RISE8

cATO or cRMF? A Better Path to follow

BRYON KROGER
CHIEF EXECUTIVE OFFICER

Agenda

1.0 A brief history of cATO

2.0 Continuous RMF

3.0 Recap

Some Definitions

WHAT DOES THIS EVEN MEAN?

Authority to Operate (ATO) - “The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.”

Ongoing Authorization - “security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organizational information”

Continuous Authority to Operate (cATO) - A branded term I made up for the Kessel Run SOP for ongoing authorization that was adopted by the AirForce and now the DoD (sorry)

Continuous Risk Management Framework (cRMF) - Shifting RMF left in the development lifecycle such that it runs concurrent with development (what we should have called it)

Continuous ATO = Continuous RMF

THE CONVERGENCE OF RMF & THE DEVOPS SDLC

- People
  - Cybersecurity culture
  - Technical assessors
- Process
  - Perform all RMF steps
  - Living documentation inside SDLC tools
  - NIST Guidance + Implementation Playbook
  - Continuous, with high quality and *reduced* risk
- Technology /Automation
  - High common controls inheritance via opinionated cloud platform(s)
  - Security Requirements Management (e.g. SD Elements)
  - Static Application & Dependency Vulnerability Scanning (e.g. Snyk)
  - Image Scanning (e.g. Aqua)
  - Container Scanning (e.g. Aqua)

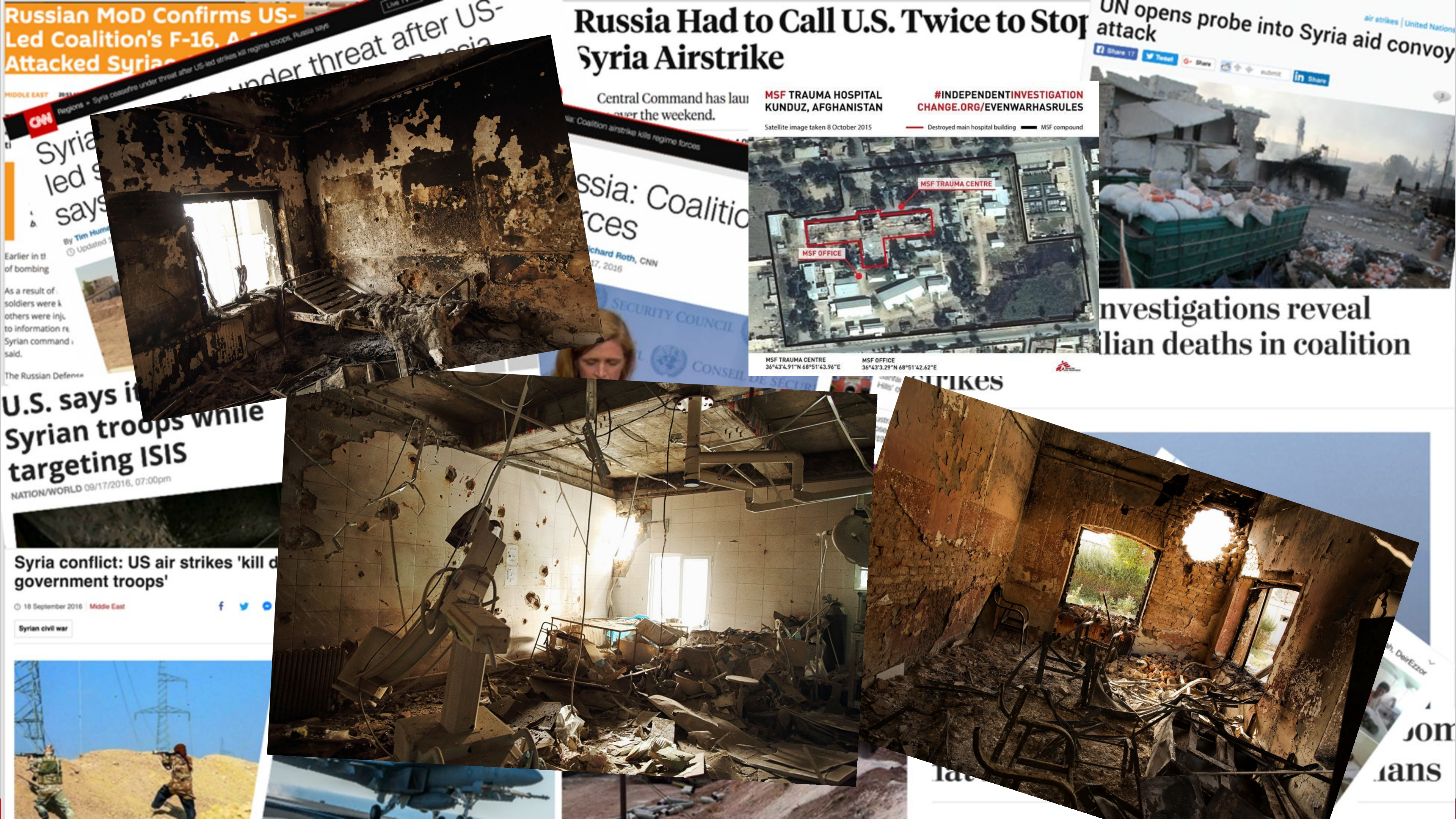
Myths

WHAT IT ISN'T

- A way to avoid having to do RMF
- Authorizing the people and/or the process
- A way to push whatever you want, whenever you want
- A pipeline
- A platform with sidecar containers
- Tied to any particular technology
- A waiver
- Something only certain people can do
- Easy
- Less documentation
- Less work

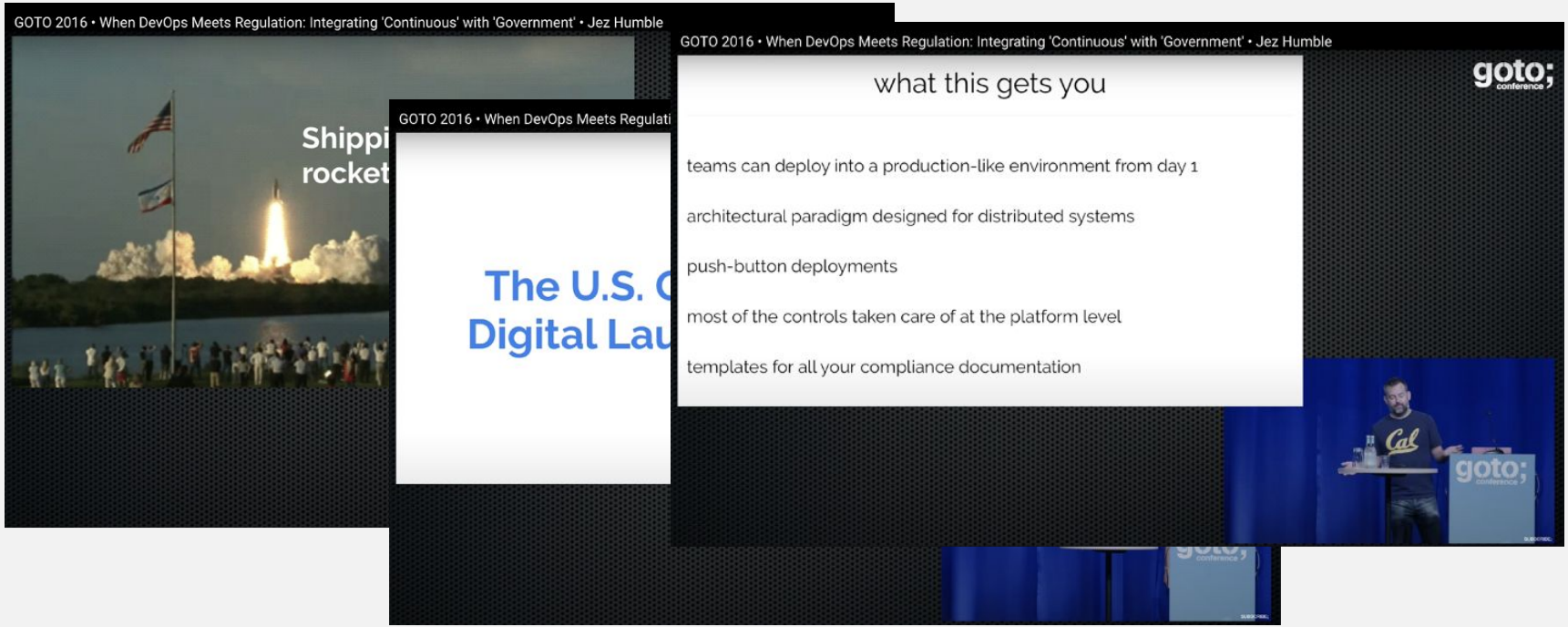
1.0

A brief history of cATO


Russian MoD Confirms US-Led Coalition's F-16, A-
Attacked Syria
Russia Had to Call U.S. Twice to Stop Syria Airstrike
Central Command has lau
over the weekend.
UN opens probe into Syria aid convoy attack
MSF TRAUMA HOSPITAL KUNDUZ, AFGHANISTAN
#INDEPENDENTINVESTIGATION CHANGE.ORG/EVENWARHASRULES
Satellite image taken 8 October 2015
Destroyed main hospital building
MSF compound
MSF TRAUMA CENTRE
MSF OFFICE
MSF TRAUMA CENTRE 36°43'4.91"N 68°51'43.96"E
MSF OFFICE 36°43'3.29"N 68°51'42.62"E
nvestigations reveal
ilian deaths in coalition
ssia: Coalitio
rces
SECURITY COUNCIL
U.S. says it
Syrian troops while
targeting ISIS
NATION/WORLD 09/17/2016, 07:00pm
Syria conflict: US air strikes 'kill d
government troops'
18 September 2016
Middle East
Syrian civil war

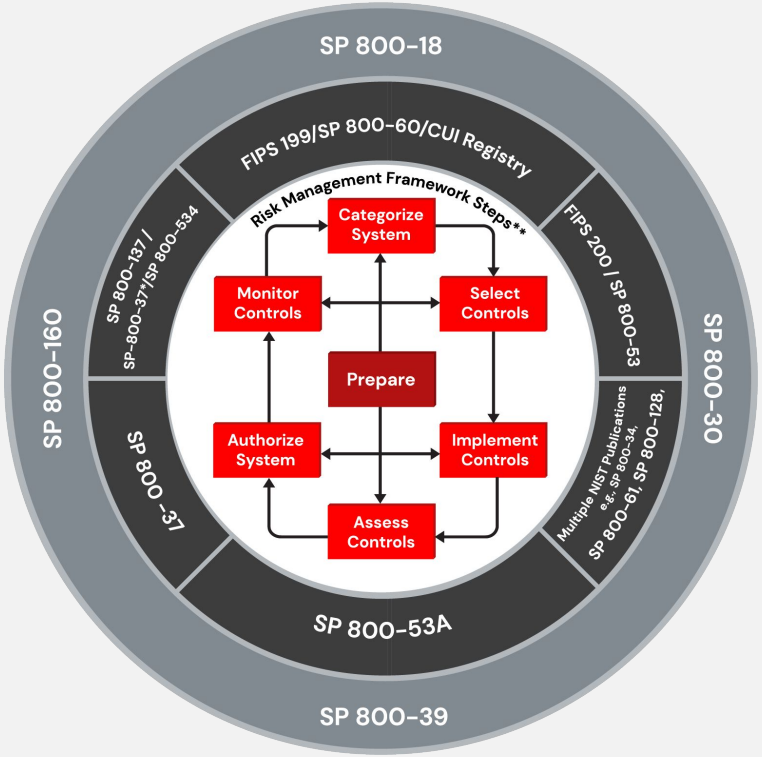
The Inspiration

INTEGRATING CONTINUOUS WITH AUTHORITY TO OPERATE



But it still wasn’t continuous...

TIME TO HIT THE BOOKS



Agile Manifesto

DON'T SKIP THE PRINCIPLES

Our highest priority is to satisfy customers through early and continuous delivery of valuable software

(If it isn't continuous, it isn't agile)

Continuous Delivery

AN EXERCISE IN RISK REDUCTION

> **The ability to get changes, features, configuration changes, bug fixes, experiments into production safely and quickly in a sustainable way.**
>
> @Jez Humble

What if you could get valuable software released on-demand, with higher quality, and reduced risk?

@Jez Humble

You can!

The barrier wasn’t RMF

RMF ENCOURAGES THIS!

FLEXIBILITY IN RMF IMPLEMENTATION

Organizations are expected to execute all steps and tasks in the RMF (apart from tasks labeled as optional). However, organizations have significant flexibility in how each of the RMF steps and tasks are carried out, as long as organizations are meeting all applicable requirements and effectively managing security and privacy risk. The intent is to allow organizations to implement the RMF in the most efficient, effective, and cost-effective manner to support mission and business needs in a way that promotes effective security and privacy. Flexible implementation may include executing tasks in a different (potentially nonsequential) order, emphasizing certain tasks over other tasks, or combining certain tasks where appropriate. It can also include the use of the Cybersecurity Framework to enhance RMF task execution.

Flexibility of implementation can also be applied to control *selection*, control *tailoring* to meet organizational security and privacy needs, or conducting control assessments throughout the SDLC. For example, the selection, tailoring, implementation, and assessments of controls can be done incrementally as a system is being developed. The implementation of control tailoring helps to ensure that security and privacy solutions are customized for the specific missions, business functions, risks, and operating environments of the organization. In the end, the flexibility inherent in RMF execution promotes effective security and privacy that helps to protect the systems that organizations depend on for mission and business success and the individuals whose information is processed by those systems.

The barrier wasn’t RMF

RMF ENCOURAGES THIS!

USE OF AUTOMATION IN THE EXECUTION OF THE RMF

Organizations should maximize the use of *automation*, wherever possible, to increase the speed, effectiveness, and efficiency of executing the steps in the Risk Management Framework (RMF). Automation is particularly useful in the assessment and continuous monitoring of controls, the preparation of authorization packages for timely decision-making, and the implementation of ongoing authorization approaches—together facilitating a real-time or near real-time risk-based decision-making process for senior leaders. Organizations have significant flexibility in deciding when, where, and how to use automation or automated support tools for their security and privacy programs. In some situations, automated assessments and monitoring of controls may not be possible or feasible.

The barrier wasn’t RMF

RMF ENCOURAGES THIS!

