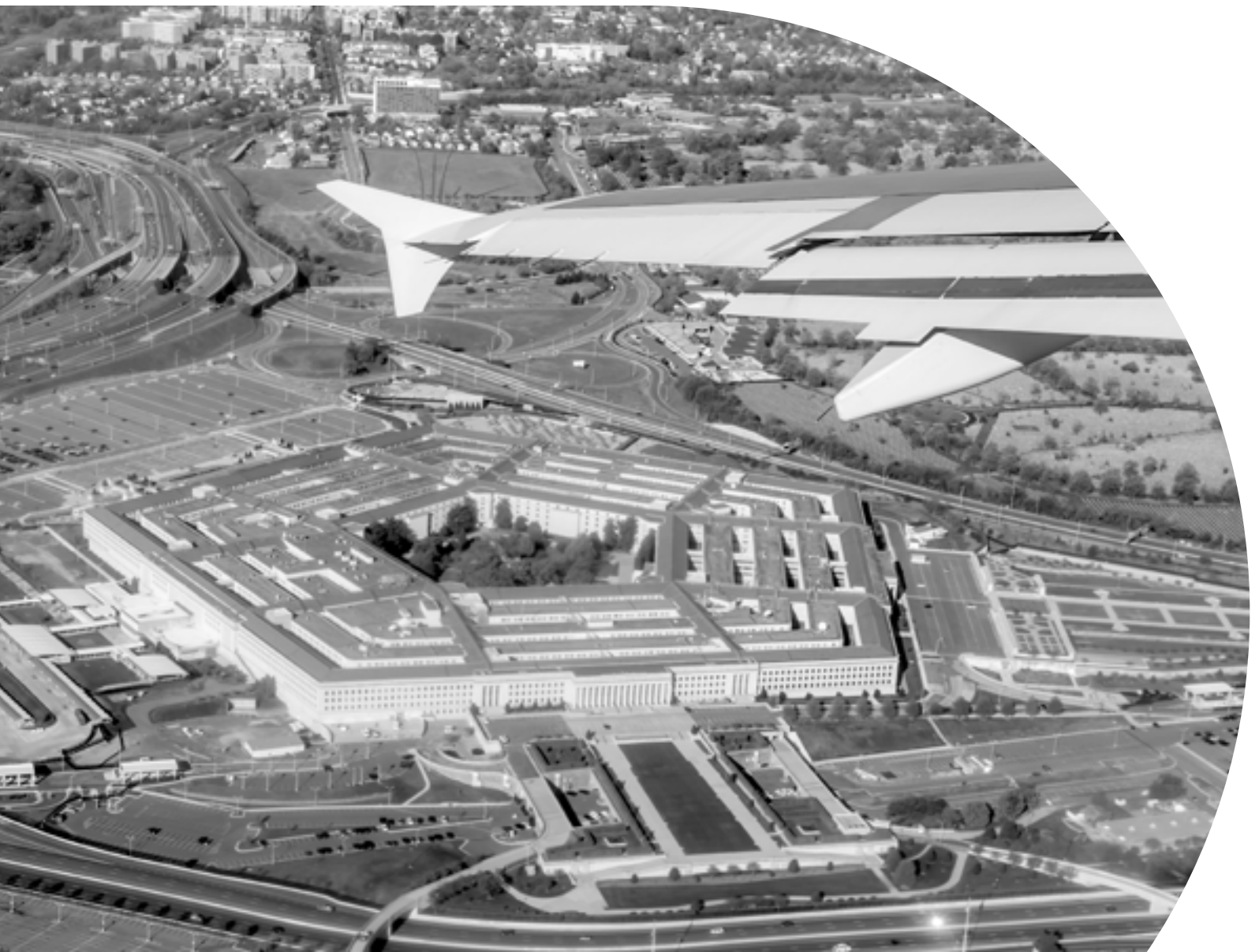


DevSecOps, a key to achieving CMMC and FedRAMP compliance

A modern approach to development addresses the DoD's cyber security requirements



Baking security into agile software development is always a good idea for businesses, but ensuring that code is secure has become even more urgent for companies in the aerospace and defense (A&D) industries that do business with the U.S. Department of Defense (DoD).

Following several serious data breaches of unclassified information involving supply chain partners, the DoD announced that, as of June 2020, any company submitting an RFP must have achieved a new type of certification called Cybersecurity Maturity Model Certification (CMMC).

According to the DoD's latest draft of the new regulations, the Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between \$57 billion and \$109 billion in 2016.¹ And the majority of this theft of intellectual property is directly attributable to immature cyber security and ineffective implementation of controls necessary to protect sensitive data. Sharing data with defense contractors expands the DoD's risk of attack because sensitive data is distributed beyond the DoD's information security boundary.

The DoD is working with researchers and industry to develop the CMMC, and while details have yet to be finalized, generally the new certification will combine previous National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) standards into one unified measure of a company's "institutionalization of cybersecurity practices and processes." To comply, A&D companies will have to get their processes up to speed and then become certified by a third-party auditor designated by the DoD.

A key part of earning CMMC compliance is demonstrating that procedures are in place to ensure all software delivered to the DoD is written in a secure manner. That's where DevSecOps comes in. Just as DevOps created efficiencies by merging software development and IT operations teams, DevSecOps applies security principles at each step in the development process to significantly reduce bugs in application code that can lead to security vulnerabilities.

While CMMC compliance may be the impetus for A&D companies to invest in DevSecOps, the benefits of a more efficient, automated and secure development process also apply to apps being built for internal consumption, for private sector customers and for other government agencies. In addition, DevSecOps pays dividends as companies move their application development and deployment activities into multi-cloud environments.

IDC puts it this way in its *FutureScape Worldwide Developer and DevOps Predictions*:² "Development without integrated security and compliance will fail. Progressive organizations have prioritized security due to uptime and compliance concerns, accelerating the need for agility and a curated open source software development portfolio. Security-led development will be a priority for 90% of organizations by 2020."

¹CMMC First Draft, Dec. 2019. <https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>

²IDC FutureScape, Worldwide Developer and DevOps 2018 Predictions (Oct. 2017)

Why aerospace manufacturers need DevSecOps

Historically, project management methodologies treated security as an afterthought. The obvious problem with this approach is that identifying security issues during the later stages of software development, or even as an application is finalized, is inefficient, risky, time-consuming and costly. In fact, having to go back and rewrite code to address security concerns can totally negate the benefits of an agile development process.

With IT and operational technology (OT) systems becoming increasingly intertwined, releasing code that has not been properly vetted puts A&D organizations at risk. Nation-state threat actors can target IoT systems and controls to disrupt production, supply chains and connected products and potentially cause physical damage and loss of life. Similarly, theft of product design and analytics data can lead to a loss of trust among developers, security teams, customers and business leaders.

Applying security checks throughout the agile development process — what has become known as shifting left — reduces risk and allows teams to correct problems early. Automating security implementation and testing procedures, as part of a DevSecOps approach, allows for the security posture to evolve along with the application throughout the development lifecycle without slowing down the process.

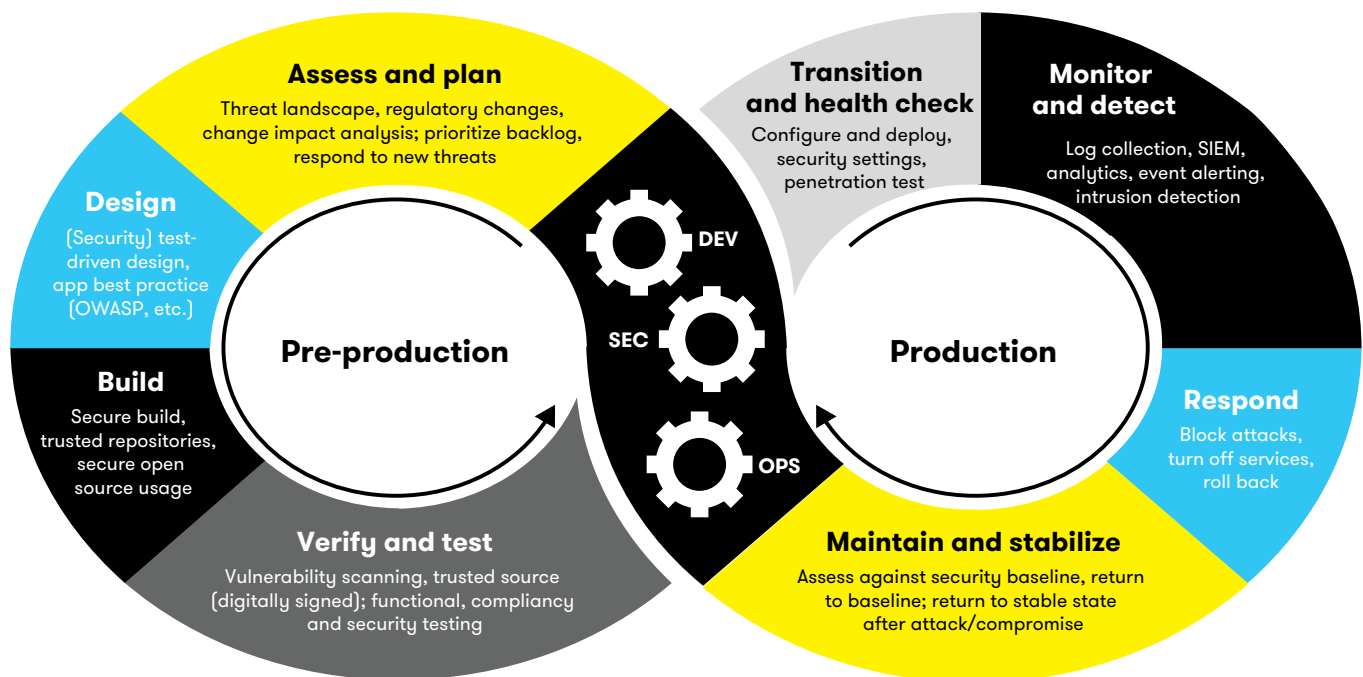


Figure 1. Automated DevSecOps processes continually assess, design, build and test security controls in the software development lifecycle.



In today's world, companies must be able to quickly adapt to changing business conditions. The old waterfall methodology, in which major software updates occur every 6 months or even every year, no longer supports the needs of the business. Agile processes with security baked in can accelerate mission-critical, data-driven decision making.

DevSecOps can be cost-effective for A&D companies to maintain compliance with existing federal requirements, such as the Federal Risk and Authorization Management Program (FedRAMP), and to meet the new CMMC requirements. With DevSecOps, every line of code goes through the necessary reviews and approvals to make sure security is improved incrementally throughout the development process. Plus, this approach enables A&D companies to meet the continuous compliance requirements from FedRAMP and CMMC. Not thinking about continuous compliance up front can result in significant rework later on.

However, putting the DevSecOps philosophy into practice isn't easy. There are significant cultural and operational obstacles to overcome.

DevSecOps challenges and how to address them

DevOps teams operate in a fast-paced world of sprints. Their goal is to hit deadlines for new code releases as quickly as possible, such as every week or every 2 weeks. Developers operate with their foot on the gas pedal, which increases the chances that errors will be made.

On the other hand, security teams tend to keep their foot on the brake. They don't want any application to go live until it has been extensively tested and validated, which takes time.

This inherent tension between security and DevOps teams can be resolved through a systematic approach. Adopting continuous integration/continuous delivery (CI/CD) and highly automated testing practices helps accelerate software development and deployment processes.

Key steps on the road to DevSecOps

The first lesson is to understand that creating a well-oiled DevSecOps team is 80 percent about process, training and culture — and only 20 percent about tools. A successful DevSecOps program requires support from senior leadership. Chief information officers have to set the tone and bring security teams, developers, operators and business unit leaders together to develop a unified approach to building secure applications. Chief information security officers should develop a system for evaluating each new application based on its risk profile and its importance to the business.

