, and code base changes

Responsible Accountability (Aligns to CDAO ORTB: NEW)

- Implement tools and/or methodologies that can elucidate model decisions
- Implement DoD Responsible AI (RAI) Principles

15


Foundational ORTB



- **ORTB AI Overview:** Explain whether each focus point has been Implemented, Partially Implemented, Not Implemented, or is Not Applicable to your organization’s AI initiatives.
- **AI Foundation:** Describe the foundational principles and policies in place to govern AI development, including ethical considerations and alignment with organizational goals.
- **Encryption:** Discuss encryption methods used to protect AI data and models, including encryption standards and practices for data at rest and in transit.
- **Regularly Patch AI Components:** Detail how AI components are regularly updated with security patches and updates to mitigate vulnerabilities and ensure system integrity.
- **Account Vetting:** Explain how user accounts are verified and authenticated to ensure only authorized access to AI systems and data.
- **Data Integrity:** Outline measures and controls implemented to verify and protect the accuracy and reliability of data used in AI models and applications.
- **Model Management:** Detail the process for model development, testing, deployment, monitoring, and retirement, including version control and model performance evaluation.
- **Operational Resilience:** Discuss strategies and contingency plans to maintain AI system functionality during disruptions or incidents, ensuring continuity of operations.
- **User Interaction:** Explain user interface design, usability considerations, and user feedback mechanisms to enhance user experience and optimize AI system interaction.

- Responsible Accountability: Outline governance frameworks, accountability measures, and transparency practices to address ethical, legal, and societal implications of AI deployment.
- It is recommended that you break each control into their own slide to break down whether that control has been satisfied and how.
- Be sure to generate a legend showing the colors used to determine implementation status (e.g., green for Implemented, yellow for Partially Implemented, red for Not Implemented, purple for Not Applicable).

3.16 CDAO ORTB Controls



CDAO ORTB
(Organizational Risk Tolerance Baseline)

<ORTB Control>

ORTB Control Status | <Implemented / Partially Implemented / Not Implemented / Not Applicable>

<Describe the ORTB Control Text description and Supplemental Guidance>

<ORTB Control>

ORTB Control Status | <Implemented / Partially Implemented / Not Implemented / Not Applicable>

<Describe the ORTB Control Text description and Supplemental Guidance>


Legend:

Green Text – Fully Implemented

Orange Text – Partially Implemented

Red Text – Not Implemented

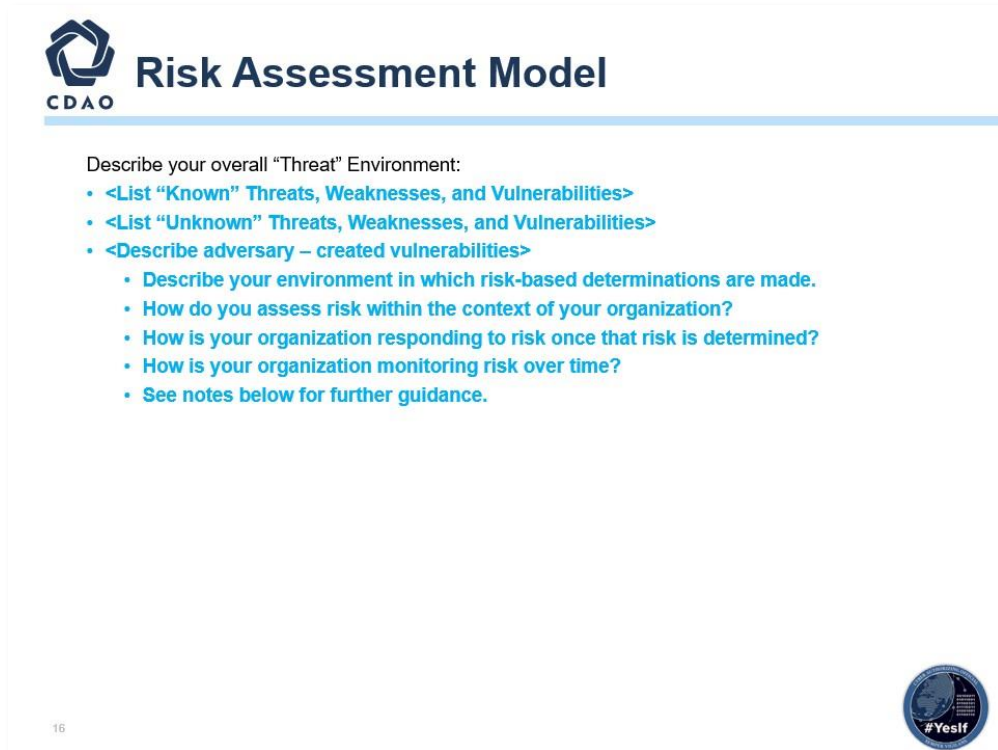
Blue Text – Not Applicable



16

- Use this slide as a template to list the status of the applicable ORTB controls being implemented within the capability. Please duplicate as many times as needed to address applicable controls.

3.17 Risk Assessment Model



The slide features the CDAO logo in the top left corner. The title "Risk Assessment Model" is centered at the top. Below the title, the text "Describe your overall 'Threat' Environment:" is followed by a bulleted list of instructions. A circular seal with the text "#YesIf" is located in the bottom right corner. The number "16" is in the bottom left corner.

Risk Assessment Model

Describe your overall "Threat" Environment:

- <List "Known" Threats, Weaknesses, and Vulnerabilities>
- <List "Unknown" Threats, Weaknesses, and Vulnerabilities>
- <Describe adversary – created vulnerabilities>
 - Describe your environment in which risk-based determinations are made.
 - How do you assess risk within the context of your organization?
 - How is your organization responding to risk once that risk is determined?
 - How is your organization monitoring risk over time?
 - See notes below for further guidance.

16

#YesIf

- Refer to *NIST SP 800-30 DoD Risk Assessment Guide Task 2.3.1*.
- Risk models define the risk factors to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determine levels of risk in risk assessments. Risk factors are also used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition. Risk factors can be decomposed into more detailed characteristics (e.g., threats decomposed into threat sources and threat events).
 1. The purpose of the risk framing component is to produce a risk management strategy that addresses how your organization intends to assess risk, respond to risk, and monitor risk, making explicit and transparent the risk perceptions that your organizations routinely use in making both investment and operational decisions. The risk management strategy establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.
 2. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood

that harm will occur. The result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

3. The purpose of your organization's risk response component is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action.
4. The purpose of your risk monitoring component is to: (i) determine the ongoing effectiveness of risk responses (consistent with the organizational risk frame); (ii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate; and (iii) verify that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

3.18 Assessment Approach



Assessment Approach

- **Assessment Details:** <Provide details of verification testing performed; who, what, when, where i.e., virtual or onsite>.
 - Organization conducting verification testing.
 - Day/Month/Year.
 - Test Plan/Location <Include Test Plan with brief>.
- **Risk:** <Describe risk approach>.
 - The risk approach should be supported by a series of security standards, best practices and guidelines necessary for managing information security risk.
- **Analysis:** <Insert analysis approach>.
 - Analysis approaches differ with respect to the orientation or starting point of the risk assessment, level of detail in the assessment, and how risks due to similar threat scenarios are treated. An analysis approach can be: (i) threat-oriented; (ii) asset/impact-oriented; or (iii) vulnerability-oriented.