RMF ALIGNMENT WITH THE SDLC

The best RMF implementation is one that is indistinguishable from the routine SDLC processes carried out by organizations. That is, RMF tasks are closely aligned with the ongoing activities in the SDLC processes, ensuring the seamless integration of security and privacy protections into organizational systems—and taking maximum advantage of the artifacts generated by the SDLC processes to produce the necessary evidence in authorization packages to facilitate credible, risk-based decision making by senior leaders in organizations.

The barrier wasn’t RMF

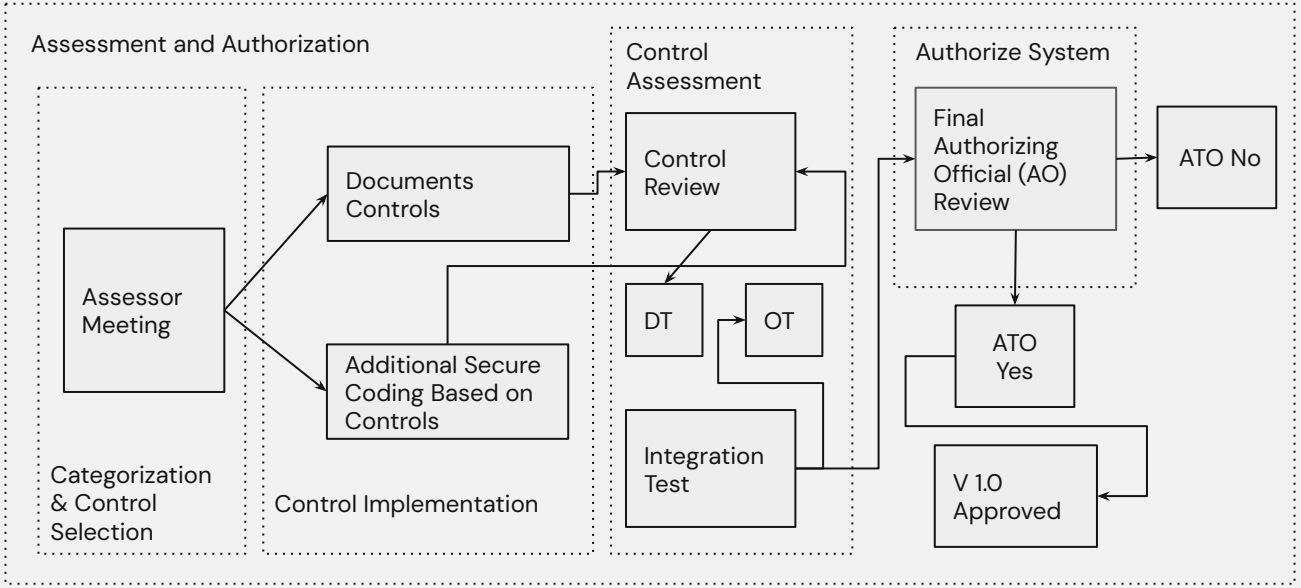
RMF ENCOURAGES THIS!

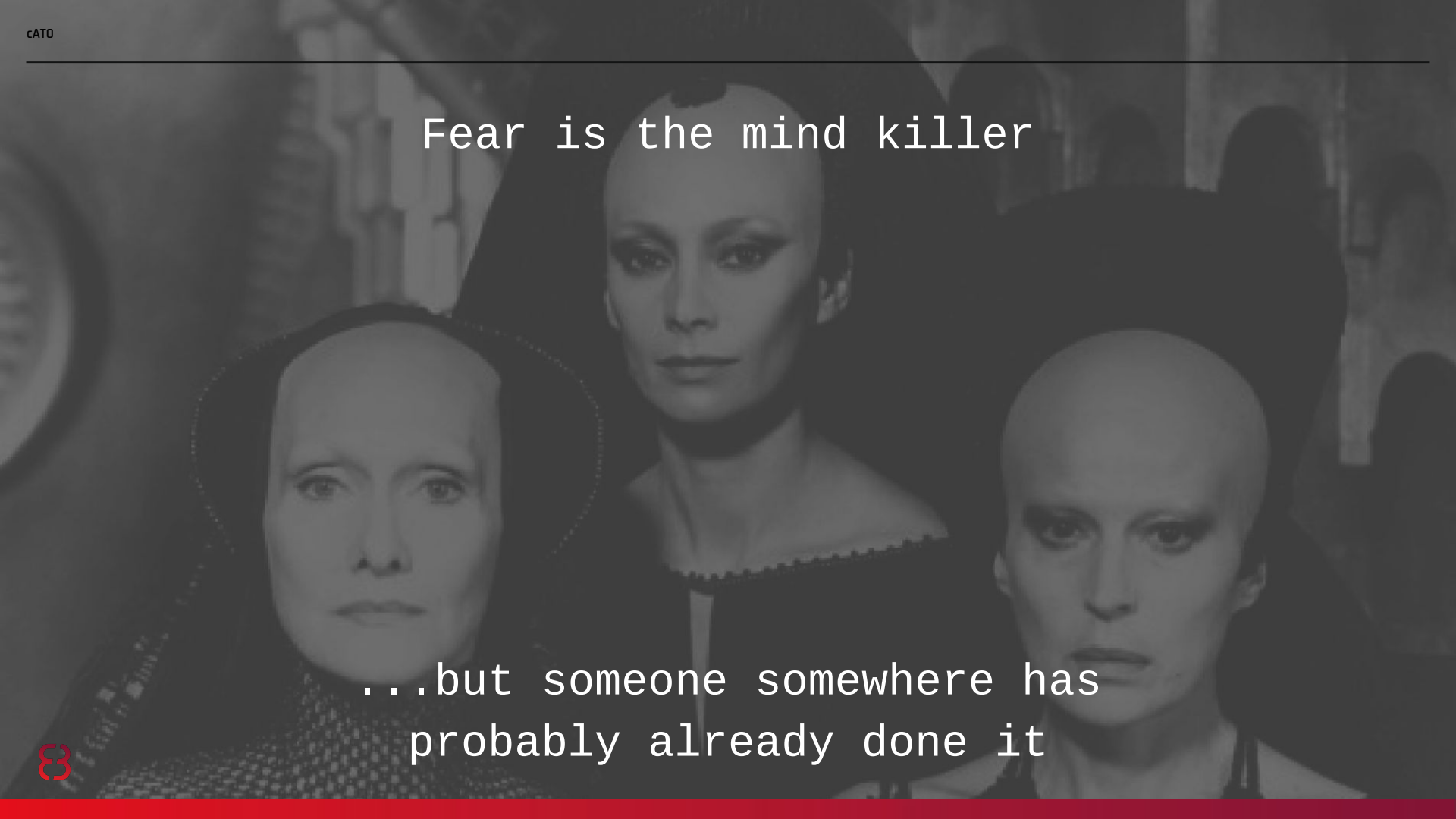
TIPS FOR STREAMLINING RMF IMPLEMENTATION

- Use the tasks and outputs of the Organization-Level and System-Level *Prepare* Step to promote a consistent starting point within organizations to execute the RMF.
- Maximize the use of *common controls* to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- Maximize the use of *shared* or *cloud-based* systems, services, and applications where applicable, to reduce the number of organizational authorizations.
- Employ *organizationally-tailored control baselines* to increase the speed of security and privacy plan development, promote consistency of security and privacy plan content, and address organization-wide threats.
- Employ *organization-defined controls* based on security and privacy requirements generated from a systems security engineering process.
- Maximize the use of *automated tools* to manage security categorization; control selection, assessment, and monitoring; and the authorization process.
- Decrease the level of effort and resource expenditures for *low-impact* systems if those systems cannot adversely affect higher-impact systems through system connections.
- Maximize the *reuse* of RMF artifacts (e.g., security and privacy assessment results) for standardized hardware/software deployments, including configuration settings.
- Reduce the *complexity* of the IT/OT infrastructure by eliminating unnecessary systems, system elements, and services — employ *least functionality* principle.
- Make the transition to *ongoing authorization* and use *continuous monitoring* approaches to reduce the cost and increase the efficiency of security and privacy programs.

“This is the way we’ve always done it”

SERIAL A&A PROCESS

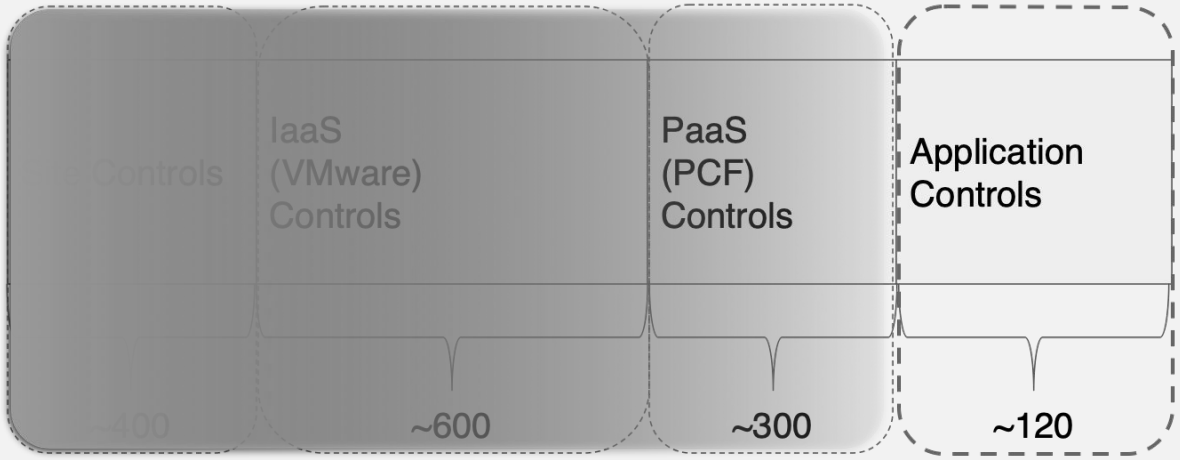



Fear is the mind killer
...but someone somewhere has
probably already done it


NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
ATO-in-a-Day
UNITED STATES OF AMERICA

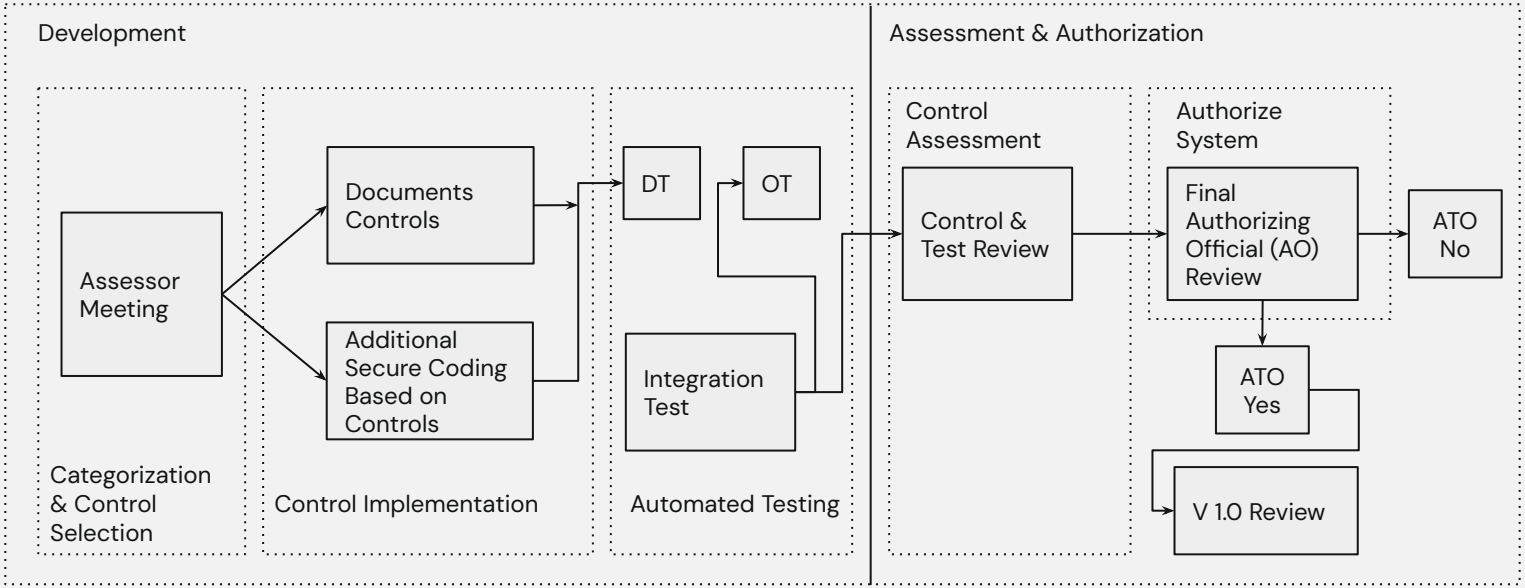
Common Controls Provided

ONLY RESPONSIBLE FOR APPLICATION CONTROLS



Better, but still not continuous...

