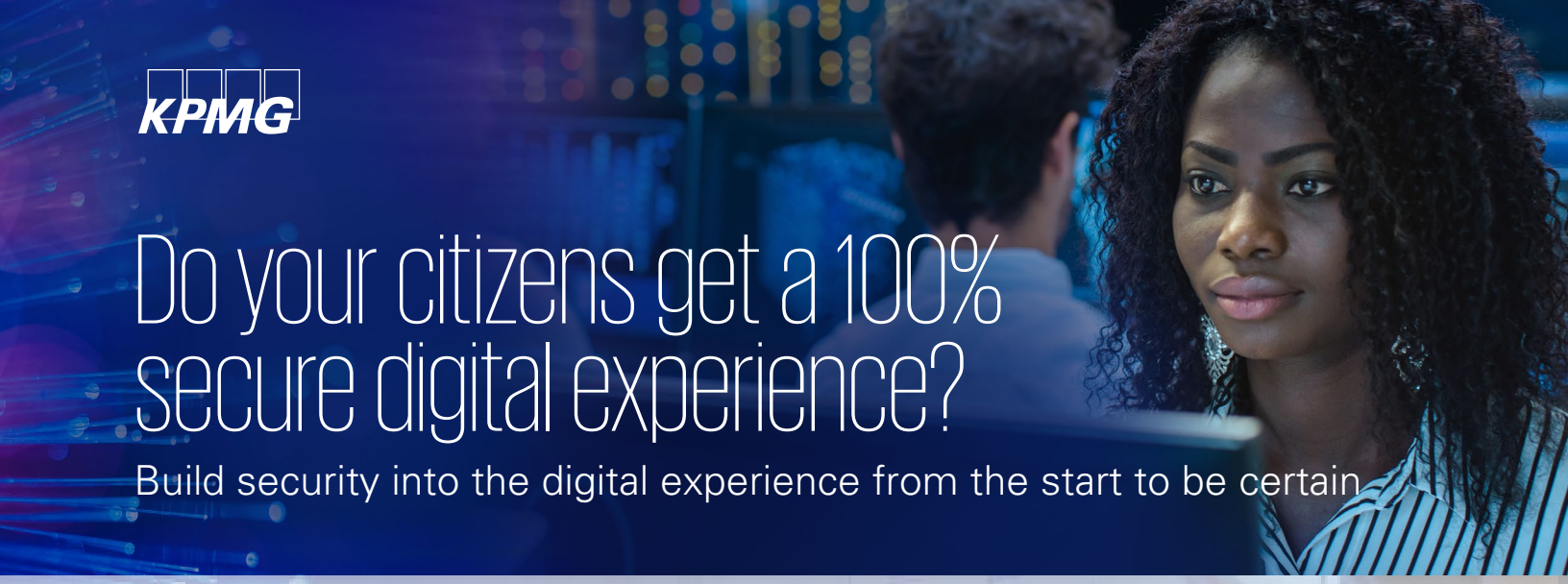


Do your citizens get a 100% secure digital experience?

Build security into the digital experience from the start to be certain

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 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.

Threats have changed

Government organizations have positive momentum 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 organizations accelerated digital services adoption. Threats such as these require government organizations to expand and adopt new security approaches to protect vital assets that include citizen data and confidential records.

- **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 jeopardize security.
- **Dramatic increases in quantity and scope of cyber threats including phishing, ransomware, and via third-party software and tools.** Understanding and building organizational 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.