17



Assessment Approach (Cont.)

- **Assumptions/Constraints:** <Identify assumptions or constraints during risk assessment>.
 - As part of the risk management process, your organization must make explicit the specific assumptions, constraints, risk tolerance, and priorities/trade-offs used within your organization to make investment and operational determinations.
- **CRA Confidence Level:** <Identify based on evidence from Body of Evidence (BOE) and/or site visit>.
 - Low: Incomplete/inaccurate BOE; System unavailable during site visit.
 - Moderate: Unable to visit site to conclude that security is implemented as documented. Relied on provided evidence.
 - High: Project Management Office (PMO) provided Pre-Risk Assessment Evidence; Onsite or Virtual validation successful.


18



- **Reference *NIST SP 800-30 Rev1; NIST SP 800-53 Rev4; NIST SP 800-39; CNSSI 4009-2015.***
- First and foremost, **THINK OUTSIDE OF THE BOX!** Do not rely on a checklist approach when conducting your analysis and assessments.
- Leveraging the tools and resources available to you via the RMF will ensure you are mitigating the necessary risks from a DoD standard, but you **MUST** always examine each assessment individually and ensure it is properly tailored to meet the amount of security that makes the most strategic and mission sense moving forward.
 - a. How?
 - Analysis approaches differ with respect to the orientation or starting point of the risk assessment, level of detail in the assessment, and how risks due to similar threat scenarios are treated. An analysis approach can be (i) threat-oriented, (ii) asset/impact-oriented, or (iii) vulnerability-oriented.
 - b. Why?
 - A threat-oriented approach starts with the identification of threat sources and threat events and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent.
 - An asset/impact-oriented approach starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying threat events that could lead to and/or threat sources that could seek impacts or consequences.
 - A vulnerability-oriented approach starts with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environments in which the systems operate and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised. Each analysis approach takes into consideration the same risk factors and thus entails the same set of risk assessment activities, albeit in a different order.
 - Differences in the starting point of the risk assessment can potentially bias the results, causing some risks not to be identified. Therefore, identification of risks from a second orientation (e.g., complementing a threat-oriented analysis approach with an asset/impact-oriented analysis approach) can improve the rigor and effectiveness of the analysis.

- c. CRA Recommendation:
- Based on the Body of Evidence provided, the CRA must be able to summarize risk assessment results in a form enabling decision makers to quickly understand the overall risk while considering the number of threat events for different combinations of likelihood and impact and the relative proportion of threat events at different risk levels.


3.19 Cyber Test Schedule



Cyber Test Schedule


System Name	Testing Entity	SYSTEM NAME Environment	Status	Start Date	End Data

Identify all cyber-related testing that provides insight in the risk posture



- Detail any Capability testing that is projected to occur (e.g., Tabletop exercises, Penetration Testing, etc.).

3.20 PenTest Schedule




PenTest Schedule

- <Provide stakeholder agreed upon Testing Schedule in support of this specific effort.>
 - Pen Test Playbook (Vendor Dependent).
- <Insert Schedule>
 - <If testing has been completed, provide results via appropriate channels.>

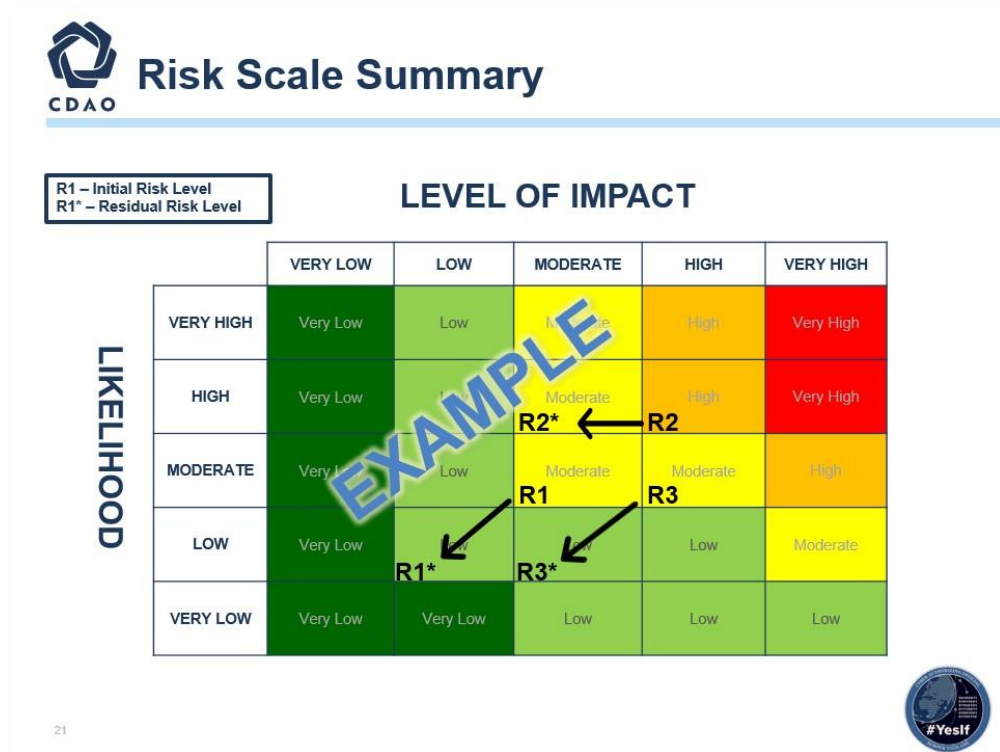
System Name	Environment	Status	Start Date	End Date

Persistent Pen Testing is key to having continuous COMMON




- This chart and the next chart will show what Pen Tests or other tests are planned and when. There is a holistic site picture.
- This could also be augmented by a traditional schedule view.
- Provide stakeholder agreed upon Testing Schedule in support of this specific effort.
- If testing has been completed, provide results via appropriate channels.
- Please see *NIST SP 800-115, Technical Guide to Information Security Testing and Assessment*.**
- A Penetration Test, also known as a “Pen Test” or “Ethical Hacking,” is an authorized, simulated cyberattack on an Information System performed to evaluate the security state of the system.
- Pen Testing is an augmentation to the overall risk assessment and continuous monitoring.
- Coordinate and schedule with your contracted Pen Testing team to ensure that you are getting your Information System Pen Testing accomplished and that the findings of the Pen Test are published to the organization and are submitted as part of the Authorizing Official’s required Body of Evidence.
- Penetration Testing usually relies on performing both network port/service identification and vulnerability scanning to identify hosts and services that may be targets for future penetration. Also, multiple technical ways exist to meet an assessment requirement, such as determining whether patches have been applied properly.

