Department of the Air Force

Integrity - Service - Excellence

Operation Vulcan Logic (OVL): Risk Management with Agility

Daniel C. Holtzman, HQE
Director, Cyberspace Innovation (A);
Cyber Technical Director;

Authorizing Official for:
JSF F-35 ALIS;
F-35 Cloud & DevSecOps;
DAF Cloud & DevSecOps
GBSD Cloud and DevSecOps;
Command & Control Systems;
Rapid Cyber Acquisitions (RCA);
Enterprise IT as a Service (EITaaS);
SAP Command and Control Systems;
SAP Rapid Cyber Acquisitions (RCA);
SAP Enterprise IT as a Service (SEITaaS)

6 December 2021
NDIA

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Operation Vulcan Logic

VULCANLOGIC@US.AF.MIL

Handout

OPERATION VULCAN LOGIC

Operation Vulcan Logic (OVL) is the operationalization of the DAF Fast Track process.

BACKGROUND:

[illegible]

PHASE 1

System/Systems Security Engineering Evidentiary Data & Analysis

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

Standard Acquisition Systems Engineering Data

PHASE 2

Collaboration with AO/CRA

- [illegible]

PHASE 3

Executive Risk Assessment

- [illegible]

PROGRAM MANAGEMENT

- Facilitate Risk management across SAF Acquisition, Operations & Sustainment

COLLABORATIVE EXECUTION

- Partnerships with PEO's, DOD, FAA, SAF [illegible]

ENABLERS

- Single, lead AO for each Weapon System
- Streamline expectations and increase Agility

FAST-TRACK ATO PROCESS: WHAT IS IT?

- [illegible]

CONTACT US: VULCANLOGIC@US.AF.MIL

OPERATION VULCAN LOGIC

COMMUNITY FEEDBACK

CRA Training – [illegible]

CRA Training – [illegible]

CRA Training – [illegible]

DSOP – [illegible]

DSOP – [illegible]

Fast Track – [illegible]

SAMPLE ONBOARDING MODULES

[illegible]

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Integrity - Service - Excellence

Agenda

- **Areas of Responsibility**
- **AF Authorizing Official Perspective**
- **Strategic Challenges/Initiatives**

Be around the light-bringers,
the magic makers,
the world shifters.

They challenge you,
break you open,
uplift and expand you.

They don’t let you play small
with your life.

These heartbeats are your people.
These people are your tribe.

- Danielle Doby

Areas of Responsibility (AOR)
Perspective across AF Weapon systems

AF
Cyber Technical Director
AFLCMC/EN

Cyber Security Engineering and Resilience (CSER) Senior Leader.

Technical authority for:

- Security engineering, cyber resiliency and systems, and mission assurance.
- Engineering resilient systems.
- Defensive security engineering.

AF
Authorizing Official,
SAF/CN

Authorization Boundaries:

- Cloud and DevSecOps.
- Command and Control Systems.
- SAP Command and Control Systems.
- Rapid Cyber Acquisition.
- SAP Rapid Cyber Acquisitions.
- Enterprise IT as a Service (EITaaS).
- SAP Enterprise IT as a Service (SEITaaS).
- F-35 (JSF); Cloud and DevSecOps.
- F-35 ALIS;
- Ground-Based Strategic Deterrent (GBSD); Cloud and DevSecOps.

AF
Director, Cyberspace
Innovation,
SAF/CN

- Innovation thought leadership of risk-based cyber security across the DAF (USAF and USSF).
- Accelerate DAF understanding and mastery of commercial best practices.
- Collaborate across Government, Industry, Allies, and Partners.
- Manage DAF technical standard setting and adoption process.
- Represent DAF/DoD interests in the international standard-setting process.

Data is current as of 01 May 2021.

Authorization Boundary at a Glance:
Cross-Section of Air Force Programs

CRC

- JADC2/ABMS
- Kessel Run/AOC
- Cloud One/Platform One
- E3 AWACS and JSTARS
- F-35 ALIS
- F-35 Cloud and DevSecOps
- GBSD Cloud and DevSecOps

E-3

- ShOC-N
- Wide-Area Surveillance
- RADSIL
- BACN
- ACBN
- C2IMERA

cUAS

- EITaaS
- SEITaaS
- RDT&E DREN
- NGAD
- Commercial UAS
- TORCC

TAC-P

- PRC2
- WaRTAK
- GCCS / DCGS
- Pocket-J
- TBMCS
- Mission Planning
- Special Programs

AOC

Authorizations as of 1 Nov 2021 = 260

Agenda

- **Areas of Responsibility**
- **AF Authorizing Official Perspective**
- **Strategic Challenges/Initiatives**

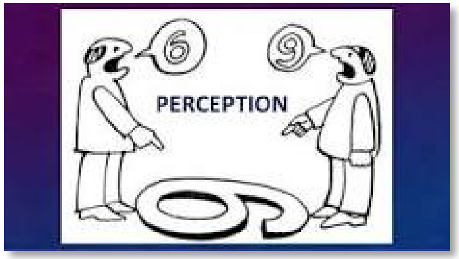
> Cyber Security
>
> and
>
> Resiliency
>
> is a journey,
>
> not a destination.

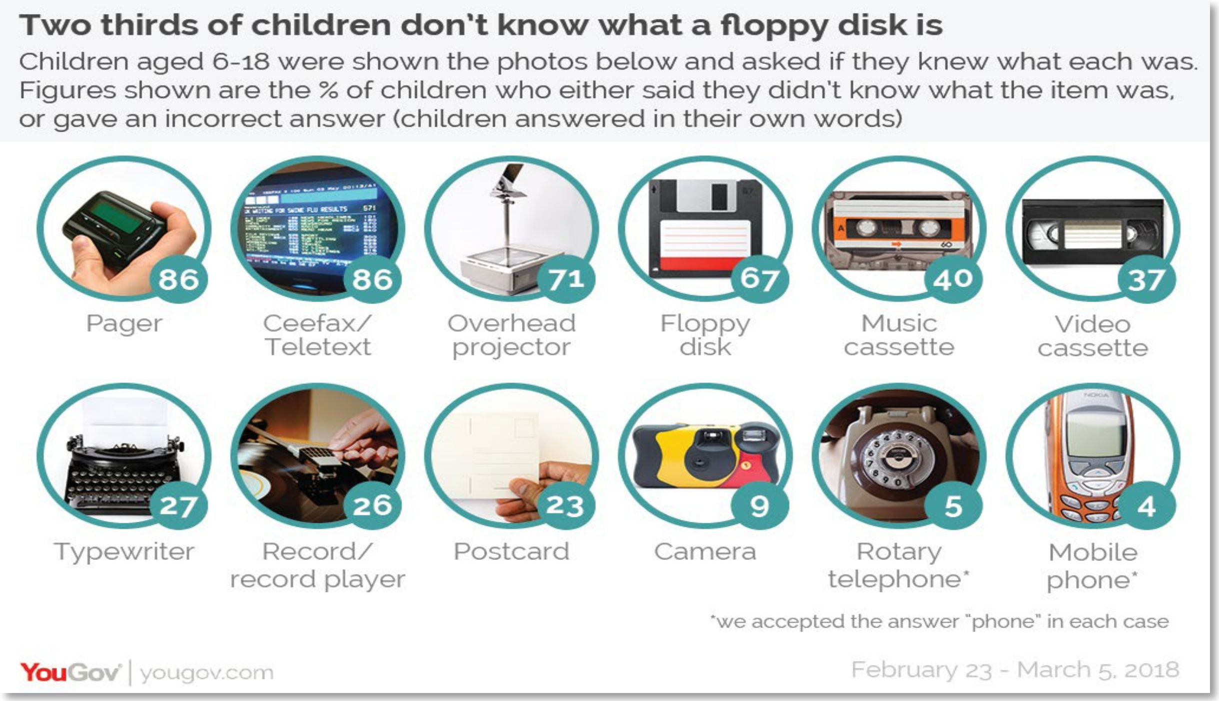
- D.C. Holtzman

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Culture Change Challenge
Unperceived Bias

“Cool, you 3D-printed the save icon!”





Two thirds of children don’t know what a floppy disk is

Children aged 6-18 were shown the photos below and asked if they knew what each was. Figures shown are the % of children who either said they didn’t know what the item was, or gave an incorrect answer (children answered in their own words)

Item	%
Pager	86
Ceefax/ Teletext	86
Overhead projector	71
Floppy disk	67
Music cassette	40
Video cassette	37
Typewriter	27
Record/ record player	26
Postcard	23
Camera	9
Rotary telephone*	5
Mobile phone*	4

*we accepted the answer “phone” in each case

YouGov | yougov.com

February 23 - March 5, 2018

Do you know the answers to these?

Do you realize your own bias?

Communication is key to culture change.

