DevOps for Defense

August 2020

Fast Track and Continuous ATO

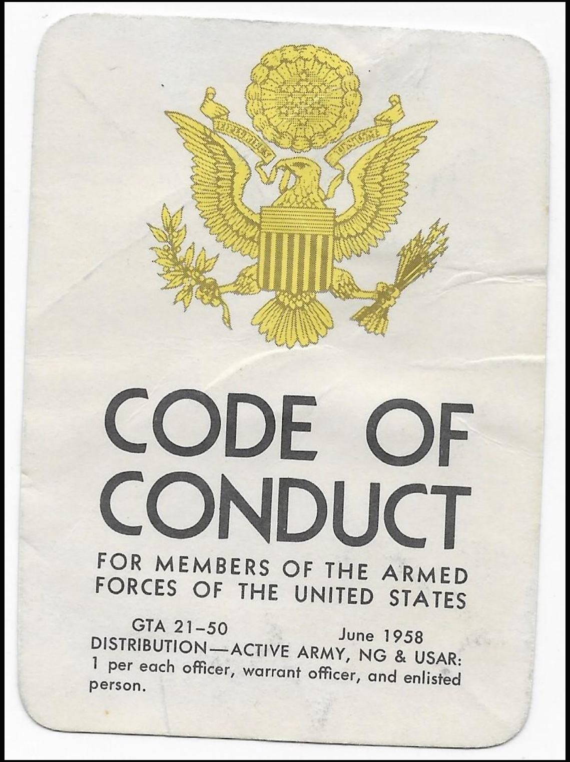
Rick Tossavainen and Tom Marlow
Dark Wolf Solutions

https://devopsfordefense.org
https://www.meetup.com/DevOps-for-Defense/
https://github.com/jondavid-black/DevOpsForDefense
devopsfordefense@gmail.com
https://twitter.com/devops4defense

Sponsored by: TEKsystems Own change

DevOps for Defense Meetup: Code of Conduct

- UNCLASSIFIED ONLY!!!!
- Treat each other with respect and professionalism.
- Do not talk about private, sensitive, or proprietary work.
- Do talk about your experiences, needs, desires to improve work in our domain.
- Do share your thoughts.
- Do learn from others.
- Do mute yourself while others are speaking!



CODE OF CONDUCT

FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES

GTA 21-50 June 1958

DISTRIBUTION—ACTIVE ARMY, NG & USAR:
1 per each officer, warrant officer, and enlisted person.

DARK WOLF SOLUTIONS

Rick Tossavainen, Chief Executive Officer

Tom Marlow, Deputy Director, Cybersecurity Practice

Fast Track and Continuous ATO

Software That Supports Missions

DARK WOLF SOLUTIONS

> “One of the most ironic examples is when we are using Agile methodologies to produce new capability for the warfighter on a daily or weekly basis, but can’t deliver to the user for months due to accreditation. This is not sustainable.”

Lauren Knausenberger
Director, Cyberspace Innovation,
U.S. Air Force

ATO Types

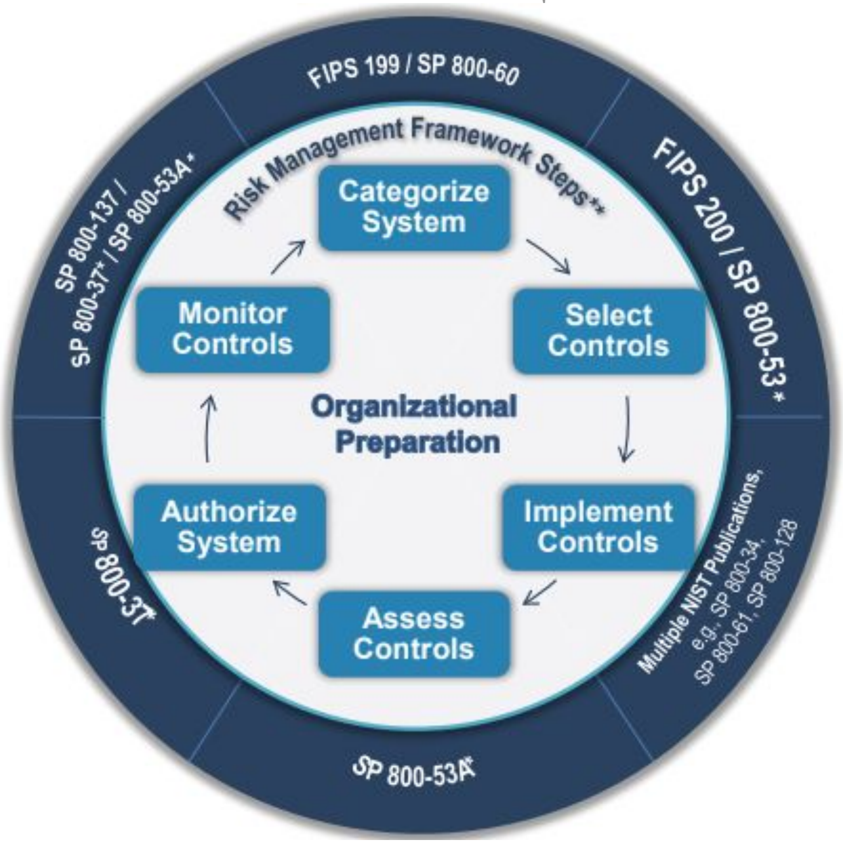
- **Traditional RMF**: a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.
- **FT-ATO**: Fast Track ATO streamlines accreditation decisions by focusing on demonstrated security. Authorizing Officials must see evidence that a system adheres to standard cyber hygiene principles, has been validated through penetration testing, and has an Information System Continuous Monitoring (ISCM) strategy.
- **C-ATO**: For DevSecOps software factories with validated security policies and processes adhering to a Continuous ATO playbook, Continuous ATO facilitates automatic and immediate accreditation for all releases in compliance with Risk Management Framework requirements.

