



Re-engineer digital experiences

Embed the resilience to evolve innovation

KPMG Smart Government

Catalyse digital progress

Insight Briefing



The question is not if, but when to consider security

Companies like Uber and Lyft operate with the goal to provide the ultimate digital experience. Users' experiences are seamless while locations, maps, credit cards, traffic, and other personal and private information moves at high speed. Common experiences we have every day inspire great ideas. They spawn citizen digital experiences where designers and developers focus on seamless functionality and convenience. Often security is an afterthought.

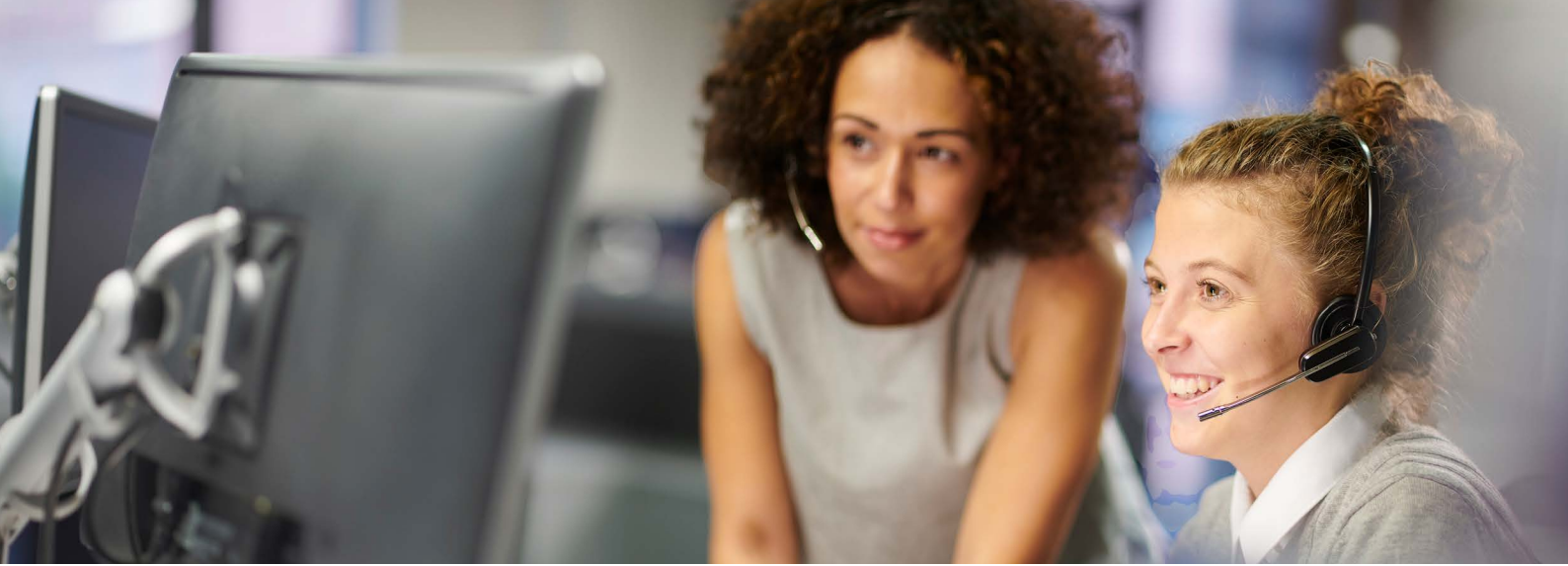
Securing the digital experience is not new. What's new and critically needed is to build security in from the first vision of the citizen digital experience. Security is traditionally a separate topic. One that many believe gets in the way of innovation. Some project teams prefer to address security later in the development process to avoid delays and additional cost. This article is intended to help government program managers as well as leaders who oversee technology, information, and security understand why it is vital to build security into the digital experience from the beginning, and recommended methods to start.



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.



Threats have changed

Government organisations experience positive momentum when adding digital capabilities. Since 2020, many also progressed in transforming their infrastructures, including adopting cloud services, to enable more digital services. Some are also learning how new and expanded data privacy risks and attack surfaces accompany these digital capabilities.

Cybersecurity, risk, and information technology professionals must understand how threats have changed since organisations accelerated digital

services adoption. Threats such as these require government organisations to expand and adopt new security approaches to protect vital assets that include citizen data and confidential records.

Government websites can present a significant vulnerability. 23 UK Ministerial department domains are among the 3,220 domains hosted on Gov.UK for several government councils, offices, assemblies, etc. The website observes an average traffic of 3.6 million visits a day¹. Many of these websites are outdated, which could cripple digital functions on which people depend. For example, there are some 122 public and private (contracted) sector, male, female and minor (under 18) prisons in the UK². If a hacker breaches a website, the operational impact would be huge. Officials could not track prisoners and attorneys and families would be unable to schedule visits. Once a website opens a door to a bad actor, networks, data, and systems are at risk.