3.21 Risk Scale Summary




- **Reference only; replace with your program's Risk Scale Summary diagram.**
- Show initial risk and residual risk after mitigation.
- This table is from the *DoD Risk Assessment Guide* based on *NIST SP 800-30*, but **reference *NIST SP 800-39, Managing Information Security Risk* to determine Level of Impact.**

3.22 Risk Analysis Report



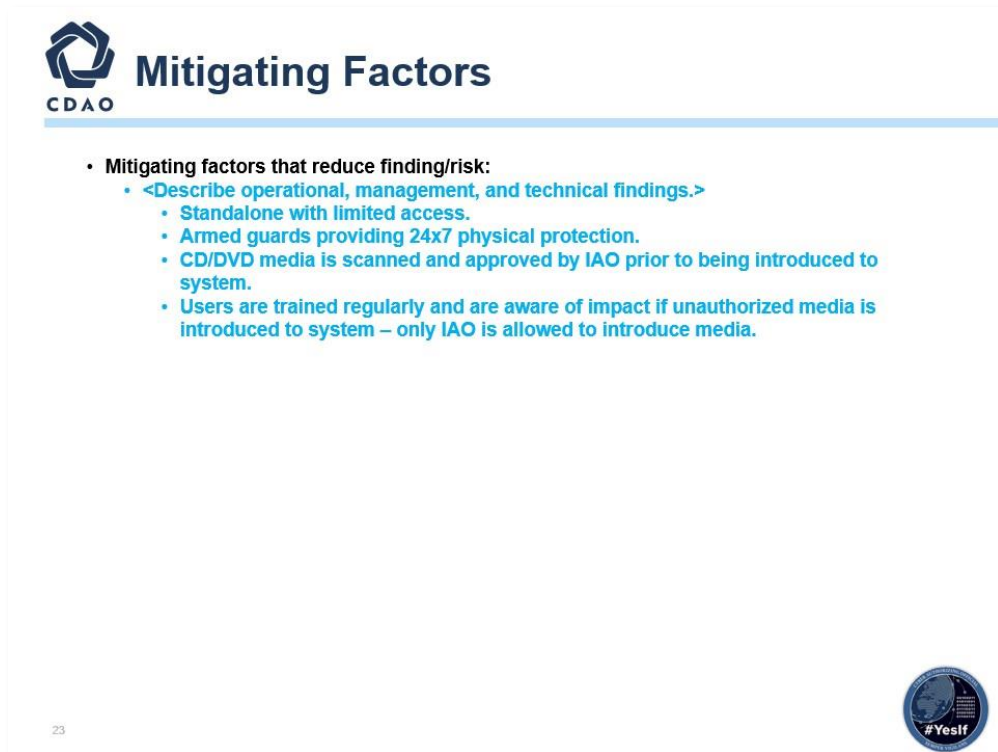
Risk Analysis Report

Risk # R1	Area of Concern (xxx)	Mechanisms (xxx)	Initial Risk Level (xxx)
<i>Threat:</i> <Describe the specific threat/threats that can potentially exploit this vulnerability.>			
<i>Vulnerability:</i> <Describe the vulnerability.>			
<i>Likelihood:</i> <What is the likelihood? Describe the likelihood of the vulnerability being exploited. Use means and opportunity.>			
<i>Impact:</i> <What is the impact? Describe the impact of the vulnerability being exploited. Use criticality and impact.>			
<i>Mitigations In Place:</i> <Describe the mitigations already in place.>			
ADDITIONAL MEASURES APPLIED TO THE SYSTEM			
<i>Countermeasures Added:</i> <Describe additional mitigations to lower the likelihood or impact of this vulnerability being exploited.>			
<i>Residual Risk:</i> <If mitigations in place and or added countermeasures lowered the likelihood or impact, then the residual risk level could be lowered.>			Residual Risk (xxx)
<i>Additional Countermeasures Suggested:</i> <What further actions will be taken to reduce likelihood/impact in the future?>			

22


- **Reference only; replace with your program's Risk Analysis Report.**
- **Reference *NIST SP 800-30 Rev.1*.**
- This is the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security risks planned or in place. Synonymous with risk analysis.

3.23 Mitigating Factors



The slide features the CDAO logo and title at the top. It lists mitigating factors for a finding, with a sub-header in blue text. The factors are bulleted and include specific security measures. A small circular seal with the text '#YesIf' is in the bottom right corner. The number '23' is in the bottom left corner.

Mitigating Factors

- Mitigating factors that reduce finding/risk:
 - <Describe operational, management, and technical findings.>
 - Standalone with limited access.
 - Armed guards providing 24x7 physical protection.
 - CD/DVD media is scanned and approved by IAO prior to being introduced to system.
 - Users are trained regularly and are aware of impact if unauthorized media is introduced to system – only IAO is allowed to introduce media.

23

#YesIf

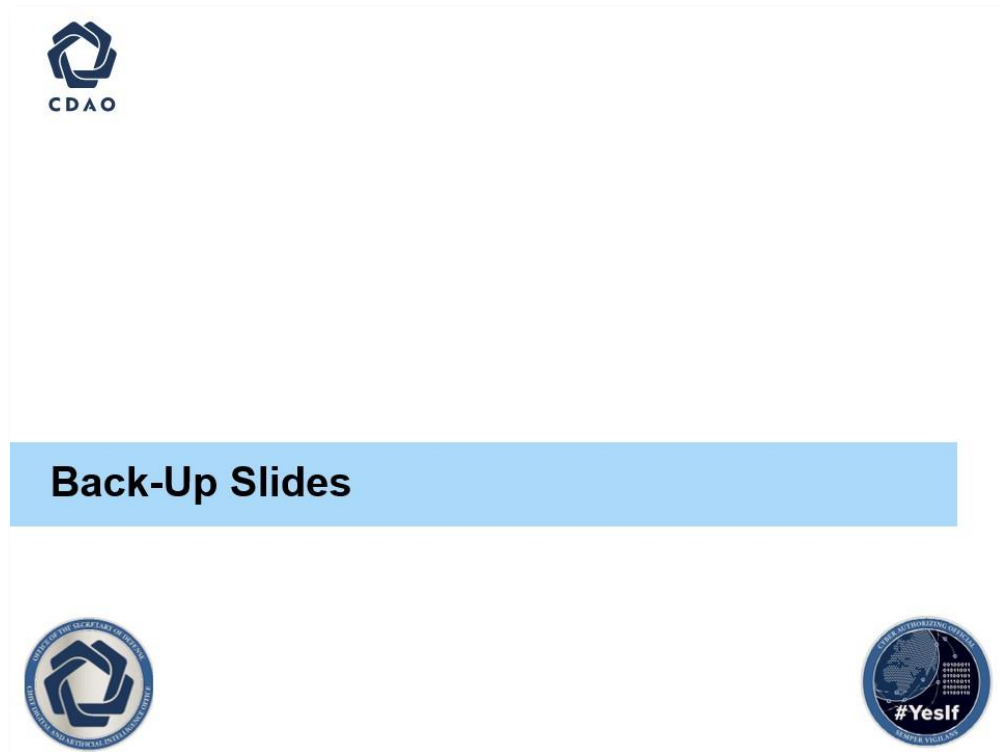
- You have identified the risks; now explain how to mitigate each of the findings.
- Reference *NIST SP 800-39, Managing Information Security Risk* (i.e., Scan Results, Penetration Test Findings, PPSM).

3.24 Summary




- This is the summary template chart.
- The intent is for a program to add its own summary here.
- **NOTE: this is not the AO summary; the CRA is to add their own summary.**

3.25 Backup Slides



- Provide any additional information in the backup slides as needed.