The Risk Management Framework

- A holistic and comprehensive risk management process.
- Integrated into the System Development Life Cycle (SDLC)
- Provides processes (tasks) for each of the six steps at the system level.

🟦 = Step

■ = Instructions to Complete the Step


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53*
Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A*
SP 800-37*
SP 800-137 / SP 800-37* / SP 800-53A*
Risk Management Framework Steps**
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organizational Preparation

RMF Artifacts for ATO

DARK WOLF SOLUTIONS

1

System Security Plan

- System risk categorization
- Responsible organizations
- System Boundary
- Security Policies

2

Control Matrix

- Security Controls from NIST 800-53
- Implementation Details
- Crosswalk to other security requirements

3

Test Report

- Executive Summary
- Details of test procedures and results
- Detailed findings
- Residual risk summary

4

POA&M

- Task-oriented plan for closing vulnerabilities.
- Presents schedule
- Identifies accountable parties
- Living document

Fast Track ATO Background

Objectives

1. Provide an alternative pathway to ATO that better manages security risk by shifting the focus from exhaustive documentation of controls to the assessment of demonstrable cybersecurity in an operationally relevant environment.
2. Reduce the time required for an ATO when systems are transitioning to FedRAMP approved cloud environments.

Authority

- NIST SP 800-37 rev 2, *RMF for Information Systems and Organizations*
  - Incorporates *Supplemental Guidance on Ongoing Authorization*
  - Approval to Connect (ATC) remains at the discretion of the receiving AO, but reciprocity shall be used to the maximum extent possible.
  - If the operational environment is similar, the AO can use the existing adversarial assessment to inform their decision. Otherwise, the AO will require a new adversarial assessment.

FT-ATO Approach

18 March 2019 – Deputy CIO of Air Force signs "Fast-Track ATO" Memorandum

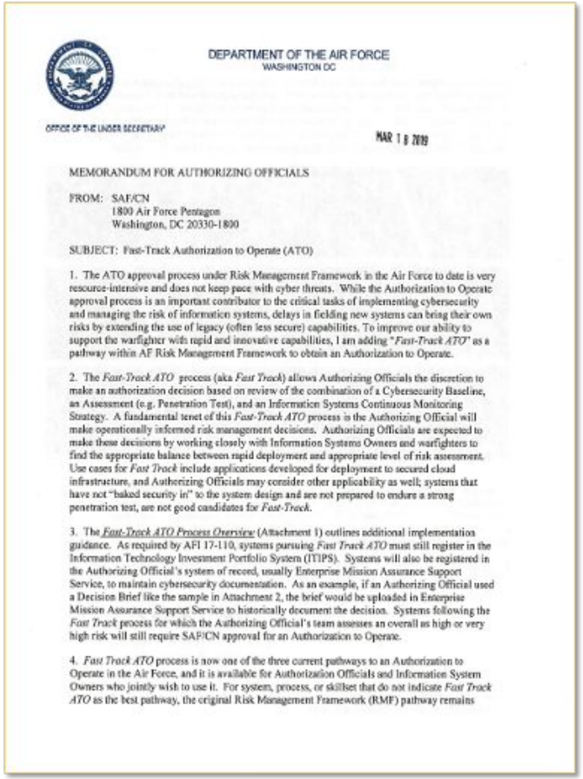
- "The ATO approval process under Risk Management Framework in the Air Force to date is very resource-intensive and does not keep pace with cyber threats."
- The AO is expected to make "operationally informed risk management decisions" based on three key elements.

