DevSecOps for modern governments

Solution development that embeds security from the start

Governments use DevSecOps, but they can do more

The state of Colorado learned a difficult lesson while modernizing a system recently. The state's collaborative internal and vendor software team invested two years of development before security scanning the code just prior to go-live. The security scan detected more than 10,000 vulnerabilities. They now use tools to enhance security from the start.[1]

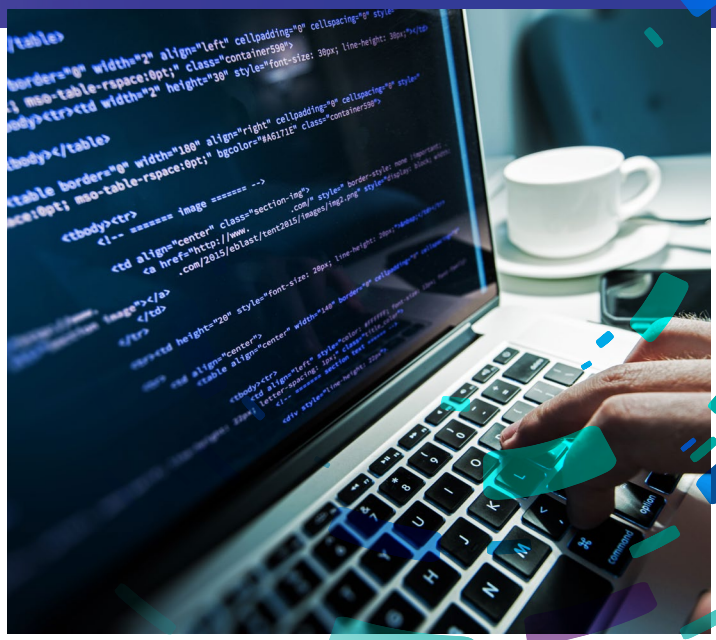
Many federal, state, and local governments successfully use development, security, and operations—or DevSecOps—in their solution development and delivery. However, many organizations hold onto traditional approaches to address security after development and operations. Teams that use DevSecOps correctly embed security up front and throughout the entire solution development lifecycle.

In federal government, the Department of Defense accounted for most use in 2020 while civilian agencies DevSecOps adoption is increasing.[2] However, there may be a road bump since the co-head of the Defense Department's Enterprise DevSecOps initiative, who also was software lead for the Air Force, recently resigned. He cited lack of support from senior leadership as his primary reason.[3]

Senior leaders must escalate DevSecOps implementation as a top priority to show support and get ahead of new and growing vulnerabilities and cyber risk concerns. These concerns put development, security, and operations teams under greater pressure to reduce risk across the solution development lifecycle. Most important, citizens trust these team members to protect their personal and private information. Support from organizations' top leaders for a more effective DevSecOps framework can help lessen these risks. This article shows why it is critical to embed security into the solution development process from the beginning. We present practical methods federal, state, and local governments can use to avoid slowing down developer teams and measure progress.

Why modern government is important

Government agencies in the U.S. must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.



[1] Phil Goldstein, "How DevSecOps Helps Government Security and Innovation," State Tech Magazine, June 4, 2021.

[2] Dave Nyczepir, "2020 in review: Pentagon leads DevSecOps efforts," FedSCOOP, December 31, 2020.

[3] Brandi Vincent, "Leader of a Pentagon-wide DevSecOps initiative, Nicolas Chaillan cited lack of support from senior leadership as one reason for his departure," Nextgov, September 2, 2021.

Build a governance structure that empowers developers

Government technology organizations should **adapt their DevSecOps to prioritize speed and agility and support a modern government**. At the same time, they should **implement a comprehensive governance framework** with relevant **controls, security scanning**, and **automated testing**. DevSecOps allows for the most cost-effective, agile, and secure implementation from start to finish. DevSecOps empowers development teams to deliver value faster and more often since they contribute code at higher rates, reduce incident mean-time to repair, and shorten lead time to production without interrupting their abilities to achieve the mission. With these, operational budgets are also lower.