3.26 Impact Level Comparison



Impact Level Comparison

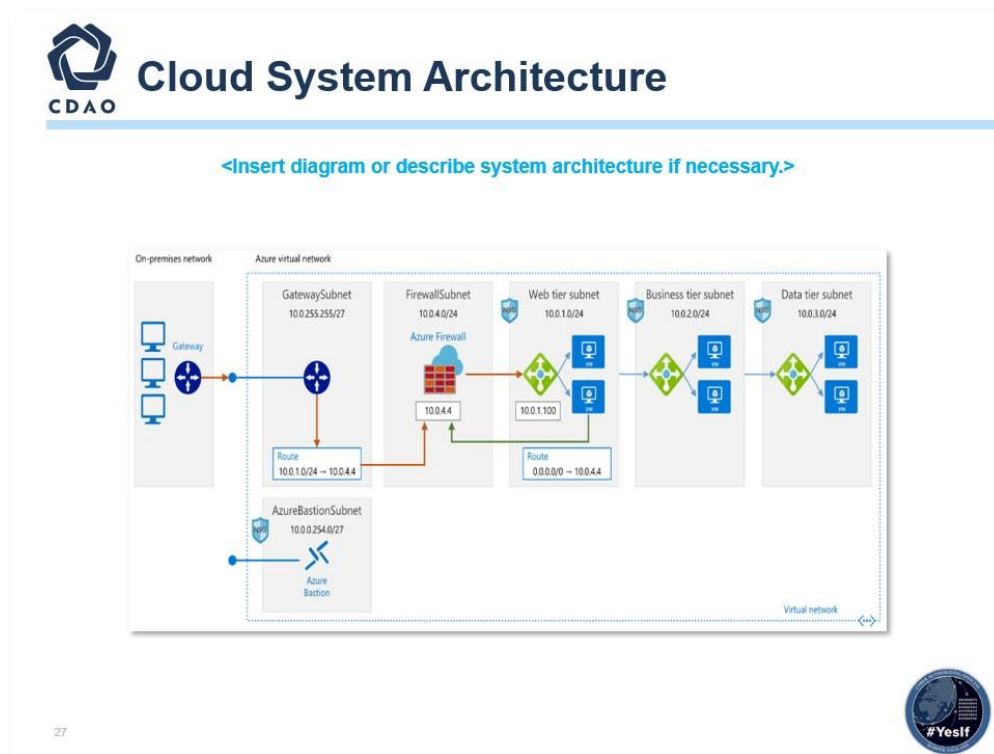
<Note: Remove this slide prior to presenting brief.>

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

26


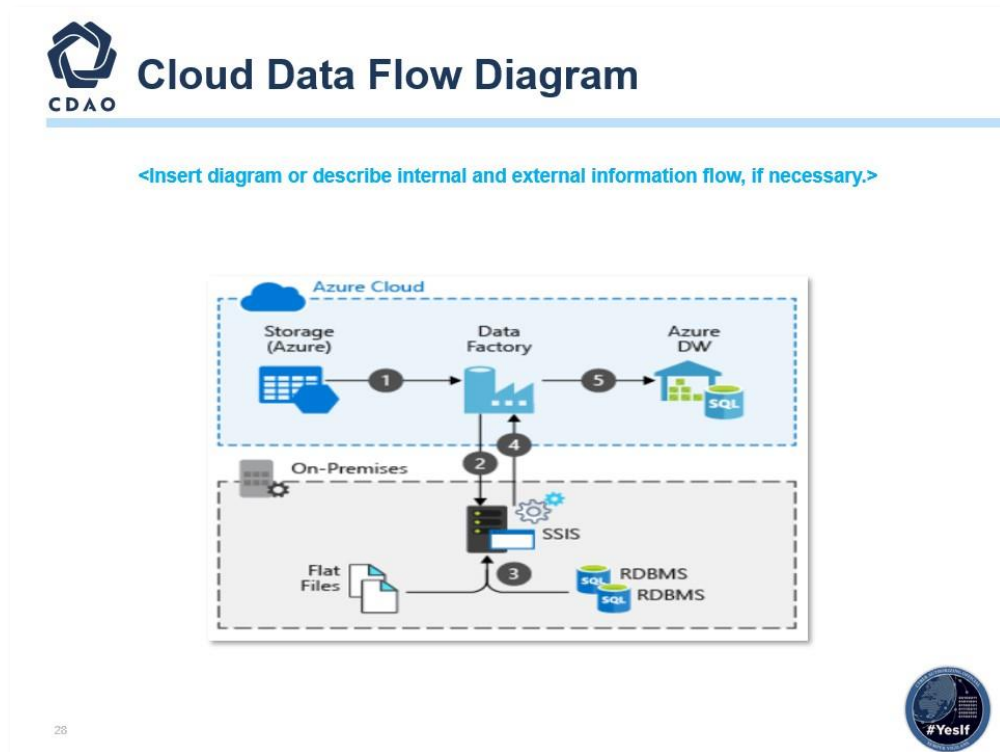
- Reference only; remove slide before submission.
- Reference “DoD Cloud Computing SRG v1 Rev 3, Section 3.2 Information Impact Levels” for further guidance.

3.27 Cloud System Architecture



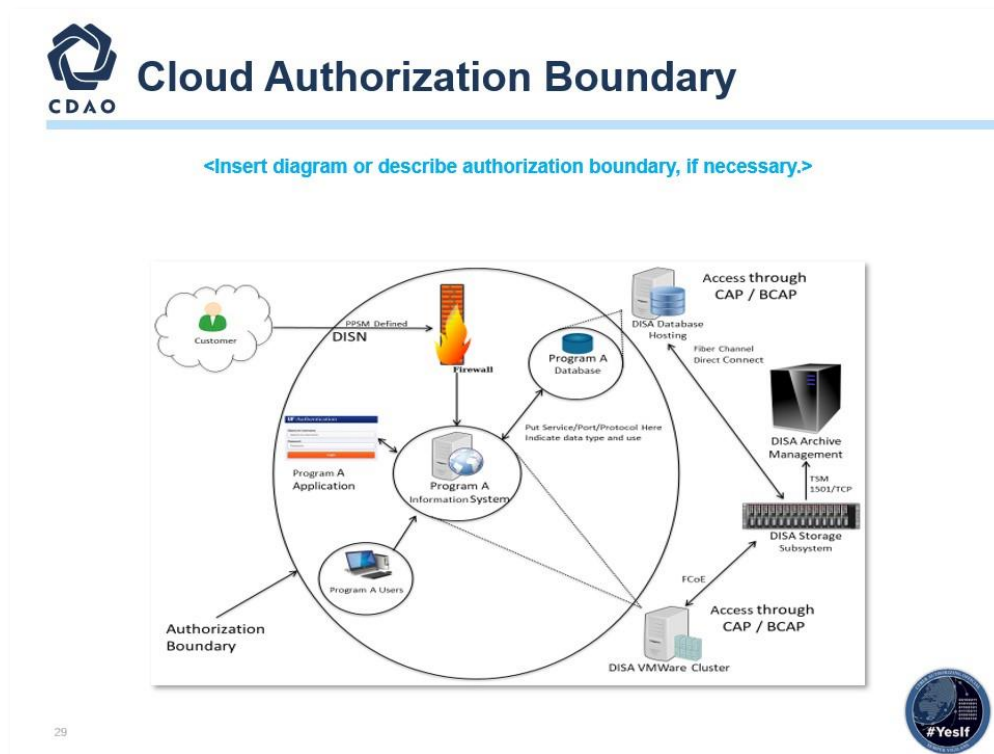
- **Reference only; replace architecture.**
- **Reference *DoD Secure Cloud Computing Architecture Functional Requirements (SCCA)*.**
- https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/SCCA_FRD_v2-9.pdf.
- The system architecture should show the AO what the architecture is, its physical location, encryption, interfaces and protocols, physical and technical protection mechanisms, vendor access, etc.
- Ensure you are showing your supporting infrastructure service(s) (IaaS, SaaS, PaaS), and show your Development Security Operations Platform (DSOP).
- A system architecture is the conceptual model defining the structure and behavior and supplying more views of a system. An architecture description is a formal description and representation of a system organized in a way that supports reasoning about the structures and behaviors of the system. Identify the architecture, locations, encryption, interfaces, protocols, physical and technical protection measures, vendor access, etc.

