okta

# How Cloud Identity Can Reduce Costs, Improve Collaboration and Drive Digital Transformation in the UK Public Sector

## Introduction

The UK government describes itself as “one of the most digitally advanced in the world.” In its continuing efforts to transform internal and externally facing services, a long-awaited strategy for the Government Digital Service (GDS) was unveiled in February 2017. Its ambitious goal is to use a £450 million budget to save £3.5 billion by the end of 2020, whilst continuously improving and accelerating the delivery of services for civil servants, citizens and government partners.

The GDS is leading this new Government Transformation Strategy. It will seek to:

- Work with the rest of government to make public services simpler and better
- Ensure government data is good data, and more usable for all
- Enable departments to make better-informed decisions when purchasing technology
- Help departments provide their staff with valuable technologies that serve as tools, rather than barriers
- Build platforms like GOV.UK Verify—a way to confirm that users are who they say they are

Identity is therefore at the centre of the new Government Transformation Strategy, which seeks to improve interoperability and collaboration inside a vast and often siloed public sector. To this end, the government wants to have 25 million users of its GOV.UK Verify service onboard by 2020. It also wants to extend the service out to the commercial sector, banks and local authorities in another sign of the scale and ambition of its digital transformation strategy.

Yet there are challenges: complex, heterogeneous legacy infrastructure running alongside newer cloud and app-based platforms; cost pressures; cybersecurity risk; regulatory compliance; and the difficulty of integration with potentially thousands of applications running outside core systems.

Only Identity as a Service (IDaaS) has the blend of capabilities needed to support and secure government digital transformation efforts. With the right provider, public sector organisations will be able to deliver better services, more efficiently whilst keeping key data and systems safe and secure.

### Government digital challenges

The UK government needs to connect its citizens to both legacy and next-generation digital services, to connect civil servants to each other and the right resources, and to do all of this securely. With this in mind, here are just some of the challenges facing its digital transformation efforts:

**Costs:** Finding the necessary funding to start a new project is always a challenge — one made even more intense in an age of austerity, and with significant sums of public funding also being diverted to Brexit. This is where more efficient digital technologies can help; reducing the long-term costs associated with manual processes while helping to make employees more productive.

**Shorter time frames:** Public sector budgets are tied to political cycles, meaning new projects must show results quickly for stakeholders.

**Legacy infrastructure:** Many public sector organisations operate a range of outdated systems that need replacing with newer, more efficient digital technologies.

**Disparate teams:** As of March 2017 there were over 5.4 million employees in the public sector, with almost

three million in central government. Due to legacy technologies and dispersed teams, many of these employees find it difficult to collaborate across different platforms.

**Compliance:** Government data is, of course, highly sensitive and regulated. Any personally identifiable information (PII) on citizens or employees is regulated by the forthcoming EU General Data Protection Regulation (GDPR), which mandates it is secured with "state-of-the-art" technologies. That will require up-to-date, best practice approaches to identity management.

**Security:** The government's National Cyber Security Centre (NCSC) dealt with over 1,100 cyber-attacks in just its first year of operation. Some 590 were classed as "significant" and more than 30 serious enough to require a cross-government response. Highlighting the escalating threat level, UK parliament online account holders, including dozens of MPs and their staff, were targeted with a brute force email attack in 2017 since blamed on Iranian state hackers.

While the risk from financially motivated cybercriminals and nation state hackers remains very real, there is arguably an even bigger threat closer to home, from government employees themselves. Local government data breach incidents reported to privacy watchdog the Information Commissioner's Office (ICO) jumped by 29% from Q2 2016/17 to Q2 2017/18. Previous studies have suggested that most incidents the ICO deals with are caused by human error.

The challenges associated with identity assurance will only increase as more public sector services migrate to the cloud. It can lead to users being forced to remember multiple, complex passwords for each service, impairing the user experience and opening new security challenges. Put simply, as access processes become more complex, some users will ignore policy and put security at risk by putting passwords on Post-Its or avoiding logging out altogether. Others may take up valuable helpdesk time with endless password reset requests.

## The value of IAM

Identity and access management (IAM) supports organisations migrating to newer digital models: helping IT managers understand who is accessing each service and independently authenticate them. Three-quarters of IT leaders say IAM addresses the top challenges of security, legacy infrastructure, and high availability of infrastructure. That report also pointed to three top initiatives which depend heavily on IAM:

- Introducing new experiences for the end customer/citizen
- Improving the employee experience and partner/employee collaboration
- Effectively migrating core systems (email, HR, ERP, etc.)

However, while such tools are essential to the success of the Government Transformation Strategy, it's important to remember that not all IAM is created equal.

## IDaaS vs. on-premises

Legacy IAM doesn't fit well with the kinds of new, cloud and mobile-driven infrastructure government agencies are increasingly migrating to. It takes significant time and resources to integrate, and even then will be a constant barrier to continuous improvement. New connectors must be built at great expense each time a new cloud app is added—with the result being more maintenance and potential downtime.

Identity-as-a-service (IDaaS), on the other hand, introduces a wide range of benefits designed to support the goals of the Government Transformation Strategy whilst enhancing security and decreasing costs. It's highly scalable, reliable and easy to set-up as you're effectively outsourcing IAM to a trusted third-party expert. It secures access at the cloud app layer rather than the network perimeter and offers visibility into all your apps, users and devices from a single interface. What's more, new apps can be added and managed with ease, and no unnecessary downtime.

Here's a quick rundown of those benefits:

## Case study

The Okta Identity Cloud is already helping one UK City Council's journey to the cloud as it looks to better manage huge budget pressures. The local authority and its 1,400 employees help to provide everything from bin collections to housing benefit and local education services for over 180,000 residents. However, identity management was always a challenge for the council,

with passwords scrawled on Post-It notes a common sight hiding under users' mouse pads.

With Okta's Single Sign-On (SSO), users no longer need to remember individual passwords for each of the multiple systems they need to access. It's made staff more productive as they don't need to log-in separately for each application, and more secure as there's no need to write passwords down: instead, users access any cloud services with just one username, one password and one session. It's also freed up the council's IT staff to focus on adding value to the organisation in more strategic ways.

## Supporting government digital transformation

The Okta Identity Cloud is built with the needs of public sector digital transformation in mind. It enables the deployment of multiple cloud services, reducing security and compliance risks in the process. It supports legacy and cloud-based applications, generating enhanced ROI. What's more, it's available as a single-tenant hosted service for maximum flexibility and security, and can run from UK data centres to meet strict GDPR and other regulatory compliance requirements.

In short, it offers:

**IT cost reduction:** Delivered 100% as a service, Okta eliminates the unnecessary maintenance, operations and security costs of on-premises IAM.

**Fast and secure inter-agency collaboration:** Okta makes it easy to manage access for external collaborators to any resource: on-premises or in the cloud. Whether you need to connect to an entire agency or an individual, Okta offers flexible secure options that make collaboration easy and scalable.

**Accelerates digital transformation:** Speeds up digital initiatives by setting up identity once and for all. Okta is designed to connect any employee, vendor, partner, or citizen to anything with security that doesn't sacrifice ease-of-use, and fits perfectly with the tools you already have in place.

**Secure and convenient citizen access to government services:** Online self-service helps government run more efficiently.