Re-evaluate DevSecOps

Prioritise security to maximise operational capacity

KPMG Smart Government
Catalyse digital progress

Executive Summary

Development, security, and operations is a recipe for government success

It pays to build security into the solution development lifecycle from the start. Scanning for vulnerabilities at the final hour can unveil huge holes, stalling launch, and compromising trust.

A successful central or local government organisation uses development, security, and operations—or DevSecOps— in their solution development and delivery. The UK's Ministry of Defence (MoD) launched the Defence DevSecOps Service (D2S), in August 2022.[1] Director Chief Data at Defence Digital, Head of UK Defence & National Security, Palantir and a Rear Admiral were supportive of the UK MoD awarding Palantir a digital transformation enterprise agreement in December of 2022.[2]

The time is now for senior leaders to escalate DevSecOps as a top priority. As threats evolve and vulnerabilities grow, government departments are under huge pressure to reduce risk across the development lifecycle—making DevSecOps a priority is key.

First thing's first

Build a framework to support your developers

Modern governments have new demands on technology— and this starts with developers. This means implementing a comprehensive governance framework with relevant controls, security scanning, and automated testing.

A global survey of 5,000 software professionals by GitLab in May 2022 reported – 69 percent of those surveyed wish to combine their tool chains due to difficulties with monitoring, delays in development, and a poor developer experience.[3]

DevSecOps empowers your development team 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.

[1] John Leyden, "UK government sits out bug bounty boom but welcomes vulnerability disclosure," PortSwigger, May 16, 2022.

[2] "MOD runs first hackathon, launches OpenShift DevSecOps platform" The Stack, October 14, 2022.2022

[3] "Global DevSecOps Survey: Thriving in an insecure world," The GitLab 2022, May 2022.

Putting the Sec in DevSecOps

Five steps to keep projects on track

01 Determine everything the organisation needs to procure to build the solution and how to measure performance.

02 Remove barriers from the development team's path.

03 Give information security, governance, and compliance seats at the table from the outset.

04 Empower operations to better support what developers build and configure.

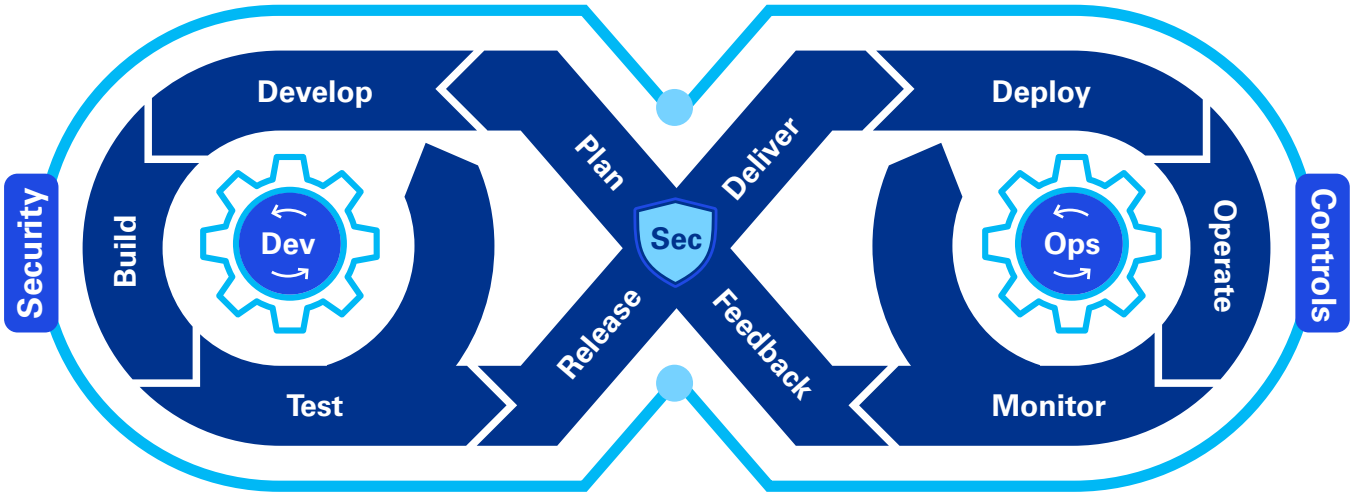
05 Visualise value across the pipeline by focusing on citizen value streams.

Build your DevSecOps case

- Organisations experience outages, failures, and high-profile cyberattacks because their DevOps delivery chains lack collaboration and security
- Cross-network collaboration and governance are critical for controlled solution releases.This ensures modern service delivery models apply security policies and controls to enable speed without compromise
- Development and delivery teams realise the 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
- In December 2022, UK MoD, with the support from Defence Digital leadership, signed a £75 million agreement with Palantir to aid its digital transformation.[4] Naming a specific person to lead DevSecOps is an effective way to keep efforts top of mind

Deliver value faster with less risk

Integrating DevSecOps throughout the solution development lifecycle



[4] Mark Say, "MoD signs £75 million enterprise agreement with Palantir," UKAuthority Office, December 23, 2022.

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

kpmg.com/uk

CREATE | CRT145789B | June 2023

Document Classification: KPMG Public