Change your thoughts and you change your world. ***– Norman Peale***

Authorizing Official North Star:
Exercising Agile Risk Management

- **Objectives:**
  - Render decisions faster: Being Transparent, foster reciprocity;
  - Enable Program Managers: More Secure Tomorrow than today;
  - Facilitate risk management: Acquisition, operations, and sustainment.
- **Enablers:**
  - Setting clear requirements: AO Determination Briefing;
  - Base Risk on Evidentiary analysis and data: Use Standard System Engineering:
  - Focus on Risk of Use: Operational-focused with enterprise view.
  - Move to Single AO for each weapon system: Streamline expectations & Seams.
- **Collaborative Execution:**
  - Cyber Risk Assessors (CRA) (formerly SCA) focus on assessing risks;
  - Authorizing Official informs decision makers on cyber risks;
  - Partnerships with PEOs, DOEs, PMs, users, and sustainers enable holistic view.

Increase decision-making agility by focusing on risk management.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

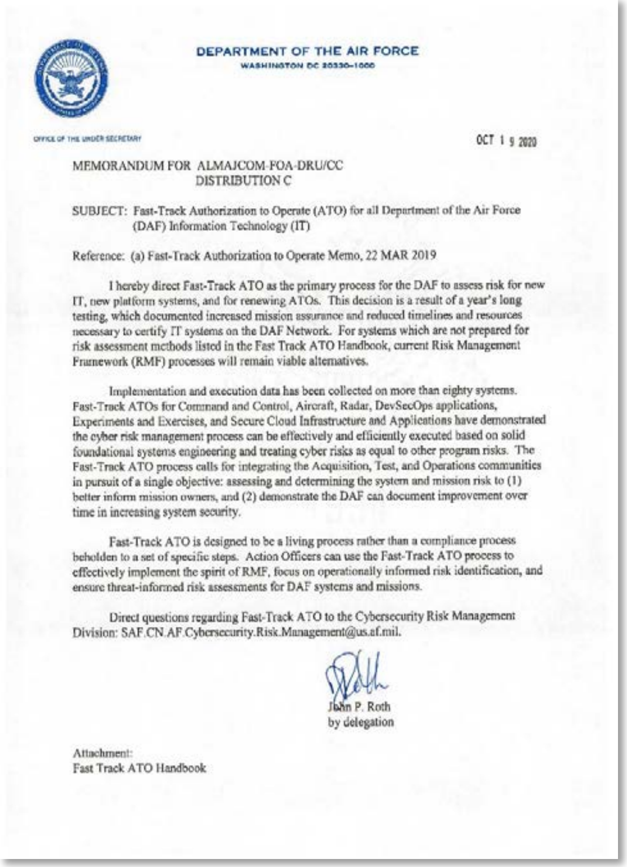
Fast-Track ATO Process: What Is It?

- Not a "new" process: Focus is on risk management.
- Complies with DOD 8510
- Provides AOs the ability to make risk-informed determinations: Spirit of RMF.
- Does not require anything "new" or compliance to a new process.

"The Fast-Track process gives [AOs] the discretion to make an authorization determination based on review of the combination of a Cybersecurity Baseline, an assessment (e.g., Penetration Test), and an Information Systems Continuous Monitoring Strategy.

"AOs are expected to make operationally informed risk determinations by working closely with information systems owners and warfighters to find the appropriate balance between rapid deployment and appropriate level of risk assessment."

- **Fast-Track is NOT an "easy" button; it requires robust systems engineering and "going slow to go fast."**



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330-1000

OFFICE OF THE UNDER SECRETARY

OCT 1 9 2020

MEMORANDUM FOR ALMAJCOM-FOA-DRU/CC
DISTRIBUTION C

SUBJECT: Fast-Track Authorization to Operate (ATO) for all Department of the Air Force (DAF) Information Technology (IT)

Reference: (a) Fast-Track Authorization to Operate Memo, 22 MAR 2019

I hereby direct Fast-Track ATO as the primary process for the DAF to assess risk for new IT, new platform systems, and for renewing ATOs. This decision is a result of a year's long testing, which documented increased mission assurance and reduced timelines and resources necessary to certify IT systems on the DAF Network. For systems which are not prepared for risk assessment methods listed in the Fast Track ATO Handbook, current Risk Management Framework (RMF) processes will remain viable alternatives.

Implementation and execution data has been collected on more than eighty systems. Fast-Track ATOs for Command and Control, Aircraft, Radar, DevSecOps applications, Experiments and Exercises, and Secure Cloud Infrastructure and Applications have demonstrated the cyber risk management process can be effectively and efficiently executed based on solid foundational systems engineering and treating cyber risks as equal to other program risks. The Fast-Track ATO process calls for integrating the Acquisition, Test, and Operations communities in pursuit of a single objective: assessing and determining the system and mission risk to (1) better inform mission owners, and (2) demonstrate the DAF can document improvement over time in increasing system security.

Fast-Track ATO is designed to be a living process rather than a compliance process beholden to a set of specific steps. Action Officers can use the Fast-Track ATO process to effectively implement the spirit of RMF, focus on operationally informed risk identification, and ensure threat-informed risk assessments for DAF systems and missions.

Direct questions regarding Fast-Track ATO to the Cybersecurity Risk Management Division: SAF.CN.AF.Cybersecurity.Risk.Management@us.af.mil.

John P. Roth
by delegation

Attachment:
Fast Track ATO Handbook

Fast-Track is a philosophy of focusing on the Risk of Use vs. compliance.

Cyber Security and Resiliency Enablers:
Systems Engineering

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 hardware (LRU) and software and the providences of each (e.g., supply chain); identify Critical Program Information (CPI), Critical Components (CC); technical orders, and operational procedures. Identify technologies being used.
4. Identify all external communications access points.
5. How does data flow into, through, and out of the system? What type of data? 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?

Establish the baseline from known data.

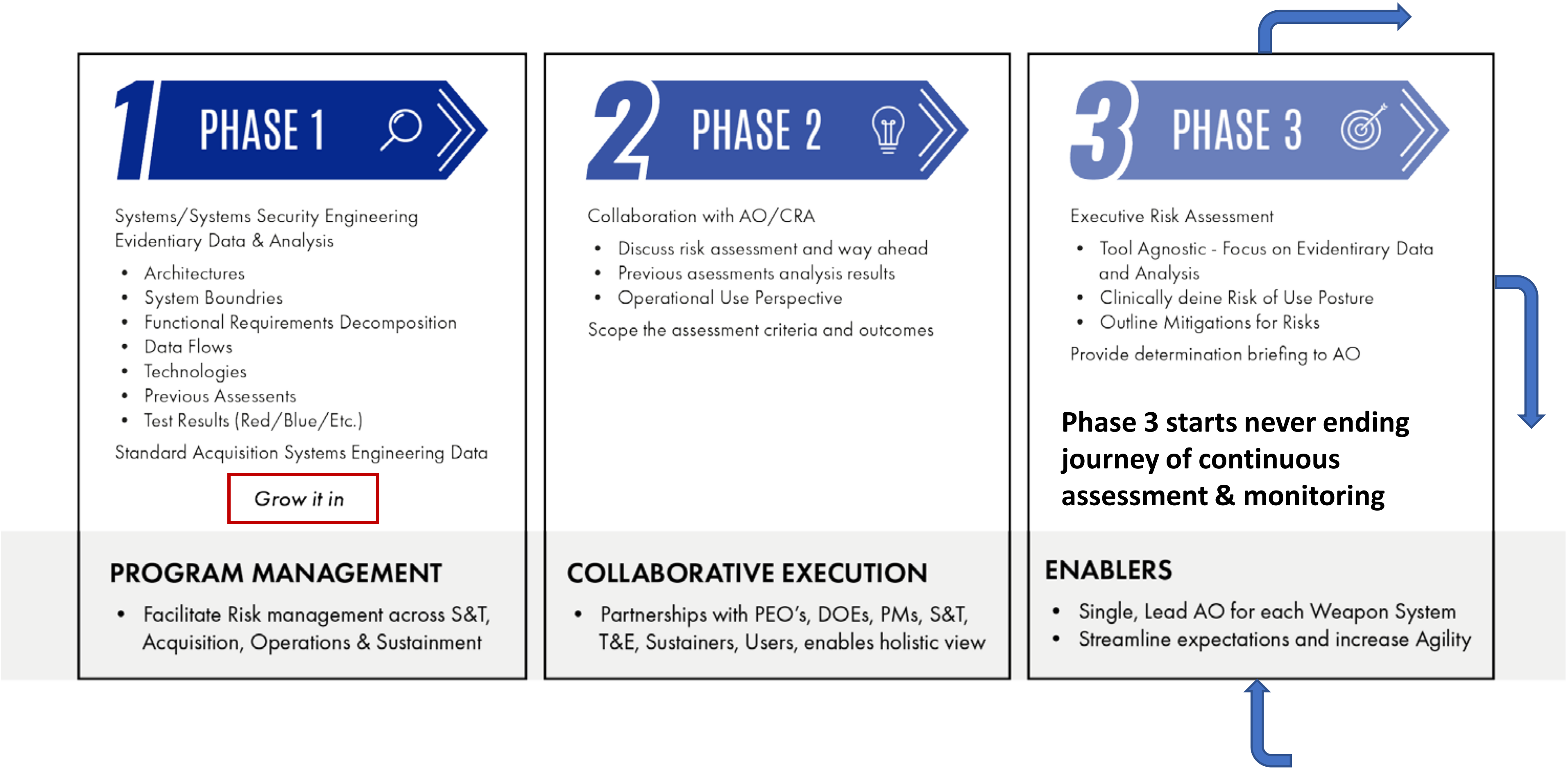
Cyber Security and Resiliency Enablers: Supply Chain