Two attachments were included

- Fast Track Overview – Highlights some terms and high level direction
- Sample Decision Brief – Includes Risk Analysis Report

Fast Track does not remove/replace requirements to comply with Federal Mandates

- RMF & FISMA are still required
- System registration (e.g. ITIPS, eMASS) are still required
- Must perform adversarial assessment once environment is established



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE UNDER SECRETARY

MAR 1 8 2019

MEMORANDUM FOR AUTHORIZING OFFICIALS

FROM: SAF/CN
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Fast-Track Authorization to Operate (ATO)

1. The ATO approval process under Risk Management Framework in the Air Force to date is very resource-intensive and does not keep pace with cyber threats. While the Authorization to Operate approval process is an important contributor to the critical tasks of implementing cybersecurity and managing the risk of information systems, delays in fielding new systems can bring their own risks by extending the use of legacy (often less secure) capabilities. To improve our ability to support the warfighter with rapid and innovative capabilities, I am adding "*Fast-Track ATO*" as a pathway within AF Risk Management Framework to obtain an Authorization to Operate.

2. The *Fast-Track ATO* process (aka *Fast Track*) allows Authorizing Officials the discretion to make an authorization decision based on review of the combination of a Cybersecurity Baseline, an Assessment (e.g. Penetration Test), and an Information Systems Continuous Monitoring Strategy. A fundamental tenet of this *Fast-Track ATO* process is the Authorizing Official will make operationally informed risk management decisions. Authorizing Officials are expected to make these decisions by working closely with Information Systems Owners and warfighters to find the appropriate balance between rapid deployment and appropriate level of risk assessment. Use cases for *Fast Track* include applications developed for deployment to secured cloud infrastructure, and Authorizing Officials may consider other applicability as well; systems that have not "baked security in" to the system design and are not prepared to endure a strong penetration test, are not good candidates for *Fast-Track*.

3. The *Fast-Track ATO Process Overview* (Attachment 1) outlines additional implementation guidance. As required by AFI 17-110, systems pursuing *Fast Track ATO* must still register in the Information Technology Investment Portfolio System (ITIPS). Systems will also be registered in the Authorizing Official's system of record, usually Enterprise Mission Assurance Support Service, to maintain cybersecurity documentation. As an example, if an Authorizing Official used a Decision Brief like the sample in Attachment 2, the brief would be uploaded in Enterprise Mission Assurance Support Service to historically document the decision. Systems following the *Fast Track* process for which the Authorizing Official's team assesses an overall as high or very high risk will still require SAF/CN approval for an Authorization to Operate.

4. *Fast Track ATO* process is now one of the three current pathways to an Authorization to Operate in the Air Force, and it is available for Authorization Officials and Information System Owners who jointly wish to use it. For system, process, or skillset that do not indicate *Fast Track ATO* as the best pathway, the original Risk Management Framework (RMF) pathway remains

