Mighty Guides

Sponsored by

SecurityCompass

7 Experts on Attaining Authority to Operate Faster in US Government Agencies

Table of Contents

Introduction

Throughout the private sector and particularly in the financial services and banking sectors, DevSecOps and agile development continue to grow in importance among software development teams. Companies that have adopted an agile mindset and integrated best practices within their development teams have seen unprecedented growth, even during the COVID-19 pandemic. According to the 15th Annual State of Agile Report, 86 percent of organizations adopted agile methodologies for their development teams in 2020, up from 37 percent in 2019.

Despite these gains, the public sector has been slow to adopt agile and DevSecOps approaches to software development. Across state, local, and federal government, agencies and organizations have struggled to adopt these best practices and have yet to capitalize on the ability to address secure development earlier in the software development life cycle (SDLC). By identifying opportunities to adopt an agile mindset and embrace a DevSecOps approach, agencies at all levels of government can improve the speed at which they deliver software while achieving better security outcomes.

Professionals at all levels of government agencies and departments can ship secure code faster with the implementation of leading practices, such as "shifting left" by integrating security checks earlier in the SDLC, benchmarking and tracking improvements in delivery speed, streamlining software onboarding, and encouraging knowledge of regulatory requirements.

This guide explores how agencies can increase the speed and security of their software development efforts, the importance of shifting left and adopting agile and DevSecOps practices, the link between Authority to Operate (ATO) and DevSecOps, and best practices for establishing and evaluating a software development approach.

All the best,
David Rogelberg
Editor,
Mighty Guides Inc.

Mighty Guides

Mighty Guides make you stronger. These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Foreword

Shifting left and building software with security and compliance integrated from the start is critical to increasing trust in our digital infrastructure. As we have seen through recent executive orders and Department of Defense (DoD) memos, creating a foundation that enables a continuous ability to quickly certify and deliver software is critical to federal organizations being responsive enough to meet their missions.

Enabling the Assessor to reduce assessment time in an Authority To Operate (ATO) process is a prerequisite to shortening software release cycles in the government. When assessors have access to audit trails generated throughout the SDLC, they can be confident that software was built to adhere with NIST and other requirements thereby reducing their assessment time.

We believe in *developer-centric* security: people, process, and technology focused on making security easy for developers to embed, with just-in-time training and detailed, relevant guidance during development. A developer-centric approach enables teams to *plan and prevent* for security and compliance rather than engaging in an endless cycle of finding and remediating security defects.

With security by design and audit trails that accelerate the ATO process, organizations can spend less time focusing on documentation and compliance, and more on delivering on their mission.

Regards,
Rohit Sethi
CEO,
Security Compass

SecurityCompass

Security Compass, a leading provider of software threat modeling and secure development solutions, enables organizations to build secure software faster. SD Elements, our flagship product, helps software development teams continuously model threats at scale, then proactively write code that significantly reduces cyber risk and remediation costs.

Security Compass is the trusted solution provider to leading financial and technology organizations, U.S. government agencies, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India.

Manual compliance processes can significantly delay ATO for federal government agencies

Learn how SD Elements speeds up the ATO process.

With SD Elements, you can obtain ATO faster and ensure:

- Reduction in software vulnerabilities
- Reduction in remediation costs
- Reduction in the time and cost spent on ATO audits
- Significant time savings for security experts

Book a Demo

TRUSTED BY

SecurityCompass

www.securitycompass.com

Meet Our Experts

Rohit Sethi,
CEO,
Security Compass

Stephan Mitchev
Director/Acting CTO
USPTO

Nicolas Chaillan
CTO,
Prevent Breach

Hannah Hunt
Chief Product and Innovation Officer,
Army Software Factory

Ian Anderson
Lead DevSecOps Engineer,
Naval Surface Warfare Center,
Dahlgren

Tom Marlow
Managing Director,
Dark Wolf Solutions

Robin Basham
CEO, CISO, Founder,
EnterpriseGRC Solutions

Traditional Waterfall Development vs. Agile Development

To its benefit, the federal government has used agile development practices since 2014 in place of waterfall methodologies.

With a waterfall approach to software development, teams follow a standard cycle, with product requirement documents driving design and development. Testing and security improvements occur at the end of this cycle and are often considered an add-on to the process.