Other important pieces of the DevSecOps puzzle include:

- **Changing the culture:** Developers should be encouraged to be mindful of the security implications of everything they do. Security professionals should also learn to move at the pace of development and to derive new security hardening methods to secure applications in order to be relevant to the business.
- **Building a team:** When putting together a DevSecOps team, organizations should look for employees with broad knowledge of how processes work.
- **Tools:** It's important to make sure employees have the latest standardized tools and are trained in how to use them regardless of which business units.
- **Governance:** Companies should create and enforce strong policies regarding compliance with DevSecOps principles.
- **Business involvement:** Establishing open lines of communication with business units is important for building internal support when moving to DevSecOps.
- **Centers of excellence:** It's a good idea to create a center of excellence, where knowledge can be shared across teams in terms of best practices and lessons learned.

Even after code goes into production, the work is not done. There should be continuous security monitoring to identify erratic or unusual behavior while systems are running. And aerospace manufacturing companies should make sure patches and fixes are applied in response to evolving security threats.

The DevSecOps toolset

The development pipeline consists of many steps and decision points, and a variety of tools and techniques can be applied. For example, security requirements gap analysis addresses security at the requirements layer, while architectural threat analysis looks at the robustness of the architecture from a security perspective.

The need for speed inevitably leads to coding errors, but there are tools that can scan for these errors. The latest versions can spot mistakes in real time, much the way that spellcheck works in Microsoft Word.

There is also a class of tools that checks applications at runtime; these include runtime scanners, application vulnerability assessment tools and penetration testing software. Finally, patching tools should be in place for cases in which buggy code makes it through all of the checkpoints and reaches the production environment.

How to accelerate and optimize change

While the details regarding what it will take for A&D companies to comply with the new CMMC requirements are still to be released, there are some basic strategic decisions companies can make now and some best practices that will help accelerate compliance.

Aerospace manufacturers should take advantage of any certifications and guidelines that can speed the process and help them avoid reinventing the wheel. For example, development teams can leverage products that have been certified in the government's FedRAMP marketplace, a searchable dashboard of all cloud services that are FedRAMP-authorized, FedRAMP-ready or in the process of being reviewed.

Using cloud-native services that have already achieved FedRAMP certification — for example, Azure Active Directory — enables companies to reduce the amount of certification work required, which makes it faster and easier to implement these cloud solutions. Starting from scratch without using a precertified component will add to project scope, timeline and budget.

Aerospace and defense organizations should also take advantage of current guides and protocols, including:

- **Security Technical Implementation Guides:** STIGs lay out configuration standards for DoD devices and systems.
- **Security Content Automation Protocol:** This protocol allows for automatic verification of compliance and should be included as part of an organization's CI/CD pipelines.
- **Azure Blueprints:** This Microsoft service enables cloud governance at scale with templates for creating and managing cloud environments.
- **AWS Quick Starts:** Similarly, Amazon Web Services has templates that help customers automate the deployment of solutions on AWS making use of best practices for security and resiliency.
- **Trusted Internet Connections:** This is a Homeland Security initiative that optimizes and standardizes the security of external network connections used by federal agencies.

Finally, A&D organizations should think about whether they want to take the do-it-yourself approach to building out DevSecOps teams and implementing other processes required for CMMC compliance, or whether it makes more sense to bring in outside experts that have extensive industry experience and can help them achieve their goals faster than they could on their own.

About the authors



Zach Levy is a Digital Strategist and Solution Designer for DXC Technology, supporting clients through their digital transformation journey. He leverages his former career experiences in U.S. government and military service to enhance DXC's client engagement model and solution design processes.



Praveen Cherukuri is a Chief Technologist for Aerospace & Defense and Manufacturing in the Americas for DXC Technology. He is responsible for delivering innovative business outcomes using emerging technologies. He holds multiple certifications in AWS, Azure and Google clouds and is passionate about applying data science and robotics to create innovative solutions for A&D customers.

Learn more at https://www.dxc.technology/aerospace_defense

D Get the insights that matter.
www.dxc.technology/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at www.dxc.technology.