LACK OF TRUST COMBINED WITH LACK OF INVOLVEMENT DROVE SERIAL PROCESS



Trust & Involvement

EMPATHY OVER FINGER POINTING

Assessors and authorizers don’t trust:

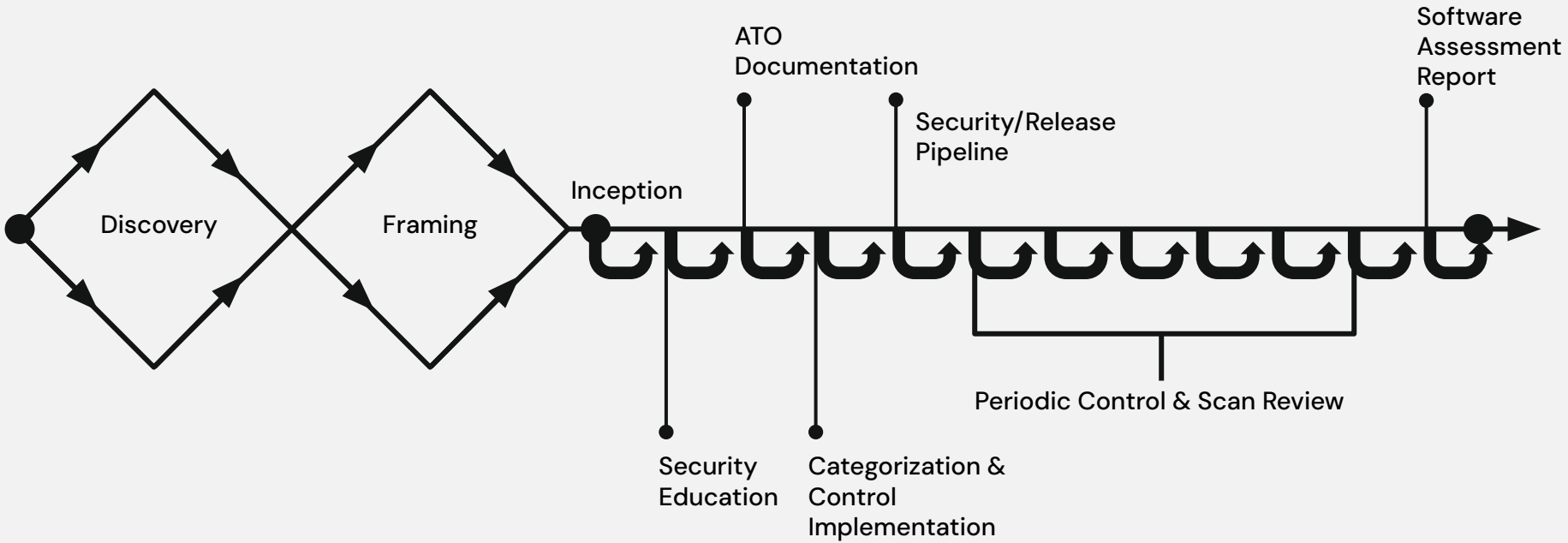
- Developers
- Program leadership
- Documentation

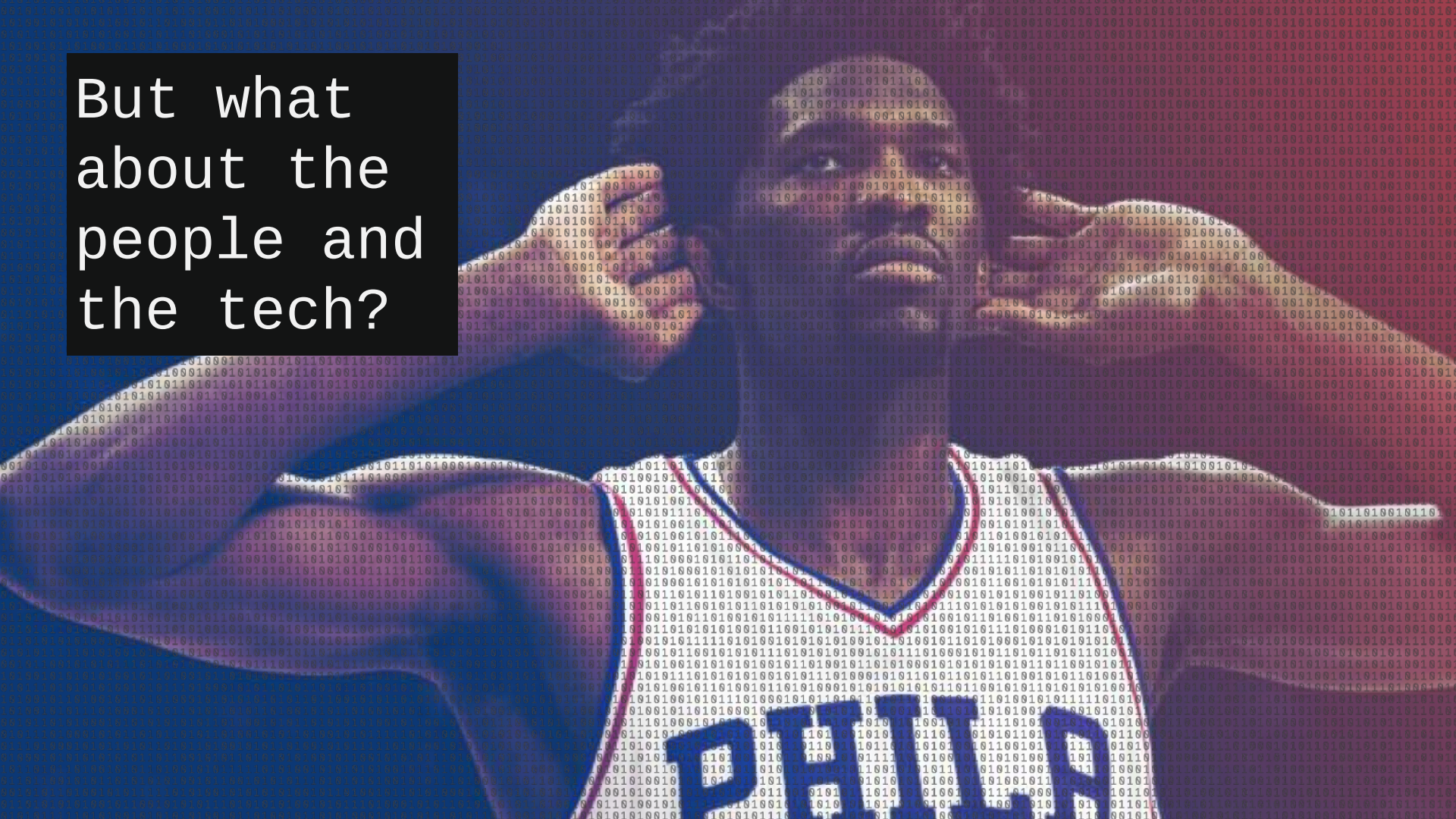
Assessors and authorizers aren’t involved in any aspect of the SDLC until software is submitted for A&A, with the exception in some cases of categorization and selection.


Trust the Process

Secure Lean Agile Software Development

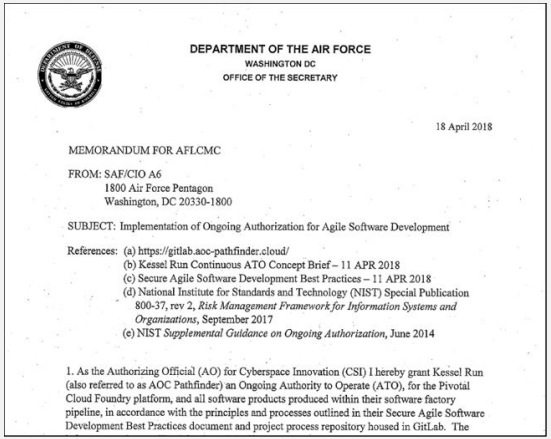
INSTILL TRUST IN THE PROCESS THROUGH INVOLVEMENT




But what about the people and the tech?

The cATO was signed

BUT NOTICE… IT'S ACTUALLY ONGOING AUTHORIZATION AND REFERENCES NIST!



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC
OFFICE OF THE SECRETARY

18 April 2018

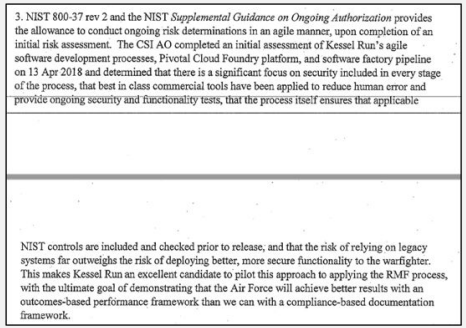
MEMORANDUM FOR AFLCMC

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

SUBJECT: Implementation of Ongoing Authorization for Agile Software Development

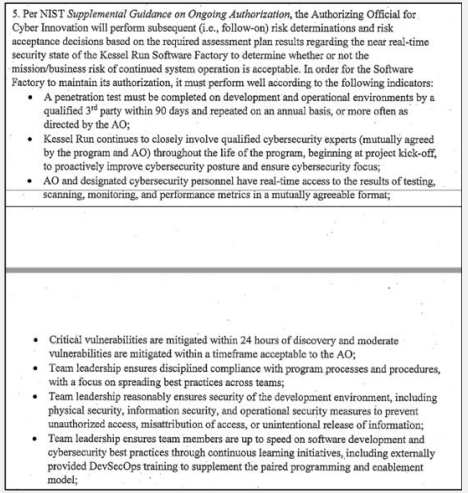
References: (a) https://gitlab.aoc-pathfinder.cloud/
(b) Kessel Run Continuous ATO Concept Brief – 11 APR 2018
(c) Secure Agile Software Development Best Practices – 11 APR 2018
(d) National Institute for Standards and Technology (NIST) Special Publication 800-37, rev 2, *Risk Management Framework for Information Systems and Organizations*, September 2017
(e) NIST *Supplemental Guidance on Ongoing Authorization*, June 2014

1. As the Authorizing Official (AO) for Cyberspace Innovation (CSI) I hereby grant Kessel Run (also referred to as AOC Pathfinder) an Ongoing Authority to Operate (ATO), for the Pivotal Cloud Foundry platform, and all software products produced within their software factory pipeline, in accordance with the principles and processes outlined in their Secure Agile Software Development Best Practices document and project process repository housed in GitLab. The



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 Kessel Run's agile software development processes, Pivotal Cloud Foundry platform, and software factory pipeline on 13 Apr 2018 and determined that there is a significant focus on security included in every stage of the process, that best in class commercial tools have been applied to reduce human error and provide ongoing security and functionality tests, that the process itself ensures that applicable

NIST controls are included and checked prior to release, and that the risk of relying on legacy systems far outweighs the risk of deploying better, more secure functionality to the warfighter. This makes Kessel Run an excellent candidate to pilot this approach to applying the RMF process, with the ultimate goal of demonstrating that the Air Force will achieve better results with an outcomes-based performance framework than we can with a compliance-based documentation framework.



5. Per NIST *Supplemental Guidance on Ongoing Authorization*, the Authorizing Official for Cyber Innovation will perform subsequent (i.e., follow-on) risk determinations and risk acceptance decisions based on the required assessment plan results regarding the near real-time security state of the Kessel Run Software Factory to determine whether or not the mission/business risk of continued system operation is acceptable. In order for the Software Factory to maintain its authorization, it must perform well according to the following indicators:

- A penetration test must be completed on development and operational environments by a qualified 3rd party within 90 days and repeated on an annual basis, or more often as directed by the AO;
- Kessel Run continues to closely involve qualified cybersecurity experts (mutually agreed by the program and AO) throughout the life of the program, beginning at project kick-off, to proactively improve cybersecurity posture and ensure cybersecurity focus;
- AO and designated cybersecurity personnel have real-time access to the results of testing, scanning, monitoring, and performance metrics in a mutually agreeable format;

- Critical vulnerabilities are mitigated within 24 hours of discovery and moderate vulnerabilities are mitigated within a timeframe acceptable to the AO;
- Team leadership ensures disciplined compliance with program processes and procedures, with a focus on spreading best practices across teams;
- Team leadership reasonably ensures security of the development environment, including physical security, information security, and operational security measures to prevent unauthorized access, misattribution of access, or unintentional release of information;
- Team leadership ensures team members are up to speed on software development and cybersecurity best practices through continuous learning initiatives, including externally provided DevSecOps training to supplement the paired programming and enablement model;

The automated pipeline was put in place as a partnership between the Air Force, DIUX, and DevSecOps experts at Pivotal Labs, and was modeled on the NGA automated pipeline that is the cornerstone of NGA's ATO in a Day program. This continuous process of updating the tasks needed to keep the project compliant creates a valuable feedback loop between the security and development teams, and creates a Trackable Identifier for any task in the process from control to task to code.