How does an organisation confirm every website is secure? How do scarce workers efficiently comb through pages of code to identify vulnerabilities? Organisations rarely audit websites and they are often disconnected from back-end systems and data. These steps are easier with systems than websites, but the websites are part of the overall citizen experience.

Workers often consider security efforts drudge work. When team members view security as one of the most critical pieces of the citizen experience and the foundation of citizen trust, opinions will change and leaders will move more resources to security. It is cybersecurity that allows employees to make data-driven decisions with confidence, whether they are on site or remote, because they know bad actors have not manipulated the data. Security protects the digital experience as well as the entire organisation while also maintaining agility. Security enables the mission and does not slow down work like some believe. Also, organisations use some of the latest tools and technologies to boost security efforts.



Perimeters to protect no longer have boundaries. Work from home and other factors have created environments with no perimeters. Building resilience into the digital experience can avoid costly rework.



Data quickly moving to cloud environments. Adopting a cloud security shared responsibility model will help ensure rapid cloud adoption does not jeopardise security.



Dramatic increases in quantity and scope of cyber threats including phishing, ransomware, and via third-party software and tools. Understanding and building organisational security capabilities into the digital experience framework enables trust in the program.



Pervasive use of mobile apps and self-service technologies. Citizens prefer to interact with governments with mobile devices. While they enhance the digital experience, security must be at the forefront to build citizen trust.

¹ "List of .gov.uk domain names" Gov.UK.

² "Prisons data", data.justice.gov.uk

Governments are responsible for securing digital experiences

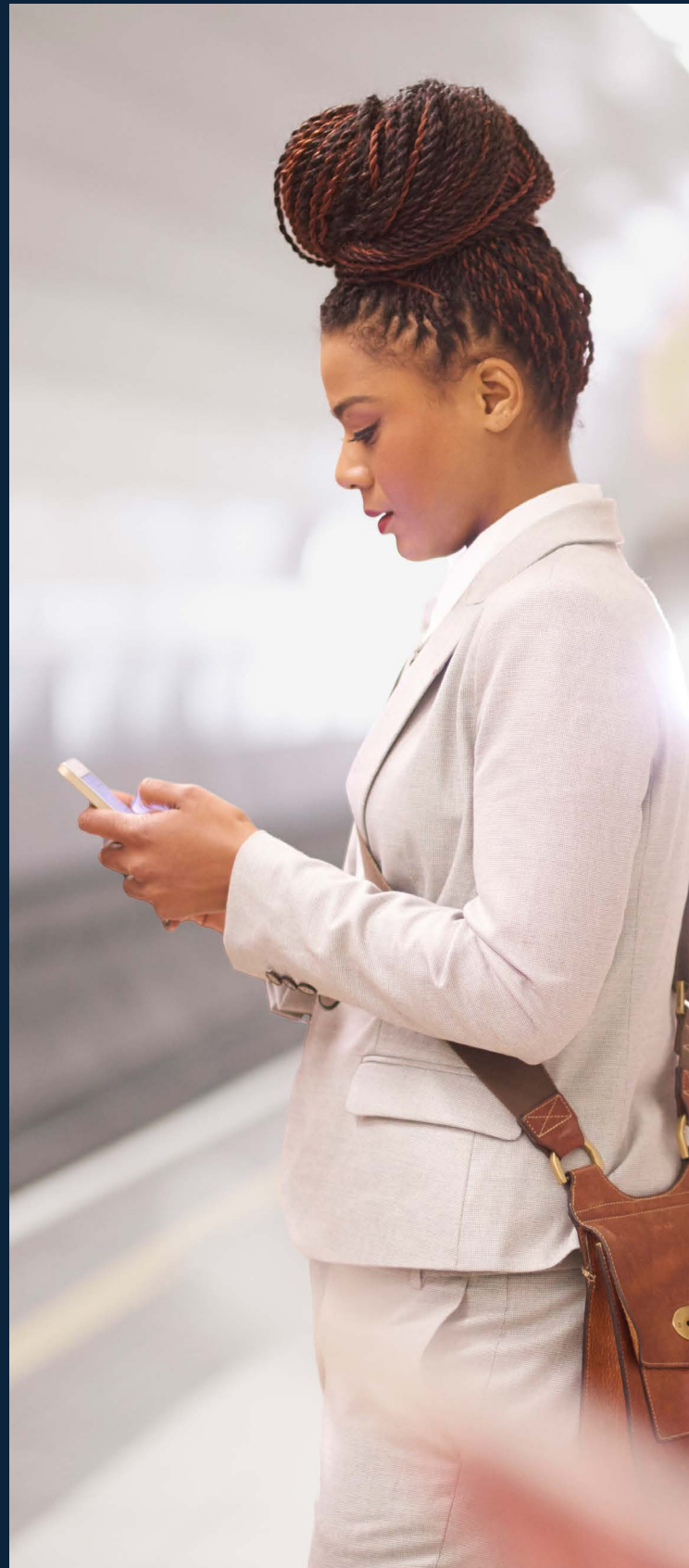
Citizens expect their digital experiences and their personally identifiable information are fully secure when they interact with central and local governments. 68% of UK citizens do not trust their government in terms of personal data management³. Government organisations are responsible for securing data in the cloud and across the entire digital experience to maintain citizens' trust.