3.28 Cloud Data Flow Diagram



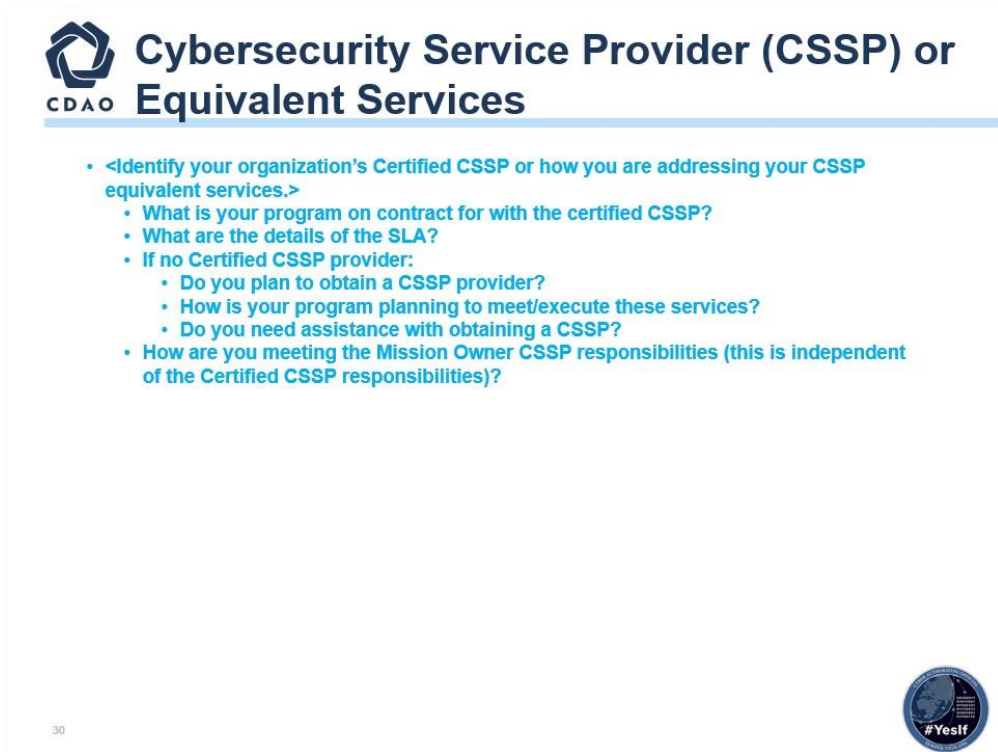
- Replace with your program's information systems data flow diagram.
- Reference *NISTIR 8179 Criticality Analysis Process Model*.
- <https://csrc.nist.gov/CSRC/media/Publications/nistir/8179/draft/documents/nistir-8179-draft.pdf>.
- The data flow diagram must specifically identify what the data flow connections look like within and while leaving the defined boundaries. The AO risk acceptance determination will be strictly based on threat/vulnerability pairs identified within the specific boundary.
- In computing, the path of data flows from source document to data entry, processing, and then final reports. Data changes format and sequence (within a file) as it moves from program to program. A data flow diagram is a way of representing a flow of data through a process or a system (usually an information system). The data flow diagram also provides information about the outputs and inputs of each entity and the process itself. A data flow diagram has no risk flow; there are no decision rules and no loops. Data flow diagrams are used to graphically represent the flow of data in a business information system. Data flow diagrams describe the processes involved in a system to transfer data from the input to the file storage and reports generation. Data flow diagrams can be divided into logical and physical. Data flow diagrams are built using standardized symbols and notation to describe various entities and their relationships.

3.29 Cloud Authorization Boundary



- Replace with your program's information system boundary diagram.
- Identify all areas to be included within the authorization determination. Any major component/device used within or by the system must be included in the boundary diagram unless the component/device has its own authorization (proof required).
- Interconnection(s)/Interface(s).
- **Reference NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems.**
- Include any/all Interconnection(s)/Interface(s) that would be leveraged – See below for further details.
- The intent of the ISA is to document and formalize the interconnection arrangements between "Organization A" and "Organization B" and to specify any details that may be required to provide overall security safeguards for the systems being interconnected. ISAs are always negotiable.
- General guidance regarding the contents of an ISA is provided below; however, an ISA may be tailored by mutual consent of the participating organizations.
- A system that has an interconnection with another organization's system should meet the protection requirements equal to or greater than those implemented by the other organization's system.


3.30 Cybersecurity Service Provider (CSSP) or Equivalent Services



CDAO Cybersecurity Service Provider (CSSP) or Equivalent Services

- <Identify your organization's Certified CSSP or how you are addressing your CSSP equivalent services.>
 - What is your program on contract for with the certified CSSP?
 - What are the details of the SLA?
 - If no Certified CSSP provider:
 - Do you plan to obtain a CSSP provider?
 - How is your program planning to meet/execute these services?
 - Do you need assistance with obtaining a CSSP?
 - How are you meeting the Mission Owner CSSP responsibilities (this is independent of the Certified CSSP responsibilities)?

30



- If you are providing your own services, please explain what services are being conducted and include what DISA support has been approved or needed.
- Per DoD Mandate 17-0019, DoDI 8530.01, you need a Cybersecurity Service Provider (CSSP), or your organization needs to be able to support similar services that meet the DoD requirements. CSSPs are required for both on-premises and Cloud information systems. Establish Cyber Defense (CD) services through one of the 23 DoD-certified CSSPs for Mission Cyber Defense (MCD).

3.31 Equivalent CSSP Services



Equivalent CSSP Services

CSSP services include but are not limited to:


- External Vulnerability Scans (EVS)
- Web Vulnerability Scanning (WVS)
- Malware Notification Protection (MNP)
- Support and Training (S&T)
- Network Security Monitoring (NSM)
- Attack Sensing & Warning (ASW)
- Warning Intelligence (WI)
- Incident Reporting (IR)
- Incident response Support (IRS)
 - Volatile Data Analysis (VDA)
 - Forensic Media Analysis (FMA)
 - Reverse Engineering and Malware Analysis (RE/MA)
 - Cyber Hunt/Intrusion Assessment (IA)
 - Incident Response (IR)
- Sustainment & Configuration Management (SCM)
- HBSS or DoD approved equivalent Anti-Virus
- Port Whitelisting through DISA

<Note: Remove this slide prior to presenting brief.>

27



3.32 OVL Authorization Package



OVL Authorization Package

The authorization package consists of the Authorization Memo with four attachments: Determination Brief, Conditions, Capability Categorization Summary, and Select Body of Evidence (BOE).


