Controlling Information Technology Chaos,

through migration to a Continuous Authorization To Operate (cATO) environment

A journey that must be taken – introduction and service offering

ProCap 360, offering SBOM / RBOM, Knowledge Graph and Professional Services

Table of Contents

Contents

Table of Figures

Achieving continuous Authorization to Operate

Objective

As cybercrimes and technical problemsPast attempts to resolve this issue, like the C=DHS Continuous M rise allowing virus and malware problems for organizations, it has finally been realized that a new approach must be developed. An approach that incorporates a means for detecting and mitigating problems in real, or near real, time. A number fo new laws and regulations have been initiated lik:

1. Executive Order 14028 [1]– Improving the Nation's Cybersecurity
2. Office of Management and Budget, M-22-18 [2]– Enhancing the security of the software supply chain
3. SEC Rule 2023-139 - rules on cybersecurity and material breaches

Previous attempts to address the issue of identifying and mitigating technical problems and cybercrimes, like the DHS Continuous Diagnostics and Mitigation (CDM) system that address the entire United States infrastructure.

New approaches are presently being developed by government and private sector groups, but none have been fully realized as yet. Guidelines that have surfaced are:

1. Secure by Design – an effort to define a foundation by which secure systems can be created.
2. SBOMs – Software Bill of Materials used to define software components and their owners/status, including if a software component of an application has an existing vulnerability.
3. DevSecOps – Agile methodology to incorporate security within the application development cycle.
4. Continuous Threat Exposure Management (CTEM) – used to identify and repair encountered technology problems and cybercrimes in real, or near real, time.

All of these new guidelines are being developed to best safeguard the production environment and maintain the company's ability to provide applications and services to the public, or protect the warfighter defending the United States.

I am working with Internet Infrastructure Services, Corporation (IIS-Corp) on brining a product to market called ProCap 360, which has an SBOM, RBOM (Release Bill of Materials), and a Knowledge Graph that will allow your DevSecOps team eliminate vulnerabilities during the testing phase, so that cATO can be

---

[1] https://www.bing.com/ck/a?!&&p=e5938110b05d21eaJmltdHM9MTcwNzI2NDAwMCZpZ3VpZD0yZjZkZGI3Zi00Zjk1LTY2ZTUtMGNiMC1jYjc2NGI5NTYwYWQmaW5zaWQ9NTIwOA&ptn=3&ver=2&hsh=3&fclid=2f6ddb7f-4f95-66e5-0cb0-cb764b9560ad&psq=OMB+M-22-18&u=a1aHR0cHM6Ly93d3cud2hpdGVob3VzZS5nb3Yvd3AtY29udGVudC91cGxvYWRzLzIwMjIvMDkvTS0yMi0xOC5wZGY&ntb=1https://www.bing.com/ck/a?!&&p=4af8da9e4b612afaJmltdHM9MTcwNzI2NDAwMCZpZ3VpZD0yZjZkZGI3Zi00Zjk1LTY2ZTUtMGNiMC1jYjc2NGI5NTYwYWQmaW5zaWQ9NTIxNQ&ptn=3&ver=2&hsh=3&fclid=2f6ddb7f-4f95-66e5-0cb0-cb764b9560ad&psq=Executive+Order+14028&u=a1aHR0cHM6Ly93d3cuZ3NhLmdvdi90ZWNobm9sb2d5L2l0LWNvbnRyYWN0LXZlaGljbGVzLWFuZC1wdXJjaGFzaW5nLXByb2dyYW1zL2luZm9ybWF0aW9uLXRlY2hub2xvZ3ktY2F0ZWdvcnkvaXQtc2VjdXJpdHkvZXhlY3V0aXZlLW9yZGVyLTE0MDI4&ntb=1

[2]

achieved. We realize that attaining the "Golden Level" or cATO requires planning and change. You must understand the concept, accept its direction, build a foundation on which you can achieve cATO, and implement the set of products needed to achieve this goal. Of course, mot important is the training of your staff and awareness of management on the benefits that can be achieved through achieving cATO.

You will change Information Technology from a cost center to a profit center, through reduction in encountered technical problems and cybercrimes, more staff time can be devoted to proactive work instead of reacting to encountered problems, the IT Operations will be more secure, and the brand and reputation of the company will be enhanced.

Overview

The Risk Management Framework (RMF) establishes the continuous management of system cybersecurity risk. Current RMF implementation focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached. Efforts in the Department are attempting to emphasize the continuous monitoring step of RMF to allow for continuous authorization (cATO). Real-time or near real-time data analytics for reporting security events is essential to achieve the level of cybersecurity required to combat today's cyber threats and operate in contested spaces.

The purpose of this memo is to provide specific guidance on the necessary steps to allow systems to operate under a cATO state.[3]

Active Cyber Defense

Active cyber defense is the ability to respond to cyber threats in real, or near real time. As the IT Department adopts a data centric model, so too must our cyber defenses. The focus should be on using threat driven dashboards and metrics to establish patterns and discern threats before they are able to wreak havoc on DoD domains.