> **Outdated development methodologies and manual security processes are roadblocks to timely product releases. These two factors have a significant impact on the public sector's ability to release software and applications with speed and safety.**
>
> 
>
> **Rohit Sethi**
> CEO, Security Compass

By contrast, in an agile development cycle, testing and security evaluations are continuous, resulting in early discovery of bugs and vulnerabilities, and providing an opportunity to address them much earlier in the cycle (Figure 1). This approach integrates security at several points along the SDLC, so development teams can correct security shortcomings while minimizing rework.

Some elements of government information security and software development in general have made adopting such an approach challenging. The benefits of an agile approach to development, however, when combined with DevSecOps, are significant efficiency gains, reduced costs, and faster time to market.

"Two challenges to attaining a streamlined software development shop include traditional ATO documentation requirements and the complexities of collaboration in current work environments. These challenges stifle implementation of a mature agile framework and hold programs back from fully transitioning away from the waterfall methodology."

Tom Marlow
Managing Director,
Dark Wolf Solutions

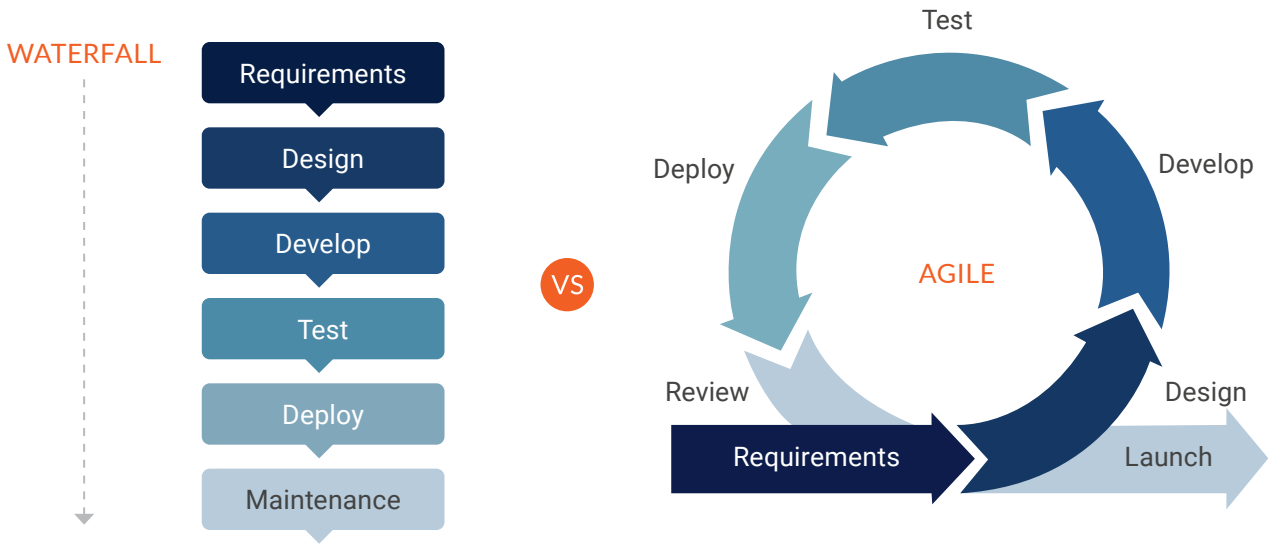

Figure 1: The differences between waterfall development and agile development

As reported in The State of Secure Development & ATO in U.S. Government Agencies in 2021, responses from cybersecurity professionals in federal, state, and local government agencies indicated that speeding software time to market is a priority.

"When I speak to my teams, I always illustrate [outdated technology] as this 40 year long tail that we're dragging with us. How are you expected to run if that's the load that you carry?"

Stephan Mitchev

Director, Office of Application Engineering and Development, Acting CTO, USPTO

The report provides the following additional insights:

- More than half of respondents (55 percent) indicated that shifting left is either a top priority or one of the top three priorities in their organization's SDLC.
- More than a third (34 percent) of respondents in federal agencies indicated that improving software time to market is the top priority for their team this year.
- A quarter of respondents (24 percent) indicated that they do not track the speed with which their teams produce software, and another 7 percent are unsure if or how such acceleration is accomplished.
- Of respondents who track the speed with which their teams produce software, 72 percent indicated that increasing the speed with which their team onboards or develops and deploys applications is the top priority.

The agile methodology emphasizes the continuous delivery of working software. The approach can help mitigate risks by engaging customers (internal and external) in development cycles early, giving them an opportunity to adapt to changing requirements and environments. It can also be particularly useful with modern, highly dynamic environments, such as the cloud. An agile approach and a shift-left methodology reduce the likelihood of letting security problems and vulnerabilities go unaddressed until later in the development cycle, when they become more difficult and costly to resolve.