It is not uncommon for solution development teams to bypass security protocols similar to the opening example. Each person, team, and agency has different reasons for not adopting DevSecOps. A recent survey of nearly 300 federal, state, and local technical professionals highlights one reason—40 percent reported using 10-plus tools in the development lifecycle. Using so many tools complicates the development process and requires teams to spend too much time managing the tools rather than delivering solutions.[4] Addressing security late in the development cycle is costly. Also, compromising security for the sake of an implementation date is risky.

Some organizations see the benefits of building a governance structure their developers will use. For example, developers working on the U.S. Air Force Ground-Based Strategic Deterrent program incorporated DevSecOps from the start and saved "at least 18 months".[5] An Air Force team uses DevSecOps to develop military tools to lessen the risk for enemies to hack into their networks, especially critical while people work remotely.[6]

[4] "ATARC Federal; DevSecOps Landscape Survey Findings," Advanced Technology Academic Research Center, U.S. Air Force, February 2021.

[5] Greg Hadley, "Air Force Leadership Needs to 'Walk the Walk' in Baking Security into Cyber, Software Boss Says," Air Force Magazine, August 12, 2021.

[6] Dave Nyczepir, "2020 in review: Pentagon leads DevSecOps efforts," FedSCOOP, December 31, 2020.

Five essentials to include "Sec" in DevSecOps for a modern government

We recommend following these five essential steps to achieve DevSecOps and keep projects on track.[7]

1. **Determine everything the organization needs to procure to build the solution and how to measure performance.** Government developers spend more time creating low code and configuration than traditional coding. Instead, they collaborate with vendors to complete the solution development process.

   Implication. With collaborative teams made up of on-staff developers, security, and operations professionals with multiple vendors, processes can become disjointed and expectations off track. These teams often leave security to the end in order to deliver faster. When they do, they end up adding more time to the process like in the opening situation.

   What to do about it. Planning what the team will need to build the solution as well as how to measure whether the internal team and vendors are on track are critical for a smooth process and secure code. Does the solution need vendors to provide cloud, DevSecOps, database services, or other pieces of the solution development process? Will each build security into the software or service throughout the entire development process? What milestones and metrics will the team use to measure performance? Example metrics include use of defined tools and processes, code contributed each day, and regular security scan results.

2. **Remove barriers from development team's path.** As demand for new features and functions grow, development teams must work faster. Knowing code they work on will be deployed to production and used to help achieve mission-critical goals motivates many government developers, so the fewer barriers that slow the process down the better in keeping teams motivated.

   Implication. Many developer teams already use automated continuous integration and continuous delivery (CI/CD) pipelines so they can develop, build, test, and deliver solutions quickly. Some take shortcuts to circumvent governance to maintain speed, but CIOs, chief risk, or security officers get the frantic email or call when there is an outage or failure. While developers may want autonomy, they must realize autonomy cannot replace security and compliance. Sidestepping governance exposes organizations to avoidable risks.

   What to do about it. Organizations can achieve an automated DevSecOps pipeline by adopting security, governance, and change-control mechanisms. Leaders can make it easy for development teams by embedding controls directly into the CI/CD pipeline from the start. This approach enables developers to operate at full speed without exposing the organization to risk and regulatory penalties.

3. **Give information security, governance, and compliance seats at the table from the outset.** One of the toughest challenges for development teams is managing security in cloud-native, automated DevOps environments. Security teams have to protect sensitive citizen and department data and limit exposure to hackers and bad actors to maintain citizen trust.

   Implication. Information security professionals work with developers to make hundreds or thousands of projection changes each day. When organizations rush to release application upgrades, they often bypass security controls, leaving them vulnerable to cyber incidents.

   What to do about it. Embedding security and governance controls into existing development pipelines does not slow the CI/CD process. This gives security teams native control of the pipelines by automating security scanning, controls, and testing to the same degree developers have automated their environments. When security has this level of control, organizations help ensure development teams can innovate and deliver new features and capabilities without slowing down the process, sacrificing safety, or exposing the organization to risk.

[7] Adapted from "Five keys to an effective DevSecOps framework," KPMG LLP, 2021.