1. **Bill of Material (BOM): As part of the SE process, especially in a legacy system, programs already know all parts (HW and SW).**
2. **Existing supplier management process identifies source of suppliers, End of Life (EOL) analysis, and alternate-part analysis**
   - Document the "As Is"
3. **Is existing criteria, being used by primes and flowed down to subs, known on purchasing of parts?**
4. **What is the supply chain mapping? Does one exist already?**
   - Graphical representation of supply chain down?

- **With the data collected from items 1-4 above, review of the potential risks of the supply chain can be done rather quickly at low cost ("As Is/Known").**
- **Available intel/threat info can be applied against the list of parts or suppliers identified (or technologies) if known.**
- **Provide an assessment of risk of the current supply chain:**
  - Better than we have today.

Establish the baseline from known data.

Operation Vulcan Logic
Fast Track Implementation: Agile Authorizations



PHASE 1

Systems/Systems Security Engineering
Evidentiary Data & Analysis

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

Standard Acquisition Systems Engineering Data

Grow it in

PHASE 2

Collaboration with AO/CRA

- Discuss risk assessment and way ahead
- Previous asessments analysis results
- Operational Use Perspective

Scope the assessment criteria and outcomes

PHASE 3

Executive Risk Assessment

- Tool Agnostic - Focus on Evidentirary Data and Analysis
- Clinically deine Risk of Use Posture
- Outline Mitigations for Risks

Provide determination briefing to AO

Phase 3 starts never ending journey of continuous assessment & monitoring

PROGRAM MANAGEMENT

- Facilitate Risk management across S&T, Acquisition, Operations & Sustainment

COLLABORATIVE EXECUTION

- Partnerships with PEO's, DOEs, PMs, S&T, T&E, Sustainers, Users, enables holistic view

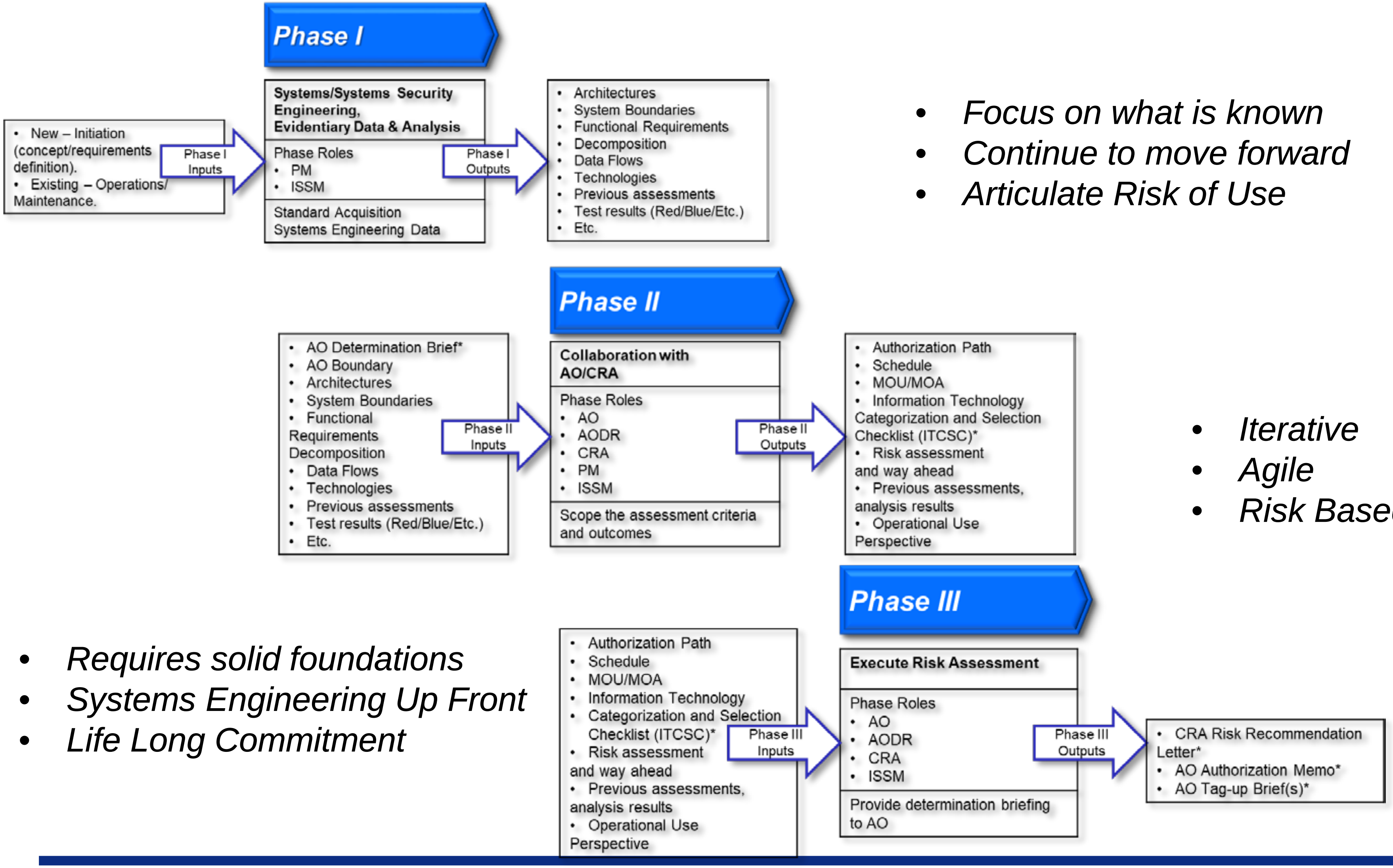
ENABLERS

- Single, Lead AO for each Weapon System
- Streamline expectations and increase Agility

Operationalizing the Fast Track ATO Process

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Agile Authorizations:
Enabled by Disciplined Systems Engineering



Phase I

- New – Initiation (concept/requirements definition).
- Existing – Operations/ Maintenance.

Phase I Inputs

Systems/Systems Security Engineering, Evidentiary Data & Analysis

Phase Roles
- PM
- ISSM

Standard Acquisition Systems Engineering Data

Phase I Outputs

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

Phase II

- AO Determination Brief*
- AO Boundary
- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous assessments
- Test results (Red/Blue/Etc.)
- Etc.

Phase II Inputs

Collaboration with AO/CRA

Phase Roles
- AO
- AODR
- CRA
- PM
- ISSM

Scope the assessment criteria and outcomes

Phase II Outputs

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

Phase III

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology
- Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