Continuous ATO Background

Objectives

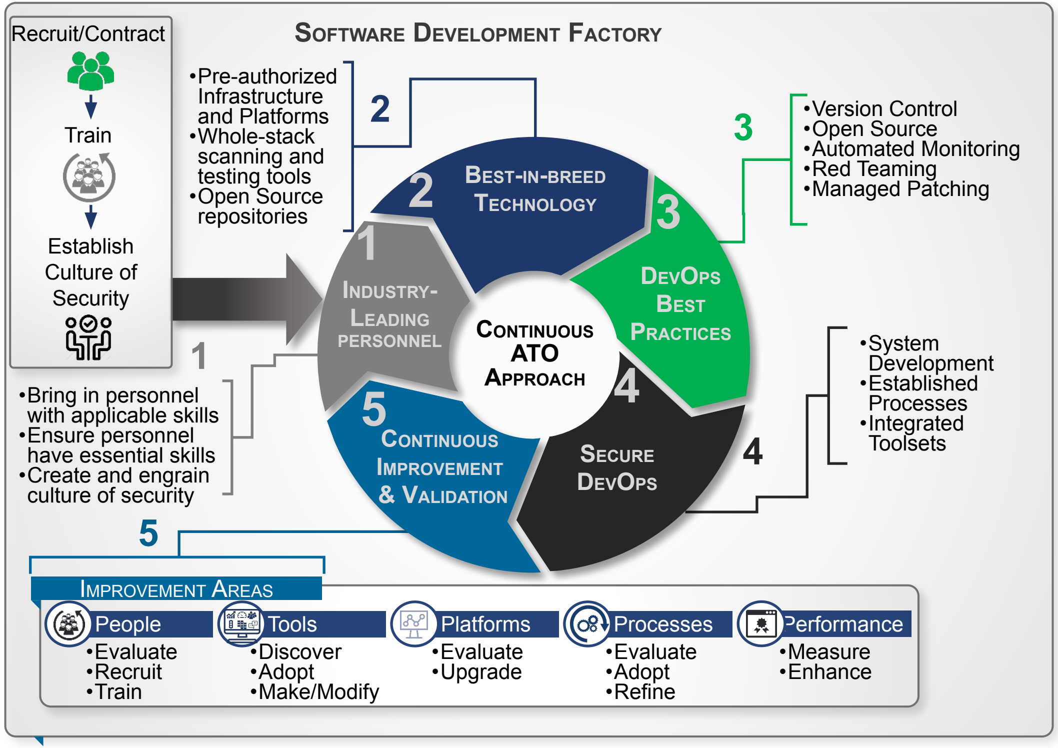
1. Enable a performance framework based on outcomes rather than compliance.
2. Reshape security processes to enable continuous integration and deployment.
    a. The current RMF process is designed for waterfall.
3. Create intrinsic software security
4. Accredits the platform and process and certifies the team that produces a product under a continuous monitoring process that maintains the residual risk within the risk tolerance of the AO

Authority

- NIST SP 800-37 rev 2, *RMF for Information Systems and Organizations*
    - Incorporates *Supplemental Guidance on Ongoing Authorization*

Accelerating Development

- C-ATO begins with the establishment of a well designed and implemented software factory.
- There are five components that must be built into a software factory in order for C-ATO to work.
- By authorizing the factory, all applications developed within the factory will be granted ATO upon release to production.



2
- Pre-authorized Infrastructure and Platforms
- Whole-stack scanning and testing tools
- Open Source repositories

3
- Version Control
- Open Source
- Automated Monitoring
- Red Teaming
- Managed Patching

1
- Bring in personnel with applicable skills
- Ensure personnel have essential skills
- Create and engrain culture of security