"DevSecOps is the only way to do business in 2021. It enables innovation by failing fast, learning fast, fixing fast, and not failing twice for the same reason."

Nicolas Chaillan

CTO,

Prevent Breach

Key Points

- Review the agency's development processes, and introduce techniques such as agile development, DevSecOps, and development best practices where possible.
- Implement security reviews and early testing cycles to help developers shift left.
- Focus on continuous delivery to improve developer velocity.

"Many organizations claim they are building software using DevSecOps principles and methodologies, but when you look under the hood, you learn they are still manually configuring applications, relying on limited security scanning and integration testing, and using manual stop gaps before applications reach production."

Hannah Hunt
Chief Product and Innovation Officer,
Army Software Factory

How to Shift Left and Deliver Requirements Before Coding Begins

Understanding how to build software securely while complying with all government cybersecurity regulations is a major challenge when developing for federal, state, or local government agencies. As an example, the National Institute of Standards and Technology (NIST) has defined myriad compliance standards, and it can be challenging to integrate them into a project correctly without overwhelming developers or accidently delivering on requirements that do not actually apply to the project. Additionally, all this complexity adds time to the SDLC and can extend the project. Adhering to government guidance or requirements that shift mid-project or simply do not apply translates to wasted development time and the risk of potential rework.

> **By shifting left and incorporating security efforts earlier in the SDLC, more teams will identify areas where they can automate and improve their existing software development approach and ultimately improve their overall security posture.**
>
> 
>
> **Rohit Sethi**
> CEO, Security Compass

By using agile development processes and breaking down requirements into relevant, tactical tasks, developers can focus their efforts on shorter development sprints (typically two weeks per sprint), deliver code more frequently, and integrate security and standards regulations into the cycle more efficiently. In this way, they insulate the project against the risk of implementing security as an add-on at the end of development.

"Many companies use out-of-date compliance rules, failing to maintain correct content and attributes. They need to invest in compliance teams and tools that allow them to update the control framework schema at the same pace as those schemas change."

Robin Basham
CEO, CISO, Founder,
EnterpriseGRC Solutions

This approach of continual releases, testing, and evaluation also helps avoid release delays when weaknesses in code that threat actors can exploit are found late in the SDLC.

Agencies should also consider the adoption of tracking tools to help document the secure development steps that developers take when writing code. Traditionally, organizations track developers' secure coding efforts manually, often in spreadsheets, and conduct interviews to understand how developers followed a particular regulation or secure coding practice. This time-intensive process is inefficient both for auditors and developers. Vast quantities of developer time are tied up in this manual documentation process to achieve ATO.

A leading practice is to track and monitor these security efforts as developers write their code. Organizations that follow this approach may also have an easier time when applying for ATO certification.

ATO is a US government requirement that any IT provider must attain to work with a federal agency. An ATO certificate is valid for just three years and is applicable to the single system for which it is applied.

Clearly demonstrating the security efforts, improvements, testing, and monitoring that took place during the SDLC can help establish a pattern of security. By considering security from the start, organizations are more likely to code "watertight systems" that have fewer vulnerabilities. Leaving the security review until the end of the development process increases the probability that issues and vulnerabilities buried deep within code paths will be discovered late in the release cycle, contributing to significant delays and project overruns.

"It is much easier to ensure compliance requirements are met along the way than to wait for a long-term assessment that finds hundreds of issues to fix. Shifting testing, security, and continuous compliance left is the only option to deliver capabilities continuously and successfully to end users."

Nicolas Chaillan

CTO,

Prevent Breach

Developing a DevSecOps Mindset and a Shift-Left Approach

Adopting an agile development method (where appropriate) can make a significant difference in secure software development. These benefits are enhanced when agile is combined with DevSecOps and a shift-left approach.

In a traditional (waterfall) software development model, development teams are responsible for coding and implementation; then testing occurs to identify and address bugs and vulnerabilities (Figure 2). Security fixes are addressed during testing or, often, during a postrelease maintenance cycle. This approach risks introducing zero-day vulnerabilities into the wild and can lead to extended patch cycles.