Phase III Inputs

Execute Risk Assessment

Phase Roles
- AO
- AODR
- CRA
- ISSM

Provide determination briefing to AO

Phase III Outputs

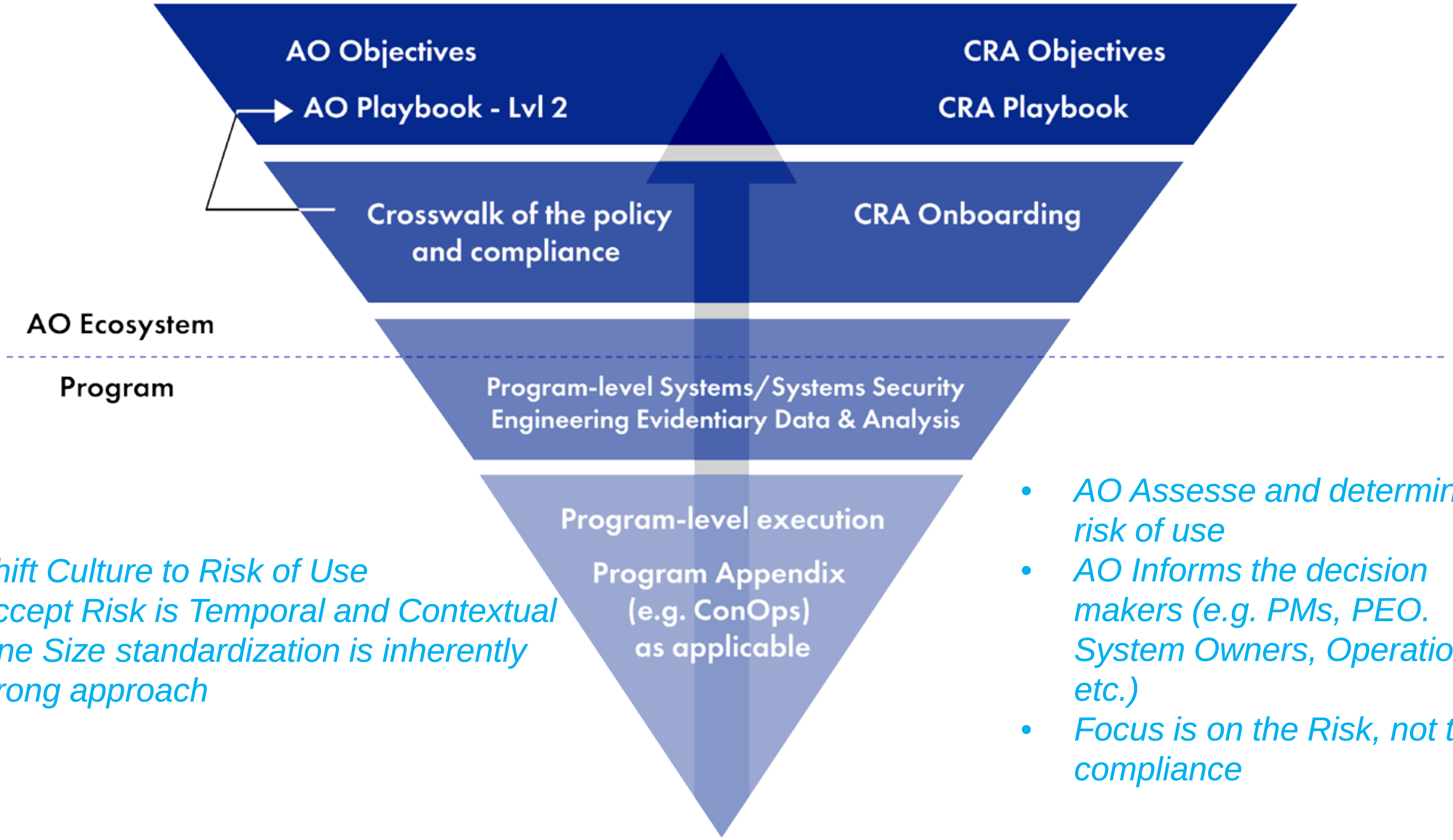
- CRA Risk Recommendation Letter*
- AO Authorization Memo*
- AO Tag-up Brief(s)*

- *Focus on what is known*
- *Continue to move forward*
- *Articulate Risk of Use*

- *Iterative*
- *Agile*
- *Risk Based*

- *Requires solid foundations*
- *Systems Engineering Up Front*
- *Life Long Commitment*

Operation Vulcan Logic: Agile Authorizations Execution NorthStar


AO Objectives
AO Playbook - Lvl 2
CRA Objectives
CRA Playbook
Crosswalk of the policy and compliance
CRA Onboarding
AO Ecosystem
Program
Program-level Systems/Systems Security Engineering Evidentiary Data & Analysis
Program-level execution
Program Appendix (e.g. ConOps) as applicable

- *Shift Culture to Risk of Use*
- *Accept Risk is Temporal and Contextual*
- *One Size standardization is inherently wrong approach*

- *AO Assesse and determines risk of use*
- *AO Informs the decision makers (e.g. PMs, PEO. System Owners, Operations, etc.)*
- *Focus is on the Risk, not the compliance*

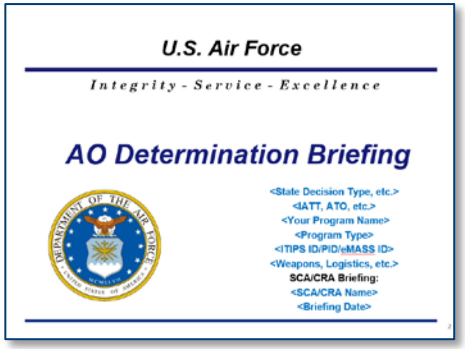
The holistic, continuous authorization ecosystem is focused on Risk of Use.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Operation Vulcan Logic

Authorization Templates
Simple, Effective, Agile

- **Determination Brief**



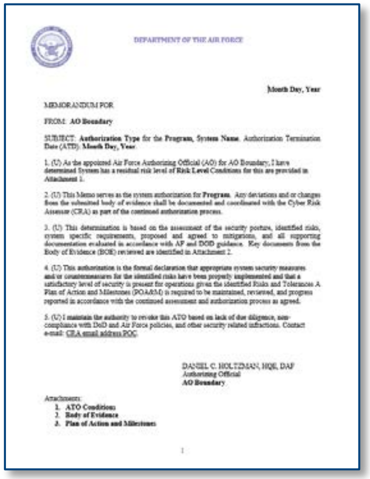
U.S. Air Force

Integrity - Service - Excellence

AO Determination Briefing

<State Decision Type, etc.>
<IATT, ATO, etc.>
<Your Program Name>
<Program Type>
<ITIPS ID/PID/eMASS ID>
<Weapons, Logistics, etc.>
SCA/CRA Briefing:
<SCA/CRA Name>
<Briefing Date>

- **Authorization Package**



DEPARTMENT OF THE AIR FORCE

Month Day, Year

MEMORANDUM FOR

FROM: **AO Boundary**

SUBJECT: **Authorization Type** for the **Program, System Name**. Authorization Termination Date (ATD): **Month Day, Year**.

1. (U) As the appointed Air Force Authorizing Official (AO) for AO Boundary, I have determined System has a residual risk level of **Risk Level** Conditions for this are provided in Attachment 1.

2. (U) This Memo serves as the system authorization for **Program**. Any deviations and or changes from the submitted body of evidence shall be documented and coordinated with the Cyber Risk Assessor (CRA) as part of the continued authorization process.

3. (U) This determination is based on the assessment of the security posture, identified risks, system specific requirements, proposed and agreed to mitigations, and all supporting documentation evaluated in accordance with AF and DOD guidance. Key documents from the Body of Evidence (BOE) reviewed are identified in Attachment 2.

4. (U) This authorization is the formal declaration that appropriate system security measures and/or countermeasures for the identified risks have been properly implemented and that a satisfactory level of security is present for operations given the identified Risks and Tolerances A Plan of Action and Milestones (POA&M) is required to be maintained, reviewed, and progress reported in accordance with the continued assessment and authorization process as agreed.

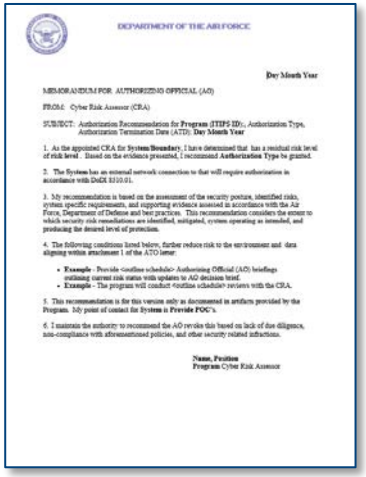
5. (U) I maintain the authority to revoke this ATO based on lack of due diligence, non-compliance with DoD and Air Force policies, and other security related infractions. Contact e-mail: CRA email address POC.

DANIEL C. HOLTZMAN, HQE, DAF
Authorizing Official
AO Boundary

Attachments:
1. **ATO Conditions**
2. **Body of Evidence**
3. **Plan of Action and Milestones**

1

- **CRA Risk Recommendation**



DEPARTMENT OF THE AIR FORCE

Day Month Year

MEMORANDUM FOR AUTHORIZING OFFICIAL (AO)

FROM: Cyber Risk Assessor (CRA)

SUBJECT: Authorization Recommendation for **Program (ITIPS ID)**:, Authorization Type, Authorization Termination Date (ATD): **Day Month Year**

1. As the appointed CRA for **System/Boundary**, I have determined that has a residual risk level of **risk level** . Based on the evidence presented, I recommend **Authorization Type** be granted.

2. The **System** has an external network connection to that will require authorization in accordance with DoDI 8510.01.

3. My recommendation is based on the assessment of the security posture, identified risks, system specific requirements, and supporting evidence assessed in accordance with the Air Force, Department of Defense and best practices. This recommendation considers the extent to which security risk remediations are identified, mitigated, system operating as intended, and producing the desired level of protection.

4. The following conditions listed below, further reduce risk to the environment and data aligning within attachment 1 of the ATO letter:

- **Example** - Provide <outline schedule> Authorizing Official (AO) briefings outlining current risk status with updates to AO decision brief.
- **Example** - The program will conduct <outline schedule> reviews with the CRA.