Authorization Package

- Authorization Memo
 - Attachment 1 – AO Determination Brief
 - Attachment 2 – Conditions
 - Attachment 3 – Capability Categorization Summary
 - Attachment 4 – Select Body of Evidence


Body of Evidence
(Example listing, but not limited to)

- Plan of Actions and Milestones (POA&M)
- Cyber Tech Order *(Example list)*
 - * Concept of Operations (CONOPS)
 - * Cybersecurity Strategy
 - * Incident Response Plan (IRP)
 - Continuous Monitoring Strategy
 - Contingency Plan
 - System Security Plan (SSP)
- Hardening Evidence
 - Security Technical Implementation Guide (STIG) Results
 - ACAS Scans
- Other evidence as required


Authorization Package




Body of Evidence



* = Minimum required documentation



3.33 SAP Protection Levels




SAP Protection Levels

<Note: If not Special Access Program, remove slide prior to presenting brief.>

Protection Level (PL)	Lowest Clearance	Formal Access Approval	Need-to-Know
PL-1	At Least Equal to Highest Data.	All users have ALL.	All users have ALL.
PL-2			Not all users have ALL.
PL-3		Not all users have ALL.	
PL-4	Secret	(Not contributing to decision)	
PL-5	Uncleared		

Lowest Clearance	Formal Access Approval	Need-to-Know	Protection Level
At Least Equal to Highest Data	All Users Have ALL	All Users Have ALL	1
At Least Equal to Highest Data	All Users Have ALL	NOT ALL Users Have ALL	2
At Least Equal to Highest Data	NOT ALL users have ALL	Not Contributing to Determination	3
Secret	Not Contributing to Determination	Not Contributing to Determination	4

<Note: Define the Protection Level to set the Risk Assessment Tolerance.>




- The concept of Protection Levels applies only to confidentiality. Having verified that an IS will maintain, process, or transmit intelligence information and therefore that its Level of Concern for confidentiality must be High, the AO will ascertain the appropriate Protection Level for the IS based on the required clearance(s), formal access approval(s), and need-to-know of all direct and indirect users who receive information from the IS without manual intervention and reliable human review. It indicates an implicit level of trust that is placed in the system's technical capabilities.
- Determining Protection Levels:
 1. An IS operates at Protection Level 1 when all users have all required approvals for access to all information on the IS. This means that all users have all required clearances, formal access approvals, and the need-to-know for all information on the IS.
 2. An IS operates at Protection Level 2 when all users have all required formal approvals for access to all information on the IS, but at least one user lacks administrative approval for some of the information on the IS. This means that all users have all required clearances and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the IS.
 3. An IS operates at Protection Level 3 when at least one user lacks at least one required formal approval for access to all information on the IS. This means that

all users have all required clearances, but at least one user lacks formal access approval for some of the information on the IS.

4. An IS operates at Protection Level 4 when at least one user lacks sufficient clearance for access to some of the information on the IS, but all users have at least a Secret clearance.
5. An IS operates at Protection Level 5 when at least one user lacks any clearance for access to some of the information on the IS.

3.34 SAP Body of Evidence



SAP Body of Evidence

<Note: If not Special Access Program, remove slide prior to presenting brief.>



- **Authorization Package (AO Responsibility)**
 - AO Determination Brief.
 - Authorization Memo:
 - Attachment 1 – Conditions.
 - Attachment 2 – BOE.
 - Attachment 3 – Signed ITCSC.

Body of Evidence (PM Responsibility)
(Example listing, but not limited to):


- POA&M.
- CONOPs.
- Cybersecurity Strategy.
- ConMon Plan.
- Incident Response Plan.
- Contingency Plan.
- SSP.
- SCTM.
- STIGs.
- ACAS Scans.
- Topology*.
- Hardware List*.
- Software List*.
- Security Technical Implementation Guide (STIG) applicability list.
- Ports, Protocols, and Service Matrix and registration number.
- Vulnerability scans (if applicable, analyzed and sated within 60 days of submission).
- STIG Compliance scans (if applicable, analyzed and dated within 60 days of submission).

* Items Marked can be included as part of the System Security Plan Or can be referenced in the AO Determination Briefing

Note: BOE Items Required to be in CORE folder prior to Authorization approval.



3.35 SAP Connection Package Required Documentation




SAP Connection Package Required Documentation

<Note: If not Special Access Program, remove slide prior to presenting brief.>


- Interconnection Security Agreement (ISA) signed by AO.
- Authorization to Operate - Signed by AO.
- Existing ISAs/ATCs and ATOs for other external connections.
- RAW Scan files (Nessus, XCCDF, etc.).
- Evidence that all scans were credentialed.
- Topology includes device function, OS, IP address, make/model.
- POA&M must include all CAT I and Critical findings from scans on all devices.

Note: BOE Items Required to be in CORE folder prior to Authorization approval.

36



3.36 SAP ORTB



SAP ORTB

Account Management (AC-2):

- Monitor and Enforce user and group account creation/deletion.

Administrative Privileged Accounts (AC-3):

- Privileged user/service accounts are only authorized to perform security-relevant functions. Review and approve annually.

Audit Review, Analysis, and Reporting (AU-6):

- Review and analyze Information System (IS) audit logs for indications of inappropriate or unusual activity, and report findings to designated personnel IAW IRP.

Boundary Protection (SC-7):

- Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.

Continuous Monitoring (CA-7):

- System-level monitoring metrics, including control monitoring frequencies, are defined by the organization and approved by the AO.

Least Privilege ((AC-6) AC-6(1); DoD JSIG Non-Tailorable Control):

- Reviews, at least annually, the privileges assigned to privileged user accounts including Designated Transfer Agent and Trusted Cloud Credential Manager roles.


Proposed Equipment ((SA-22) DoD JSIG Non-Tailorable Control):

- Lock down all mission support systems and migrate off unsupported operating systems. Review support agreements (hardware/software/firmware) annually.

Protection of Information at Rest ((SC-28) DoD JSIG Non-Tailorable Control):

- Encryption is implemented to complement the protection of information at rest, using approved cryptographic methods for data encryption.


<Note: If not Special Access Program, remove slide prior to presenting brief.>

37


- **Defer to Department of Defense (DoD) Joint Special Access Program (SAP) Implementation Guide (JSIG), 11 April 2016.**
- Cyber hygiene describes recommended mitigations for the small number of root causes responsible for many cybersecurity incidents. Implementing a few simple practices can address these common root causes.
- The final determination of the appropriate set of risk areas supported by the risk mitigations is necessary to harden the IS, and the environment in which those systems operate is a function of the assessment of risk and what is required to sufficiently mitigate the risks to the overall operations and assets, individuals, other organizations, and the Nation. In many cases, additional areas or enhancements will be required to address specific threats to and vulnerabilities in your organizations, mission/business processes, and/or information systems and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations. The risk assessment in the risk mitigation process provides essential information in determining the necessity and sufficiency of the risk areas and enhancements in the initial baselines.
 1. AC-2; Account Management - Information System (IS) account types are defined by the organization, and supporting mission and business functions are clearly defined.