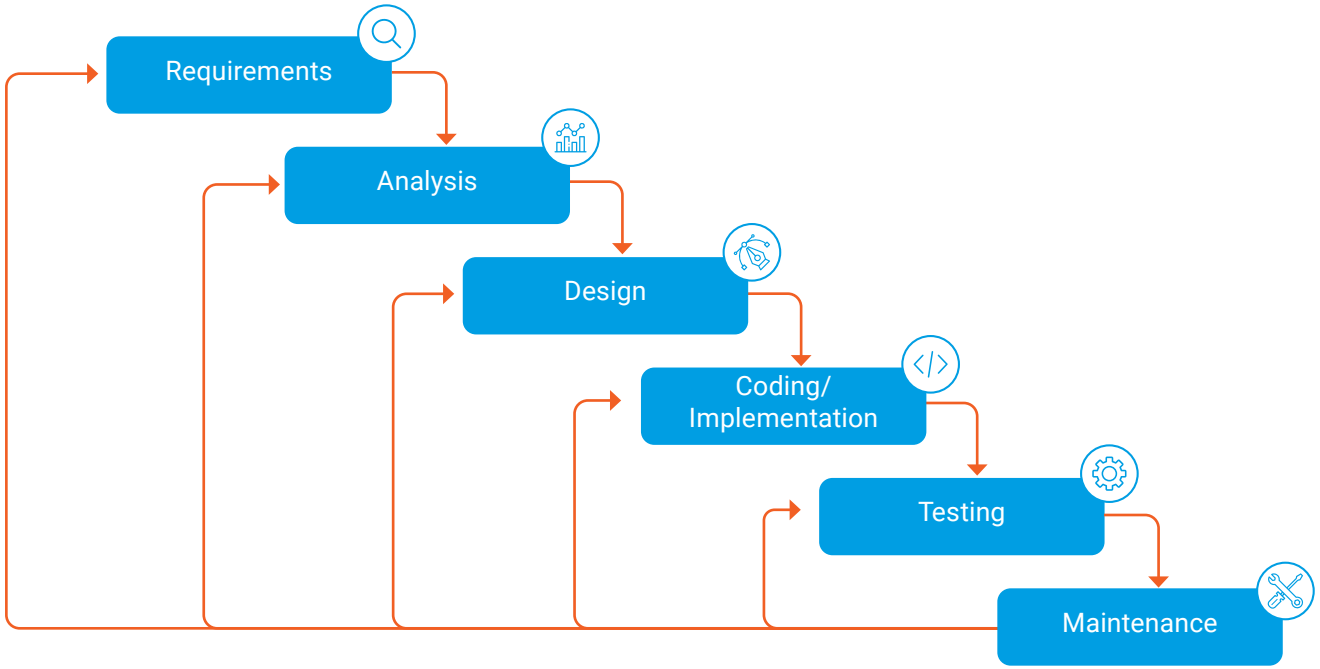

Figure 2: Traditional waterfall software development cycle

By contrast, adopting an agile approach, embracing DevSecOps, and shifting security reviews and assessments left can help identify gaps earlier, reduce software flaws, and speed secure development. In this model (Figure 3), developers take an active role in identifying risks, modeling threats, and remediating security concerns early.

"Too often, security serves as a stage gate at the end of the software development lifecycle. Organizations spend 12-18 months receiving an ATO while their code sits in a code repository. Instead, security should be baked in from the beginning."

Hannah Hunt

Chief Product and Innovation Officer, Army Software Factory

People and Organization	Roles and Responsibilities
"Developers" or the Product Owner(s)	• Threat modeling • Code development • Quality assurance/testing • Code deployment • Data management • User management • Vulnerability management • Cloud configuration scanning • User behavior monitoring • Data security monitoring
Platform Engineering or Site Reliability Engineering	• Templates and standardized components • Monitoring and operations support • Security operations • Threat intelligence

Figure 3: DevSecOps helps drive change across the SDLC

Many organizations, including IBM, have studied the impact and benefits of shifting security earlier in the software development life cycle (Figure 4). By shifting left throughout the process, organizations can reduce the cost of remediation significantly.

