Re-evaluate DevSecOps

Prioritise security to maximise operational capacity

KPMG Smart Government

Catalyse digital progress

Insight Briefing

Some government organisations use DevSecOps, but they can do more

The UK Ministry of Defence has supported bug bounty programmes as they help to increase the security and robustness of its web applications. They ran a successful bug bounty programme in 2021 in conjunction with HackerOne. Additionally, they encourage users of UK government websites to contact the NCSC to report vulnerabilities.

Many central and local government organisations successfully use development, security, and operations—or DevSecOps—in their solution development and delivery. However, many organisations 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. DevSecOps automation can help organisations scale development while adding security, as well as uniformly adopt security features and reduce remedial tasks.

The UK's Ministry of Defence (MoD) launched the Defence DevSecOps Service (D2S), in August 2022. D2S intends to give developers a single DevSecOps platform for creating and deploying contemporary software applications across security classifications within the MoD and beyond.[2] 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.

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 importantly, citizens trust these team members to protect their personal and private information. Support from organisations' 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 central and local governments can use to avoid slowing down developer teams and measure progress.

Why smart government is important

Government organisations and departments around the world should modernise in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders involved in government modernisation are reviewing their user's experiences to plan what upgrades are needed in their business processes and service delivery models.

This article is one of a series that features how modernising can affect the government workforce and the user experience, improve security and public trust, and accelerate the digital journey. KPMG offers insights intended to help guide governments and public sector organisations in their modernisation efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organisations.

[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.

[3] Greg Hadley, "UK Ministry of Defence awards Palantir £75 million Enterprise Agreement," PR Newswire, December 21, 2022.

Build a framework to support your developers

Government technology organisations should **adapt their DevSecOps to prioritise 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. Each person, team, and department has different reasons for not adopting DevSecOps. A global survey of 5,000 software professionals by GitLab in May 2022 reported – 69 percent of those surveyed wish to combine their toolchains due to difficulties with monitoring, delays in development, and a poor developer experience. According to the poll conducted, organisations place the highest emphasis on security while making investments.[4] Addressing security late in the development cycle is costly. Also, compromising security for the sake of an implementation date is risky.

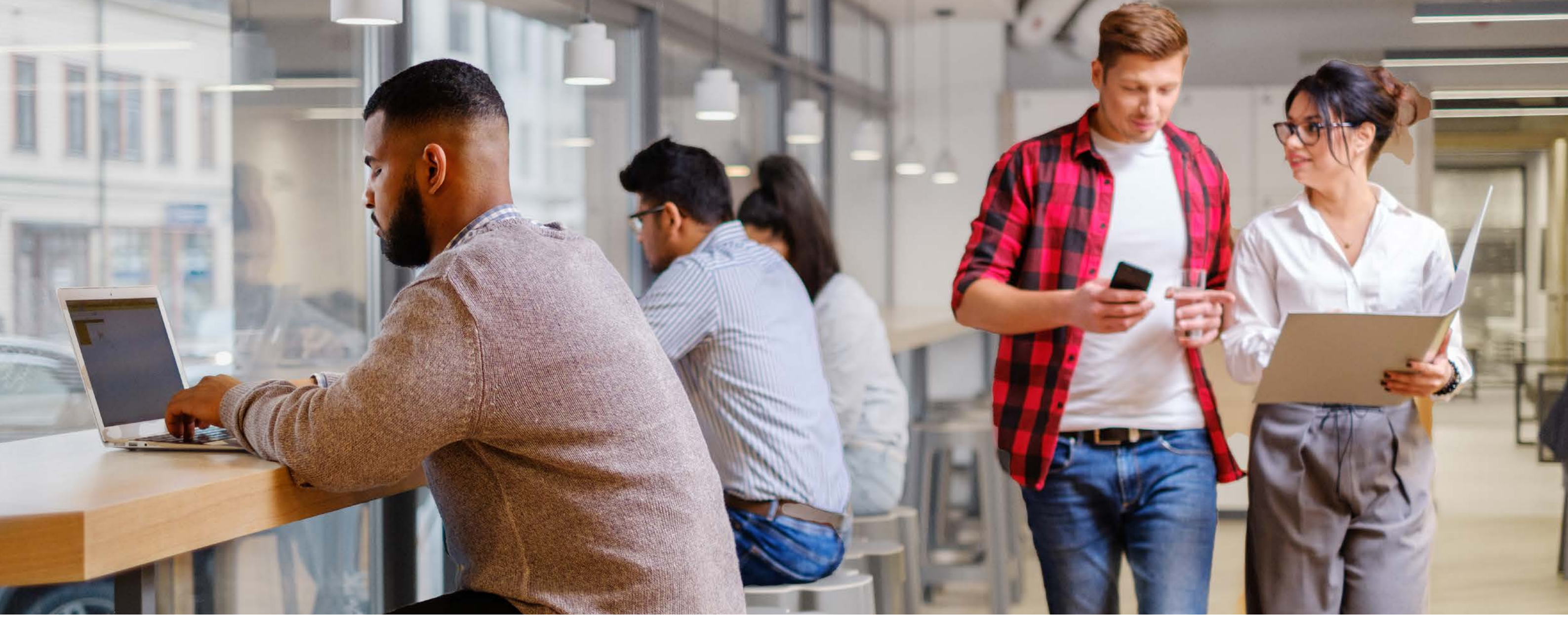
DevSecOps can also help your organisation with the speed of response in a world where attackers are increasingly automating everything they do. DevSecOps is a way to respond more quickly and efficiently to these attacks through a number of different methods: continuous security testing, vulnerability testing solution, and libraries.