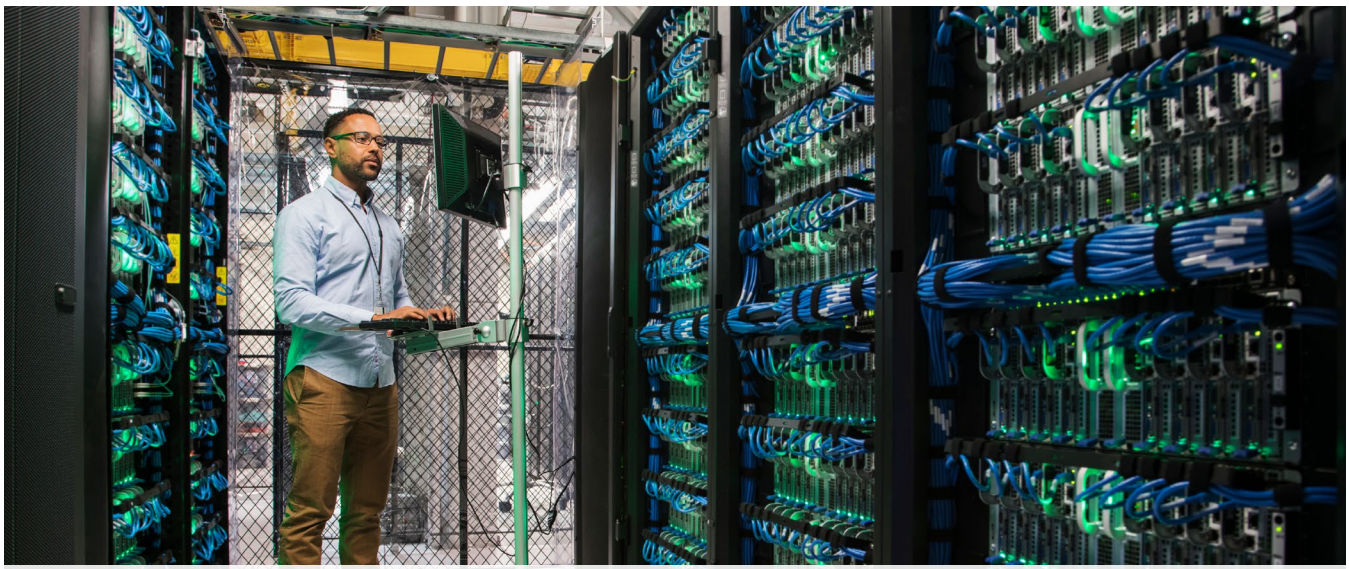
Government websites can present a significant vulnerability. Federal, state, and local organizations maintain approximately 7,600 .gov domains, including more than 1,450 for federal government.[1] Many of these websites are outdated, which could cripple digital functions on which people depend. For example, there are some 7,000 federal, state, and local prisons, correctional facilities, and jails.[2] 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 organization confirm every website is secure? How do scarce workers efficiently comb through pages of code to identify vulnerabilities? Organizations 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 organization while also maintaining agility. Security enables the mission and does not slow down work like some believe. Also, organizations use some of the latest tools and technologies to boost security efforts.

[1] "Data," dotgov.gov, July 16, 2021.

[2] Wendy Sawyer and Peter Wagner, "Mass Incarceration: The Whole Pie 2020," PrisonPolicy.org, March 24, 2020.



Governments are responsible for securing digital experiences

Citizens expect their digital experiences and their personally identifiable information are fully secure when they interact with federal, state, and local governments. A 2021 study found 64 percent of Americans do not trust federal agencies with their personal information.[3] Government organizations 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 specialized 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 organization to organization, these steps apply to all organizations and will 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.