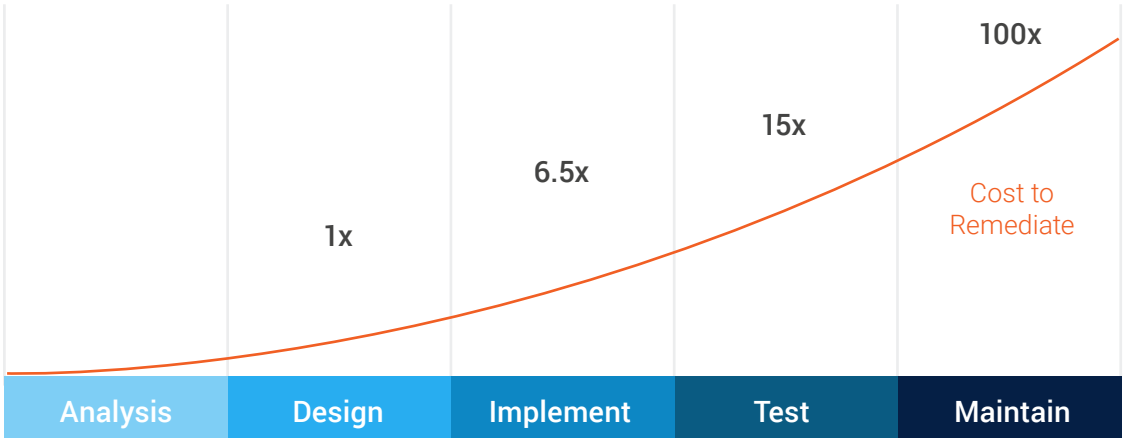

Figure 4: Earlier visibility to vulnerabilities pays dividends *(Source: IBM Systems Sciences Institute)*

"Shifting the process left entails relying on our teams to understand the risks, to be trained to recognize them, and to be able to deploy solutions and scanning processes to catch them early."

Stephan Mitchev
Director, Office of Application Engineering and Development, Acting CTO, USPTO

Key Points

- Manual tools for tracking developers' secure coding efforts are time-intensive and inefficient.
- Adopting an agile development method can make a significant difference in a secure development approach.
- Shifting left helps identify gaps earlier, reduce software flaws, and speed secure development.

"Shifting left is essential to prevent bottlenecks and technical debt to accrue at massive costs down the road. Instead of letting technical debt kill projects on the launch pad, make the launch pad something continuous, incrementally in production and in the hands of the actual end users."

Nicolas Chaillan
CTO,
Prevent Breach

> On the commercial side, companies such as Netflix and Google are releasing secure software hundreds of times a day. The public sector, at all levels, can achieve similar results by using a DevSecOps approach and shifting left while maintaining the quality and security needed for ATO.

Rohit Sethi
CEO, Security Compass

Include Security Seamlessly in the Software Development Process

In traditional software development, security was included at the end of the SDLC. Today, security requirements as well as implementation and verification of controls should be baked into the entire process. The security lead defines requirements up front, then pushes requirements down to developers as tasks in systems such as Atlassian Jira.

At a high level, Table 1 shows how organizations implement a shift-left strategy at each stage of software development without slowing the process.

Requirements	All stakeholders, including developers, must have a clear understanding of the requirements of each sprint or code development project so that they can effectively build securely from the start. This understanding is essential before beginning development.
Design	With code review, monitoring, and testing integrated earlier in the process, testers and developers can effectively implement best practices for user-driven design, security, and threat modeling. This approach helps reduce anomalies and vulnerabilities in the later stages of development. It also helps ensure that the team will develop code based on a shared vision.
Development	With a shift-left and DevSecOps approach, the development team should be encouraged to write code with testability in mind. By integrating testing and development at this stage, teams can help ensure that all units of code work well together when integrated. This approach also provides transparency across the team.
Testing	To get the greatest benefit from shifting left, teams must embrace testing and automation as part of the process. In this way, they can integrate security best practices, identify vulnerabilities early, improve test coverage, and speed continuous delivery.
ATO Certification	Obtaining an Authorization to Operate (ATO) certificate is essential for operating in highly secure environments, like government agencies or businesses subject to federal requirements. The ATO is a formal declaration that authorizes operation of a business product. Any ATO is signed after a review and certification that the system meets and passes all requirements to become operational.

Table 1: How to implement a shift-left strategy in the SDLC

"Shift-left is not shifting the work left; it's shifting the understanding of the work being done to the left. By doing this, fewer mistakes are made, more impactful changes occur, and the overall time to deployment decreases."

Ian Anderson

Lead DevSecOps Engineer,

Naval Surface Warfare Center,

Dahlgren

ATO and DevSecOps

Software development within the federal government often begins with an alignment to ATO and related, required security processes. Acquiring an ATO is a complex challenge for US federal agencies. Developers must not only comply with thousands of security controls, all of which are too frequently updated, but do so as quickly and effectively as possible. If they do not, mounting inefficiencies waste money, delay software releases, and take a toll on team morale.

It is a significant challenge to achieve ATO when the development team is burdened with outdated manual processes, such as spreadsheets, email, and other siloed tools, to track the process and communicate issues. Such a manual approach creates confusion, redundant work, and version-control issues.

> **When agencies embed ATO in the development effort, they streamline the entire auditing process. All the time and effort that used to go into supporting an audit now get turned into productive developer time. It's a real game changer.**
>
> 
>
> **Rohit Sethi**
> CEO, Security Compass

To eliminate this challenge, agencies should move to a more modern approach that embraces DevSecOps, which helps avoid bottlenecks caused by a waterfall approach and outdated software modalities. By integrating security at all points of the development process, the DevSecOps engine improves security across the entire SDLC.

"Any organization can utilize DevSecOps. It requires a significant culture change, decreased risk aversion, and a desire to do things differently. That's a big shift for a lot of organizations, but they can 100% do it!"

Hannah Hunt

Chief Product and Innovation Officer, Army Software Factory

Organization must take two steps to shift certification left:

- **Identify relevant requirements specific to ATO**. Agencies that want to shift ATO as far left as possible must meet numerous requirements, such as process- and development-related controls, early in the SDLC. Many of these controls go beyond normal security requirements: They are process-oriented requirements. Figure 5 shows the steps for attaining ATO.

- **Ensure effective control mitigation by employing a layered compliance perspective**. In a layered enterprise service model, one control can mitigate multiple identified threats or vulnerabilities. The challenge the organization faces is visibility into each issue and how many instances of that issue its controls can mitigate. Without this visibility, an organization often deploys redundant or inefficient controls.

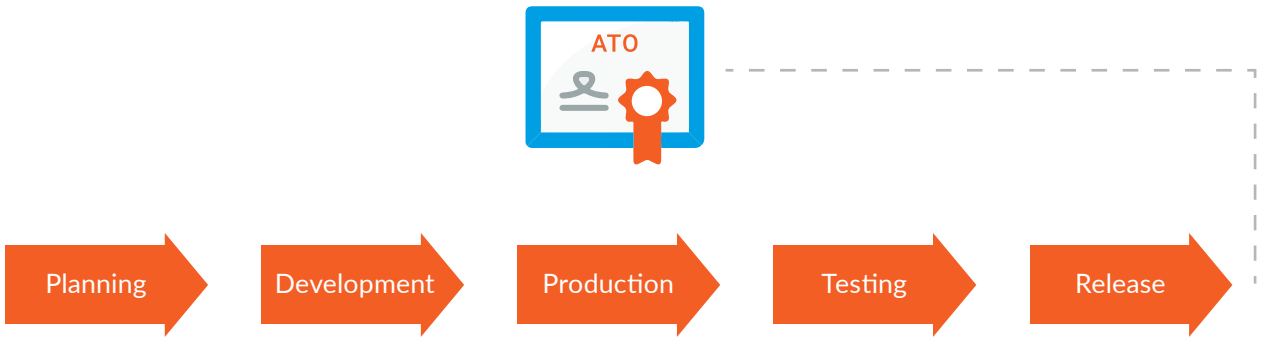

Figure 5: The steps for attaining ATO

"Traditional ATO processes require a more-or-less freeze on development during testing. Then updates and changes have to be assessed and documented prior to release to production, which causes further delays."

Tom Marlow

Managing Director,

Dark Wolf Solutions

Key Points

- Benchmark your program.
- Accelerate your development and release cycles.
- Streamline your security efforts by using a DevSecOps and continuous ATO approach.

"DevSecOps is the belief of ownership and collaboration across an organization. It is a cultural transition from how we used to do work before—in which teams were siloed and passed balls across fences—into one integrated, technically aligned, and autonomous team that owns its product."

Stephan Mitchev

Director, Office of Application Engineering and Development, Acting CTO, USPTO

Chapter Four

Ensure Developers Follow Secure Development Best Practices

When implementing a major shift (such as a shift left) across development teams, it is important to leverage techniques like just-in-time training, integration of regulatory guidance, and fine-grained documentation to support the developers as they write code. The benefit of this approach is higher developer velocity with strong compliance with regulatory standards and practices. By integrating these techniques throughout the development process, high-performing organizations can also document all the needed information to support ATO audits and certification.

High-performing organizations that have significantly higher developer velocity use the following techniques:

- Documented best practices tuned to the agency or department.
- Automation of testing, monitoring, and verification.
- Just-in-time training delivered in short formats to keep developers informed and focused.
- Verified code libraries and repos to foster efficient code reuse.
- Additional process optimizations to help teams develop with speed and safety.

By supporting developers with just-in-time training and reinforcement, developers are freed from the expectation of having to remember secure coding best practices they learned years ago in class.