Some organisations see the benefits of building a governance structure their developers will use. For example, Palantir's products and services are assisting the UK MoD in becoming an integrated digital enterprise with data exploitation and more integrated defence as a strategic partner in a complex defence data eco-system. MoD staff carry out advance scenario planning, testing hypothesis, and modelling how it would play out in real-time with the Palantir data model in place.[5] Through D2S, the MoD is creating a modern development environment based on industry-standard cloud technology, but tailored to defence security requirements. Skyral, a platform for developing Synthetic Environments (SE), will be used by Improbable Defence and D2S to deploy a complicated environment application.[6]

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

[5] Greg Hadley, "UK Ministry of Defence awards Palantir £75 million Enterprise Agreement," PR Newswire, December 21, 2022.

[6] Hayley P and J. Kennedy, "Improbable Defence and D2S: Working together to shape the future of Defence DevSecOps," GOV.UK, October 11, 2022.



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]

01

Determine everything the organisation 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.

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.

02

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 realise autonomy cannot replace security and compliance. Sidestepping governance exposes organisations to avoidable risks.

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

What to do about it. Organisations 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 organisation to risk and regulatory penalties.

03

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 organisations 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, organisations help ensure development teams can innovate and deliver new features and capabilities without slowing down the process, sacrificing safety, or exposing the organisation to risk.

04

Empower operations to better support what developers build. When developers are under pressure to deliver code faster, teams often prioritise 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 maximise 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. Organisations 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.

05

Visualise 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 organisation creates value and identify where issues arise along the delivery supply chain.

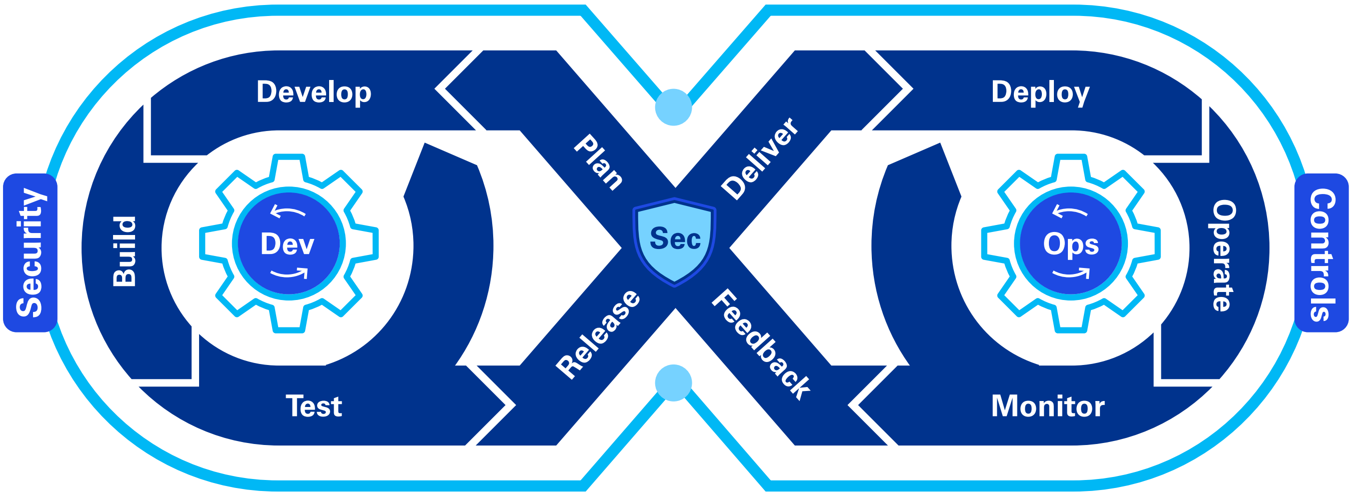
Implication. In our dynamic, digital world, people expect to see quick, transparent, and seamless value. This pushes governments to provide products and services faster and with better user experiences.

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, high quality, and continuously improves. When used with DevOps, value streams enable organisations 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 specialised tools, processes, and architecture to accelerate delivery as illustrated in the below graphic. This approach makes security as frictionless as possible so the organisation 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,

KPMG perspective

- A growing reason organisations 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 realise 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. In December 2022, the UK MoD, with the support from Defence Digital leadership, signed a £75 million agreement with Palantir to aid its digital transformation.[8] Naming a specific person to lead DevSecOps is another way to keep efforts top of mind. In 2020, the UK MoD appointed someone as Service Owner for Defence DevSecOps Service(D2S).[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.