2.0

Continuous RMF

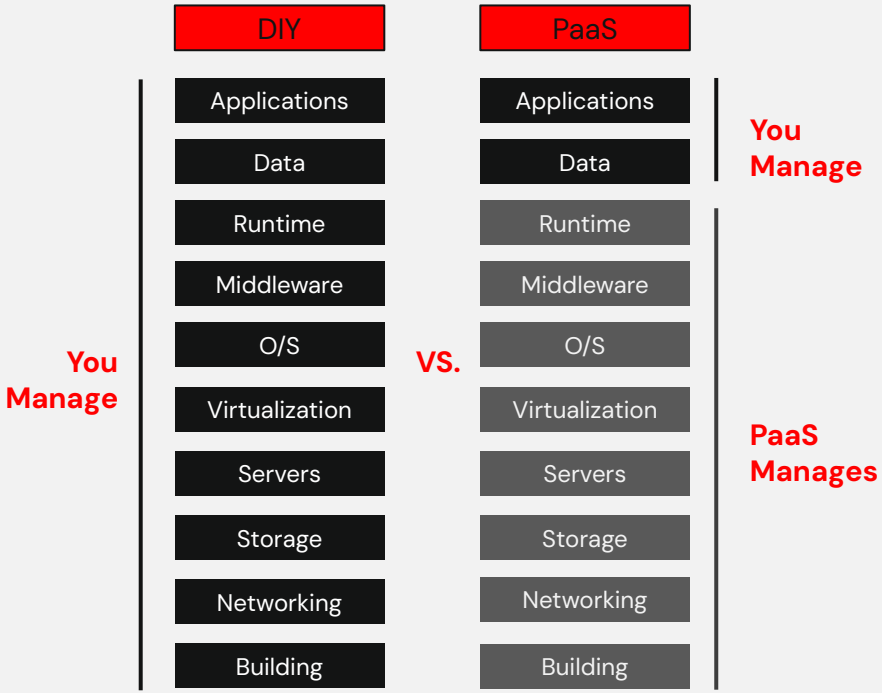
Prepare, Categorize, & Select

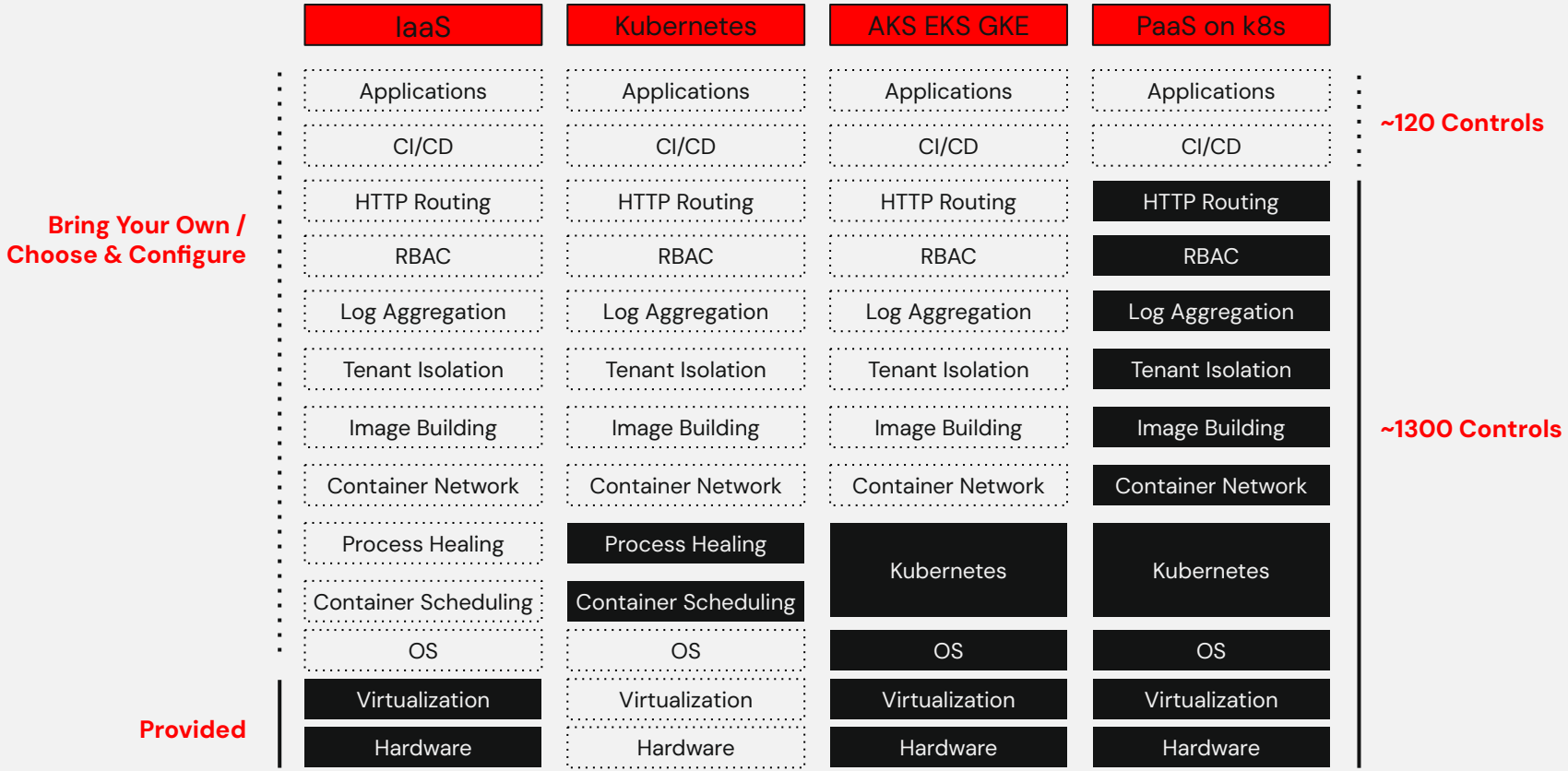
INTRODUCE ALL THE THINGS

- Use the Prepare step to align all stakeholders to an ongoing authorization strategy using people, process, and technology to achieve near real-time continuous monitoring of controls and cybersecurity (this presentation ;-)
    - Present plan for maximizing common controls inheritance
    - Present tools and automation to be used for both digitization of documentation (the entire BOE) and automation of workflows and tasks
    - Define the authorization boundary in a cloud context and how any -aaS situations between AOs will be handled (we recommend shared responsibility model with SLOs/SLAs)
- The Categorize step remains largely the same, but is the first opportunity to show that tasks (C-1, C-2, & C-3) can be done more quickly with cross functional team
- During the Select step, make use of control tailoring (Task S-2). This is one of the most overlooked tasks and is critical to efficacy and efficiency of your cRMF
    - Think about compensating controls when necessary for things like the use of SaaS awaiting FedRAMP and/or DISA SRG IL P-ATO

The Platform

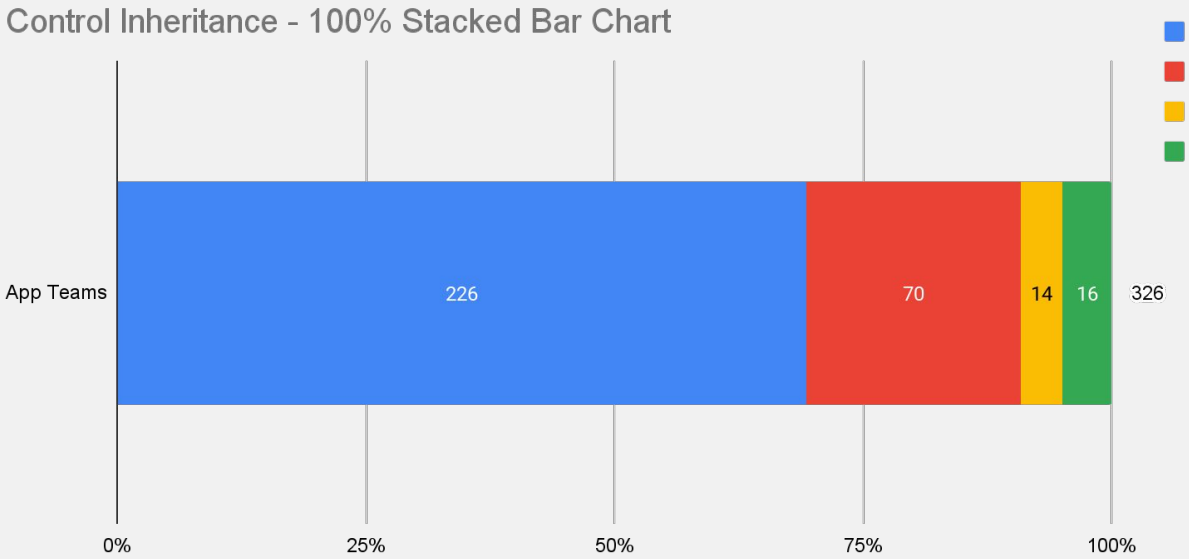
PAAS IS A PRE-REQ FOR DEVOPS OUTCOMES IN THE ENTERPRISE




IaaS
Kubernetes
AKS EKS GKE
PaaS on k8s
Applications
CI/CD
HTTP Routing
RBAC
Log Aggregation
Tenant Isolation
Image Building
Container Network
Process Healing
Container Scheduling
OS
Virtualization
Hardware
Kubernetes
Bring Your Own / Choose & Configure
Provided
~120 Controls
~1300 Controls

Example Inheritance Metrics

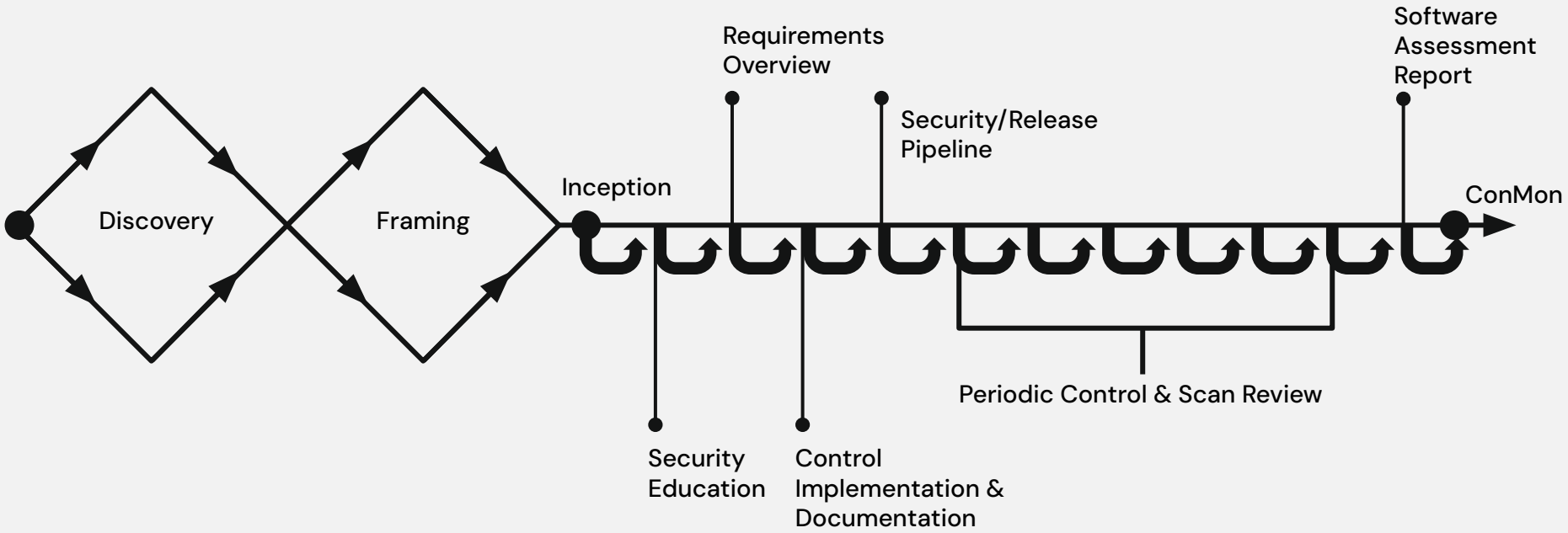
Shown by control family



Nearly 70% of controls are inherited at the Application level, and 27% of that inheritance comes directly from the Platform (with plenty of room to grow)

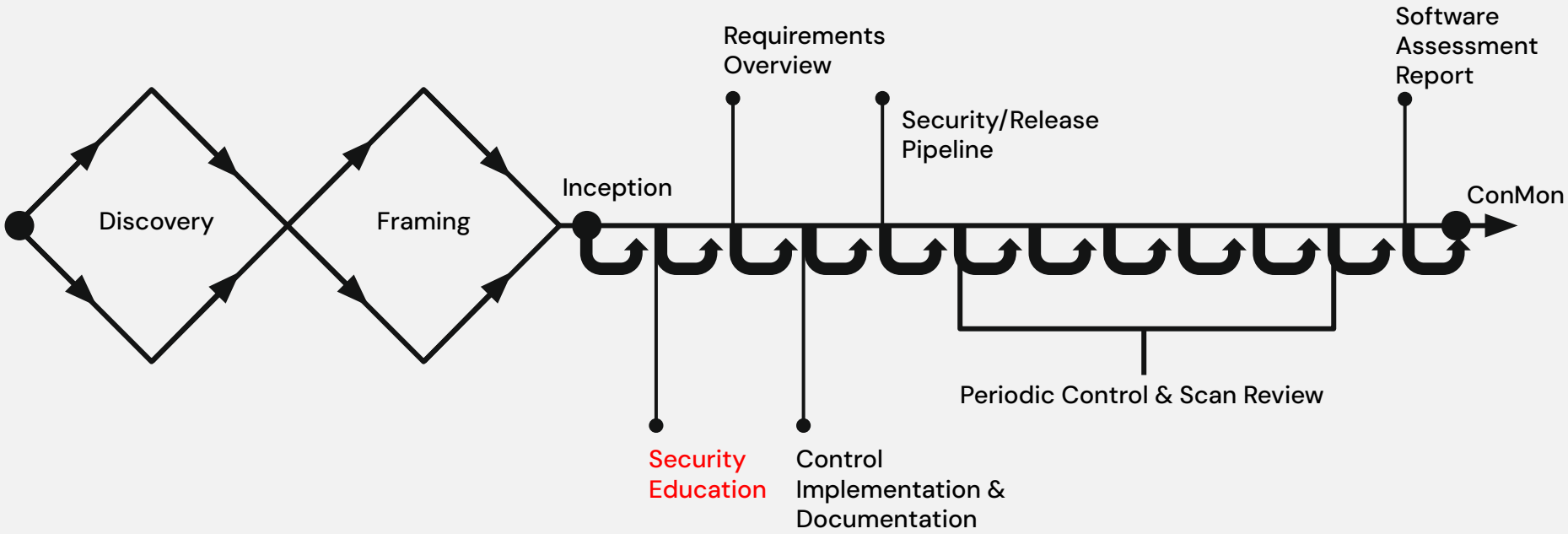
Secure Lean Agile Software Development

INSTILL TRUST IN THE PROCESS THROUGH INVOLVEMENT



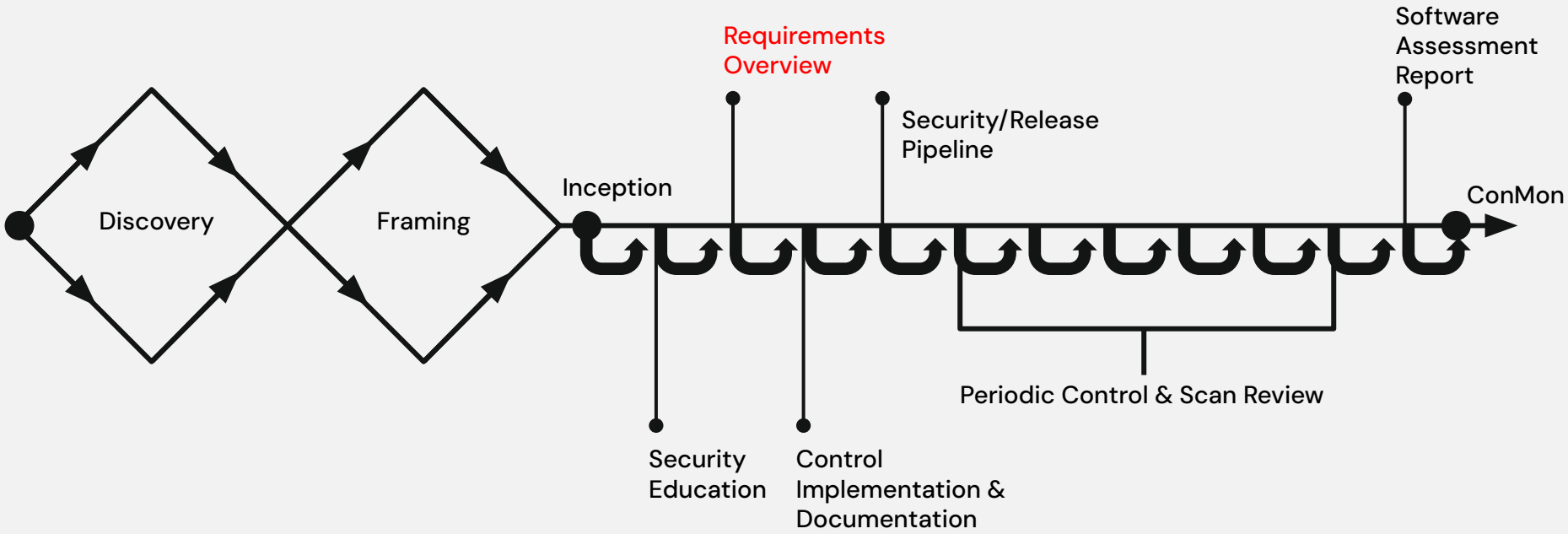
Security Education

SHORTLY AFTER TEAM INCEPTION



ATO Requirements Overview

INSTILL TRUST IN THE PEOPLE & PROCESS THROUGH INVOLVEMENT




UP TO DATE DOCUMENTATION
NOW THAT'S SOMETHING I'VE NOT SEEN IN A LONG TIME

ATO Documentation Required

INTRODUCE ALL THE THINGS

- ATO Checklist
- Plan of Action
- System Security Plan
- Architecture Diagram
- Fortify, threadfix, sonarqube scans

Plan of Action

Plan of Action for Kessel Run Sample Application

Test App, MVP and Beyond

Note: The Test App consists of a subset of features that will comprise our MVP.