2. AC-4; Information Flow Enforcement - The organization ensures that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.
3. AC-5; Separation of Duties - Obtains and examines the documented duties to ensure the organization defines the duties of individuals that are to be separated.
4. AC-6; Least Privilege - The organization obtains and examines the documented processes to ensure that the organization implements the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
 - **LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES** The organization: (a) Reviews at least annually the privileges assigned to privileged user accounts, including DTA role to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
 - AC-6(1), Enhancement for Least Privilege needs to be addressed.
5. AU-6; Audit Review, Analysis, and Reporting - The organization defines the frequency for the review and analysis of information system audit records for organization-defined inappropriate or unusual activity.
6. SC-7; Boundary Protection - Obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.
7. CM-6; Configuration Settings - Obtains and examines the documented process to ensure the organization monitors changes to the configuration settings in accordance with organizational policies and procedures.
8. RA-5; Vulnerability Scanning - Obtains and examines the contracts/agreements to ensure the organization requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.
9. SA-22, Unsupported System Components - Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and provides justification and documents approval for the continued use of unsupported system components required to satisfy mission and business needs.
10. SC-28, Protection of Information at Rest - Obtains and examines the documented information at rest to ensure the organization defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information.

3.37 SAP ORTB (Continued)



SAP ORTB (Cont.)

External Connections (CA-3):

- Agreement/authorization used to approve external connections and manage the exchange of information should be defined (ATC, ISA, CSA, ICD, etc.) and reviewed annually.

External Media (AC-4, MP-7):

- If authorized, place configuration control process on all external media including auditing. Institute external media whitelisting. Implement processes to monitor logs and audit usage.

Information Flow Enforcement (AC-4):

- The information system enforces approved connections for controlling the flow of information within the system and between interconnected systems.

Secure Baseline Configuration (CM-2, CM-6):

- This Information System's secure configuration includes DoD Security Technical Implementation Guides or industry best practices and verified conformance prior to introduction into production or operational environments.

Security Categorization (RA-2):

- Enforce proper security categorization and review annually.


Separation of Duties (AC-5):

- Separates defined duties of individuals and documents separation of duties of individuals.

Vulnerability/Anti-Virus Scanning (RA-5):

- Conduct routine anti-virus scans on traditional IT systems and hosted applications.

<Note: If not Special Access Program, remove slide prior to presenting brief.>

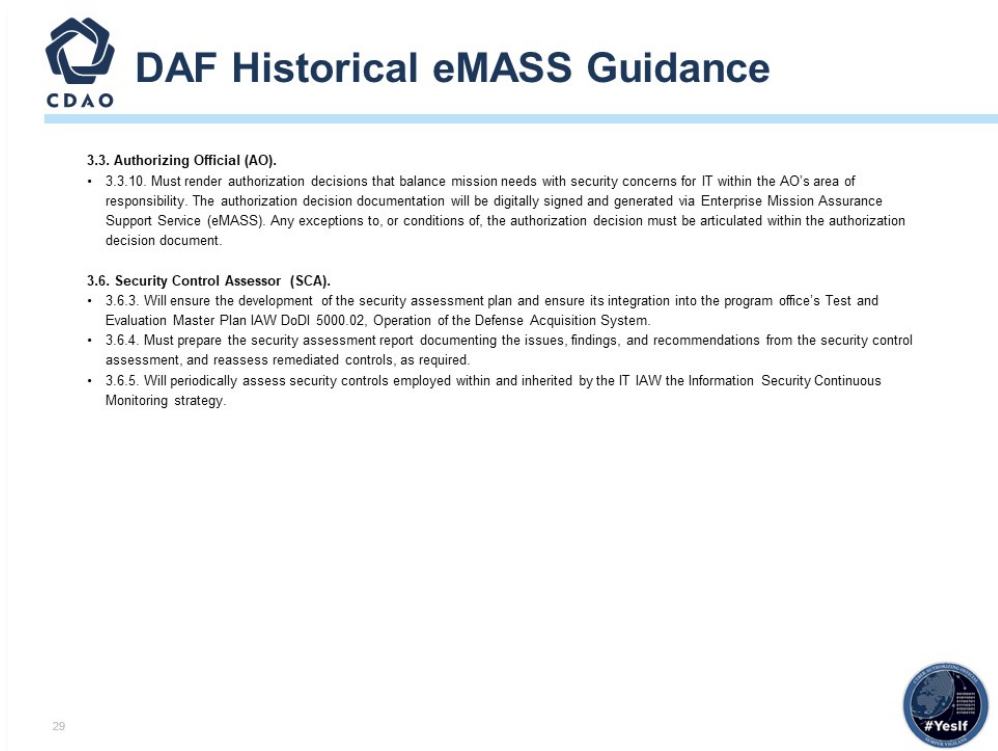
38


- **Defer to Department of Defense (DoD) Joint Special Access Program (SAP) Implementation Guide (JSIG), 11 April 2016.**
- Cyber hygiene describes recommended mitigations for the small number of root causes responsible for many cybersecurity incidents. Implementing a few simple practices can address these common root causes.
- The final determination of the appropriate set of risk areas supported by the risk mitigations is necessary to harden the IS, and the environment in which those systems operate is a function of the assessment of risk and what is required to sufficiently mitigate the risks to the overall operations and assets, individuals, other organizations, and the Nation. In many cases, additional areas or enhancements will be required to address specific threats to and vulnerabilities in your organizations, mission/business processes, and/or information systems and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations. The risk assessment in the risk mitigation process provides essential information in determining the necessity and sufficiency of the risk areas and enhancements in the initial baselines.
 1. AC-2; Account Management - Information System (IS) account types are defined by the organization and supporting mission and business functions are clearly defined.

2. AC-4; Information Flow Enforcement - The organization ensures that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.
3. AC-5; Separation of Duties - Obtains and examines the documented duties to ensure the organization defines the duties of individuals that are to be separated.
4. AC-6; Least Privilege - The organization obtains and examines the documented processes to ensure that the organization implements the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
 - **LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES** The organization: (a) Reviews at least annually the privileges assigned to privileged user accounts, including DTA role to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
 - AC-6(1), Enhancement for Least Privilege needs to be addressed.
5. AU-6; Audit Review, Analysis, and Reporting - The organization defines the frequency for the review and analysis of information system audit records for organization-defined inappropriate or unusual activity.
6. SC-7; Boundary Protection - Obtains and examines network topology diagrams, architecture documentation, or any other documentation identifying component partitioning to ensure the organization implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.
7. CM-6; Configuration Settings - Obtains and examines the documented process to ensure the organization monitors changes to the configuration settings in accordance with organizational policies and procedures.
8. RA-5; Vulnerability Scanning - Obtains and examines the contracts/agreements to ensure the organization requires that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.
9. SA-22, Unsupported System Components - Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and provides justification and documents approval for the continued use of unsupported system components required to satisfy mission and business needs.
10. SC-28, Protection of Information at Rest - Obtains and examines the documented information at rest to ensure the organization defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information.

4. ADDITIONAL DAF BACK-UP SLIDES

4.1 eMASS Guidance AFI 17-101



The slide is titled "DAF Historical eMASS Guidance" and features the CDAO logo in the top left corner. It contains two main sections: "3.3. Authorizing Official (AO)." and "3.6. Security Control Assessor (SCA).". The "3.3. Authorizing Official (AO)." section includes a bullet point stating that authorization decisions must be digitally signed and generated via Enterprise Mission Assurance Support Service (eMASS). The "3.6. Security Control Assessor (SCA)." section includes three bullet points detailing requirements for the security assessment plan, the security assessment report, and the periodic assessment of security controls. A small circular logo with the text "#YesIf" is located in the bottom right corner of the slide.