Secure Software Supply Chain

The number of components required to build, deploy, operate, and secure modern systems continues to expand rapidly, where underlying software architectures and deployment topologies have moved well beyond a single binary installed from physical media. These advancements are too often invisible to the end-user, where modern software applications are backed by an array of additional network services that include remote configuration updates, advanced analytics, artificial intelligence (AI)-powered rulesets that update cyber defense systems automatically, etc. As the Department's operations become increasingly dependent on software, we must ensure that this software is created in a secure, protected, and controlled environment that instills confidence in the user base that it will perform as designed. To prevent any combination of human errors, supply chain interdictions, unintended code, and support the creation of a software bill of materials (SBOM), the adoption of an approved software platform and development pipeline(s) are critical.

cATO Issuance

If an AO (Authorizing Official) determines their system provides the required real time risk posture to achieve a cATO, the AO will notify the component CISO of the intention to move that system to a cATO

[3] CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF (defense.gov)

status. Together the AO and component CISO will present this request and the supporting body of evidence to the DoD CISO for consideration. Systems desiring to move from a traditional ATO model to a cATO model must demonstrate: complete understanding of activities inside of their AO boundary with a robust continuous monitoring of RMF controls; the ability to conduct active cyber defense in order to respond to cyber threats in real time; and the adoption and use of a specific DoD Enterprise DevSecOps Reference Design.

Maintenance

The approval of cATO does not guarantee a system will stay in that state, systems that have been granted permission to operate under a cATO may have this revoked for several reasons. This may include, but is not limited to: poor cybersecurity posture as identified through continuous monitoring or external assessments; changes in risk tolerance; or a cybersecurity incident resulting from poor adherence to cybersecurity practices. A system can temporarily lose its cATO privilege without any loss of existing ATO.

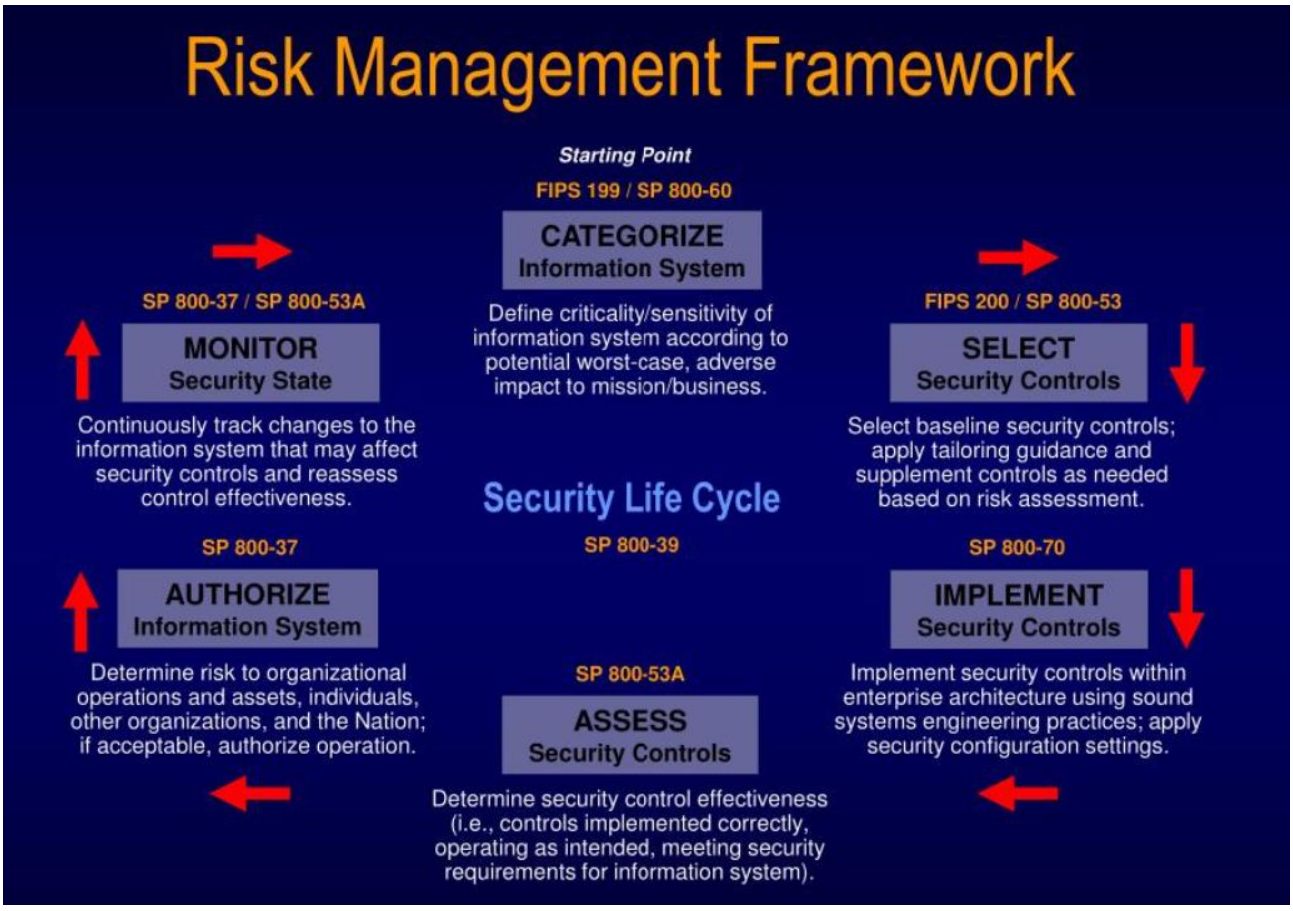

Figure 1: NIST Guidelines to achieve Risk Management Framework for cATO[4]