After an organization has fully integrated its product and software life cycle workflows, monitoring, documenting, and verifying the environment becomes markedly easier. It is essential that security is an integral part of the process to both minimize costs but also accelerate product delivery.

"Focus on the end goal we are trying to reach: confidence that our systems are trustworthy and secure from day zero until end-of-life."

Ian Anderson

Lead DevSecOps Engineer,

Naval Surface Warfare Center,

Dahlgren

Streamlining the Process for Tracking, Verifying, and Documenting Implemented Controls

When the development team has shifted left, adopted a DevSecOps mindset, and embraced an agile development approach, the organization must support these modernization efforts through automation, monitoring, and the right tools. Manual processes that include spreadsheets and issue tracking by email are not efficient or scalable.

To streamline developer efficiency and the ATO certification process, agencies should support development teams:

- With tools to help integrate automation and speed into the development, testing, and approval processes.
- By evaluating bottlenecks to implementing the right tasks for the right project.
- By integrating systems with other tools used in the continuous integration/continuous delivery pipeline.

> **Leading organizations integrate security throughout the process. They support secure development by using approved code snippets and techniques such as just-in-time training to ensure that developers adhere to secure guidelines. Elite organizations monitor and track that activity to provide strong audit documentation effortlessly.**

Rohit Sethi
CEO, Security Compass

"Developers need tools and training to be able to integrate resources that apply static and dynamic rules to an array of configurable items and code modules and to receive updates about the severity of any misconfiguration or actual exploit."

Robin Basham
CEO, CISO, Founder,
EnterpriseGRC Solutions

In addition to making investments in developer efficiency, organizations need visibility to all their processes—an easy way to identify, assess, and remove bottlenecks. Such visibility requires detailed reporting and analytics on what has been done and the ability to report on completed tasks and implemented controls. Giving teams a way to track these efforts throughout the SDLC helps minimize the drain on development efforts.

Effective monitoring and reporting help streamline ATO certification efforts and support security assessors, who need to audit what has been done during the development cycle, assess security and compliance efforts, and determine whether the software meets requirements.

Other best practices include integration with code scanners and testing to show and validate which controls have been implemented correctly. Software developers gain efficiencies through early testing and understanding how to address security early and often.

"The entire team should be aware of all of the components, how they function and interact with each other, and how to fix common issues."

Tom Marlow

Managing Director,

Dark Wolf Solutions

Key Points

- Manual processes start and end with bottlenecks. Automation and scanning are essential to improving development efforts.
- Antiquated tools and a manual process will likely prevent a smooth ATO.
- A commitment to shifting left liberates the software team to build faster and safer software.

"Whereas compliance assessments are periodic, security is a constant challenge for organizations. Strong mitigation plans paired with trusted technologies for monitoring and automation seek to solve that challenge."

Ian Anderson
Lead DevSecOps Engineer,
Naval Surface Warfare Center

Chapter Five

Achieve ATO Faster with a Modern, Agile Environment

Obtaining ATO to build software for the federal government can take months because it involves compliance with nearly 900 security controls. If teams lack knowledge or training in the use of these controls, the process can be delayed further.

Agencies seeking to accelerate their development efforts should embrace modern development approaches, including agile frameworks, DevSecOps, and:

- Help integrate configuration, integration, and change planning across critical software platforms and development efforts, including integrating software development elements from existing issue-tracking systems (e.g., Jira) and security testing tools (e.g., Checkmarx, Fortify, Veracode).
- Look for ways to use internal resources and time efficiently, focusing on all aspects of the modernization transformation.
- Develop new systems without creating friction or draining resources to bring on the new approach.
- Establish processes, roles, and responsibilities across teams to support the agile and DevSecOps transformation.
- Look for opportunities to adopt custom guidance and methods to embed best practices to demonstrate value quickly; focusing on early wins helps ensure adoption across the organization.
- Allow time to define project goals, align priorities, and build meaningful stakeholder relationships by creating an honest assessment of the organization's security culture, future goals, technology portfolio, regulatory requirements, and project priorities.
- Plan for future staff needs, including just-in-time training, consolidating relevant content and documentation, and updating materials to stay current with compliance and regulatory changes. This plan should include a curriculum for existing employees, additions to the team, program managers, and administrators.

Moving from a traditional waterfall development process to a modern, agile DevSecOps environment not only helps agencies and departments ship code faster, it helps ensure developers embrace security, deliver better outcomes, and achieve ATO.