5. This recommendation is for this version only as documented in artifacts provided by the Program. My point of contact for **System** is **Provide POC**'s.

6. I maintain the authority to recommend the AO revoke this based on lack of due diligence, non-compliance with aforementioned policies, and other security related infractions.

Name, Position
Program Cyber Risk Assessor

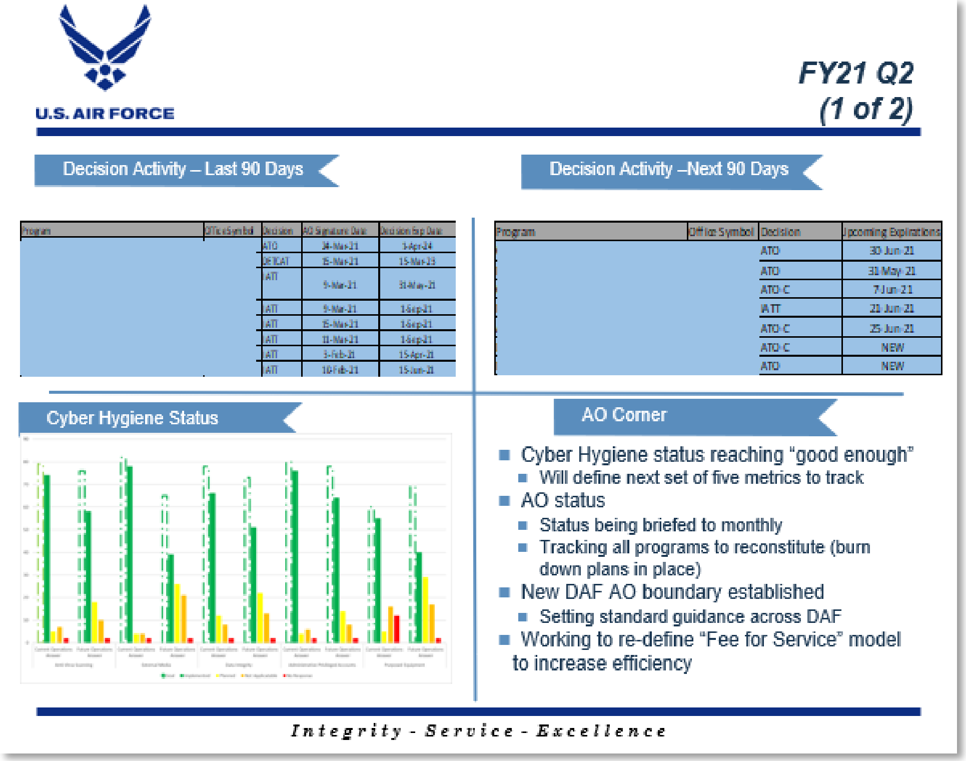
- *Meets all DoDI 8510 and DAF policy requirements for RMF*
- *Authorization Memo has list of BOE that was used to increase reciprocity*
- *Not a work flow or set of "artifacts'*
- *Risk Analysis informed by threat/intel, stakeholder tolerance and operational mission parameters*

- *Provides the AO with an independent Assessment*
- *Not a one time product, developed over time working hand in hand*
- *Authorization starts the life long commitment to improving cyber every day*

Standardization is flexible for authorization packages: There is no one-size-fits-all approach.

Operation Vulcan Logic
AO / PEO Partnership

- **AO provides PEO Quarterly Update.**
  - **Communicate Status.**
  - **Provides Awareness of AOR items & Challenges**
  - **Real time changes communicated by exception**
- **Fosters Collaboration**
  - **Cross PEO challenges**
  - **Opportunities for synergies**
  - **Same Site Picture**
- **PEO AODR-Assigned:**
  - Works for PEO DOE.
  - OPCON to AO.
  - Integrates Cyber into SE/SSE.
- **PEO AODRs collect metrics and status.**



U.S. AIR FORCE

FY21 Q2
(1 of 2)

Decision Activity – Last 90 Days

Program	Office Symbol	Decision	AO Signature Date	Decision Exp Date
		ATO	24-Mar-21	1-Apr-24
		DETCAT	15-Mar-21	15-Mar-23
		IATT	9-Mar-21	31-May-21
		IATT	9-Mar-21	1-Sep-21
		IATT	15-Mar-21	1-Sep-21
		IATT	11-Mar-21	1-Sep-21
		IATT	3-Feb-21	15-Apr-21
		IATT	10-Feb-21	15-Jun-21

Decision Activity –Next 90 Days

Program	Office Symbol	Decision	Upcoming Expirations
		ATO	30-Jun-21
		ATO	31-May-21
		ATO-C	7-Jun-21
		IATT	21-Jun-21
		ATO-C	25-Jun-21
		ATO-C	NEW
		ATO	NEW

Cyber Hygiene Status

AO Corner

- Cyber Hygiene status reaching "good enough"
  - Will define next set of five metrics to track
- AO status
  - Status being briefed to monthly
  - Tracking all programs to reconstitute (burn down plans in place)
- New DAF AO boundary established
  - Setting standard guidance across DAF
- Working to re-define "Fee for Service" model to increase efficiency

Integrity - Service - Excellence

Model works for PEO "Like" (e.g. COCOMs)as well

Cyber is Commanders Business

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Operation Vulcan Logic

Risk Adjudication Process: Cyber is a Commander’s Business

- **Authorizing Official (AO) determines risk is high:**
  - **AO communicates with Program Manger (PM):**
    - Agree and mitigate = Stop here.
  - **AO and PM jointly present to the PEO:**
    - Agree and mitigate = Stop here.
  - **AO and PEO present to the Risk Board.**
    - Risk Board: CIO, SAE, System Operational Commander.
    - Risk Board weighs risk, tolerance, mission, and enterprise.
- **Agile, Efficient, Effective.**
  - Informs relevant stakeholders quickly, allows for more informed decisions

Risk of Use communicated to: Acquisition, Enterprise, & Operational stakeholders.

Operation Vulcan Logic
Collaborative Partnerships

- **DAF CSO, CAO, CEO, CDO, CIO = Leadership Strategic Alignment.**
- **Air Force and Space Force Collaborations.**
- **AF Authorizing Officials:**
  - Weapon Systems AOs: Reciprocity agreement in place.
  - AFRL AO: Collaborating on Fast-Track ATO and reciprocity.
  - HAF/A4 AO: Collaboration and Reciprocity.
  - AF Innovation AO: Collaboration on DevSecOps and cloud migration.
  - AF Global Strike Command: Collaborating on reciprocity.
  - Enterprise AO: Reciprocity across boundary.
  - AF IC AO: Collaboration on reciprocity; ADSV exemplar.
  - 16th AF AO: Collaboration on reciprocity and the AO process.
  - AF OSI/PJ: Collaboration on reciprocity, sharing of resources.
  - DOD CIO: Reciprocity agreement in place.
- **Industry:**
  - Collaboration via AF/Industry Authorization Round Table.
- **External Agencies:**
  - NSA, National Nuclear Security Agency (NNSA), DHS, DLA, USDA, Army RCO, Army NETCOM, DOJ, Navy, etc.

- **Agile execution based on collaborative partnerships, vice policy, and memos.**
- **Building confidence and trust.**

Cyber Risk is Shared – Contextual and Temporal.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Agenda

- **Areas of Responsibility**
- **AF Authorizing Official Perspective**
- **Strategic Challenges/Initiatives**

The most dangerous phrase in language is:

"We've always done it this way."

- Admiral Grace Hopper

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

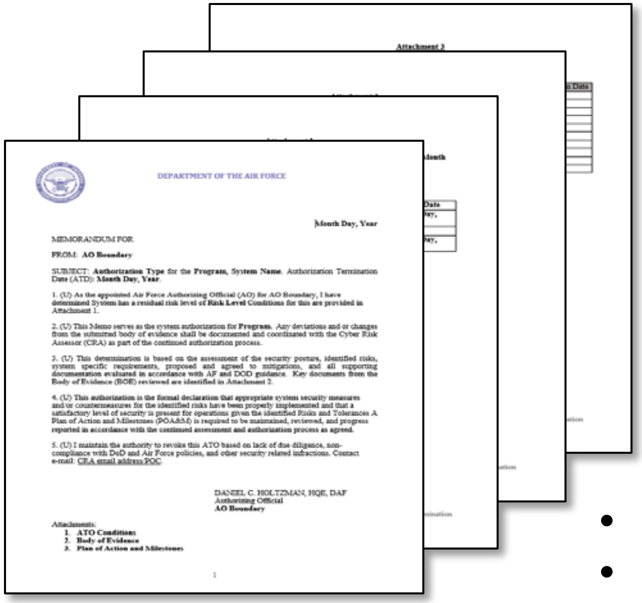
Strategic Challenges

- **Reciprocity:**
  - The myth of the lowest common denominator.
- **Culture of Compliance:**
  - Compliance masquerading as risk management.
- **Operational Risk Integration:**
  - Risk is temporal and context-sensitive.
- **Command and Control:**
  - Too many cooks makes for bad-tasting chili.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

ATO Package of the Future

- **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 3
Date
Month
Day,
Day,

DEPARTMENT OF THE AIR FORCE

Month Day, Year

MEMORANDUM FOR

FROM: **AO Boundary**

SUBJECT: **Authorization Type** for the **Program, System Name**. Authorization Termination Date (ATD): **Month Day, Year**.