[4] PPT - Next Generation Risk Management Information Security Transformation for the Federal Government DNSSEC Day FOSE Conferenc PowerPoint Presentation - ID:1631004 (slideserve.com)

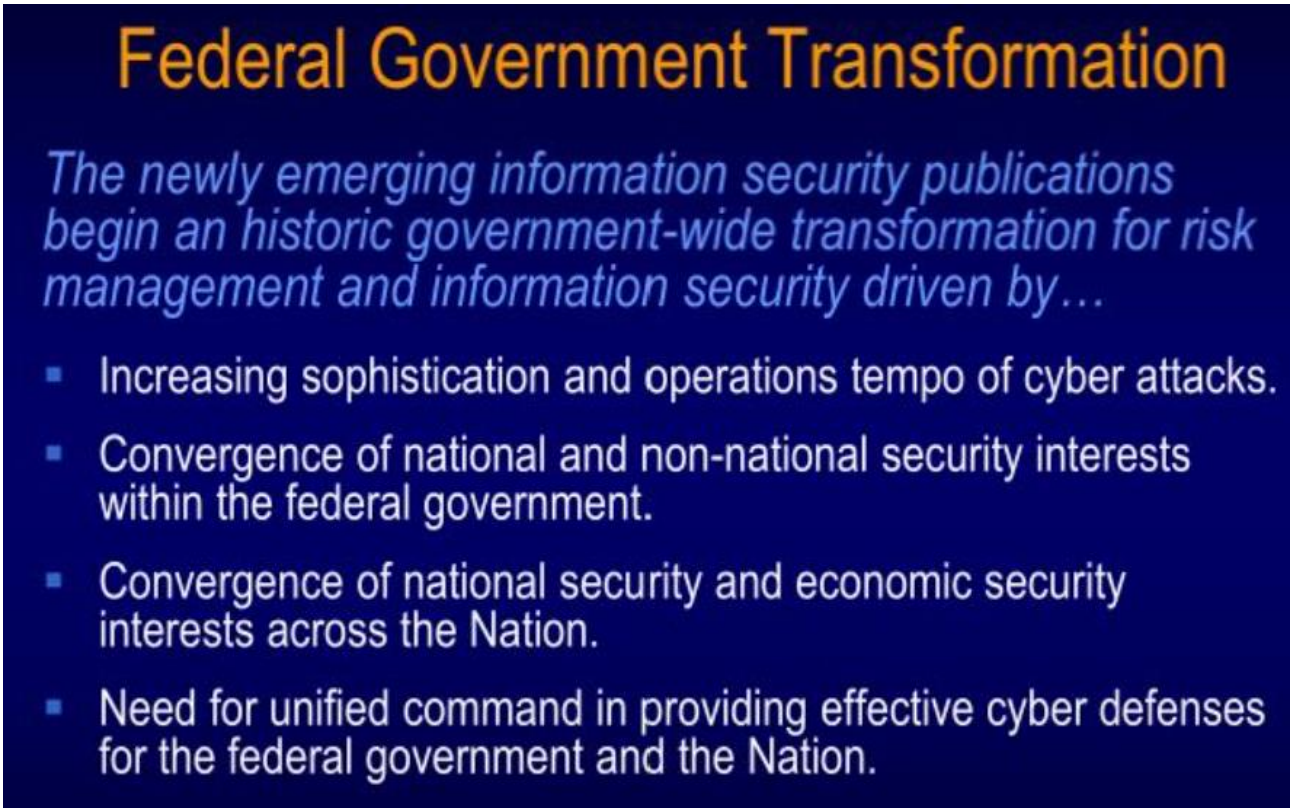

Figure 2: The government is transforming how it prevents cyber crimes

cATO represents a challenging but necessary enhancement to our cyber risk approach to accelerate innovation while outpacing expanding cybersecurity threats. To achieve cATO, the Authorizing Official (AO) must be able to demonstrate three main competencies:

1. On-going visibility of key cybersecurity activities inside of the system boundary with robust continuous monitoring of RMF controls.
2. The ability to conduct active cyber defense in order to respond to cyber threats in real time; and
3. The adoption and use of an approved DevSecOps reference design.

Improvements from government authorities are researching many new techniques to achieve CONMON (Continuous Monitoring) that can lead to detection of technology problems and cybercrimes. Once detected, these problems must be reported to the owners of the failing component so that the encountered error can be repaired. When cybersecurity repairs are made, or problem resolution based on software drivers identified, they are documented within a Vulnerability Report and submitted to a public Vulnerability Repository along with their resolution in the form of a software patch or new release announcement. This process has recently been improved upon by adding a Vulnerability Exposure eXchange (VEX) system that reports on vulnerabilities that have been reported but their resolution is still be created. The VEX report can also tell you of the severity of the reported vulnerability and if it impacts your area of concern.

A sample approach to automated problem detection and repair

Systems are rarely produced or deployed as a singular system; they operate as a system of systems. The goal of a cATO is to formalize and monitor the connections across these systems of systems to deliver cyber resilient capabilities to warfighters at the speed of relevance. CONMON requires the AO have the ability to monitor the cumulative set of security controls that span the AO's area of responsibility (AOR) in order to make real time risk decisions. The AO must approve, support and manage an organization's CONMON plan for all applications.

An example of how problems can be detected and responded to are shown in the following diagram.