Cloud-enabled technology plays a critical role in helping governments transform their infrastructures in ways that can help them operate more efficiently and provide new citizen-centric services. The recent rapid cloud services adoption highlights the need for a strategy to **secure cloud environments**. Everything moves faster in the cloud, so some governments struggle to involve security early. It also takes specialised skills to deploy data into the cloud so it is available only to those who need it and can be recovered if there is a problem.

We recommend **three actions to enhance cloud security**. While digital experiences vary from organisation to organisation, these steps apply to all organisations and can help ensure security is included from the start. First, regularly stress test possible incidents to prove the response plan works for cloud-based applications. Also, automate early stages of incident response procedures. Finally, collaborate with departments outside the security team to learn how threat actors think and ways to spot attacks early.

Based on KPMG firms experiences working with private and public sector organisations worldwide, the following considerations to enable secure digital experiences are also recommended.

Government organisations and their service providers share the responsibility for securing their cloud footprint. They should work closely together to define and understand who is responsible for which security functions. We call this process the **cloud security shared responsibility model**. While the model varies by provider and type of service, each government organisation should understand this model in order to secure its digital experience.⁴



³ "Most British people don't trust government with personal data," ComputerWeekly.com, Jan 7, 2021.

⁴ "Demystifying the Cloud Shared Responsibility Security Model," KPMG and Oracle, research conducted in partnership with ESG, 2020.

Shared responsibility security model

	On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
● Customer Responsibility	User Access/Identity	User Access/Identity	User Access/Identity	User Access/Identity
● Cloud Service Provider Responsibility	Data	Data	Data	Data
	Application	Application	Application	Application
	Guest OS	Guest OS	Guest OS	Guest OS
	Visualisation	Visualisation	Visualisation	Visualisation
	Network	Network	Network	Network
	Infrastructure	Infrastructure	Infrastructure	Infrastructure
	Physical	Physical	Physical	Physical

KPMG and Oracle, research conducted in association with ESG, 2020.

Practice a modern third-party risk management strategy, a cornerstone to securing the digital experience. As governments rely more on third parties to accelerate digital transformations, they need effective third-party risk management to evaluate and monitor risks before, during, and after contracts are in place. We recommend four steps. Start by defining or enhancing a third-party risk management program. Next, evaluate how continuous controls monitoring can align with program goals, and then identify continuous controls monitoring upfront. Finally, address third-party contractual security, operational requirements, and risk remediation.

Government organisations cannot expect citizens to always use secure devices in cyber safe areas. **Provide citizens an easy-to-use digital storefront secured with multi-factor authentication** to manage citizen digital identities.

In 2021, the UK government committed to invest over £2.6 billion over the next 3 years to build a resilient digital environment in the country.⁵ As governments make these investments, more jobs will require digital capabilities than ever before. Government organisations should identify the capabilities employees will need, **upskill or hire employees with digital capabilities**, and provide an employee value proposition that includes upskilling and career development.

Here are a few additional reminders to enable **secure digital experiences**. Provide employees with secure networks and devices along with training to use them in virtual work environments. Also, when designing citizen experiences, do not ask for **personal or private information** the organisation does not have to obtain. Finally, lawmakers will continue to introduce new and enforce existing **privacy and cybersecurity legislation**, so project teams also need to continue to follow regulatory requirements.

⁵ "UK Digital Strategy," Gov.uk, October 4, 2022.



Employees are the daily digital experience stewards

Government leaders are obligated to prepare their employees with policies and training and also hold every individual accountable to adhere to all policies. Leaders should make sure each employee understands and follows organisation information security policies to avoid intentional and unintentional insider threats. For example, they should know to never open unfamiliar emails that can lead to phishing schemes, use unapproved file transfer services that can open networks to hackers, or connect personal devices to work networks.

KPMG firms are helping governments navigate these new security challenges so they do not delay new digital capabilities that can improve the citizen experience. For example, KPMG professionals have developed a number of security chatbots for clients. These bots inform employees on what they need to do to maintain security. Building policies and manuals into chatbots or websites helps to create more streamlined and secure citizen experiences.