1. (U) As the appointed Air Force Authorizing Official (AO) for AO Boundary, I have determined System has a residual risk level of **Risk Level** Conditions for this are provided in Attachment 1.

2. (U) This Memo serves as the system authorization for **Program**. Any deviations and or changes from the submitted body of evidence shall be documented and coordinated with the Cyber Risk Assessor (CRA) as part of the continued authorization process.

3. (U) This determination is based on the assessment of the security posture, identified risks, system specific requirements, proposed and agreed to mitigations, and all supporting documentation evaluated in accordance with AF and DOD guidance. Key documents from the Body of Evidence (BOE) reviewed are identified in Attachment 2.

4. (U) This authorization is the formal declaration that appropriate system security measures and/or countermeasures for the identified risks have been properly implemented and that a satisfactory level of security is present for operations given the identified Risks and Tolerances A Plan of Action and Milestones (POA&M) is required to be maintained, reviewed, and progress reported in accordance with the continued assessment and authorization process as agreed.

5. (U) I maintain the authority to revoke this ATO based on lack of due diligence, non-compliance with DoD and Air Force policies, and other security related infractions. Contact e-mail: CRA email address/POC.

DANIEL C. HOLTZMAN, HQE, DAF
Authorizing Official
AO Boundary

Attachments:
1. **ATO Conditions**
2. **Body of Evidence**
3. **Plan of Action and Milestones**

1

- **Attachment 1: Conditions**
  - Documents any conditions on the ATO.
  - Security is a journey, never a destination.

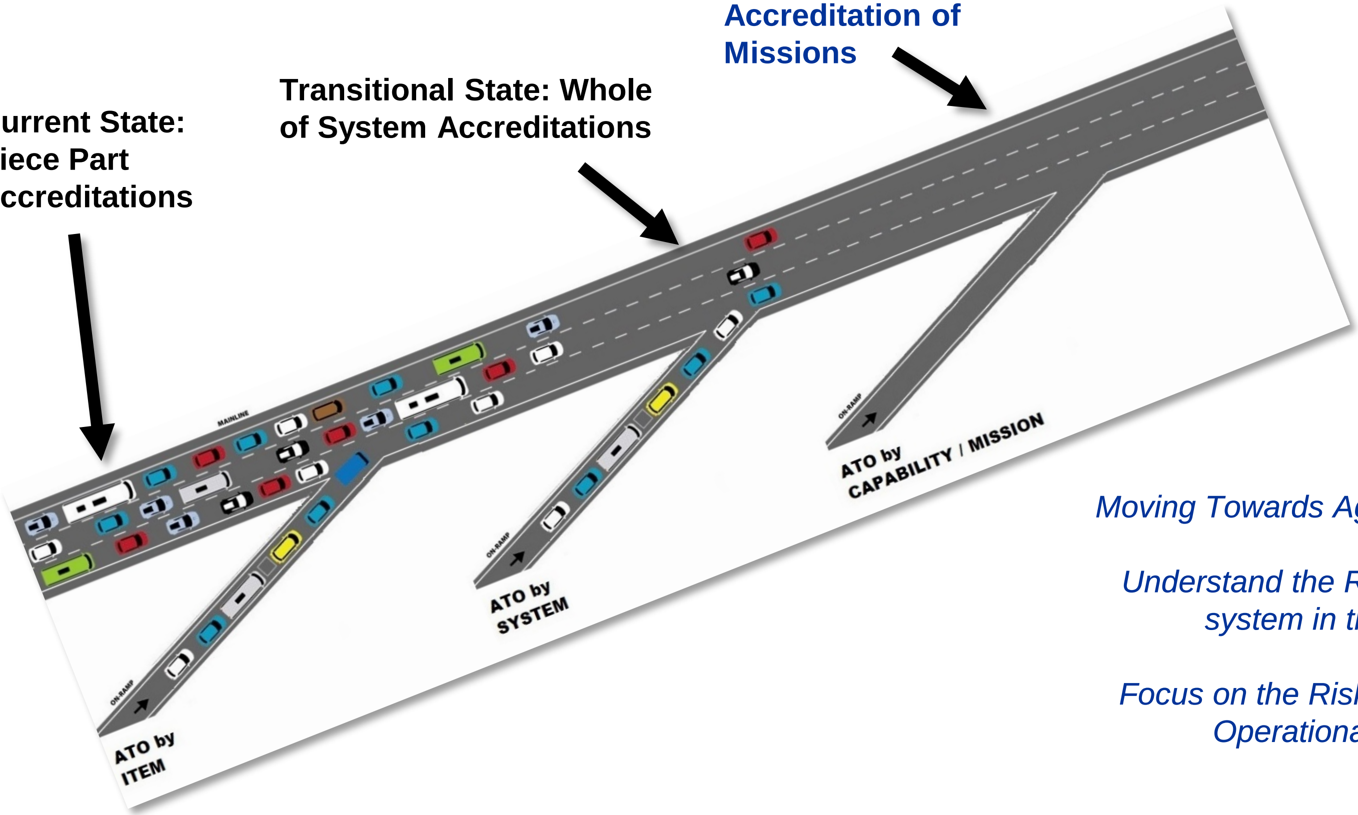
- **Attachment 2: Body of Evidence**
  - Key artifacts that supported the authorization.
  - Informs other AOs and consumers to increase reciprocity.

- **Attachment 3: Plan of Action and Milestones.**
  - Can be a Classified appendix.

- *Provided to the requesting consumer as a contract*
- *Documented in enterprise tools (e.g. eMass, XACTA….)*

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Highway to Resilient Capabilities



Current State: Piece Part Accreditations

Transitional State: Whole of System Accreditations

To-Be State: Holistic Accreditation of Missions

Moving Towards Agile Authorizations.

Understand the Risk of Use of the system in the context.

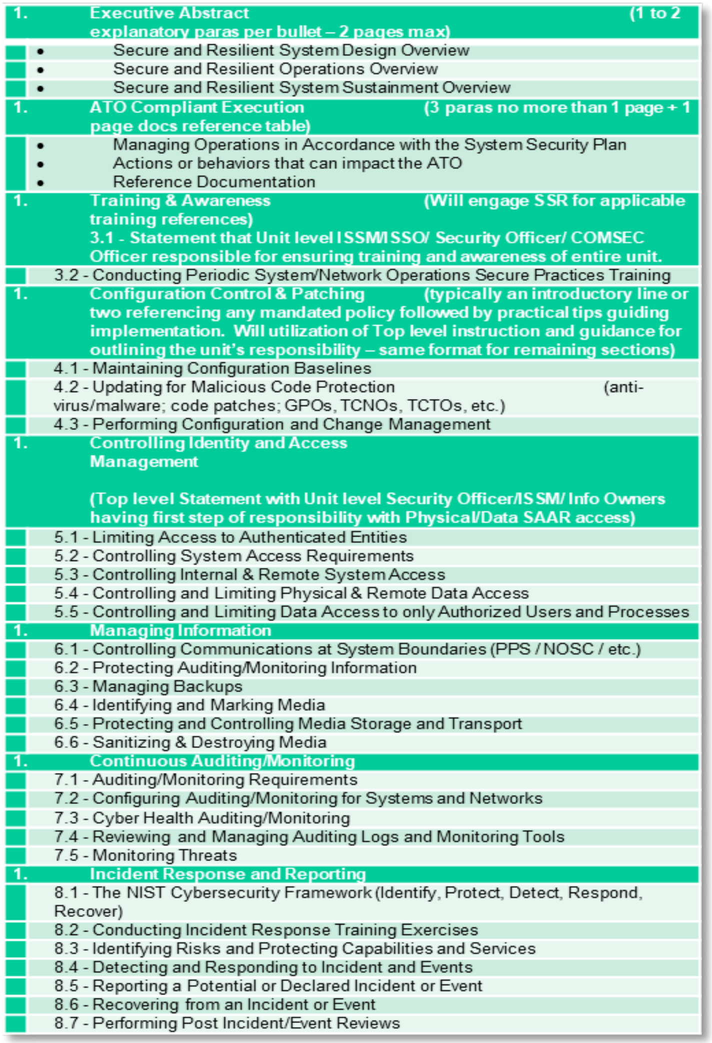
Focus on the Risk Management in Operational Context.