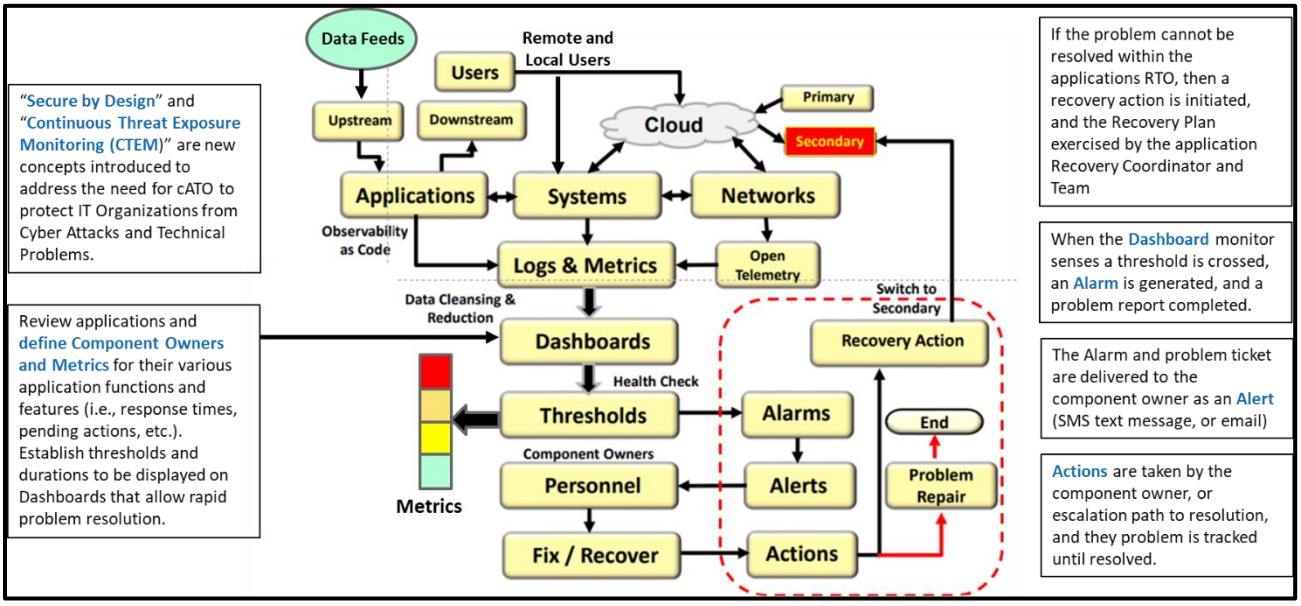

Figure 3: An automated approach to problem recognition, resolution, or recovery.

A united framework to achieve cATO.

When attempting to implement a new process like that which is needed to achieve cATO, it is necessary to combine resources, conduct open discussions and brainstorming meetings to decide on an approach that is best suited to your needs. This approach must combine people, procedures, Commercial Off-The-Self-Tools (COTS), and products that can aid personnel in detecting and resolving problems prior to their entering the production environment.

Gone are the days when we implement a product and then spend most of our time fixing the encountered cybercrimes and technical problems. We will not waste time reacting, and spend more time proactively planning, testing, and implementing successful products that raise our reputation and provide our customers with a higher standard of success.