- **Kick-off Date:**
- **Inception Date:**
- **MVP Date:**

Vision

Strategy

Summary

This project is to educate new and existing dev teams on current and future projects to read and interpret the plan as presented in the **Kessel Run Sample Application* __..__ Reduce the time it takes for dev teams to onboard and be prepared

Goals and Metrics

Release Focus

- Increase confidence in dev teams ability to onboard

Release Functionality

- Provides developers with an application to get started

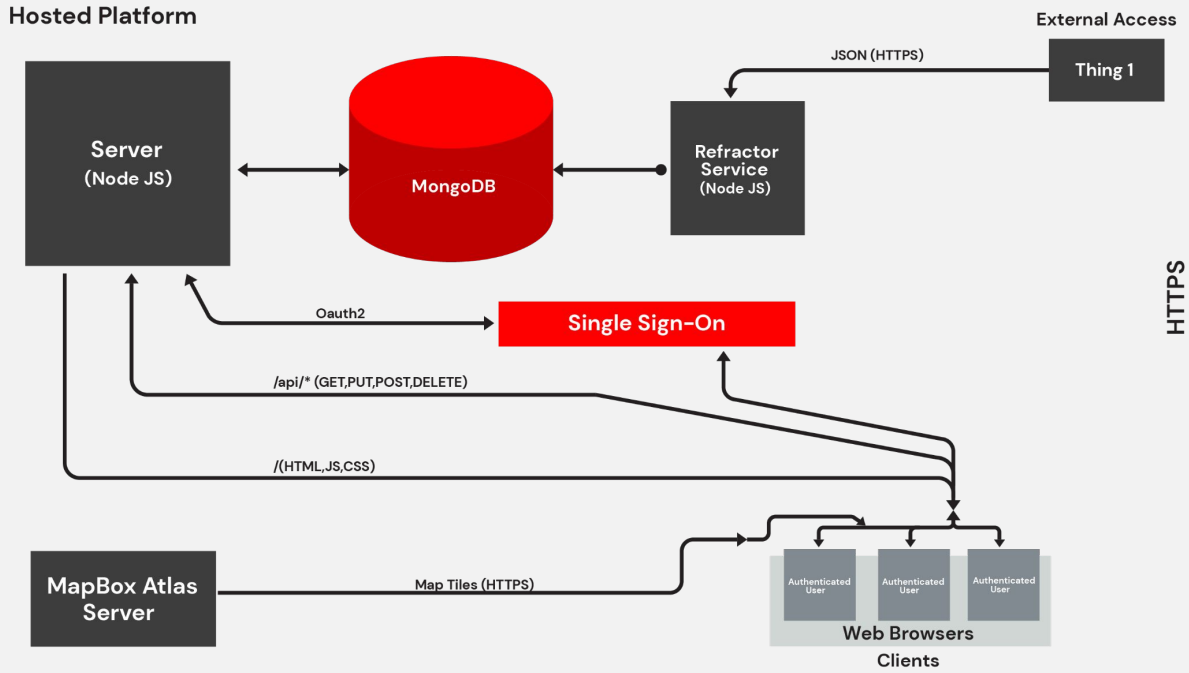
System Integration Considerations

- Integrates with the continuous ATO pipeline
- Reduces onboarding hassel for dev teams

Architecture Diagram

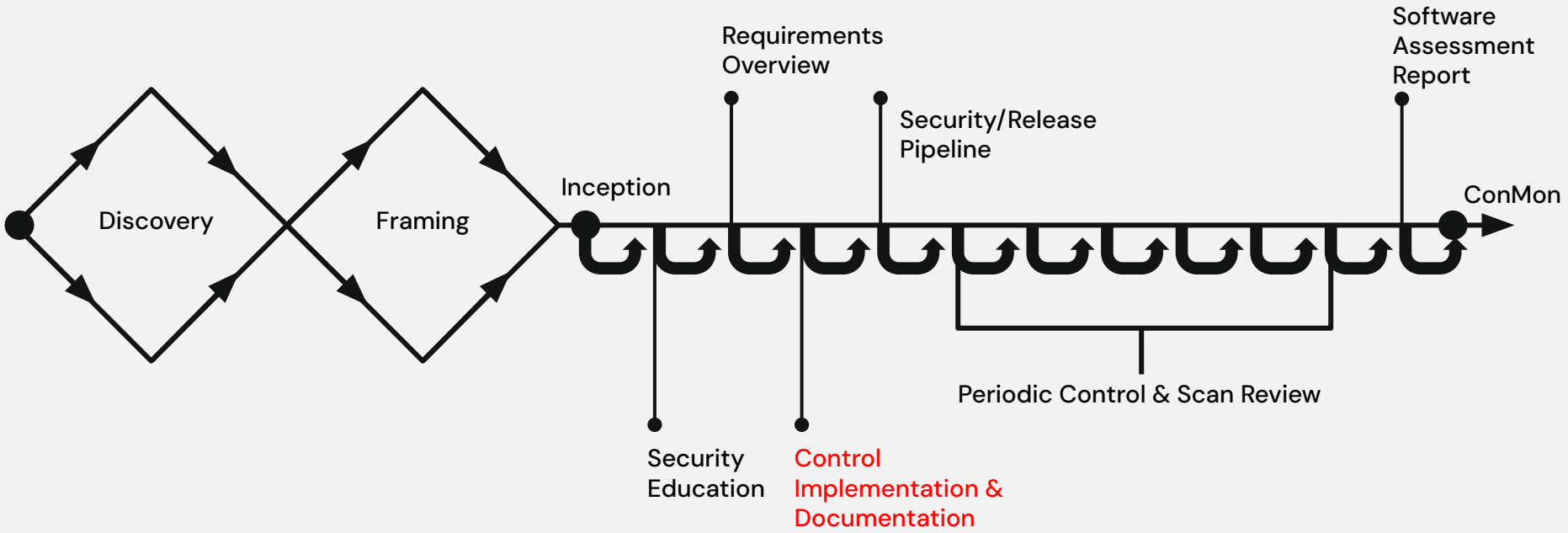
THESE STILL MATTER

- Frontend Requirements
- Backend Requirements
- Database Use
- Languages
- Connections
- 3rd Party Services



Implementation & Documentation

INSTILL TRUST IN THE PEOPLE & PROCESS THROUGH INVOLVEMENT



Implementation

GOALS

- An hour meeting
- Assign the team an assessor
- Perform product architectural analysis
- Determines app-level categorization
- Select and assign team controls
- Assigned assessor will help team prioritize backlog security items

Categorization

Confidentiality (C)

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

A loss of confidentiality is the unauthorized disclosure of information.

Integrity (I)

Guarding against improper information modification or destruction, and includes ensuring information and non-repudiation and authenticity.

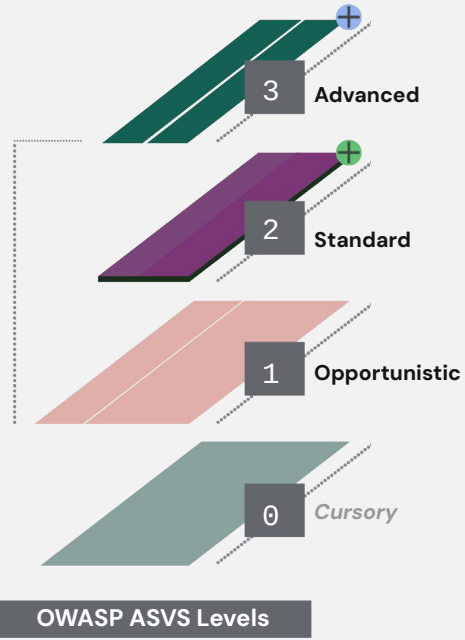
A loss of integrity is the unauthorized modification or destruction of information.

Availability (A)

Ensuring timely and reliable access to and use of information.

A loss of availability is the disruption of access to or use of information or an information system.

ASVS defines detailed verification requirements for levels 1 and above; whereas level 0 is meant to be flexible and is customized by each organization.

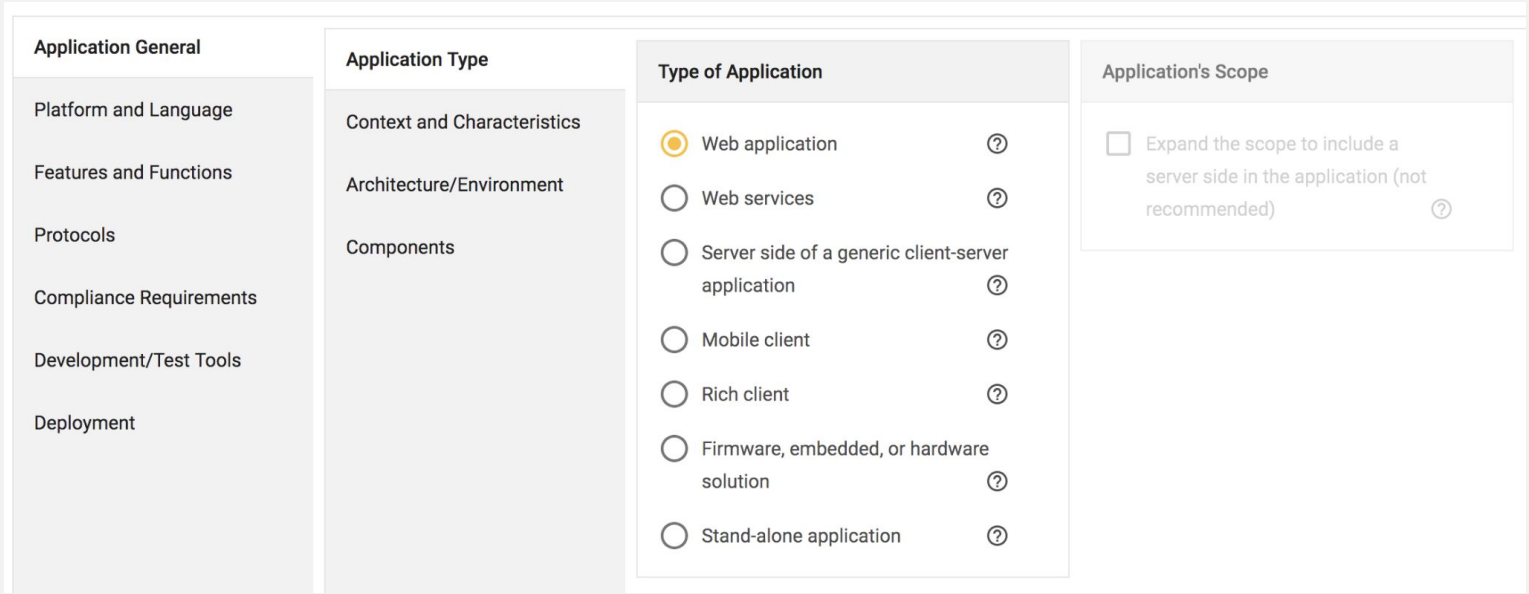


OWASP ASVS Levels

SD ELEMENTS

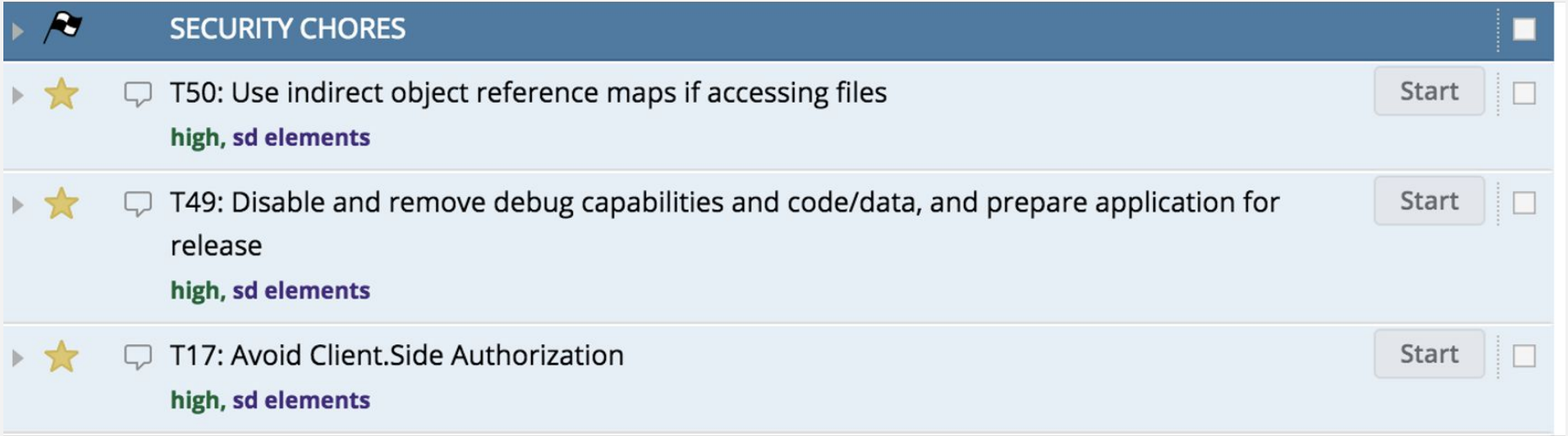
Project Survey

CATEGORIZATION



Security Product Backlog

SD ELEMENTS PUSHES STORIES TO THE BACKLOG



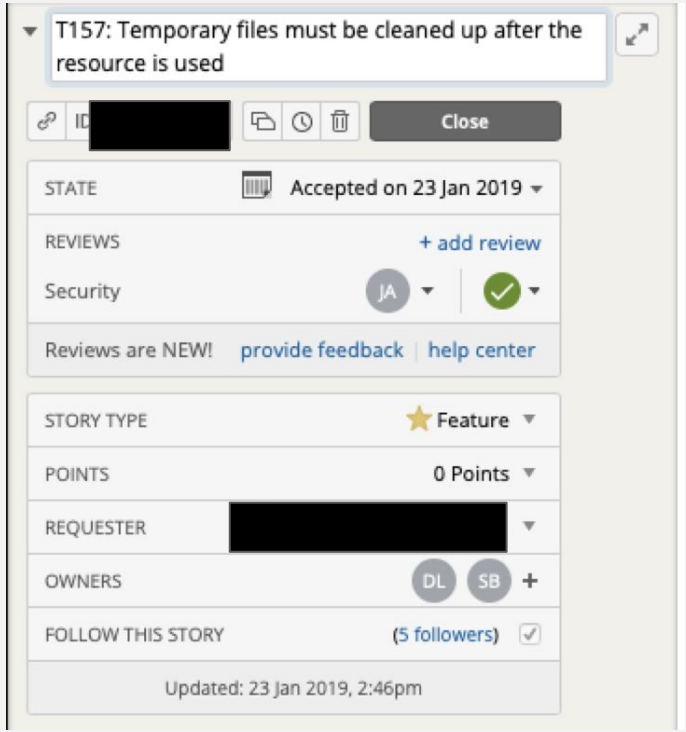
Preferred SD Element Task Comments

For every SD Elements task in the backlog, please compose the comments in the following way:

1. Describe the team's technical decision on implementation for the task
2. Provide a link to the code and context to make reviewing easier
3. Provide a technical point of contact with name and email, who signed for the task completion
4. Add a security assessor assigned to the project as a reviewer for the completion of this story

Example SD Elements Reviewer

Make sure to mark your security assessor as a reviewer to mark the task as complete

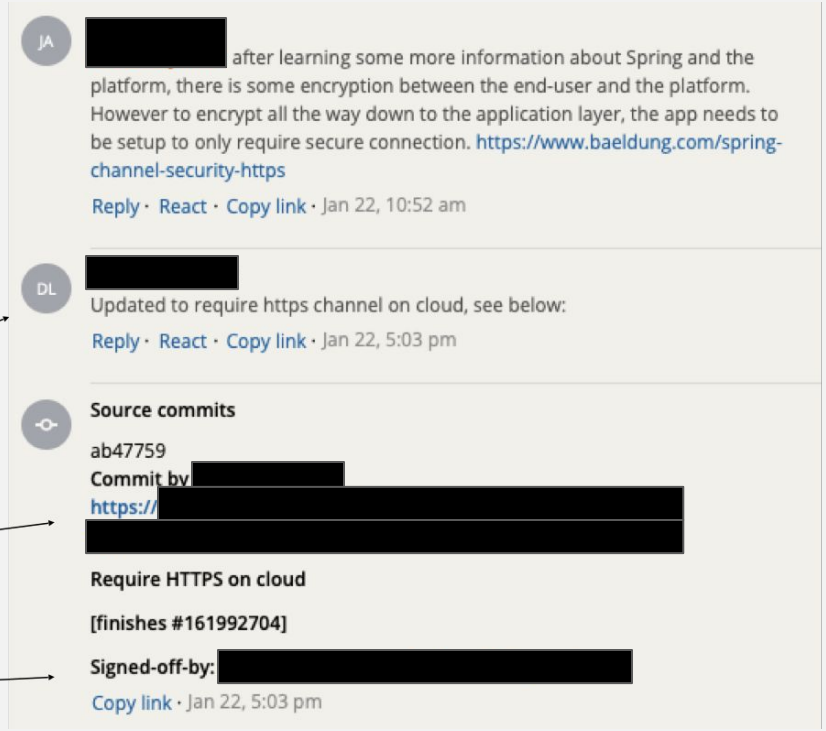


Example SD Elements Chore Comments

Task technical decision

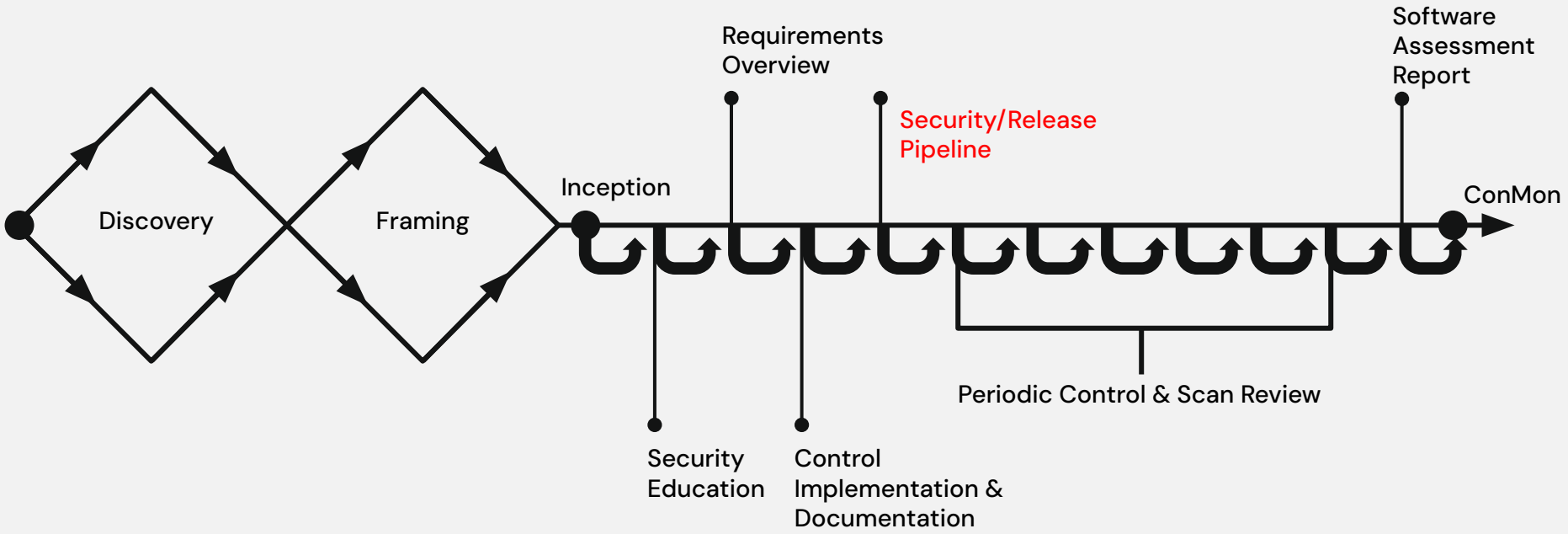
Implementation Link

Signed off by (name/email)



Secure Lean Agile Software Development

INSTILL TRUST IN THE PEOPLE & PROCESS THROUGH INVOLVEMENT



Security and Release Pipeline

AUTOMATE CHECKS

Performs security scans on application focusing on three areas

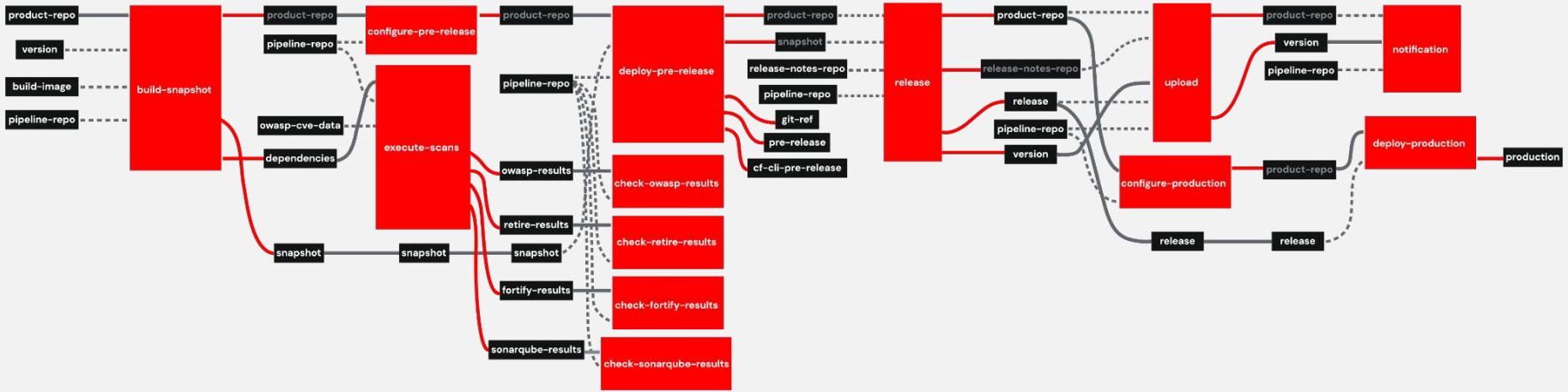
- Dependency checking
- Vulnerability analysis
- Code coverage

Also performs unit, journey, and integration testing

Enforces release engineering best practices

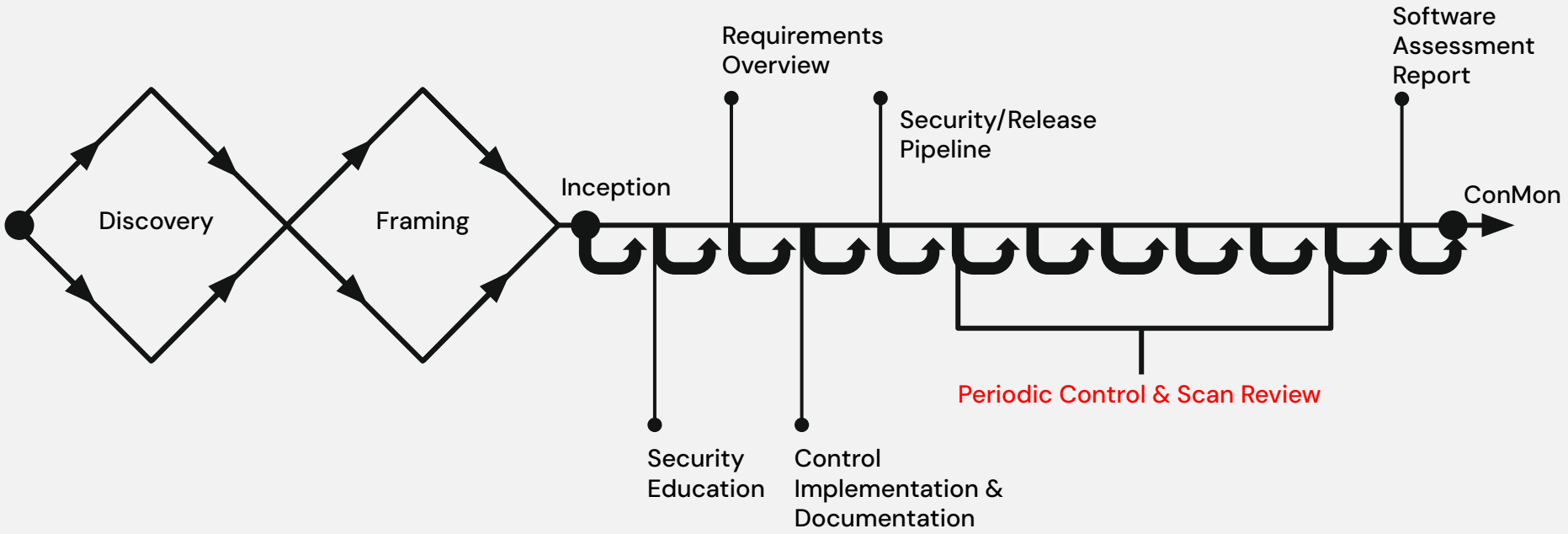
Security Pipeline

AUTOMATE CHECKS



Secure Lean Agile Software Development

INSTILL TRUST IN THE PEOPLE & PROCESS THROUGH INVOLVEMENT



Periodic Controls and Scan Review

Weekly meeting will be set between assessor and team

Assigned assessor must have access to the team's backlog

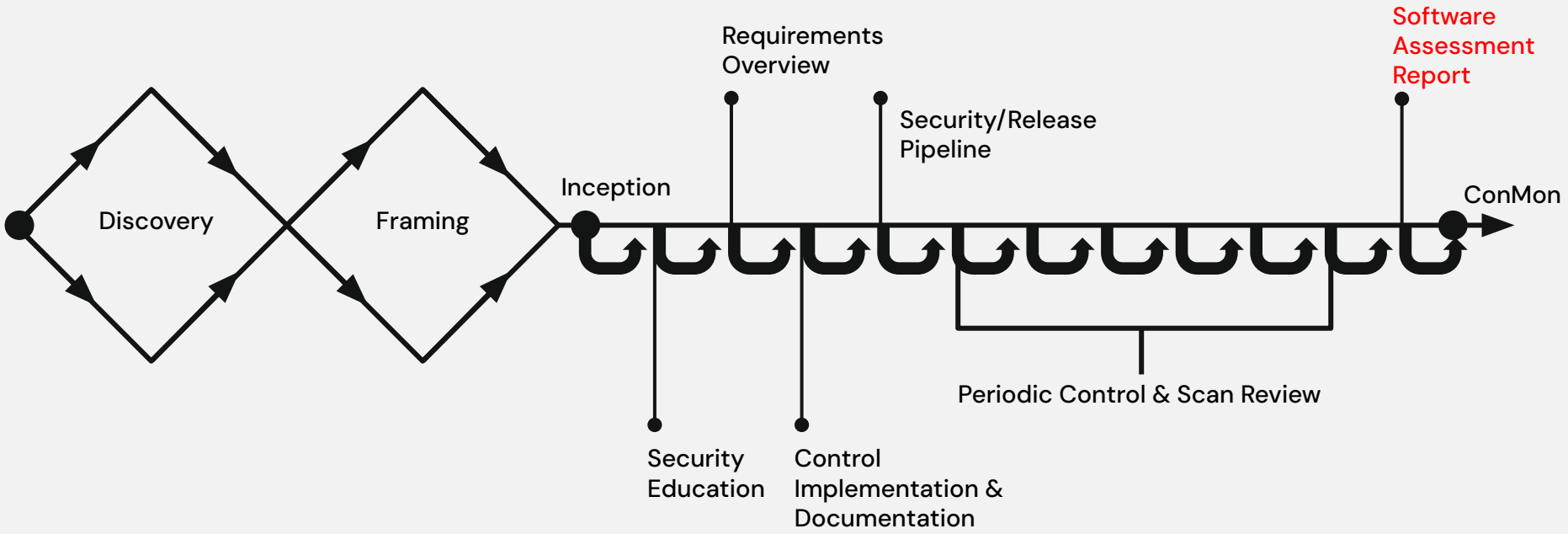
Help prioritize security controls

Determine product security progress

Answer any questions or concerns by the team

Secure Lean Agile Software Development

INSTILL TRUST IN THE PEOPLE & PROCESS THROUGH INVOLVEMENT



Software Assessment Report (SAR)