Traditional Boundary Configuration Management is no longer sufficient in a software-defined, ubiquitous, connected environment.

Cyber Tech Order and Continuous Monitoring

- **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.
  - Integrate Mission Defense Teams into CONMON plans.
    - It is the first line of defense.



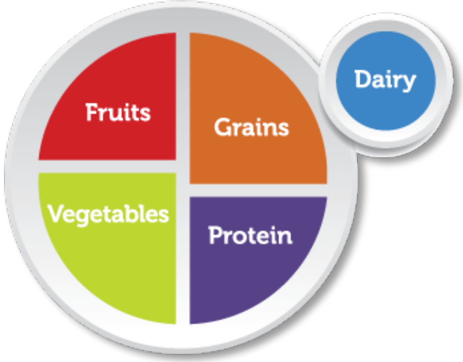
1.	**Executive Abstract (1 to 2 explanatory paras per bullet – 2 pages max)**
•	Secure and Resilient System Design Overview
•	Secure and Resilient Operations Overview
•	Secure and Resilient System Sustainment Overview
1.	**ATO Compliant Execution (3 paras no more than 1 page + 1 page docs reference table)**
• • •	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 ISSM/ISSO/ Security Officer/ COMSEC Officer responsible for ensuring training and awareness of entire unit.**
	3.2 - Conducting Periodic System/Network Operations Secure Practices Training
1.	**Configuration Control & Patching (typically an introductory line 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 (anti-virus/malware; code patches; GPOs, TCNOs, TCTOs, etc.)
	4.3 - Performing Configuration and Change Management
1.	**Controlling Identity and Access Management** **(Top level Statement with Unit level Security Officer/ISSM/ Info Owners having first step of responsibility with Physical/Data SAAR access)**
	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
1.	**Managing Information**
	6.1 - Controlling Communications at System Boundaries (PPS / NOSC / 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
1.	**Continuous Auditing/Monitoring**
	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
1.	**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 Risks Facts Label

- **Application Security is NOT just about the security of the application itself:**
  - It is a layered perspective (hosted environment, TTPs, etc.).
  - As one goes lower in an application architecture, the potential for harm increases.

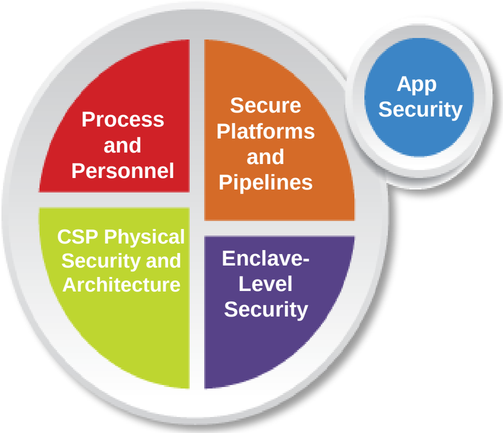
- **An Authority to Operate (ATO) is a risk-based determination and includes many factors:**
  - The technology employed, the execution processes, the hosting environment, the risk tolerance, etc.
  - The ATO is a statement of the "Risk of Use," informing the consumer.

Food



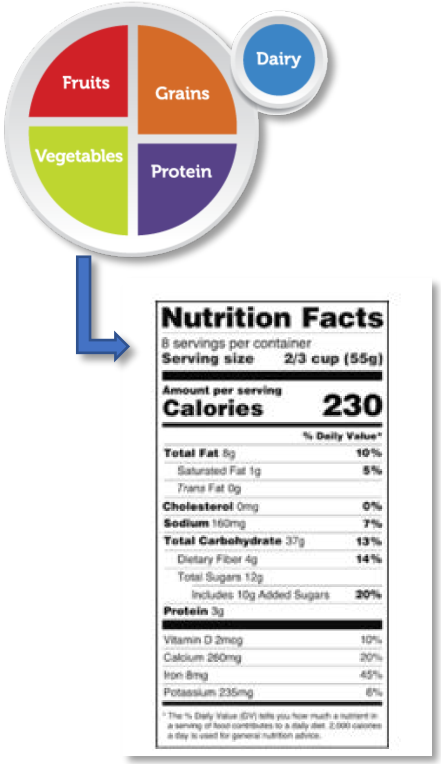
Just like a well-balanced meal, risk is made up of several ingredients

ATO


App Security
Process and Personnel
Secure Platforms and Pipelines
CSP Physical Security and Architecture
Enclave-Level Security

Cyber risk is made up of several ingredients.

Cyber Risks Facts Label: Allowing for an Informed Consumer



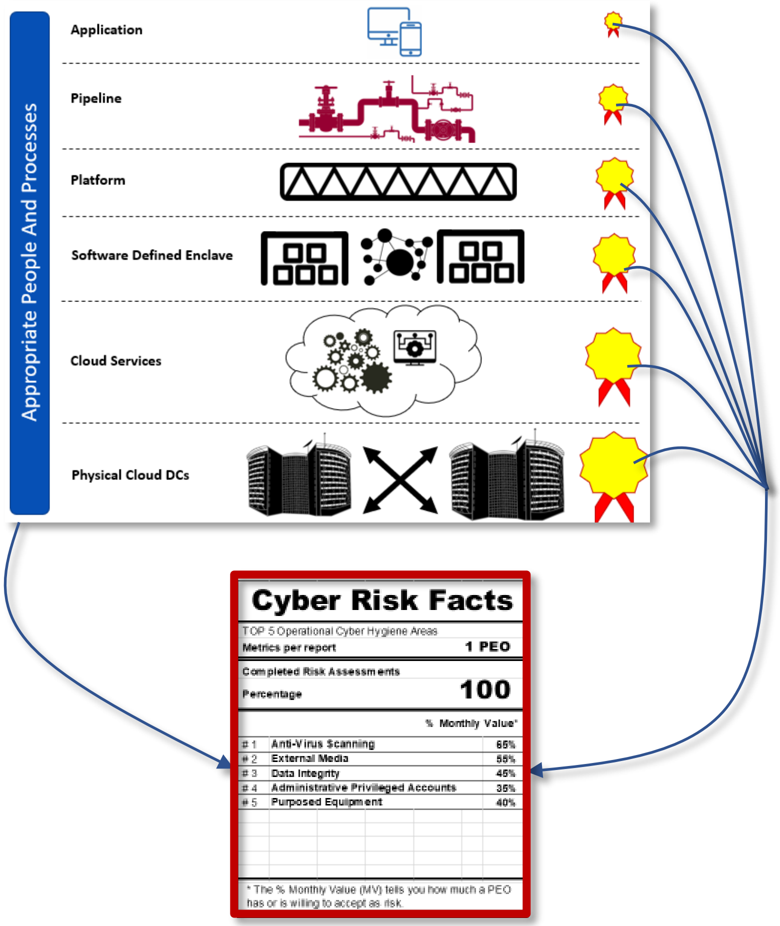
Nutrition Facts

8 servings per container

Serving size	**2/3 cup (55g)**
Amount per serving	
Calories	**230**
	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 1g	**5%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 160mg	**7%**
Total Carbohydrate 37g	**13%**
Dietary Fiber 4g	**14%**
Total Sugars 12g	
Includes 10g Added Sugars	**20%**
Protein 3g	
Vitamin D 2mcg	10%
Calcium 260mg	20%
Iron 8mg	45%
Potassium 235mg	6%

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

- **A Nutrition Facts label shows the consumer WHAT nutrients are in the food based on FDA guidelines.**
- **A Cyber Risk label shows the consumer what the RISK OF USE is for an application based on ATO Guidelines.**