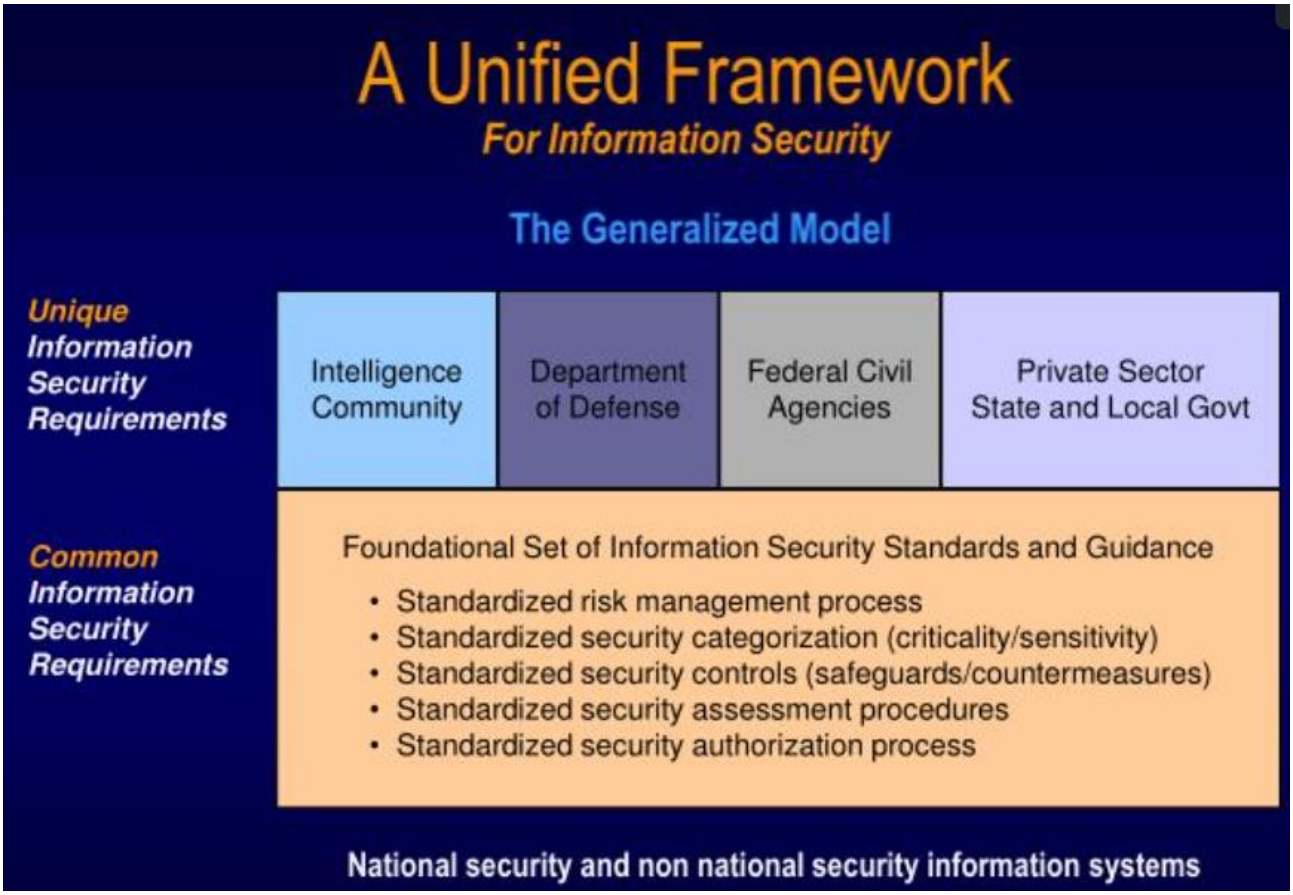

Figure 4: A Unified Approach to achieving error-free applications.

Transformation…. Getting There

Transforming your environment and educating your staff will be an effort. We would love to help you achieve these goals by developing a repository of applications and their SBOM / RBOM information accessible through a Knowledge Graph. Providing a cross-reference to where application components are used will greatly reduce the time needed to locate where a vulnerability exists and help speed it repair, thereby nipping problems in their bud and even stopping them from occurring.

Some of the effort needed to transform your environment is shown in the next diagram, but there are many other steps that may arise during your transformation. We pride ourselves on being current on these new technologies and procedures and would be happy to assist you on your journey to achieve a cATO state.

Figure 5: Transformation of your Information Technology environment to achieve cATO

Appendix:

Data Security

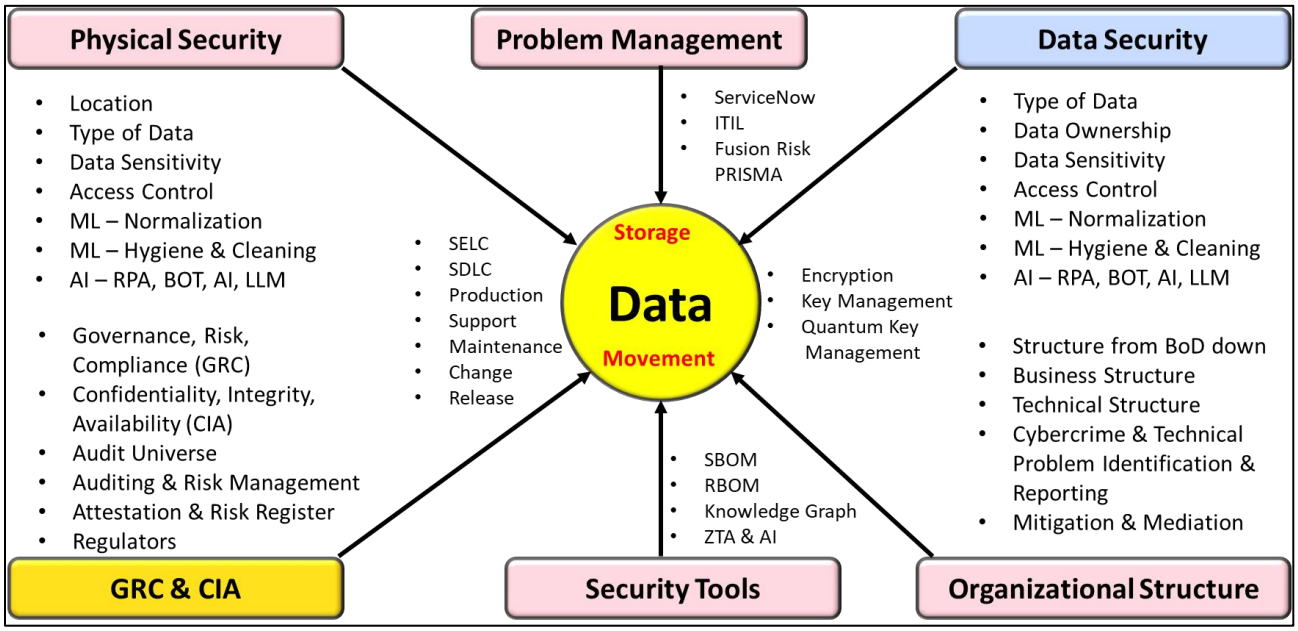

Figure 6: IT Security and its components.

Cybersecurity Framework

Function		Code	Category	Cybersecurity Framework (CSF)
Identify	ID	ID.AM	Asset Management	
		ID.BE	Business Environment	
		ID.GV	Governance	
		ID.RA	Risk Assessment	
		ID.RM	Risk Management Strategy	
		ID.SC	Supply Chain Risk Management	
Protect	PR	PR.AC	Identity Management and Access Control	
		PR.AT	Awareness and Training	
		PR.DS	Data Security	
		PR.IP	Information Protection Processes and Procedures	
		PR.MA	Maintenance	
		PR.PT	Protective Technology	
Detect	DE	DE.AE	Anomalies and Events	
		DE.CM	Security Continuous Monitoring	
		DE.DP	Detection Processes	
Respond	RS	RS.RP	Response Planning	
		RS.CO	Communications	
		RS.AN	Analysis	
		RS.MI	Mitigation	
		RS.IM	Improvements	
Recover	RC	RC.RP	Recovery Planning	
		RC.IM	Improvements	
		RC.CO	Communications	

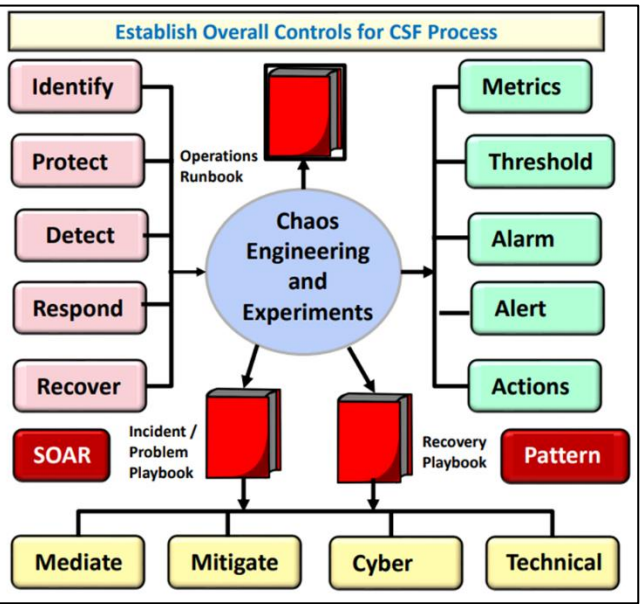

Figure 7: Cybersecurity Framework - CSF

Identity and Access Management

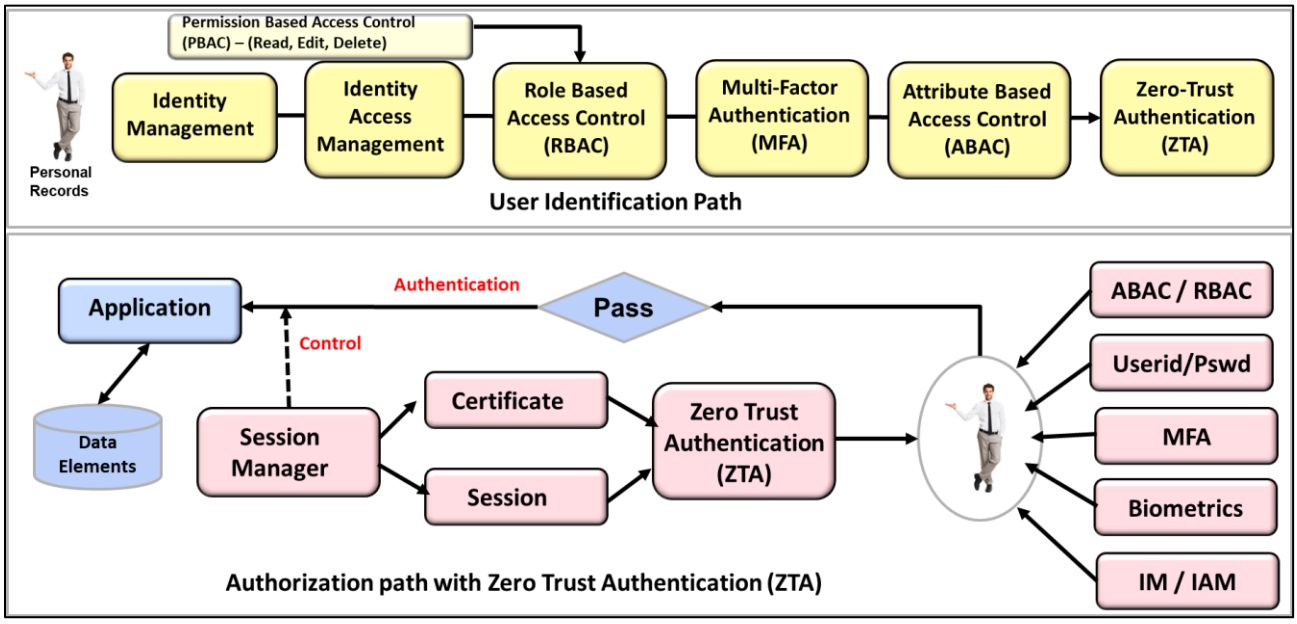

Figure 8: Identity and Access Management

DevSecOps environment Model (DoD)