4. **Empower operations to better support what developers build.** When developers are under pressure to deliver code faster, teams often prioritize deadlines over security. When problems arise, leaders lean on Operations and Risk to assess and repair the damage, often using IT Service Management (ITSM) controls to maximize updates and maintain reliability. In an ideal state, one cross-functional team working toward a common objective should support DevOps.

   Implication. Development teams operate in a rapid, iterative fashion, often releasing application changes daily. At this pace, even well-seasoned operations teams struggle to maintain capacity and governance. The pace creates challenges for legacy ITSM controls. The common practice is to provide development teams with preapproved changes or other solutions to bypass controls. The hope is that these changes will not disrupt what is already in production. Most developers are unaware of the pipeline's end-to-end vulnerabilities because they focus on a specific area or purpose. Problems arise when portions of code that ran fine on the developer's computer are unstable in production.

   What to do about it. Organizations can keep up with development teams' push for speedy releases by automating operational functions, such as complying with relevant ITSM controls. The key is to implement automated ITSM controls for change and release management, gather data and draw insight, then make strategic, policy-driven decisions to automate governance. A fully automated CI/CD pipeline includes automated security controls as well as automation IT Infrastructure Library (ITIL) controls. Maintaining ITSM controls within an automated site reliability engineering model will enable Risk to keep pace with developers as they work to ensure maximum reliability and uptime. The result is an efficient CI/CD pipeline for developers to build code, test, and safely deploy new or update solutions.

5. **Visualize value across the pipeline by focusing on citizen value streams.** The purpose for DevSecOps is to manage effectively across all citizen/customer value streams. Decision makers must have a citizen-centric point of view to understand how well their organization creates value and identify where issues arise along the delivery supply chain.

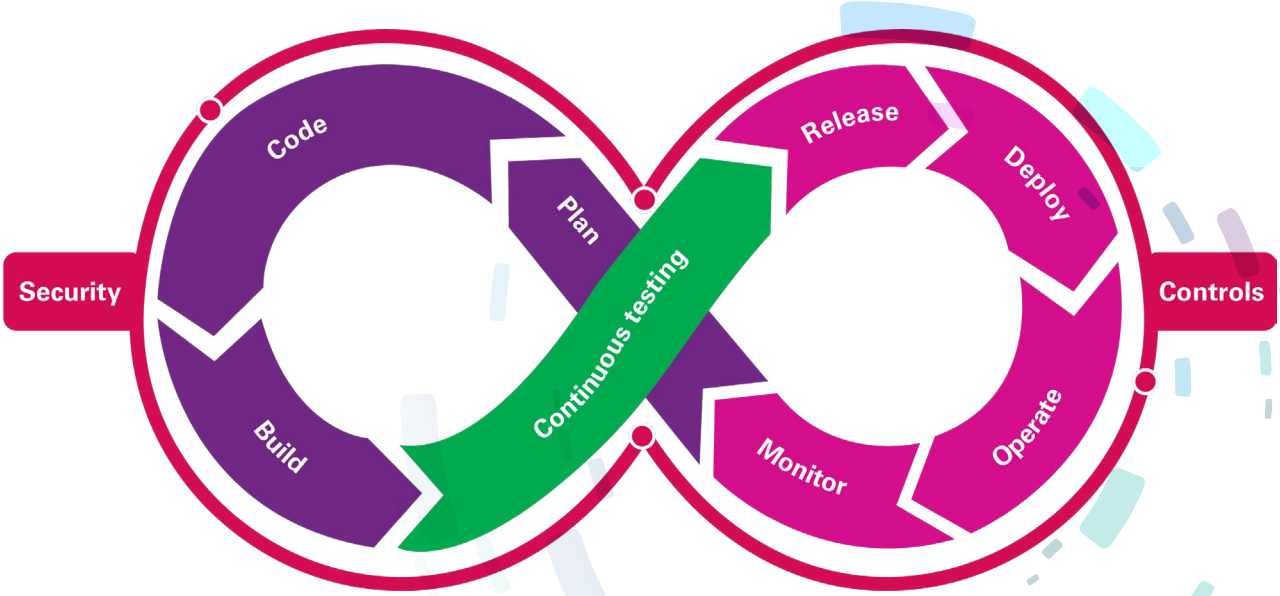
   Implication. In our dynamic, digital world, people expect to see quick, transparent, and seamless value. This pushes governments to provide products and services faster and with better user experiences.