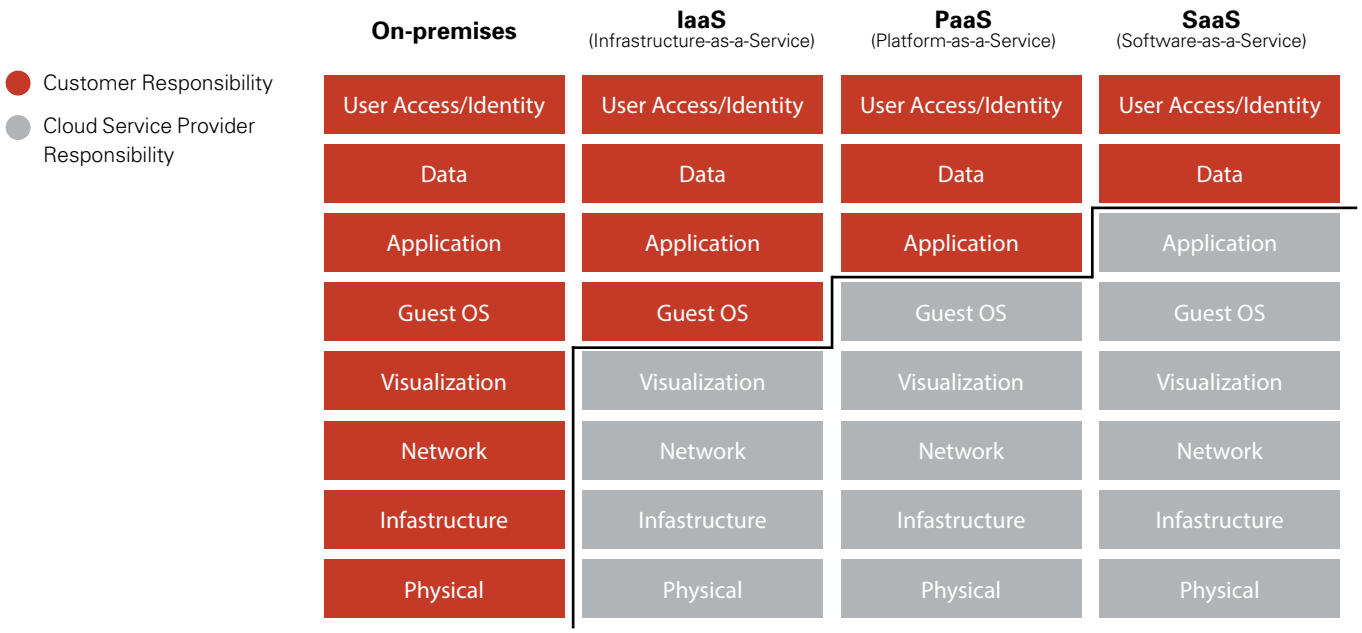
Based on our experience working with private and public sector organizations worldwide, we also recommend the following considerations to enable secure digital experiences.

Government organizations and their service providers share the responsibility for securing their cloud footprint. They must 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 organization should understand this model in order to secure its digital experience.[4]

[3] "How privacy-enhancing technologies can ease customers' confidentiality concerns," PYMNTS.com, June 17, 2021.

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

Shared responsibility security model



KPMG and Oracle, research conducted in partnership 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. Learn more about third-party risk management.

Government organizations 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. Read more on citizen experience in our series of articles.

Estimates say organizations will invest more than $7 trillion in making work more digital by 2023.[5] As governments make these investments, more jobs will require digital capabilities than ever before. Government organizations 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. Read more about building a workforce for the accelerating digital era.

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 organization does not have to obtain. Finally, U.S. and state 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] "How privacy-enhancing technologies can ease customers' confidentiality concerns," PYMNTS.com June 17, 2021.

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 organization 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 is helping governments navigate these new security challenges so they do not delay new digital capabilities that can improve the citizen experience. For example, KPMG has 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 creates more streamlined and secure citizen experiences.