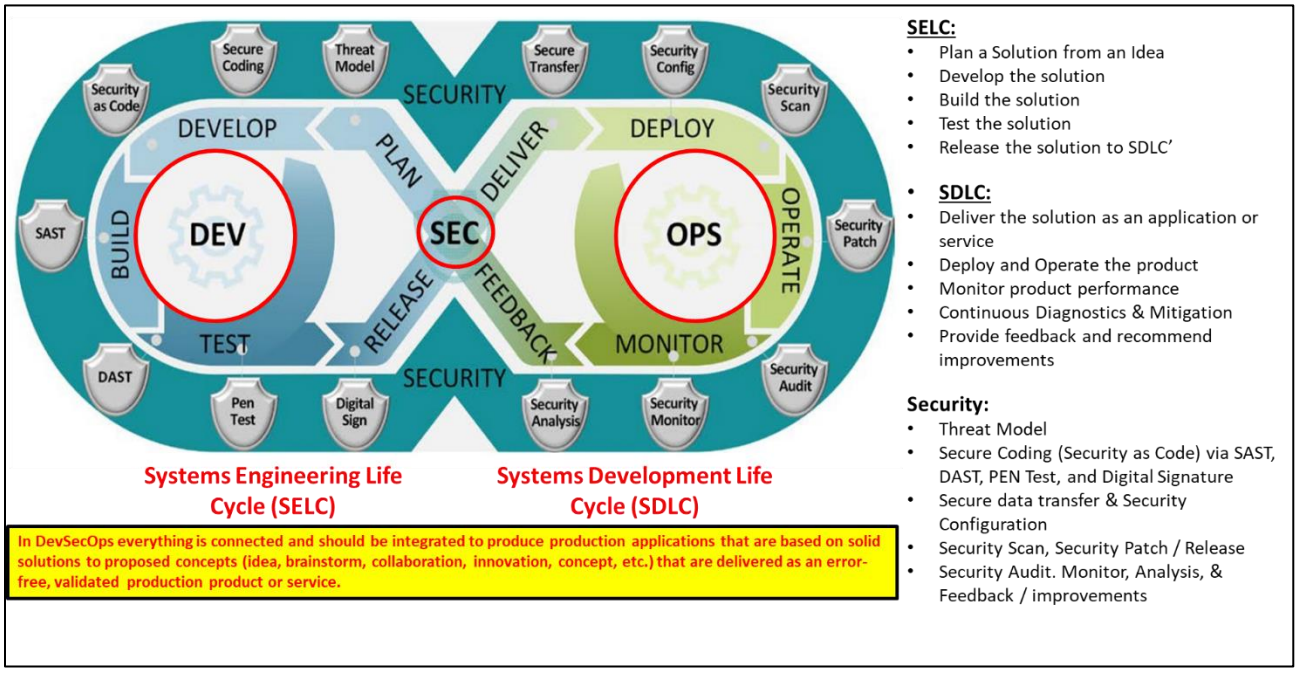

Figure 9: DevSecOps Environment Model (DoD).

Application Security Testing (Static, Dynamic, Interactive, and Real Time

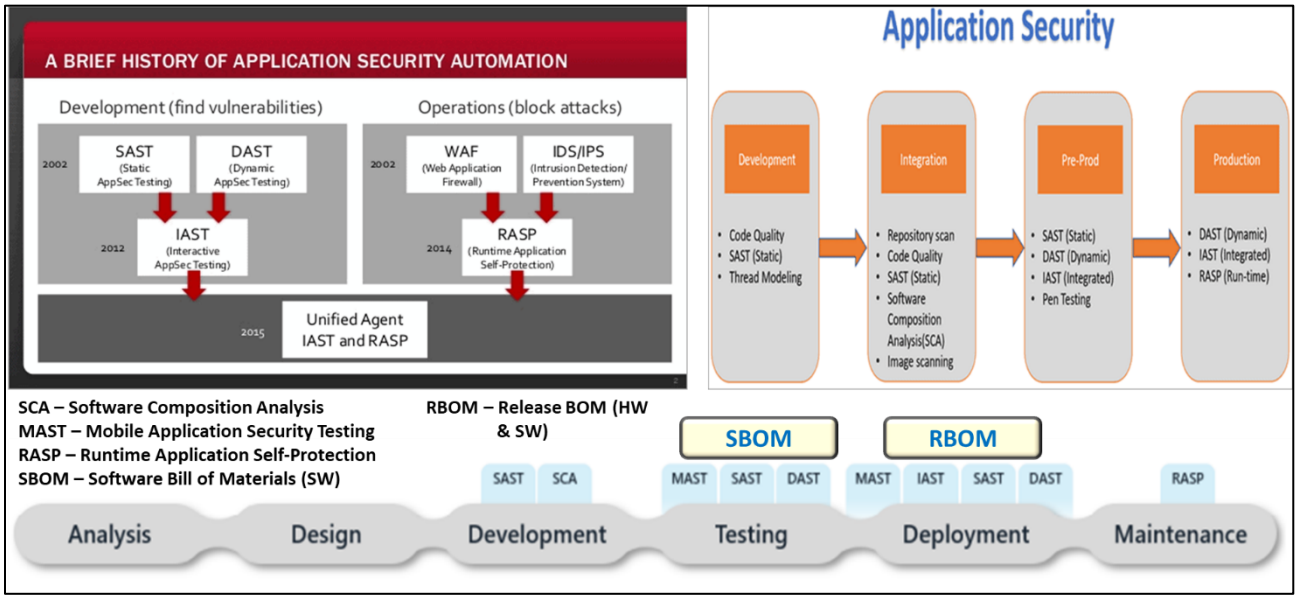

Figure 10: Application Security Testing for DevSecOps

Current method to build applications and services (SELC / SDLC)