THIS DOCUMENT SIGNIFIES THE THUMBS UP TO PROD

Developed by assessors from previously gathered data

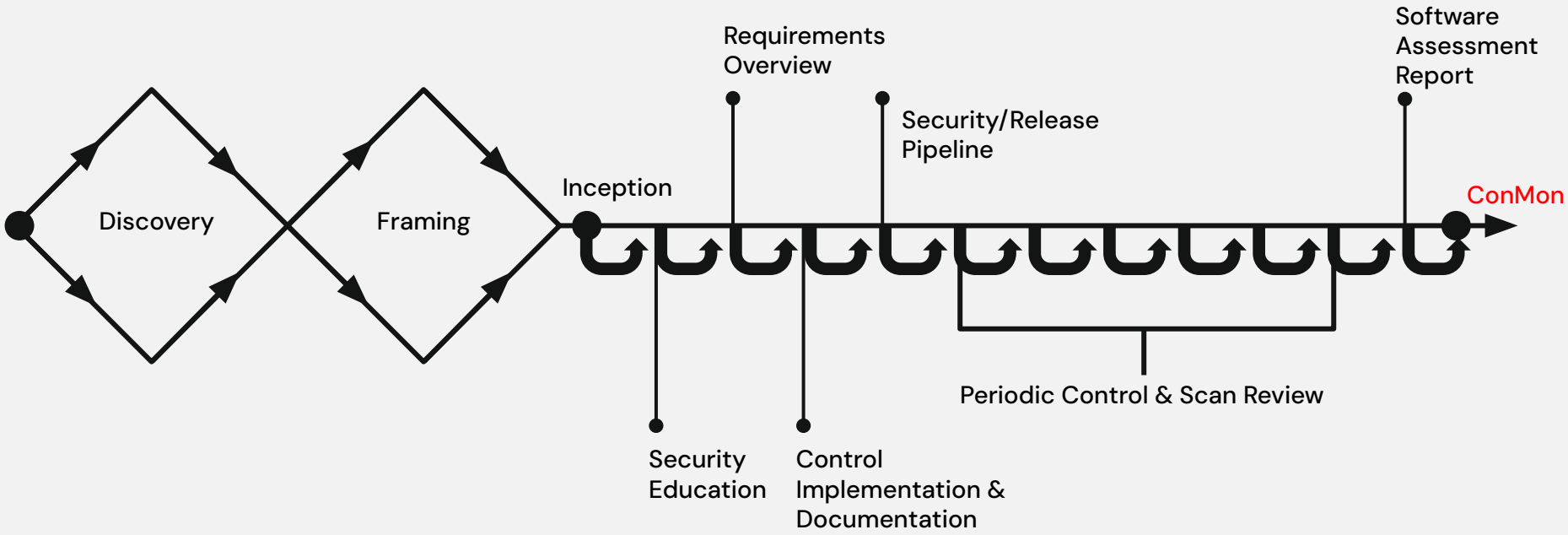
- Control implementation documentation
- Scan results and documented actions

Each application assigned a risk rating

Any additional security concerns are addressed

Secure Lean Agile Software Development

INSTILL TRUST IN THE PEOPLE & PROCESS THROUGH INVOLVEMENT



Continuous Monitoring Recommendations

KEY TO ONGOING AUTHORIZATION

Aside from monitoring via automation, an Assessor should be staffed organically to:

- Review scan results when developers mark findings as false positive
  - Provide feedback to developers if disagree
  - Assist developers with mitigations
- Review security tasks as developers complete them
  - Provide feedback to developers if task hasn't been satisfied
- Monitor system diagram and overall SSP for changes
- Perform spot checks
- Penetration Testing

Initial Authorization to Ongoing Auth

ZERO-BASED REVIEW FIRST

- Perform initial zero-based authorization for the system as whole (IaaS + PaaS + SecRel + App(s))
  - Recommend getting waiver for eMASS and using spreadsheet and/or SDE
- Grant ongoing authorization
  - Leverage a memorandum signed by the AO
  - Implement *renewal frequency* per NIST 800-37
- We recommend quarterly risk reporting to stakeholders (AO, SCA, etc.)
  - Manual via brief to start, move to automated/dashboard as you mature
  - Identify and accept risk
  - Make necessary corrections
  - Formally document renewal

Quarterly Review

IDEAS TO START WITH

- New applications shipped onto the platform
  - % security requirements (SD Elements) approved by assessor
  - Compliance with Lighthouse ongoing authorization playbook policy
  - Penetration test results
  - Control traceability metrics
- Platform
  - Control compliance
  - Penetration test results
- Organization
  - Risk
  - Roles & Responsibilities
  - Policy
  - Staffing

Communication Strategy

STAY ON TOP OF COMMS!

- RMF is our common denominator, start there
- Discuss real concerns, don’t generalize
- Compare outcomes, not intentions vs outcomes
- Afford us the ability to experiment and create a better process

3.0

Recap

Important Closing Notes

MYTHS

"The RMF is purposefully designed to be technology neutral so that the methodology can be applied to any type of information system* without modification."

cATO requires RMF excellence—it's more RMF, not less AND more work, not less

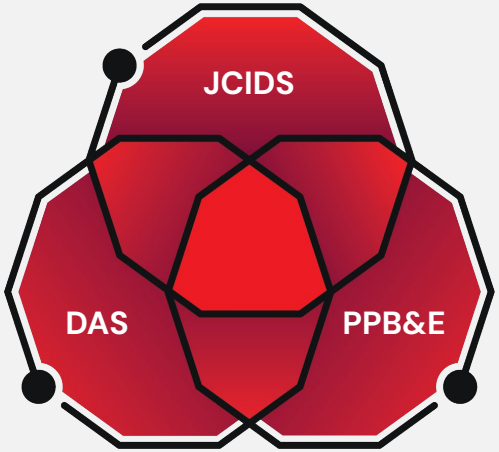
You still have to document, and if you say it's in git, it better actually be in git

Any AO can do an ongoing authorization, including one that converges RMF and the SDLC—NIST RMF says so explicitly and it meets FISMA requirements!

Last Note: Agile Everything

LOTS MORE BOTTLENECKS

- Automated DT/OT
- Automated security/ATO
- Automated fielding



- Value stream mapping
- Impact mapping

- Modular contracting strategy
- FAR 13 & GSA for contracted support
- FAR 12 & GSA for commercial items
- Use OTAs for new prototypes

- Estimate dev capacity req'd
- Size platform needs
- PPB&E on product teams & platform

Mitigate risk through metered funding
Allocate funding via growth boards
Growth boards hold product teams accountable for outcomes
JCIDS defined impacts

Questions?

4.0

Backup

NIST Pub Excerpts

WHAT YOU NEED TO KNOW

There are two approaches that can be used for the initial selection of controls: a baseline control selection approach, or an organization-generated control selection approach

When an information system is under ongoing authorization, the authorization package is presented to the authorizing official via automated reports to provide information in the most efficient and timely manner possible. Information to be presented to the authorizing official in assessment reports is generated in the format and with the frequency determined by the organization using information from the information security and privacy continuous monitoring programs.

The authorization package may be provided to the authorizing official in hard copy or electronically or may be generated using an automated security/privacy management and reporting tool. Organizations can use automated support tools in preparing and managing the content of the authorization package. Automated support tools provide an effective vehicle for maintaining and updating information for authorizing officials regarding the ongoing security and privacy posture of information systems within the organization. [DON'T USE EMASS]

The explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization.

To employ an ongoing authorization approach, organizations have in place an organization level and system-level continuous monitoring process to assess implemented controls on an ongoing basis

NIST Pub Excerpts

WHAT YOU NEED TO KNOW

The authorization termination date is established by the authorizing official and indicates when the authorization expires. Organizations may eliminate the authorization termination date if the system is operating under an ongoing authorization—that is, the continuous monitoring program is sufficiently robust and mature to provide the authorizing official with the needed information to conduct ongoing risk determination and risk acceptance activities regarding the security and privacy posture of the system and the ongoing effectiveness of the controls employed within and inherited by the system.

When the system is operating under ongoing authorization, the authorizing official continues to be responsible and accountable for explicitly understanding and accepting the risk of continuing to operate or use the system or continuing to provide common controls for inheritance. For ongoing authorization, the authorization frequency is specified in lieu of an authorization termination date. The authorizing official reviews the information with the specific time-driven authorization frequency defined by the organization as part of the continuous monitoring strategy and determines if the risk of continued system operation or the provision of common controls remains acceptable. If the risk remains acceptable, the authorizing official acknowledges the acceptance in accordance with organizational processes. If not, the authorizing official indicates that the risk is no longer acceptable and requires further risk response or a full denial of the authorization.

NIST Pub Excerpts

WHAT YOU NEED TO KNOW

The use of automated support tools to capture, organize, quantify, visually display, and maintain security and privacy posture information promotes near real-time risk management regarding the risk posture of the organization. The use of metrics and dashboards increases an organization's capability to make risk based decisions by consolidating data in an automated fashion and providing the data to decision makers at different levels within the organization in an easy-to-understand format.

NIST Pub Excerpts

WHAT YOU NEED TO KNOW

This update to NIST Special Publication 800-37 (Revision 2) responds to the call by the Defense Science Board, the Executive Order, and the OMB policy memorandum to develop the next generation Risk Management Framework (RMF) for information systems, organizations, and individuals. There are seven major objectives for this update:

To provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization;

To institutionalize critical risk management preparatory activities at all risk management levels to facilitate a more effective, efficient, and cost-effective execution of the RMF;

To demonstrate how the NIST Cybersecurity Framework [NIST CSF] can be aligned with the RMF and implemented using established NIST risk management processes;

To integrate privacy risk management processes into the RMF to better support the privacy protection needs for which privacy programs are responsible;

To promote the development of trustworthy secure software and systems by aligning life cycle-based systems engineering processes in NIST Special Publication 800-160, Volume 1 [SP 800-160 v1], with the relevant tasks in the RMF;

NIST Pub Excerpts

WHAT YOU NEED TO KNOW

To integrate security-related, supply chain risk management (SCRM) concepts into the RMF to address untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC; and

To allow for an organization-generated control selection approach to complement the traditional baseline control selection approach and support the use of the consolidated control catalog in NIST Special Publication 800-53, Revision 5. The addition of the Prepare step is one of the key changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. The primary objectives for institutionalizing organization-level and system-level preparation are:

To facilitate effective communication between senior leaders and executives at the organization and mission/business process levels and system owners at the operational level; • To facilitate organization-wide identification of common controls and the development of organizationally-tailored control baselines, reducing the workload on individual system owners and the cost of system development and asset protection;

To reduce the complexity of the information technology (IT) and operations technology (OT) infrastructure using Enterprise Architecture concepts and models to consolidate, optimize, and standardize organizational systems, applications, and services;

NIST Pub Excerpts

WHAT YOU NEED TO KNOW

To reduce the complexity of systems by eliminating unnecessary functions and security and privacy capabilities that do not address security and privacy risk; and

To identify, prioritize, and focus resources on the organization's high value assets (HVA) that require increased levels of protection—taking measures commensurate with the risk to such assets.

By achieving the above objectives, organizations can simplify RMF execution, employ innovative approaches for managing risk, and increase the level of automation when carrying out specific tasks. Organizations implementing the RMF will be able to:

- Use the tasks and outputs of the Organization-Level and System-Level Prepare step to promote a consistent starting point within organizations to execute the RMF;
- Maximize the use of common controls at the organization level to promote standardized, consistent, and cost-effective security and privacy capability inheritance;
- Maximize the use of shared or cloud-based systems, services, and applications to reduce the number of authorizations needed across the organization;
- Employ organizationally-tailored control baselines to increase the speed of security and privacy plan development and the consistency of security and privacy plan content;
- Employ organization-defined controls based on security and privacy requirements generated from a systems security engineering process;

NIST Pub Excerpts

WHAT YOU NEED TO KNOW

Maximize the use of automated tools to manage security categorization; control selection, assessment, and monitoring; and the authorization process;

Decrease the level of effort and resource expenditures for low-impact systems if those systems cannot adversely affect higher-impact systems through system connections;

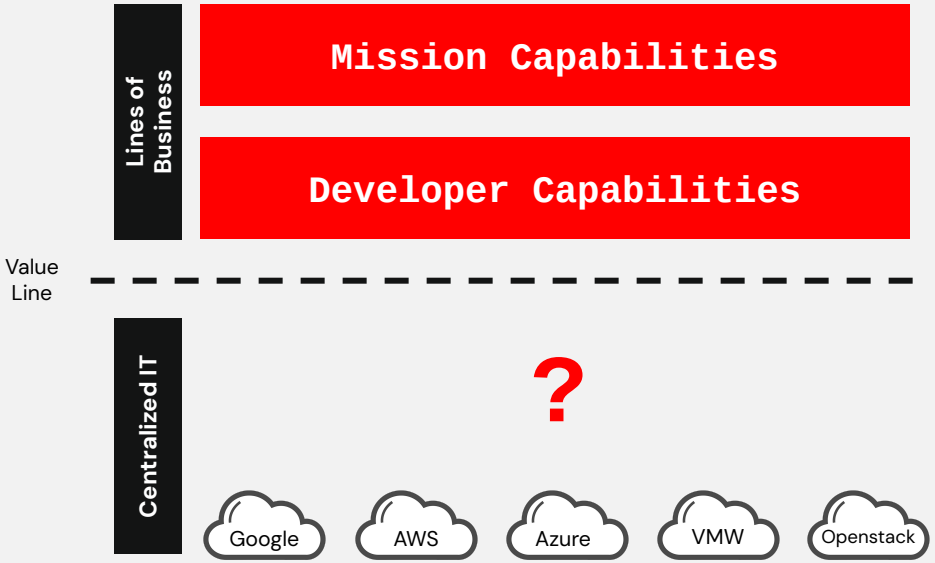
Maximize the reuse of RMF artifacts (e.g., security and privacy assessment results) for standardized hardware/software deployments, including configuration settings;

Reduce the complexity of the IT/OT infrastructure by eliminating unnecessary systems, system components, and services — employing the least functionality principle; and