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

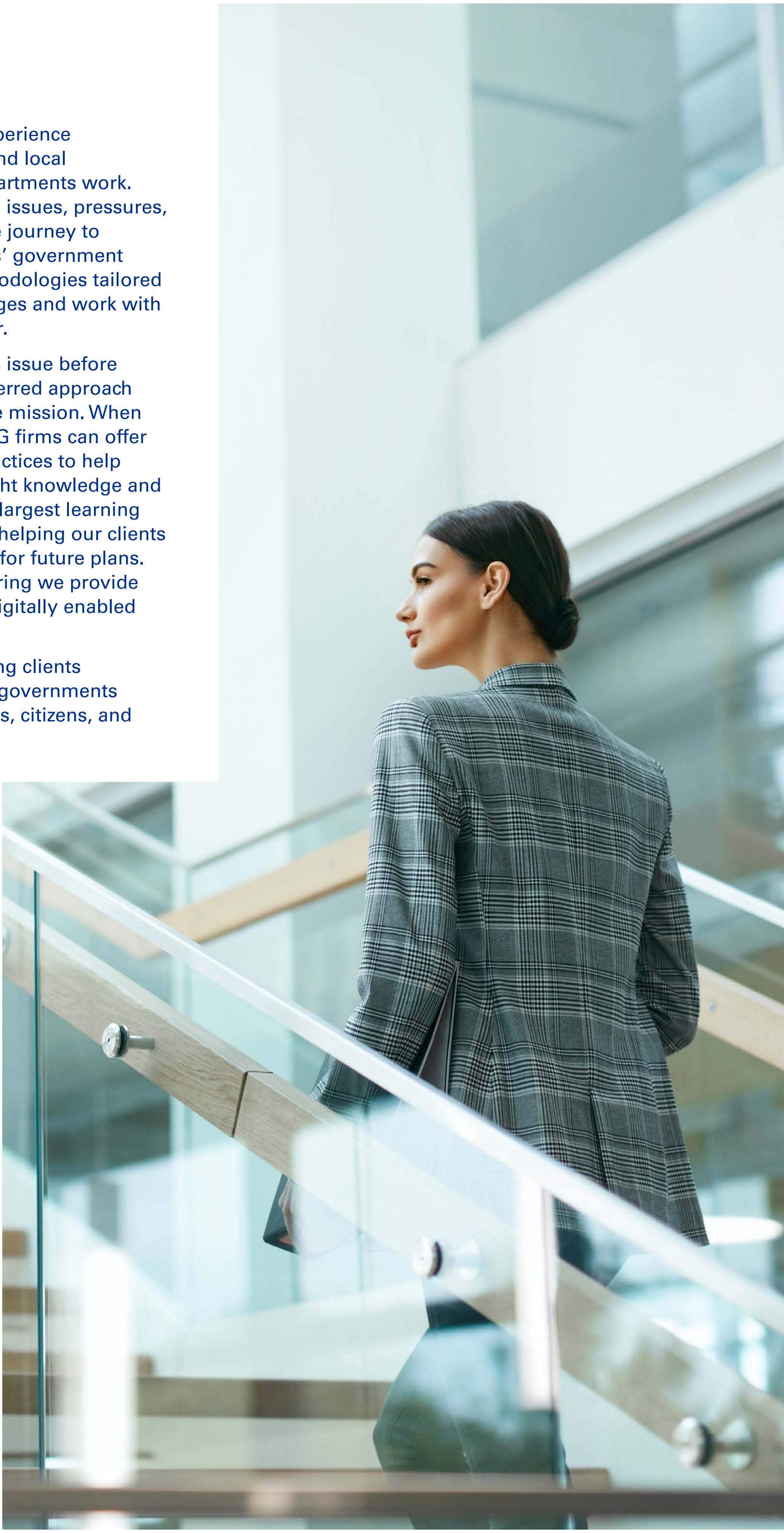
[9] Hayley P, Service Owner, Defence DevSecOps Service (D2S), LinkedIn.

About KPMG

KPMG firms have many years of experience of working with national, regional and local governments, so we know how departments work. KPMG professionals understand the issues, pressures, and challenges you encounter in the journey to modernise. Drawing on KPMG firms' government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you to deliver the results that matter.

KPMG teams start with the business issue before we help clients determine their preferred approach because we understand the ultimate mission. When the way people work changes, KPMG firms can offer client insight on leading training practices to help ensure your employees have the right knowledge and skills. KPMG in the UK is one of the largest learning providers in Europe, specialising in helping our clients build the skills and talent they need for future plans. With our Powered Government offering we provide a blueprint for a customer centric, digitally enabled public sector organisation.

KPMG firms are committed to helping clients create value, inspire trust, and help governments deliver better experiences to workers, citizens, and communities.



Contact

Nicholas Fox

Partner, Head of
Government (Justice)

KPMG in the UK

Laura Webb

Partner, Public Services
Technology Transformation

KPMG in the UK

Richard Krishnan

Partner, Technology and
Cyber Risk

KPMG in the UK

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

CREATE | CRT145789B | May 2023

Document Classification: KPMG Public