"Many projects install a Continuous Integration/ Continuous Delivery (CI/CD) tool and call it done. That's just the tip of the iceberg. True DevSecOps incorporates end-to-end automation that reduces, and ideally removes, the human-in-the-loop factor so that deployments are repeatable and predictable."

Tom Marlow
Managing Director,
Dark Wolf Solutions

Key Points

- The process to attain ATO can be accelerated by modernizing its development approaches.
- Moving from a traditional waterfall development process to a modern, agile environment ensures that developers deliver better outcomes.

"The crux of any valid assessment program is to be able to load a set of criteria and score its implementation based on environment-specific cloud development rules. There need to be sufficient design elements to track against any type of risk model or audit."

Robin Basham
CEO, CISO, Founder,
EnterpriseGRC Solutions

Learn More About Our Experts

Rohit Sethi, CEO, Security Compass

Rohit Sethi joined Security Compass as the second full-time employee. As CEO, Rohit is responsible for setting and achieving corporate objectives and company alignment and driving strategy to execution. Rohit specializes in building security into software, working with several large companies in different organizations. Rohit has appeared as a security expert on major media outlets, including Bloomberg, CNBC, FoxNews, CNN.com, the Huffington Post, and InfoQ.

Stephan Mitchev, Director, Office of Application Engineering and Development/Acting CTO, USPTO

Stephan Mitchev is the Director of the Office of Application Engineering and Development and Acting CTO at USPTO. An IT industry veteran, he led the agile transformation across telecommunications, retail, healthcare, and education domains. Prior to the USPTO, he was the director of Architecture and Standards at Universal Service Administrative Company (USAC), where he modernized IT systems and led the cloud strategy. Stephan's contributions come from his recent appearance on the Federal News Network webinar, "Modernizing mission critical apps requires a transition to DevSecOps."

Nicolas Chaillan, CTO, Prevent Breach

Nicolas Chaillan is a technology entrepreneur, software developer, cyber expert, and inventor. He was appointed as the first Air Force and Space Force Chief Software Officer and was the co-lead for the DoD Enterprise DevSecOps Initiative. Nicolas is recognized as one of France's youngest entrepreneurs after founding WORLDAKT at 15 years of age. He has founded 12 companies, including AFTER-MOUSE.COM, Cyber Revolution, Prevent Breach, and anyGuest.com, among others.

Hannah Hunt, Chief Product and Innovation Officer, Army Software Factory

Hannah Hunt (Forbes 30 Under 30, Class of 2021) currently serves as the Chief Product & Innovation Officer for the Army Software Factory within Army Futures Command, which teaches soldiers and civilians to solve army problems with cloud technology and modern software. Prior to this role, Hannah served as the Chief of Staff at Kessel Run, the Air Force's premiere software factory.

Ian Anderson, Lead DevSecOps Engineer, Naval Surface Warfare Center Dahlgren

Ian D. Anderson is a Lead DevSecOps Engineer with Naval Surface Warfare Center Dahlgren. He has helped formulate policy, processes, and training for NSWC Dahlgren to aim their efforts toward a collaborative, scalable DevSecOps environment for the Warfare Center and other DoD partners. He is a graduate of Christopher Newport University in Newport News, Virginia, with a degree in computer science and computer engineering.

Tom Marlow, Managing Director, Dark Wolf Solutions

Tom Marlow is a Managing Director at Dark Wolf Solutions and leads its Cybersecurity Practice. He possesses over 20 years of leadership, cybersecurity, and management consulting experience. At Dark Wolf, Tom oversees a portfolio of cybersecurity engagements that include penetration testing, cybersecurity consulting, ATO attainment, and DevSecOps implementation for the Intelligence Community, DoD, and commercial customers.

Robin Basham, CEO, CISO, Founder, EnterpriseGRC Solutions

Robin Basham is recognized as an ISC-2 Chapter President & Conferences Director, the Leader for the Cloud Security Alliance CCM NIST WG, and the CEO of EnterpriseGRC Solutions. Her industry expertise includes the management and development of systems, controls, and data for SaaS (IaaS and PaaS), Finance, Healthcare, Banking, Education, Defense, and High-Tech. She has graduate degrees in technology and education and numerous certifications in these fields.

Are you struggling to obtain ATO at the speed of mission?

Access this free eLearning course to learn how SD Elements can help you quickly comply with ATO security requirements

What you'll learn:

1. What ATO is
2. Different pathways to ATO
3. How you can obtain ATO faster by eliminating inefficiency and reducing redundant controls

Access Free Course

TRUSTED BY

SecurityCompass

www.securitycompass.com