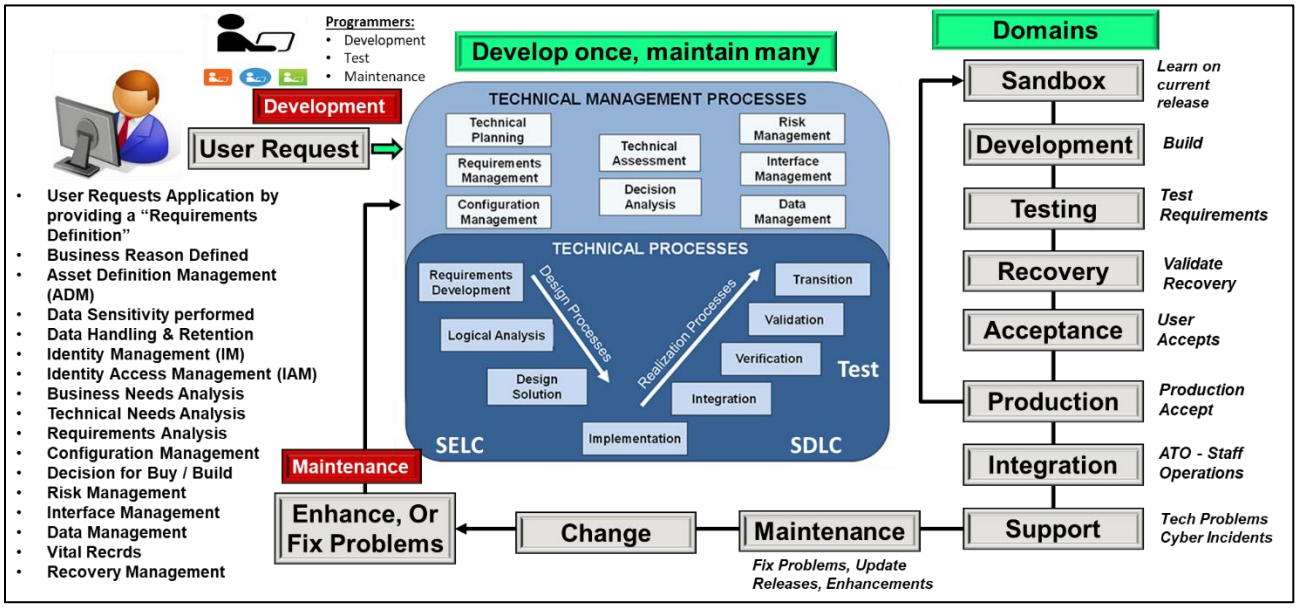

Figure 11: Current method for developing applications and providing services

DoD Continuous Authorization to Operate

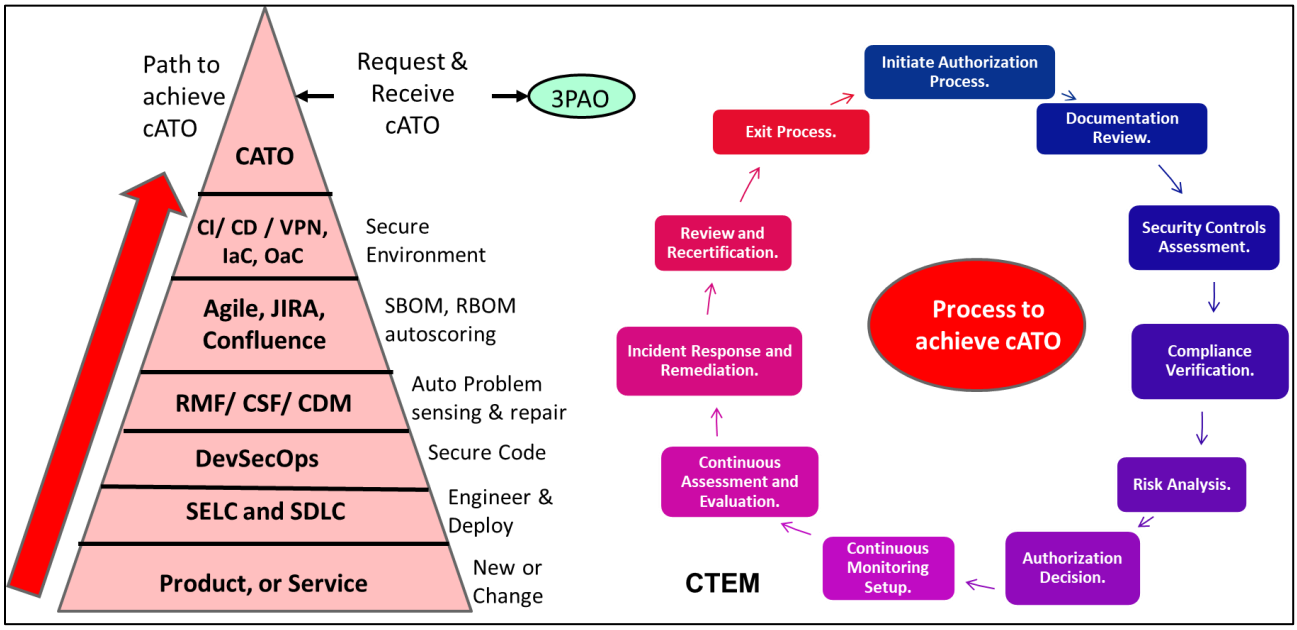

Figure 12: DoD Continuous Authorization to Operate model