   What to do about it. We believe governments can improve solution delivery with Value Stream Management principles, tools, and procedures. This approach helps ensure that the solution development lifecycle is transparent, quality, and continuously improves. When used with DevOps, value streams enable organizations to track and measure what they believe will bring most value to citizens to improve citizen satisfaction. Value stream platforms and tools provide deep insights and analytics across all delivery pipelines so developer teams can make decisions based on real-time data they extract from existing applications as well as from citizen feedback. They also help identify areas or tasks that will deliver value in the form of faster releases, more efficient operations, and overall security.

Deliver value faster with less risk

KPMG can help governments create a more collaborative DevSecOps framework for fast, compliant, and safe service delivery throughout the solution development lifecycle. We apply our internal capabilities and vast government and technology experience to tailor a DevSecOps approach that uses specialized tools, processes, and architecture to accelerate delivery as illustrated in the below graphic. This approach makes security as frictionless as possible so the organization can deliver value faster, align risk-reducing security activities to the business strategy via tighter feedback loops, and link system and business metrics.

Integrating DevSecOps throughout the solution development lifecycle



This holistic framework uses leading practices that cover project management, process management, and systems and software engineering. It supports lifecycle models such as Agile and promotes a process-improvement culture and shared learning to help increase quality, consistency, and transparency.

KPMG perspective

— A growing reason organizations experience outages, failures, and high-profile cyberattacks is because their DevOps delivery chains lack collaboration and security.
— Cross-network collaboration and governance are critical for controlled solution releases. This helps to ensure modern service delivery models apply security policies and controls to enable speed without compromise. Technology, security, and risk leaders must align priorities to achieve this goal.
— Development and delivery teams realize greater value of an integrated DevSecOps structure while also mitigating vulnerabilities and cyber risks.
— Stakeholders at all levels must change their way of thinking. Those who embrace DevSecOps will be better able to innovate, drive value, and deliver on their mission.