4
- System Development
- Established Processes
- Integrated Toolsets

5 Improvement Areas

People
- Evaluate
- Recruit
- Train

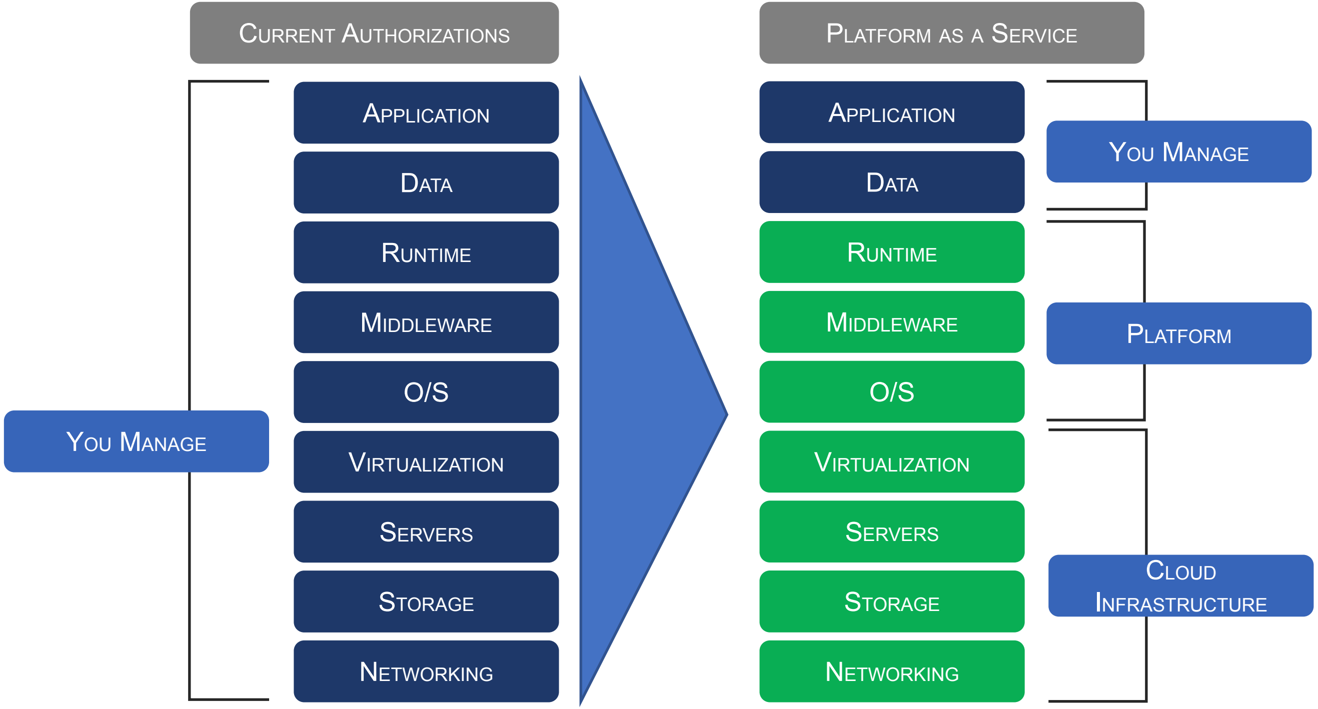
Tools
- Discover
- Adopt
- Make/Modify

Platforms
- Evaluate
- Upgrade

Processes
- Evaluate
- Adopt
- Refine

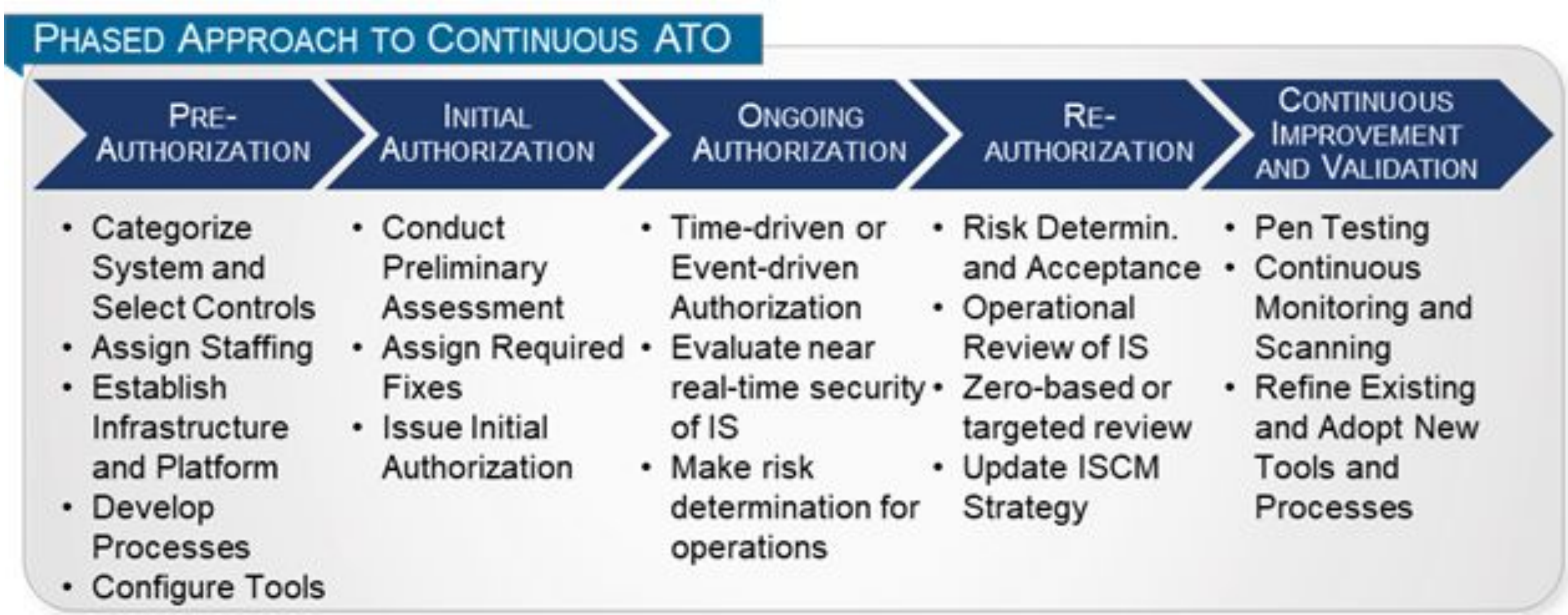
Performance
- Measure
- Enhance

Platform as a Service



- Using pre-authorized IaaS and PaaS enables maximum control inheritance for the ATO.
- When the normal components that comprise a project’s infrastructure are no longer in scope, the authorization process is simplified to the application and data layers.