Security needs will multiply

Citizens' expectations will continue to grow. Public demand for easier experiences conducting business with the government — whenever and wherever they choose — is likely to also intensify. Government organisations have a unique responsibility to maintain citizen trust. Every government worker will play a role in meeting these multiplying expectations. Each can help enable the future's seamless, hyper-secure digital experience that includes a single sign-on platform for all citizen services. To meet this future state, governments must continue to improve the usability and reliability of critical digital services. Security needs will only expand in scope, intensity, and importance. Citizens will be satisfied when they trust these services, and cybersecurity is the foundation to building this trust.

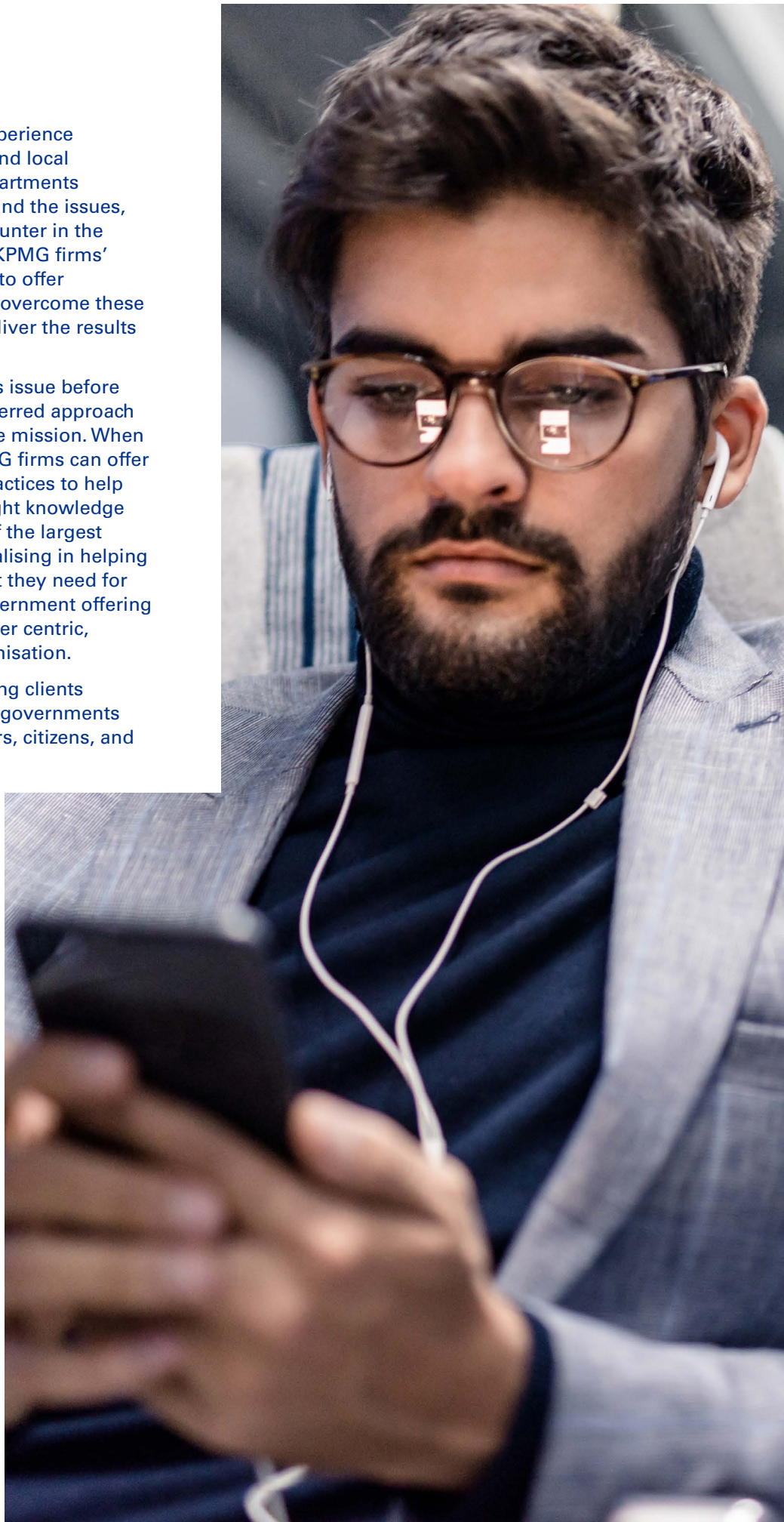
It will take time and many conversations for organisations to bring security into the digital experience at the right time. It is a needed change to develop many digital capabilities organisations must have to deliver their missions. KPMG professionals can help public sector clients navigate regulatory, security, trust, and compliance challenges. Let us help your government organisation provide innovative digital experiences that are thorough and secure.

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.

© 2023 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Public

CREATE | CRT145789B | May 2023