Security needs will multiply

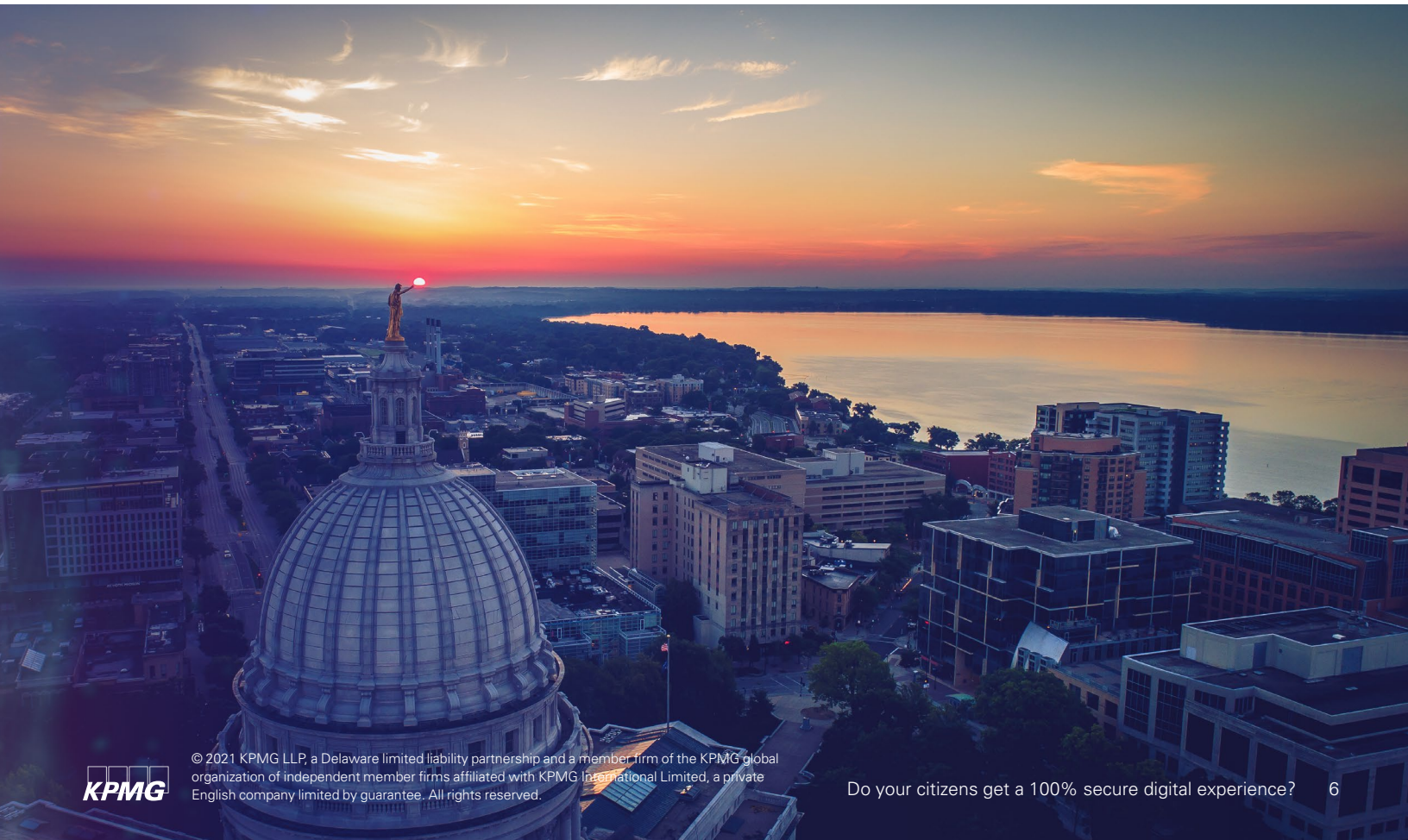
Citizens' expectations will continue to grow. Public demand for easier experiences conducting business with the government—whenever and wherever they choose—will also intensify. Government organizations have a unique responsibility to maintain citizen trust. Every government worker will play a role in meeting these multiplying expectations. Each will 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 organizations to bring security into the digital experience at the right time. It is a needed change to develop many digital capabilities organizations must have to deliver their missions. KPMG professionals help public sector clients navigate regulatory, security, trust, and compliance challenges. Let us help your government organization provide innovative digital experiences that are thorough and secure.

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.



Contact us

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

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