Cyber Risk Facts

TOP 5 Operational Cyber Hygiene Areas

Metrics per report	**1 PEO**
Completed Risk Assessments	
Percentage	**100**

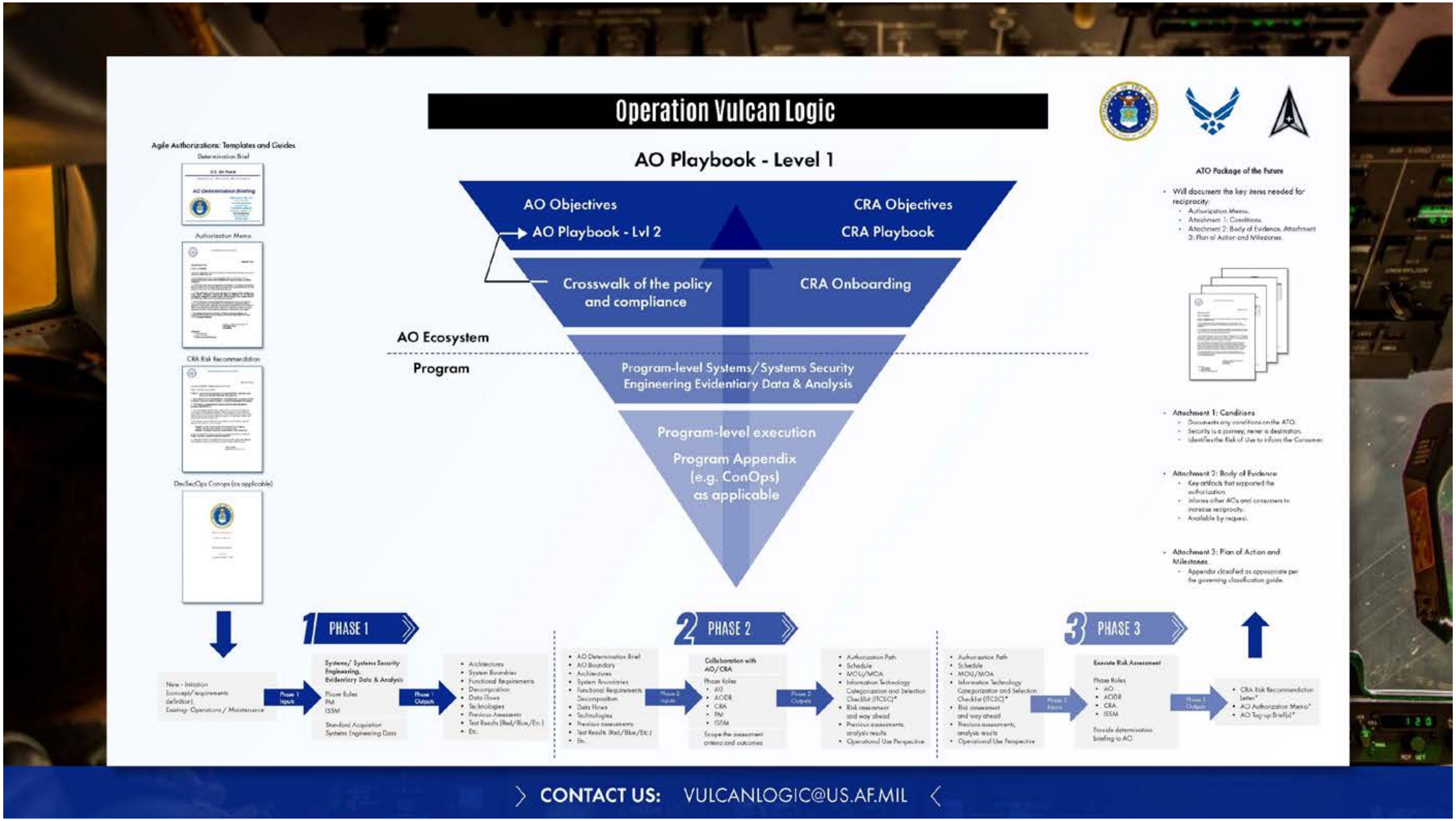
		% Monthly Value*
# 1	Anti-Virus Scanning	65%
# 2	External Media	55%
# 3	Data Integrity	45%
# 4	Administrative Privileged Accounts	35%
# 5	Purposed Equipment	40%

* The % Monthly Value (MV) tells you how much a PEO has or is willing to accept as risk.

Cyber Risk label is the foundation to an informed consumer and enables true reciprocity.

Operation Vulcan Logic Summary

VULCANLOGIC@US.AF.MIL



Operation Vulcan Logic

AO Playbook - Level 1

Agile Authorizations: Templates and Guides

Determination Brief

Authorization Memo

CRA Risk Recommendation

DevSecOps Conops (as applicable)

U.S. Air Force
AO Determination Briefing
AO Objectives
AO Playbook - Lvl 2
CRA Objectives
CRA Playbook
Crosswalk of the policy and compliance
CRA Onboarding
AO Ecosystem
Program
Program-level Systems/Systems Security Engineering Evidentiary Data & Analysis
Program-level execution
Program Appendix (e.g. ConOps) as applicable

ATO Package of the Future

- 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.
  - Identifies the Risk of Use to inform the Consumer.
- Attachment 2: Body of Evidence
  - Key artifacts that supported the authorization.
  - Informs other AOs and consumers to increase reciprocity.
  - Available by request.
- Attachment 3: Plan of Action and Milestones.
  - Appendix classified as appropriate per the governing classification guide.

New - Initiation (concept/requirements definition).
Existing- Operations / Maintenance

1 PHASE 1

Systems/ Systems Security Engineering, Evidentiary Data & Analysis

Phase Roles
PM
ISSM

Standard Acquisition Systems Engineering Data

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

- AO Determination Brief
- AO Boundary
- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous assessments
- Test Results (Red/Blue/Etc.)
- Etc.

2 PHASE 2

Collaboration with AO/CRA

Phase Roles
- AO
- AODR
- CRA
- PM
- ISSM

Scope the assessment criteria and outcomes

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments analysis results
- Operational Use Perspective

- Authorization Path
- Schedule
- MOU/MOA
- Information Technology Categorization and Selection Checklist (ITCSC)*
- Risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use Perspective

3 PHASE 3

Execute Risk Assessment

Phase Roles
- AO
- AODR
- CRA
- ISSM

Provide determination briefing to AO

- CRA Risk Recommendation Letter*
- AO Authorization Memo*
- AO Tag-up Brief(s)*

CONTACT US: VULCANLOGIC@US.AF.MIL

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168

Summary: Keys to Success

- **Assurance:**
  - Establish Confidence:
    - We have assessed all the most significant risks.
    - Authorizations are not the finish line.
    - Continuous Monitoring is a key enabler.
- **Reciprocity:**
  - Establish Trust:
    - We will be transparent.
    - Risk tolerance variance is expected.
- **Partnership:**
  - Collaborative Risk Assessments:
    - Early coordination with stakeholders key to success.
    - Includes PEOs, SML/ML/PM, other AOs, other stakeholders (ATEA, TSN), users, industry
    - Fast-Track ATO Methodology is a key enabler.

"Without trust we don't truly collaborate; we merely coordinate or, at best, cooperate. It is trust that transforms a group of people into a team."

Stephen M.R. Covey

VULCANLOGIC@US.AF.MIL

This is a work in progress. Need to continue to collaborate.

Questions and Discussion

VULCANLOGIC@US.AF.MIL

AFRMFKS Published AO Boundary Document Descriptions

- **AO Determination Brief Template:**
  - Brief to assist program personnel in understanding what the Authorizing Official is expecting to see to make an informed risk determination.
- **AO Determination Brief Guide:**
  - An AO determination brief guide has also been created to provide guidance on the completion of the above AO determination brief.
- **AO-Defined Roles and Responsibilities Chart:**
  - Roles and responsibilities for key stakeholders the AO or AO staff will interact with.
- **AO Playbook:**
  - A high-level guide on the AO objectives with Criteria, Observables, and Behavior (COB) expectations and templates used when interacting with the Authorizing Official for authorization determinations.
- **AO Tag-up Brief Template:**
  - Used to provide regular updates on system status to allow the Authorizing Official or Designated Representative to make continuous and on-going, risk-based determinations based on guidance from the Authorizing Official.
- **AODR/CRA Appointment Letter Template:**
  - Used to ensure personnel are directly appointed, in writing, to the roles of an AODR or CRA.
- **Authorization Memo Template:**
  - Leveraged to articulate the authorization determination to stakeholders. After the determination of risk from the operation or use of the information system has been made, this letter is used to inform the System Owner and other stakeholders of the authorization determination along with terms and conditions for the authorization.

AFRMFKS Published AO Boundary Document Descriptions

- **CRA Objectives:**
  - Provides an overall CRA goals and basic introduction to the Fast-Track Agile Authorization process (key steps/documents).
- **CRA Onboarding:**
  - Introduces/defines the tools (documents), websites, roles and responsibilities, engineering phases/outputs, documentation workflow, etc. (what the CRA needs to be successful in meeting the objectives/goals).
- **CRA Playbook:**
  - Outlines the Agile Authorization process, objectives, and step-by-step approach along with the templates used when interacting with the AO for authorization decisions.
- **CRA Risk Recommendation Letter:**
  - Articulates for the CRA the risk recommendation once the risk assessment is complete.
- **DSOP CONOPS:**
  - Addresses the process flows of developed code and software and the people that perform duties within that process flow, covering the hardware/software and the people operating the infrastructure.
- **Information Technology Categorization and Selection Checklist (ITCSC):**
  - Documents the security categorization of the system, including the information processed by the system and represented by the identified information types.
- **No Security Impact (NSI):**
  - Describes the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information for an information system.

DISTRIBUTION A. Approved for public release: Distribution unlimited. Case Number: AFLCMC-2021-0168