Continuous ATO Approach



Phased Approach to Continuous ATO

Pre-Authorization

- Categorize System and Select Controls
- Assign Staffing
- Establish Infrastructure and Platform
- Develop Processes
- Configure Tools

Initial Authorization

- Conduct Preliminary Assessment
- Assign Required Fixes
- Issue Initial Authorization

Ongoing Authorization

- Time-driven or Event-driven Authorization
- Evaluate near real-time security of IS
- Make risk determination for operations

Re-Authorization

- Risk Determin. and Acceptance
- Operational Review of IS
- Zero-based or targeted review
- Update ISCM Strategy

Continuous Improvement and Validation

- Pen Testing
- Continuous Monitoring and Scanning
- Refine Existing and Adopt New Tools and Processes

C-ATO Best Practices

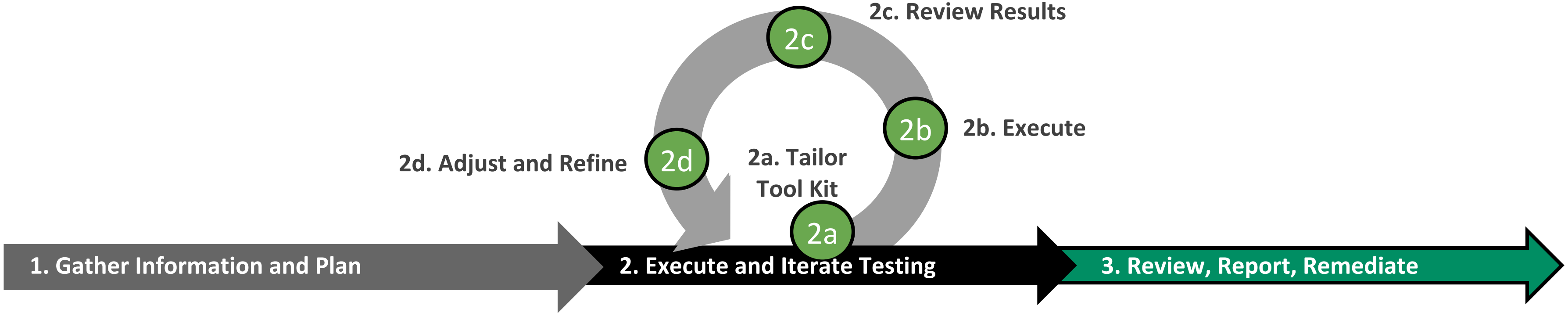
One size does not fit all

- Every AO is different and cares differently about degrees of risk
- Influencers: level of trust between the Development and Operations team, technical acumen, past experiences, willingness to lean forward and try new methods

Look for reciprocity opportunities

- Many AOs will accept reciprocity if the application, system, or component of the system was authorized by another government official, especially within the same agency or within DoD
- Using enterprise services for logging, authentication, and authorization can speed the process to ATO as many of the RMF controls are satisfied by these already accredited functions

Role of Penetration Testing



1. Gather Information and Plan

- Define scope and target systems
- Confirm rules of engagement
- Specify expected ATO inputs and exit criteria
- Assess network topology
- Cross-reference system architecture with common vulnerabilities and exposures
- Define plays to be employed

2. Execute and Iterate Testing

- Tailor custom tools to execute attacks and measure results
- Conduct a combination of automated testing, manual testing and manual verification
- Review results from each test iteration
- Adjust methods and scope to focus on critical findings

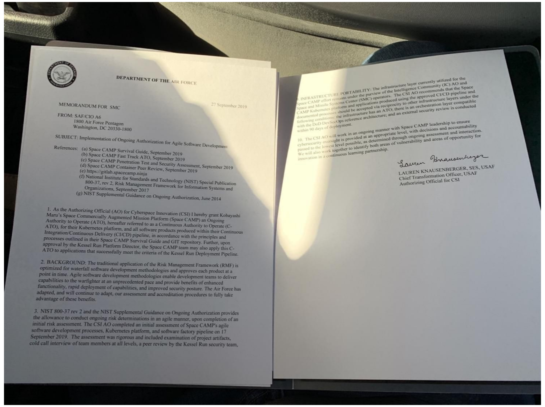
3. Review, Report, Remediate

- Review tests and compare outcomes to expected results
- Assign risk factors
- Create reports and relevant ATO inputs
- Summarize possibilities for remediation approach
- Define scope of remediation efforts, if solicited
- Report suggested changes to policy, software, and network topology