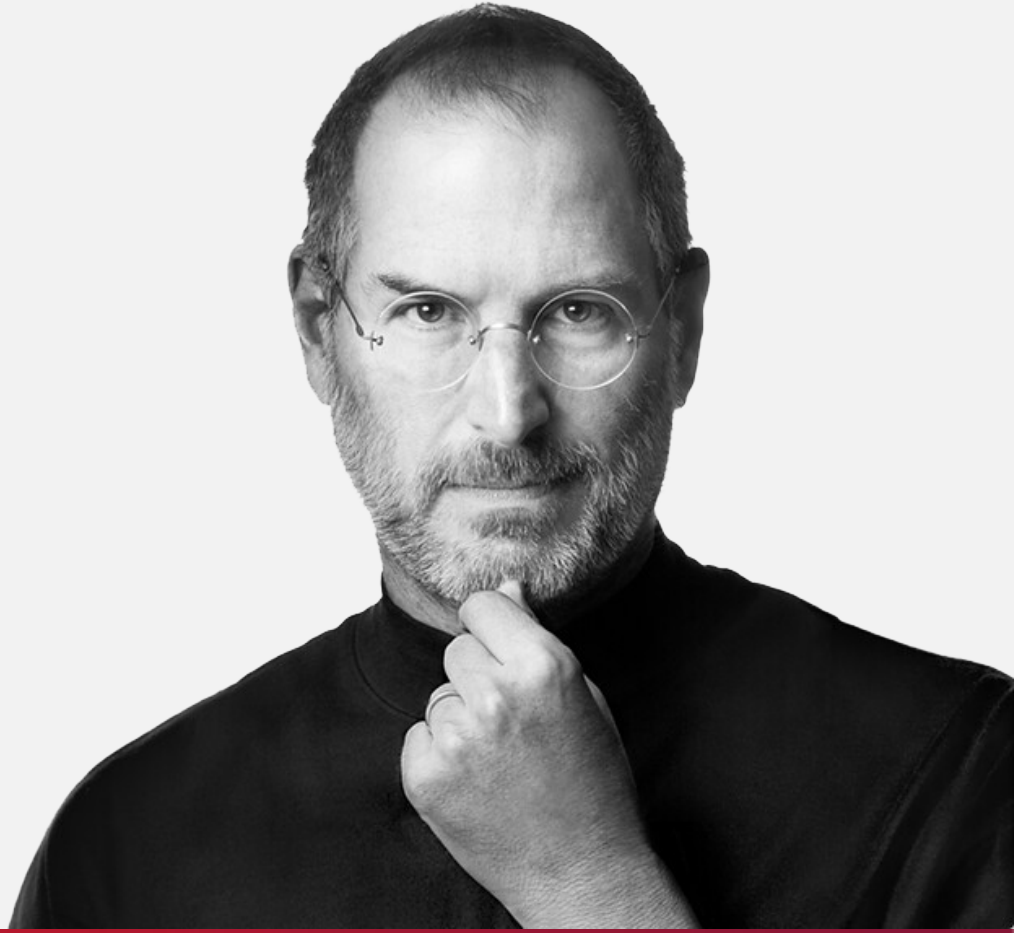
Make the transition to ongoing authorization a priority and use continuous monitoring approaches to reduce the cost and increase the efficiency of security and privacy programs

Thinking Below the Value Line

PAAS IS A PRE-REQ FOR DEVOPS OUTCOMES IN ENTERPRISE TRANSFORMATION



"You've got to start with the customer experience and work back toward the technology.



Structure and Opinionation

TOTAL COST OF OWNERSHIP

Cost to operate the platform

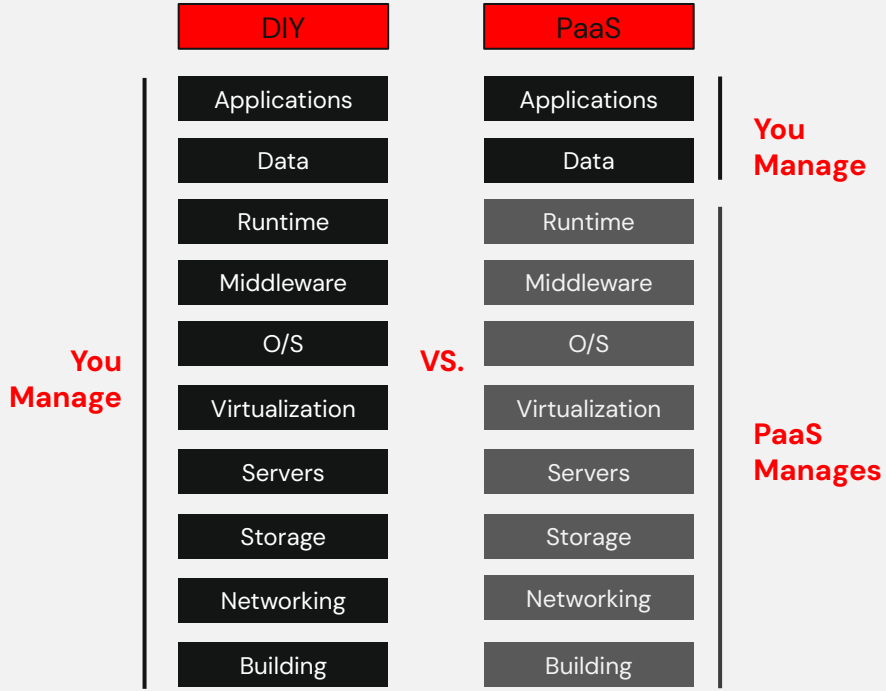
- Distinguish between Day 1 and Day 2 operations
- Consider your future complexity… Day 2 ops don't often scale linearly
- Catalytic versus thermodynamic operations

Cost to develop on the platform

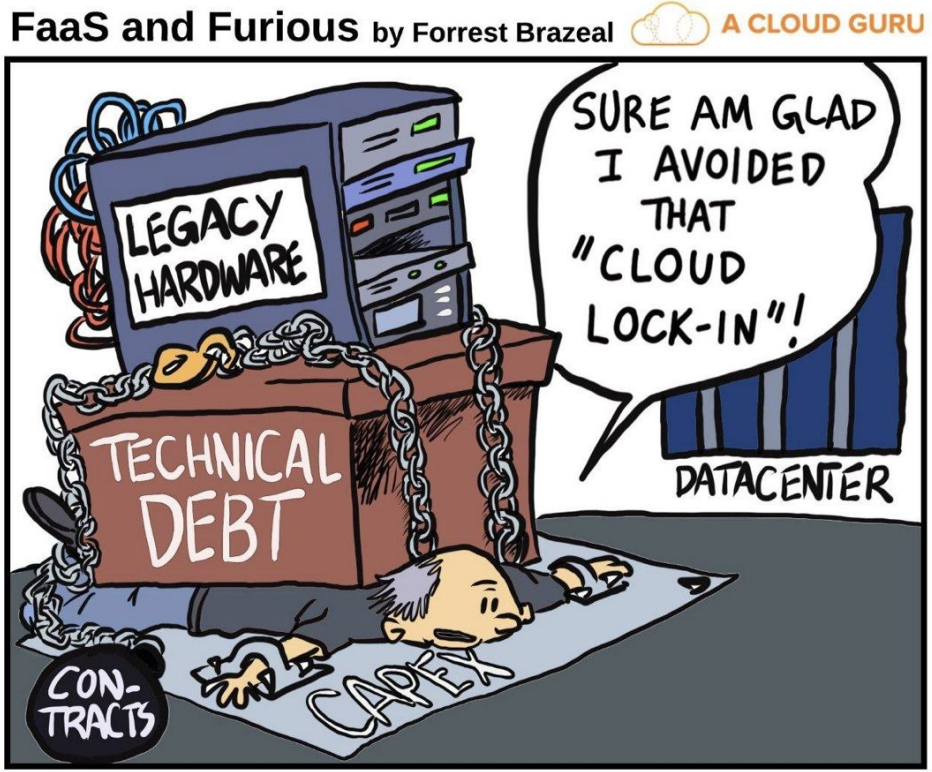
- Consider where you are at in your development maturity journey
- Remember the value line

Cost of compliance on the platform

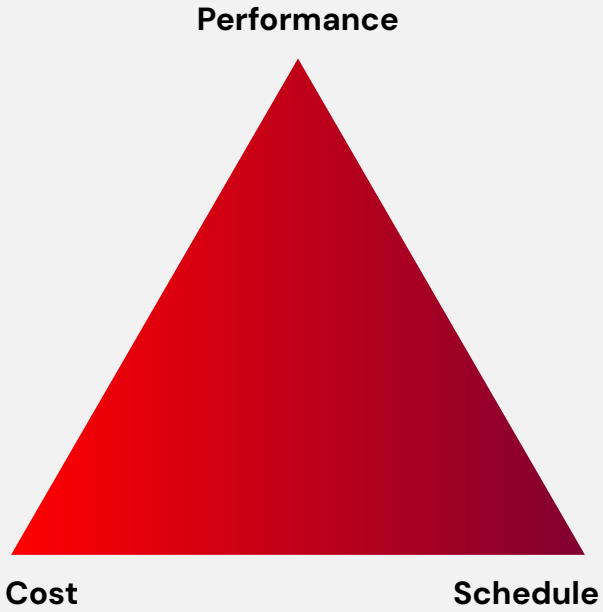
- In a highly regulated space, how much compliance occurs at the platform versus application layer
- Upgrades and patching




"VENDOR LOCK"


FaaS and Furious by Forrest Brazeal
A CLOUD GURU
LEGACY HARDWARE
SURE AM GLAD I AVOIDED THAT "CLOUD LOCK-IN"!
TECHNICAL DEBT
DATACENTER
CON-TRACTS
CAPEX
© 2018 Forrest Brazeal. All rights reserved.

Project management outcomes...



...still matter in product (value) management

REQUIREMENTS AND BUDGETING HAVE TO CHANGE TOO

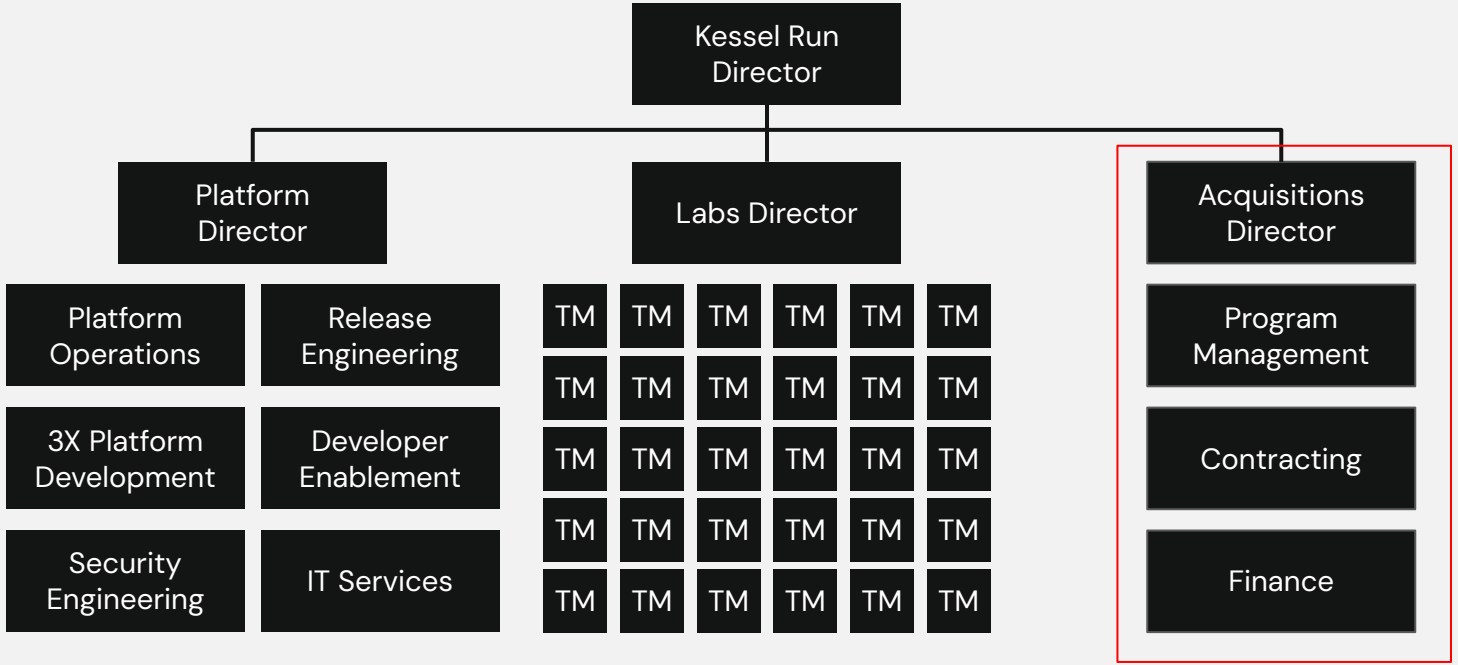
Value = Performance / Cost / Schedule

So remember...

1. If performance is near zero, your cost “savings” don’t matter
2. Not delivering is division by zero!
3. Long schedules greatly reduce value, nevermind opportunity costs.

All of this made possible by acquisitions

YOU CAN'T SCALE WITHOUT THEM!



What we learned

LEAN ENTERPRISE

All processes (acquisitions included) should create value and eliminate waste

Change One

DECENTRALIZATION AND AUTONOMY

1 **Culturally the overall theme is one of decentralization and autonomy**

DevOps

- Decentralization of dev and IT ops skill sets into cross-functional teams.

Continuous delivery

- Decentralization of the release schedule and process.

Autonomy

- Decentralization of decision making.

Change Two

PRIMARY TEAM STRUCTURES

2 **We codify decentralization into two primary structures**

Application product teams

- Cross-functional teams that make their own decisions about design, process, and release schedule.

Platform product teams

- Teams that provide the cross-functional application teams with the platform they need to operate.

Reaction from F100 CTO:
"But Netflix has a superstar dev team, we don't!"

@adrianco's (formerly from Netflix) response:
"We hired them from you."

Change Three

TECHNICAL DECENTRALIZATION

3 **Technicnically, we also decentralize control**

Monoliths to microservices

- Control of individual business capabilities is distributed to individual autonomous services.

Bounded contexts

- Control of internally consistent subsets of the business domain model is distributed to microservices.

Containerization

- Control of application packaging is distributed to business capability teams.

Choreography

- Control of service integration is distributed to the service endpoints.

RISE8

WE'RE READY

Want To Pair With Us?