DAF Historical eMASS Guidance


3.3. Authorizing Official (AO).

- 3.3.10. Must render authorization decisions that balance mission needs with security concerns for IT within the AO's area of responsibility. The authorization decision documentation will be digitally signed and generated via Enterprise Mission Assurance Support Service (eMASS). Any exceptions to, or conditions of, the authorization decision must be articulated within the authorization decision document.

3.6. Security Control Assessor (SCA).

- 3.6.3. Will ensure the development of the security assessment plan and ensure its integration into the program office's Test and Evaluation Master Plan IAW DoDI 5000.02, Operation of the Defense Acquisition System.
- 3.6.4. Must prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment, and reassess remediating controls, as required.
- 3.6.5. Will periodically assess security controls employed within and inherited by the IT IAW the Information Security Continuous Monitoring strategy.

29





DAF Historical eMASS Guidance (Cont.)

3.10. Program Manager (PM).

- 3.10.5. Will ensure the IT is registered IAW AFI 17-110, Information Technology Portfolio Management and Capital Planning and Investment Control.
- 3.10.6. Will approve initial National Security System designations via the Information Technology Categorization & Selection Checklist for AF IT.
- 3.10.9. Ensures periodic reviews, testing, or assessment of assigned IT are conducted at least annually, and IAW the ISCM strategy.
- 3.10.10. Will ensure operational systems maintain a current authorization to operate and recommend to the AO that systems without a current authorization are identified for removal from operation.
- 3.10.11. Ensures all system changes are approved through a configuration management process, are assessed for cybersecurity impacts, and coordinated with the SCA, AO, and other affected parties, such as IOs/Stewards and AOs of interconnected boundaries.
- 3.10.12. Will manage the corrective actions identified in the plan of action and milestones, in order to provide visibility and status to the ISO, information owner, AO, and CISO in accordance with DoDI 8510.01.
- 3.10.13. Reports security incidents to stakeholder organizations and the SCA. Conduct root cause analysis for incidents and develop corrective action plans as input to the plan of action and milestones.

4.3. CATEGORIZE System.

- 4.3.8. The minimum set of documentation required in support of an RMF authorization decision is the security authorization package and consists of:
 - 4.3.8.1. The security plan
 - 4.3.8.2. The security assessment report
 - 4.3.8.3. The plan of action and milestones
 - 4.3.8.4. The authorization decision document



4.2 OVL AO eMASS Guidance



OVL AO eMASS Guidance

Authorizing Official

- Render authorization decisions that balance mission needs with security concerns for IT within the AO's area of responsibility. The authorization decision documentation will be digitally signed and generated via Enterprise Mission Assurance Support Service (eMASS) "or a like system."
- Any exceptions to, or conditions of, the authorization decision must be articulated within the authorization decision document.

Cybersecurity Risk Assessors (CRAs) (Per specific boundary requirements):

- Must prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment, and reassess remediated controls, as required.
- Will ensure the development of the security assessment plan and ensure its integration into the program office's Test and Evaluation Master Plan.
- Must prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment, and reassess remediated controls, as required.
- **Validate controls to support reciprocity and assist with uploading supporting evidence as needed.**
- **Provide and submit to the AO, a risk recommendation comprising:**
 - AO Determination Brief.
 - AO Authorization Memo.
 - CRA Risk Recommendation.
 - Plan of Action and Milestones.
 - IT Categorization and Selection Checklist.
 - Reference: Supporting Evidence.
 - DevSecOps Concept of Operation (CONOPs) (If Applicable).

31



OVL AO eMASS Guidance (Cont.)


The Program Managers:

- Will ensure the IT is registered (supporting evidence inclusive) and submitted to the CRA.
- Will approve initial National Security System designations via the Information Technology Categorization and Selection Checklist.
- Will ensure operational systems maintain a current authorization to operate and recommend to the AO that systems without a current authorization are identified for removal from operation.
- Ensures all system changes are approved through a configuration management process, are assessed for cybersecurity impacts, and coordinated with the CRA, AO, and other affected parties, such as IOs/Stewards and AOs of interconnected boundaries.
- Will manage the corrective actions identified in the Plan of Action and Milestones.
- Reports security incidents to stakeholders and the CRA.

32




4.3 Authorization Package




Authorization Package

- **Will document the key items needed for reciprocity:**
 - Authorization Memo.
 - Attachment 1 – Conditions.
 - Attachment 2 – Body of Evidence Attachment 3 – Plan of Action and Milestones.

- **Attachment 1 – Conditions:**
 - Documents any conditions on the ATO.
 - Security is a journey, never a destination.
 - Includes Risk-of-Use label to inform the consumer.
- **Attachment 2 – Body of Evidence:**
 - Key artifacts that supported the authorization.
 - Informs other AOs and Consumers to increase reciprocity.
- **Attachment 3 – Plan of Action and Milestones:**
 - Classified Appendix.



33


4.4 Authorization Determination Table



Authorization Determination Table

Authorization Type	Authorization Details	Documentation
ATO	The risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is acceptable.	<ul style="list-style-type: none"> • AO Determination Brief. • AO Authorization Memo. • CRA Risk Recommendation. • Plan of Action and Milestones. • IT Categorization and Selection Checklist. • Reference: Supporting Evidence.
ATO With Conditions (ATO-C)	The risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is acceptable, but conditions exist.	<ul style="list-style-type: none"> • AO Determination Brief. • AO Authorization Memo. • CRA Risk Recommendation. • Plan of Action and Milestones. • IT Categorization and Selection Checklist. • Reference: Supporting Evidence.
Continuous ATO (c-ATO) (Applied to DevSecOps ONLY)	Accredits the platform and process and certifies team that produces a product under a continuous monitoring process that maintains the residual risk within the risk tolerance of the Authorizing Official (AO).	<ul style="list-style-type: none"> • AO Determination Brief. • CRA Risk Recommendation. • CONOPs: platform, process, and teams. • IT Categorization and Selection Checklist. • Reference: Supporting Evidence.
IATT	Operational environment or live data is required to complete specific test objectives.	<ul style="list-style-type: none"> • AO Determination Brief. • CRA Risk Recommendation. • IT Categorization and Selection Checklist. • Certification Test Plan. • Reference: Supporting Evidence.

34



Authorization Determination Table (Cont.)

Authorization Type	Authorization Details	Documentation
Authorization to Use (ATU)	AO acceptance of risk in using cloud or shared services (system, service, or application) chooses to accept the system, service, or application in an existing authorization package produced by another organization. Authorization to use is a mechanism to promote reciprocity for systems under the purview of different AOs, based on a need to use shared systems, services, or applications.	<ul style="list-style-type: none"> • AO Determination Brief. • CRA Risk Recommendation. • Plan of Action and Milestones. • IT Categorization and Selection Checklist. • Reference: Supporting Evidence.
Certificate to Field (CTF)	Trustworthiness ensures no risks exist, either of malicious or unintentional origin. Predictable execution ensures there is a justifiable confidence that software, when executed, functions as intended.	<ul style="list-style-type: none"> • AO Determination Brief. • CRA Risk Recommendation. • Plan of Action and Milestones. • IT Categorization and Selection Checklist. • Reference: Supporting Evidence.
DATO	The information system is not authorized to operate.	<ul style="list-style-type: none"> • DATO Memo.

35