Case Study: Success at Space Camp

DARK WOLF SOLUTIONS

- Testers deployed to Colorado Springs to hunt for vulns, review policy and assess culture
- Overall approach was found to be expeditious and technically sound, but policy considerations lagged behind
    - Key vulnerabilities and policy gaps were identified and corrected in real-time
    - AO support and Dark Wolf recommendations allowed SpaceCAMP to expedite a major networking infrastructure upgrade
- With issues identified and fixed or addressed, Dark Wolf passes on a positive ATO recommendation to SAF/CIO
- SpaceCAMP receives a Continuous ATO less than two months after initial tests



DEPARTMENT OF THE AIR FORCE

MEMORANDUM FOR SMC

27 September 2019

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Implementation of Ongoing Authorization for Agile Software Development

References:
(a) Space CAMP Survival Guide, September 2019
(b) Space CAMP Fast Track ATO, September 2019
(c) Space CAMP Penetration Test and Security Assessment, September 2019
(d) Space CAMP Container Peer Review, September 2019
(e) https://gitlab.spacecamp.ninja
(f) National Institute for Standards and Technology (NIST) Special Publication 800-37, rev 2, Risk Management Framework for Information Systems and Organizations, September 2017
(g) NIST Supplemental Guidance on Ongoing Authorization, June 2014

1. As the Authorizing Official (AO) for Cyberspace Innovation (CSI) I hereby grant Kobayashi Maru's Space Commercially Augmented Mission Platform (Space CAMP) an Ongoing Authority to Operate (ATO), hereafter referred to as a Continuous Authority to Operate (C-ATO), for their Kubernetes platform, and all software products produced within their Continuous Integration/Continuous Delivery (CI/CD) pipeline, in accordance with the principles and processes outlined in their Space CAMP Survival Guide and GIT repository. Further, upon approval by the Kessel Run Platform Director, the Space CAMP team may also apply this C-ATO to applications that successfully meet the criteria of the Kessel Run Deployment Pipeline.

2. BACKGROUND: The traditional application of the Risk Management Framework (RMF) is optimized for waterfall software development methodologies and approves each product at a point in time. Agile software development methodologies enable development teams to deliver capabilities to the warfighter at an unprecedented pace and provide benefits of enhanced functionality, rapid deployment of capabilities, and improved security posture. The Air Force has adapted, and will continue to adapt, our assessment and accreditation procedures to fully take advantage of these benefits.

3. NIST 800-37 rev 2 and the NIST Supplemental Guidance on Ongoing Authorization provides the allowance to conduct ongoing risk determinations in an agile manner, upon completion of an initial risk assessment. The CSI AO completed an initial assessment of Space CAMP's agile software development processes, Kubernetes platform, and software factory pipeline on 17 September 2019. The assessment was rigorous and included examination of project artifacts, cold call interview of team members at all levels, a peer review by the Kessel Run security team,

9. INFRASTRUCTURE PORTABILITY: The infrastructure layer currently utilized for the Space CAMP effort remains under the purview of the Intelligence Community (IC) AO and Space and Missile Systems Center (SMC) operators. The CSI AO recommends that the Space CAMP Kubernetes platform and applications produced using the approved CI/CD pipeline and documented processes should be accepted via reciprocity to other infrastructure layers under the following conditions: the infrastructure has an ATO; there is an orchestration layer compatible with the DoD DevSecOps reference architecture; and an external security review is conducted within 90 days of deployment.

10. The CSI AO will work in an ongoing manner with Space CAMP leadership to ensure cybersecurity oversight is provided at an appropriate level, with decisions and accountability passed to the lowest level possible, as determined through ongoing assessment and interaction. We will also work together to identify both areas of vulnerability and areas of opportunity for innovation in a continuous learning partnership.

Lauren Knausenberger

LAUREN KNAUSENBERGER, SES, USAF
Chief Transformation Officer, USAF
Authorizing Official for CSI

THANK YOU!

2019: 2nd place
Wireless Capture the Flag (CTF)

2017: 1st place IoT CTF

2016: 3rd place IoT CTF

2018: 1st place
IoT Wireless CTF

2016: 1st place
IoT CTF

Leadership & Innovation Within the DMV cybersecurity industry.

DevOps Resources

https://devopsfordefense.org/resources/

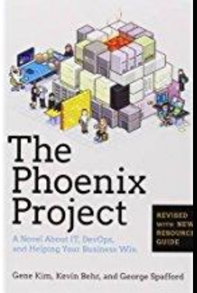
https://www.meetup.com/DevOps-for-Defense/
https://github.com/jondavid-black/DevOpsForDefense
devopsfordefense@gmail.com

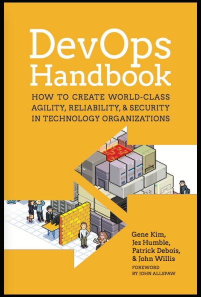
Books / Publications:

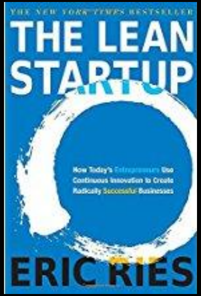
Conference Presentations (YouTube):

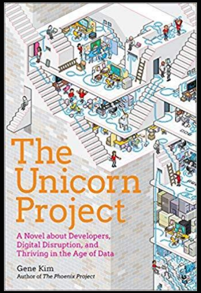
- DevOps Enterprise Summit (DOES)
- IT Revolution
- Velocity
- GoTo

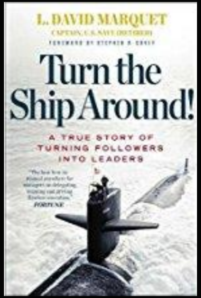
YouTube

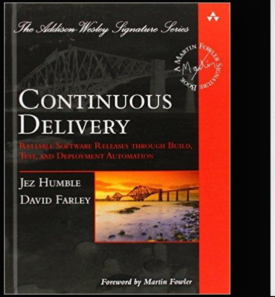

The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win
REVISED WITH NEW RESOURCE GUIDE
Gene Kim, Kevin Behr, and George Spafford

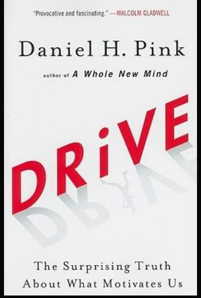

DevOps Handbook
HOW TO CREATE WORLD-CLASS AGILITY, RELIABILITY, & SECURITY IN TECHNOLOGY ORGANIZATIONS
Gene Kim, Jez Humble, Patrick Debois, & John Willis
FOREWORD BY JOHN ALLSPAW

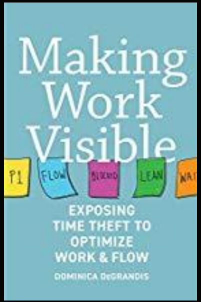

THE NEW YORK TIMES BESTSELLER
THE LEAN STARTUP
How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses
ERIC RIES

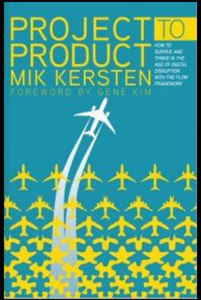

The Unicorn Project
A Novel about Developers, Digital Disruption, and Thriving in the Age of Data
Gene Kim
Author of The Phoenix Project

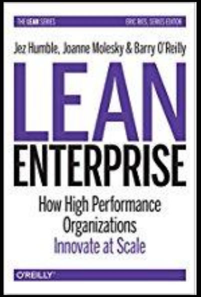


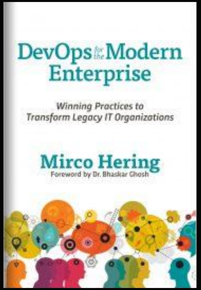

The Addison-Wesley Signature Series
CONTINUOUS DELIVERY
RELIABLE SOFTWARE RELEASES THROUGH BUILD, TEST, AND DEPLOYMENT AUTOMATION
JEZ HUMBLE
DAVID FARLEY
Foreword by Martin Fowler

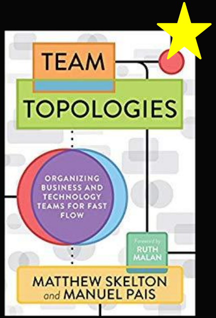

"Provocative and fascinating." —MALCOLM GLADWELL
Daniel H. Pink
author of A Whole New Mind
DRiVE
The Surprising Truth About What Motivates Us






Jez Humble, Joanne Molesky & Barry O'Reilly
LEAN ENTERPRISE
How High Performance Organizations Innovate at Scale
O'REILLY


DevOps for the Modern Enterprise
Winning Practices to Transform Legacy IT Organizations
Mirco Hering
Foreword by Dr. Bhaskar Ghosh


TEAM TOPOLOGIES
ORGANIZING BUSINESS AND TECHNOLOGY TEAMS FOR FAST FLOW
RUTH MALAN
MATTHEW SKELTON and MANUEL PAIS