Keep your software project secure

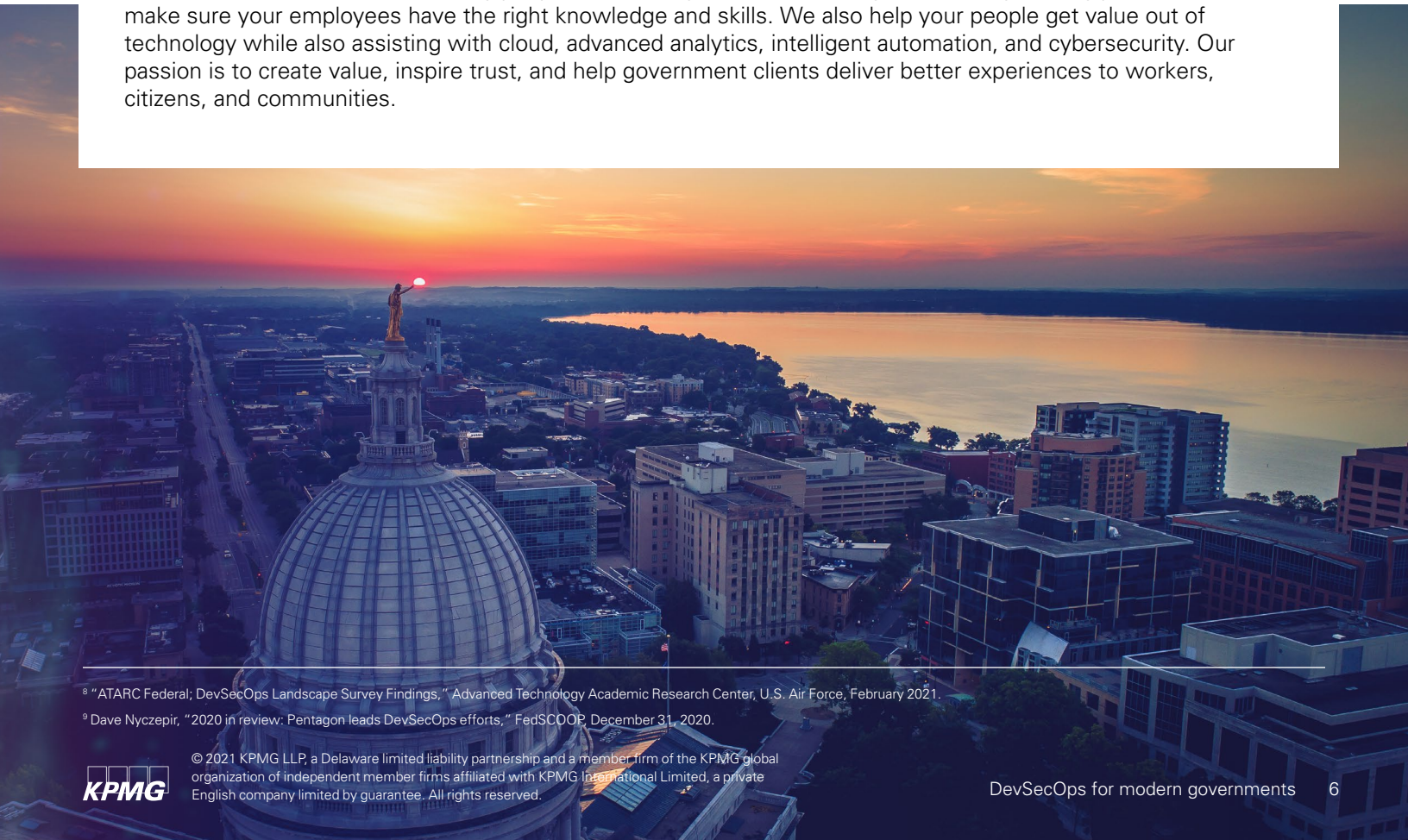
Many governments intend to improve their DevSecOps methodology. To do so, they need budget and support from top leaders. According to the survey of government technology professionals, nearly 60 percent reported DevSecOps as a fiscal year 2021 investment priority, third after cloud computing and security.[8] Naming a specific person to lead DevSecOps is another way to keep efforts top of mind. In 2020, the Department of Veterans Affairs appointed someone as its first head of DevSecOps.[9]

Done correctly, DevSecOps can effectively support a modern government—one that empowers developers to more quickly and securely deliver on the mission. Governments don't have to tackle DevSecOps alone. The GSA Tech Guides include a DevSecOps Guide that describes requirements for an implementation to be considered a Standard GSA DevSecOps Platform. KPMG can help adapt and manage DevSecOps at the start of a major project to better integrate on-staff and vendor developer teams and measure performance—so you can achieve the mission and support a modern government.

About KPMG

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.



[8] "ATARC Federal; DevSecOps Landscape Survey Findings," Advanced Technology Academic Research Center, U.S. Air Force, February 2021.

[9] Dave Nyczepir, "2020 in review: Pentagon leads DevSecOps efforts," FedSCOOP, December 31, 2020.

Contact us

Tony Hubbard
Principal, Government Cyber Security Leader
KPMG LLP
202-486-4945
thubbard@kpmg.com

Viral Chawda
Principal, Advisory
Digital Lighthouse
KPMG LLP
214-840-2000
vchawda@kpmg.com

Joseph Klimavicz
Managing Director, Federal CIO Advisory Leader
KPMG LLP
703-795-8999
jklimavicz@kpmg.com

Tom Frame
Managing Director, Advisory
Digital Lighthouse
KPMG LLP
703-286-6888
tframe@kpmg.com

Kathy Cruz
Director, Government Cyber Security Practice
KPMG LLP
916-792-3976
kathycruz@kpmg.com

---

read.kpmg.us/modgov

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia