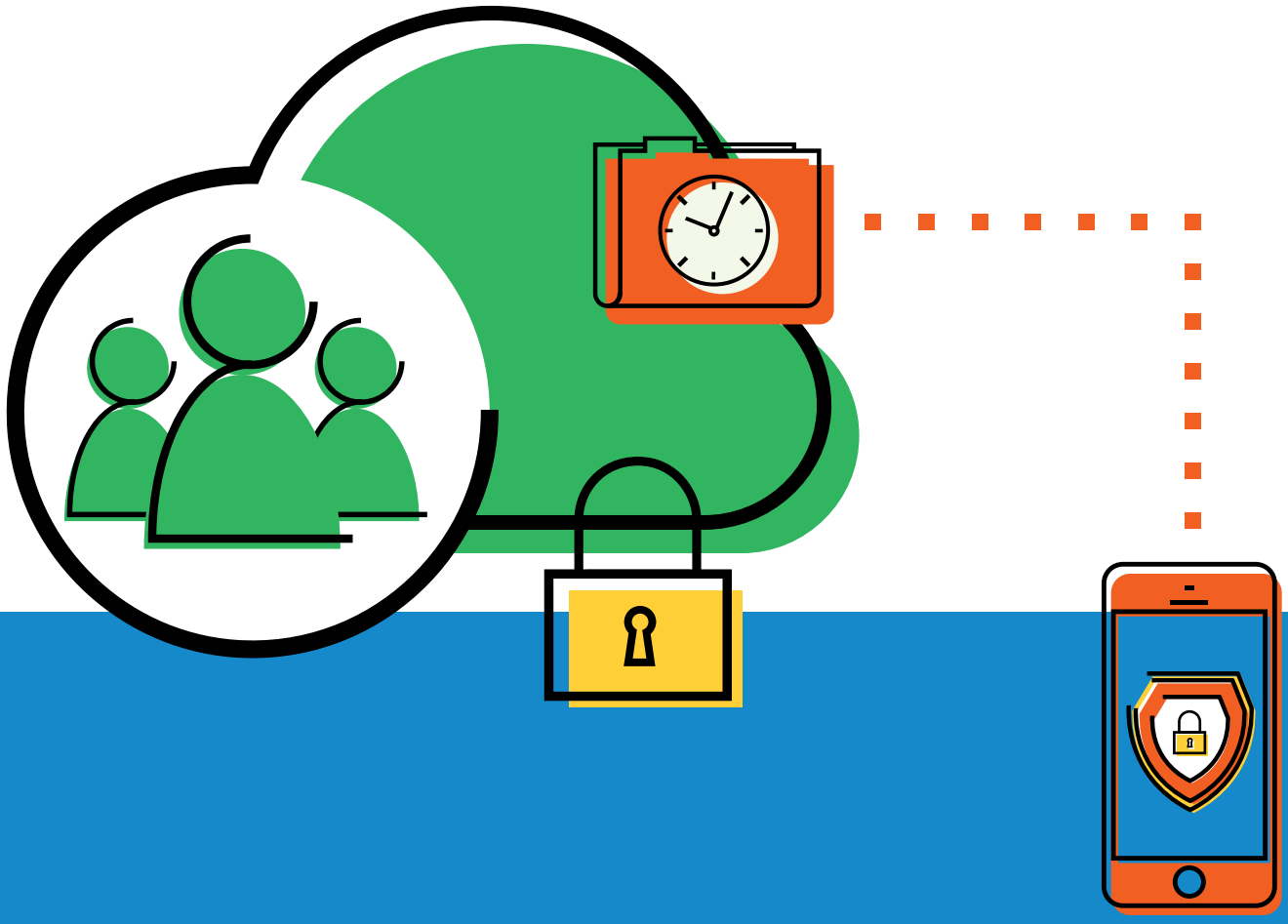


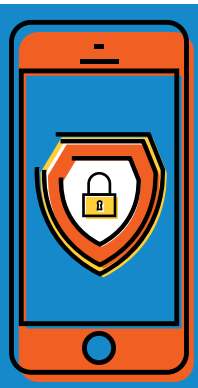
Meeting the digital challenge:

How well is the public sector embracing cloud computing?

huddle™

Meeting the digital challenge:

How well is the public sector embracing cloud computing?



One of the largest and most comprehensive surveys of its kind, with data from 5,000 public sector employees, spanning central and local government, and the NHS.

Executive Summary

Fundamental change is afoot in the way public sector professionals in central government, local government and the NHS do their jobs. Collaboration is the watch-word, and cloud technology has emerged as the critical enabling platform – though usage remains limited.

The cost benefits of moving to cloud computing has dominated much of the recent discussion around public sector IT. Yes, there are undoubtedly huge savings to be made in an era of budget cuts. But this austerity narrative obscures the transformative role that cloud platforms can have in driving more efficient, more effective public sector working practices. This narrative must change if the potential of cloud computing is to be realised.

To understand how public sector executives and IT leaders can help their organisations to embrace the cloud and evolve the way they work, Huddle commissioned Dods to understand:

1. **How public sector employees are adapting to changing ways of working**
2. **How a major perceived barrier, data security, is viewed and handled in the public sector**
3. **How public sector staff are approaching related government-mandated commitments**

One of the largest surveys ever undertaken in this area – more than 5,000 government and health professionals participated – reveals that the public sector is at an early stage in a long journey.

Particularly striking is that just 35% of public sector employees are confident using cloud IT. Of perhaps more concern is that only a little over half of staff in IT departments are self-assured using cloud platforms – and a quarter claim not to have used one at all. This is a major impediment to effectively implementing many of the government's service evolution programmes.

Part of a larger study "Meeting the digital challenge: How well is the public sector embracing cloud computing?" which collected data from 5,000 public sector employees, spanning central and local government, and the NHS.

The reasons for this uncertainty emanates from fears surrounding security, time and effort to move to cloud platforms and lack of expertise to implement them. More than half of public sector staff felt their organisations could not see the benefit in cloud computing. But the research also suggests that 95% of UK public sector staff share and work on information with external organisations. If this external data collaboration is not taking place via secure cloud platforms, then insecure and inefficient approaches are filling the void.

Perhaps the headline finding of this research is an almost 'Jekyll and Hyde' approach to the concept of data security, and the actual treatment of confidential data in practice. 9 in 10 public sector employees felt the security of their organisation's data was important or very important. But 63% of public sector employees are unaware of the government's April 2014 security classification system, or didn't believe it relevant to their organisation.

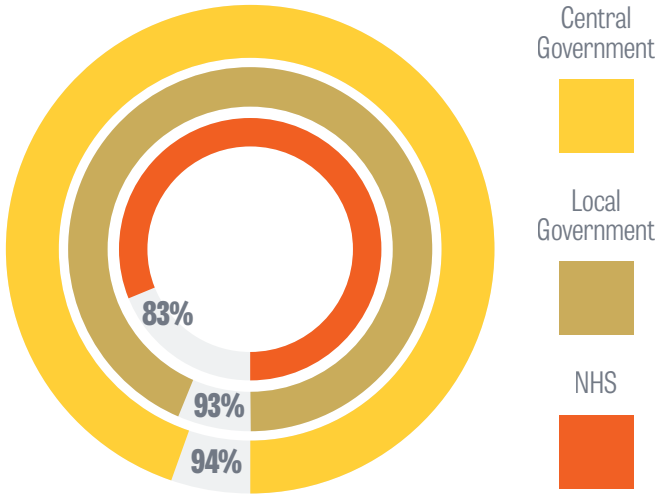
"63% of public sector employees are unaware of the government's April 2014 security classification system, or didn't believe it relevant to their organisation."

At a time when public sector staff are being asked to work efficiently, collaboratively and cross-functionally, the way in which information is routinely shared would astonish private sector employees. Two particularly unexpected data sharing behaviours stood out: 43% of public sector employees rely on hard copies sent through the post and 27% courier documents to third parties. The time delay, the cost and the potential for security breaches are astounding.

The ambitious G-cloud procurement initiative has been under fire from various quarters for some time. While there has been some phenomenal progress in getting the process up and running, there is still work to do. Only 50% of public sector IT staff have a working knowledge of the framework, but usage is much lower. 22% of central government IT departments have procured via G-cloud, but this tumbles to 12% and 5% in local government and NHS IT departments respectively.

Another key government initiative was to shift 25% of government spend to SMEs by the end of the last parliament. While the Cabinet Office announced its success in February 2015, there are clear challenges facing SMEs in working with the public sector. Employees surveyed assumed procurement processes were too time-consuming and costly for SMEs, and concerns around security were also described as barriers to working with SMEs more frequently.

Percentage of employees that agree that the security of their organisation's information is important or very important.



However, there is an important opportunity for UK SMEs looking to work with central government, local government and NHS organisations, as 64% of public sector employees (71% within IT departments) would feel more comfortable if sensitive data was stored on British soil. 63% of IT department employees prefer UK cloud vendors.

How should public sector executives and IT leaders react to these findings? This paper proposes three points of action to help foster widespread use of cloud platforms and drive forward new ways of working in the public sector:

1. **Build awareness and confidence in cloud computing by:**
   a. demonstrating the value of cloud platforms in context & only migrating when appropriate IT infrastructure, connectivity and devices are in place
   b. emphasising UK data residency in choice and communication of cloud platform
   c. addressing the issue of 'protectionism' by IT departments in pushing back against cloud migration, maintaining inefficient, inflexible and unsecure practices

2. Get to grips with the government's new security classification system quickly:

a. accept it represents a major cultural change, with interpretation and application of guidelines resting on SIROs

b. when considering certification of commercial cloud platforms, understand how the former Impact Level system maps to the new system

c. while the UK government does not offer formal security certification for cloud platforms, consider turning to the 'gold standard' – the US government's 'FedRAMP' certification

3. Embrace G-cloud within your organisations and help employees understand the drivers for working with SMEs

"64% of public sector employees would feel more comfortable if sensitive data was stored on British soil."

A rather negative narrative has emerged around the evolution of public sector working practices. The conclusions of this research are much more positive. Cloud computing platforms are an enabler of massive, supportive cultural change and their introduction will take some time and effort. Information security is complicated, but certified commercial platforms can make a pragmatic contribution for Senior Information Risk Owners (SIROs). Finally digital government, and the more efficient, more effective public sector working practices it promises, is not 'at risk' - it is a racing certainty. Every day the UK government's ambitious goal becomes that bit more achievable, supported by a gradual migration to cloud ICT platforms.

Introduction: Public Sector Service Evolution & Cloud ICT

The UK public sector is undergoing a dramatic evolution. Drives for efficiency and service improvement are changing the way in which public sector professionals work. One primary driver is better use of skills and resources - in a word, the public sector must work more collaboratively. But how prepared are they for this change?

Major government initiatives and policies abound: 'Digital Transformation', 'Digital by Default' and 'Cloud First' to name but a few. It could not be clearer. New ways of working mean more collaboration, which in turn demands new, enabling digital platforms. And because at the heart of collaboration is access to data anywhere and at any time, these have to be delivered via the cloud.

Public discussion has focused predominantly on how cloud ICT adoption will impact public sector IT costs. The government champions savings, efficiencies and a move away from "dependence on an oligopoly of large suppliers and lock-ins to long contracts". But this ignores the more fundamental, transformative effect that cloud ICT will have on how the UK public sector works collaboratively, day in, day out.

As Francis Maude, then Minister for the Cabinet Office, said in May 2013: "The Cloud First policy will embed the skills a modern civil service needs to meet the demands of 21st-century digital government and help us get ahead in the global race."

Further policies address continuous improvement methods and how interdepartmental and external collaboration – enabled by technology - can:

- **Assist mutual learning and upskilling**
- **Integrate the best skills and talents the public sector has on various key projects**
- **Reduce reliance on costly external consultants**

The 'Digital Government' discussion needs to shift away from technology-led cost arguments, towards how collaboration can be achieved in practice. Important issues of change management, information security and employee buy-in must be addressed.

To support this, Huddle – the leading cloud collaboration platform used by 85% of central government departments – worked with Dods Research to undertake one of the largest and most comprehensive surveys of its kind.

More than 5,000 public sector employees including central government (1,529), local government (1,222), and NHS (2,148), from all types of roles and levels – from clinicians to administrators, managers to Chief Executives (including more than 400 staff within IT departments) – were polled. The answers have generated deep insights across three key, core issues:

1. **How public sector employees are adapting to changing ways of working**
2. **How data security is viewed and handled in the public sector**
3. **How public sector staff are approaching government-mandated commitments**

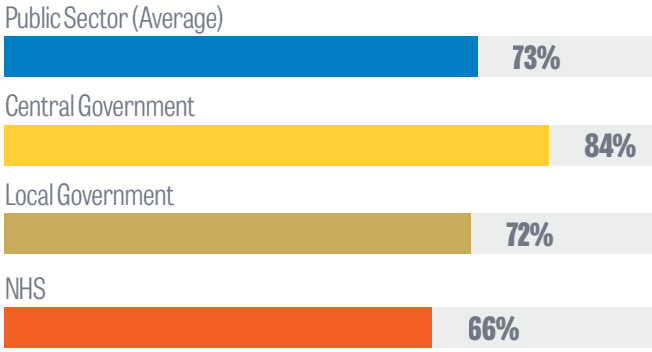
These insights are presented with overall public sector and specific central government, local government and NHS treatments. Based on these findings and government ambitions, action plans are presented for public sector leaders.

Helping public sector staff adapt to changing ways of working

Public Sector Overview

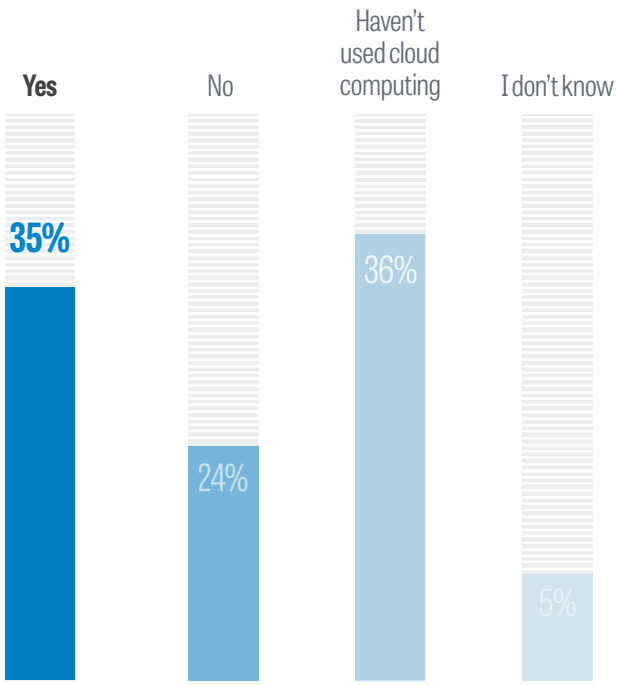
Awareness of, and confidence using, cloud computing is a strong barometer of adaptation to the concept and practice of new ways of collaborative working. In general, 73% of public sector employees are aware of cloud ICT in some capacity, though there is quite a gulf between central government (84%) and NHS (66%) staff. However, what is of very real concern is levels of confidence.

Cloud Awareness in the Public Sector

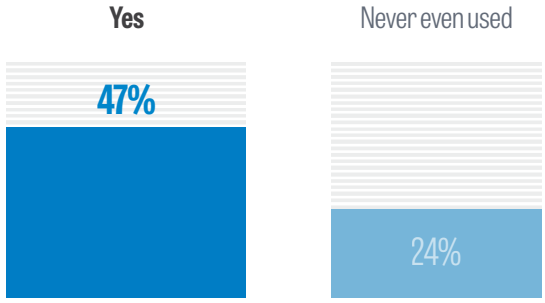


Across the UK public sector, just 35% of staff say they are confident in their own ability to use cloud computing. An almost equal number (36%) say they haven't used cloud computing before and nearly a quarter (24%) said they lacked confidence to use cloud computing. Even more worrying is the view from IT department employees. While 47% do feel confident using cloud ICT, nearly a quarter said they had never even used cloud computing services.

Confidence using cloud computing in the Public Sector



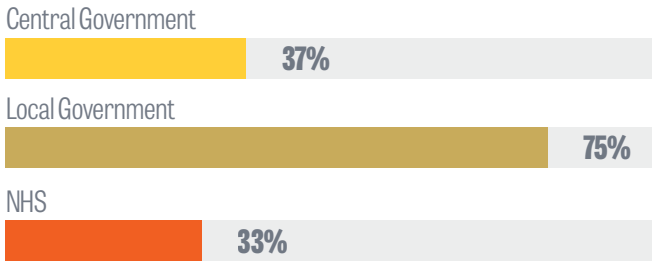
Confidence using cloud computing in the Public Sector, IT department



Cloud ICT is the major technological underpinning of much of the public sector's targeted new ways of working. That confidence in using cloud systems and platforms is so low suggests real problems in effectively implementing many of the government's service evolution programmes. To understand why this is the case, the survey probed perceived organisational barriers to cloud computing.

"82% felt that their organisation lacked the expertise to implement cloud platforms."

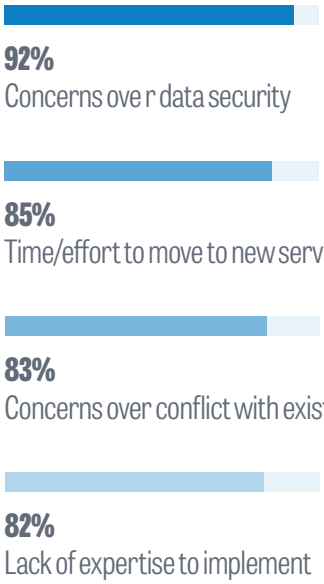
Confidence using cloud computing



The single biggest barrier is data security concerns (92%), followed by concerns around the amount of time and effort it will take to move to new services (85%), worries of conflict with existing technology (83%) and a feeling that their organisation lacks the expertise to implement cloud platforms (82%). It would appear that generally accepted messages regarding strong cloud security, ease of use, integration and implementation have not resonated in the public sector. Perhaps worse, 52% of public sector staff believe their organisations just can't see the benefit of cloud computing.

What's preventing adoption?

Poor security understanding is holding back adoption.



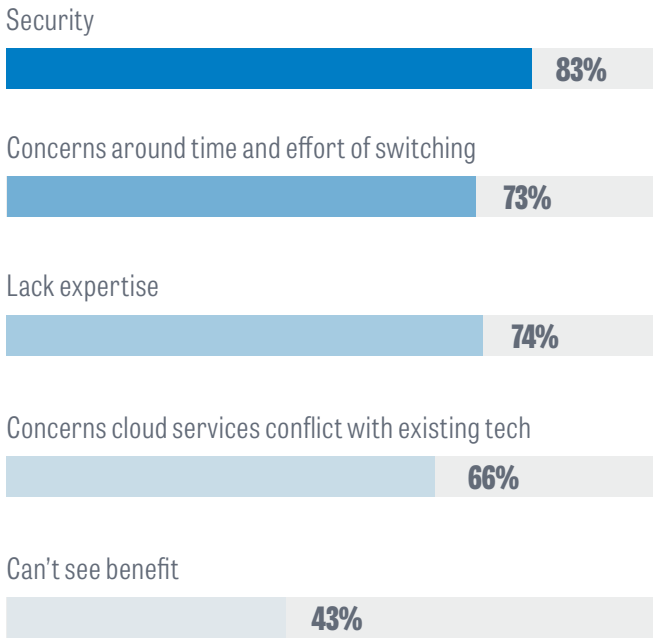
According to Forrester, 86% of knowledge workers regularly collaborate with customers or external partners. This Dods Research suggests 95% of UK public sector staff share and work on information with other organisations. Lack of confidence in cloud ICT and the number of perceived barriers should be keeping public sector executives and IT departments awake at night. If collaboration is not taking place via secure cloud platforms, then insecure and inefficient approaches are filling the void. Cloud computing can help the public sector make huge efficiency gains to existing processes. It can help deliver the financial savings which will undoubtedly will required by the upcoming Emergency Budget.

Central Government

Of all public sector staff polled, central government employees are the most likely to be aware of, and be confident using, cloud computing services. But while awareness is high among (84%), confidence in using cloud computing services is low, at 37%.

But where does this lack of confidence originate? The three main barriers to central government organisations using cloud computing services are concerns over security (83%), lack of expertise in implementing cloud computing (74%) and concerns surrounding perceived time and effort required to shift to cloud services (73%). This will make difficult reading for proponents of cloud ICT – its clear security, ease of implementation and ease of use messages are falling on stony ground.

Five barriers to using cloud ICT in Central Government (% agree)



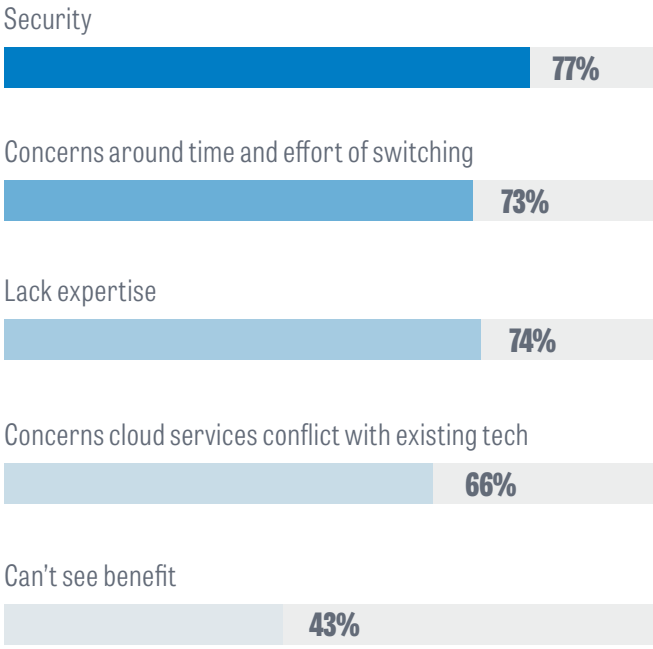
Why is this lack of adaptation a problem? With only 7% of central government employees in roles that do not require them to share information with other organisations or departments in their day-to-day roles, it's clear that many inefficient and insecure methods of collaboration are widely practiced instead.

Local Government

Approximately three quarters of local government staff are comfortable with the term 'cloud computing'. However, their level of confidence using cloud ICT is relatively low –61% either lack confidence using cloud services, or have never knowingly used them.

Confidence in new systems and technologies is bred by trust, and it's clear that local government staff see three major problems with cloud computing. Concerns over security top the list (77%). This is swiftly followed by concerns over the time and effort it might take to switch to using cloud services. Local government employees also worry that cloud services will conflict with existing core technologies (65%). This is a real challenge to IT staff and vendors advocating evolving to cloud services to support new ways of working.

Five barriers to using cloud ICT in Local Government (% agree)



"Local government employees are more likely than their central government peers to share data via the physical postal services."

With 97% of local government workers claiming to share data with other organisations during the execution of their jobs, it's easy to appreciate just what a big problem this lack of faith in cloud computing will have in the future. Local government employees are more likely than their public sector peers to share data via email and physical post – creating the potential for avoidable security risks and efficiency problems.

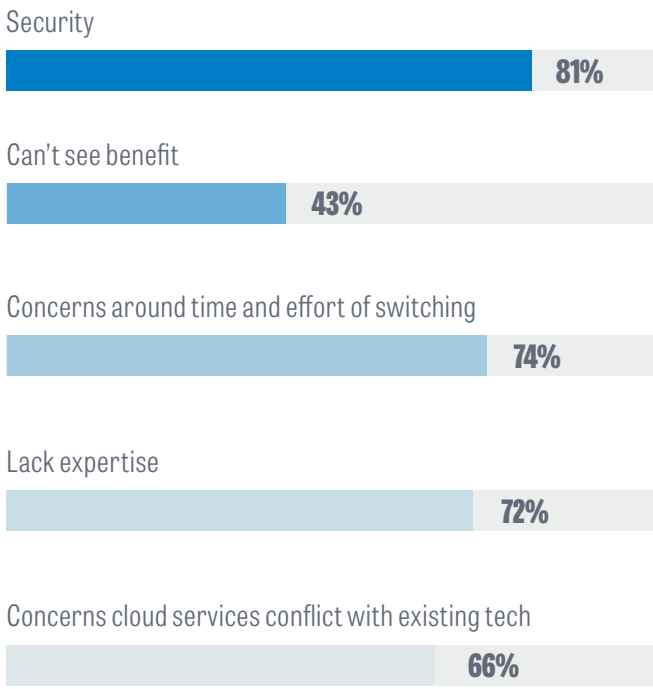
NHS

Throughout the public sector, NHS employees are least likely to be aware of cloud computing – just 66% of NHS staff polled were conscious of the cloud against an average of 73%. Confidence is also low – with just a third claiming comfort with using cloud services and 63% have either not used them or do not feel confident.

The major barriers to NHS organisations embracing cloud services and adapting to new ways of working broadly echo those of other public services. Security concerns top the list for 81% of NHS staff, issues around time and effort of switching are a turn-off for 74% and lack of expertise presents a barrier to 72% of those polled. Cloud experts will be frustrated to see that – in the most security-conscious segment of our public sector – some of the key benefits of cloud computing are failing to register.

The impact of this lack of awareness and confidence in cloud computing is potentially significant. What will make for particularly worrying reading for public sector IT chiefs is that 96% of NHS employees share information amongst internal and external teams as part of their work. A workforce with a high awareness of and confidence in using secure cloud services would find their work easier and more efficient, and better safeguard patient confidentiality, whilst providing a fully transparent and auditable record of activity.

Five barriers to using cloud ICT in NHS (% agree)



Tackling inconsistencies in public sector data security

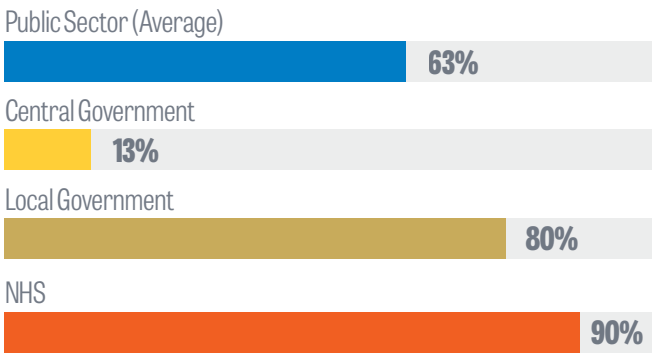
Public Sector Overview

90% of public sector employees have strong feelings that the security of their organisation's information is important or very important (94% central government, 83% local government and 93% NHS). But there are huge differences in how the government's security classification system – launched in April 2014 – has been received and adopted.

63% said they didn't know (or that they question wasn't relevant) if their organisation had adopted the government's new security classification system.

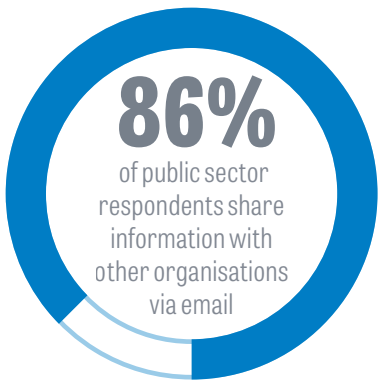
When asked if their organisations had adopted the government's new security classification system, 63% said they didn't know or that they question wasn't relevant to their organisation. But this public sector average is highly misleading and masks a significant issue: the system is only really being used by central government and a select group of other organisations. 84% of central government employees use the security classification, but this falls to 12% in local government and a tiny 2.5% in the NHS.

Unaware of or don't see relevance of security classification system



This suggests some major inconsistencies in the public sector's approach to data security, and these are brought into sharp relief by current information sharing practice. In a world where public sector staff are being driven to work efficiently, collaboratively and cross-functionally there are some surprising data sharing behaviours.

That 86% of public sector respondents share information with other organisations via email was not one of those surprises – though this does open up concerns over the security of email and the efficiency



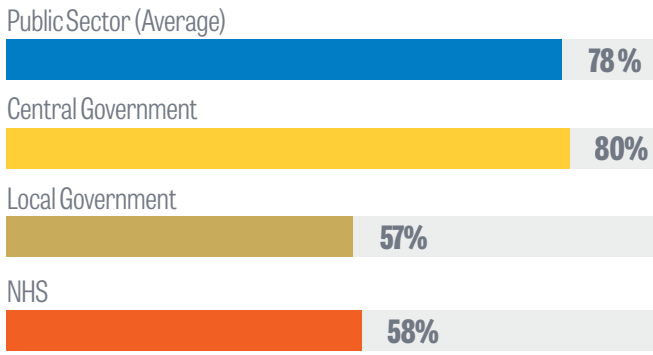
of such practice. But it's the continued use of the post and couriers to share hard copy documents at a time when 'digital government' is a major policy driver that is most staggering.

"43% of public sector respondents rely on the post to collaborate on documents."

In 2015, 43% of public sector respondents rely on the post to collaborate on documents, rising to 48% in local government. 27% use couriers to share data, rising to 32% in central government. If one ignores the blatant security and inefficiency risks here, the costs of using couriers to share information as part of a collaborative working effort is deeply disturbing. Whilst couriers used to present the only viable option for quick document exchanges and sharing, the advent of cloud computing and collaboration software means couriers are by far a slower route.

Another aspect of data security lies in IT vendor self-certification – where suppliers effectively give assurances as to the security of their services, without independent, third party validation. This is a reasonably technical question, so the survey focused on respondents working within public sector IT departments. It found that 69% of respondents were unhappy using a supplier without some form of external security accreditation, with 13% unsure.

Use of self-certified suppliers within IT departments (% of unhappiness)



Put another way, almost a fifth of UK public sector IT professionals would happily use a supplier that self-certified their own security credentials. This differs by sector, however. Central government IT departments are much less comfortable with self-certification – with 80% saying they would not be happy working with self-certified

suppliers. But the situation is more concerning in the NHS and local government where only just over half (58% and 57% respectively) were not happy using self-certified IT vendors.

From these findings, it's clear that there are some major inconsistencies in the way in which the public sector thinks about its data security, behaves in relation to data security and guards its data security. What was once black and white is now being interpreted in many shades of grey.

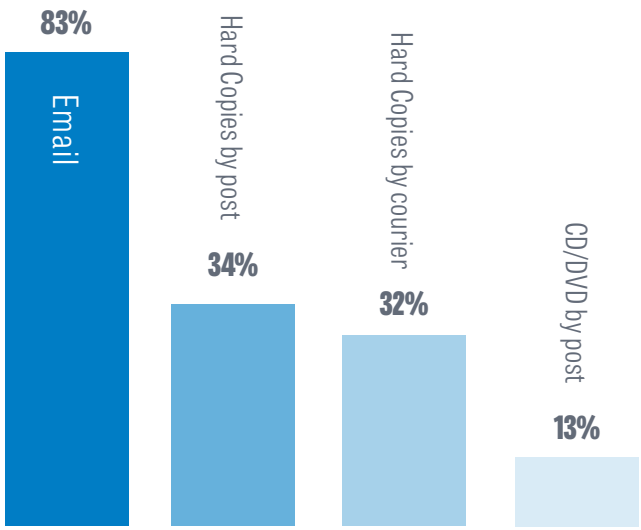
Central Government

Pleasingly, 94% of central government employees feel that the security of their organisation's data is 'important' or 'very important'. And when it comes to the government's own security classification system, central government staff are doing a superb job of following the guidelines that came into force in April 2014.

Adoption is very high – some 84% of central government employees use the new security classification system in some guise (6% still use the old Impact Level system to benchmark where to store data). This rises to 87% within central government IT departments. This is quite an achievement, compared to other public service employees.

How does this work in practice, however? Given that 93% of central government employees share and work on information with other internal and external organisations, the methods they are deploying daily highlight questions around security and efficiency.

Methods regularly used to share documents in the Central Gov't (% using):



"34%, 32% and 13% post hard copies, courier documents or send CD/DVDs by post respectively."

83% rely on email for the sharing of information. But what was surprising was the extent to which central government staff send information physically, despite myriad scare stories in the media. 34%, 32% and 13% post hard copies, courier documents or send CD/DVDs by post respectively.

These methods are costly, slow, present a wide range of security risks and have no place in a modern, digital world. Consumer cloud services and FTP services received relatively short shrift, with fewer than 10% of central government staff claiming they use them to share information.

When working with IT vendors, however, central government IT departments hold potential suppliers to a high standard. Out of all public sector IT professionals surveyed, central government staff were least happy with the idea of self-certification. 80% (against an average of 69%) would not be satisfied with self-certified vendors – no matter their size or reputation. Perhaps this explains low levels of adoption of cloud and FTP services.

Local Government

The survey suggests that local government employees are the least concerned about the security of their data compared to their public sector peers. 83% of respondents rated the security of their organisation's data as 'very important' or 'important'. This contrasts with 94% in central government and 93% in the NHS.

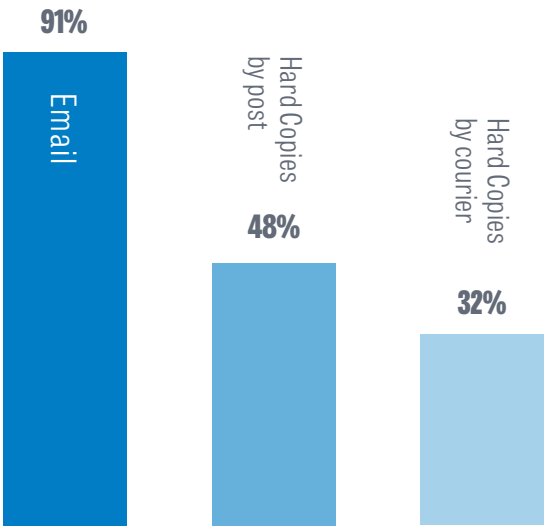
"Less than half of local government IT workers are aware of the government's new security classifications."

Perhaps it is the less sensitive nature of the information that local governments handle, but this position seems to have impacted adoption of the April 2014 government security classification system. 80% of local government employees were unaware of the application of the system, or did not think it appropriate to their organisation. Only 12% of respondents said their organisations had adopted and used the classification system in some way. And in IT departments

– where arguably knowledge should be greater – only 48% claimed awareness. This lack of awareness manifests itself in a range of data sharing behaviours that would concern information security specialists:

- **91% of local government employees use email for sharing and working on information with internal and external partners**
- **A staggering 48% - nearly half – of those surveyed use the post to share hard copies of data**
- **22% favour sending hard copies by courier**

Methods regularly used to share documents in the Local Gov't (% using):



Unfortunately, from a data security perspective, local government IT staff are comparatively happier working with 'self-certified' IT vendors. Indeed, only 57% of these individuals were unhappy at the idea of working with self-certified suppliers (against an average cross the public sector of 69%) and 19% did not know (against an average of 13%).

NHS

The NHS – especially due to the nature of its highly sensitive patient records – holds security in the highest regard of all public sector organisations. 87% of NHS staff view the security of their organisation's information as 'very important'.

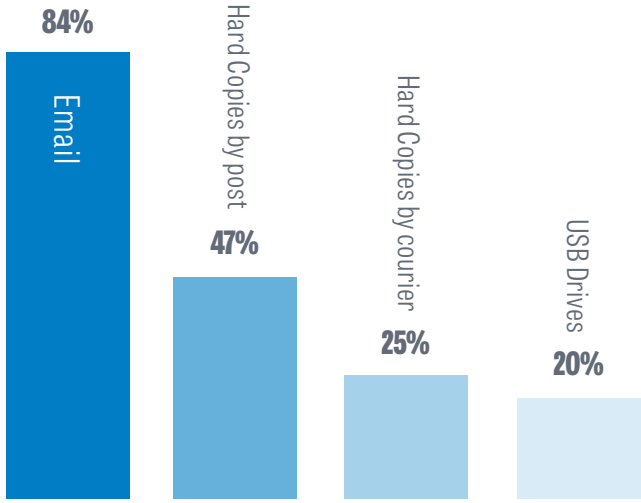
"In NHS IT departments, fewer than a fifth of respondents were aware of the government's security classification system."

In April 2014, the UK government introduced a new security classification system for information – but only 2.5% of NHS staff say their organisations have adopted the approach to securing documents. This is hugely inconsistent – paradoxical almost – considering the importance placed on security by this group. Perhaps it suggests a lack of faith in the new system. In NHS IT departments, fewer than a fifth of respondents were aware of the system.

"20% of NHS staff rely on USB drives to share information."

This security paradox goes further. As noted, 96% of NHS employees share information with other organisations in their job role. But the security implications of how this information is shared are significant. 84% of NHS staff use email to share information, 47% post hard copies and 25% use couriers. 20% rely on USB drives – the most in the public sector.

Methods regularly used to share documents in the NHS (% using):



Finally, the survey reveals that NHS IT professionals are slightly happier than average public sector IT staff to accept self-certification of vendors. Only 58% of NHS employees in an IT role (against an average of 69%) would be uncomfortable working with self-certified vendors. More evidence of a strange security paradox within the NHS.

Meeting Government-mandated commitments across public services

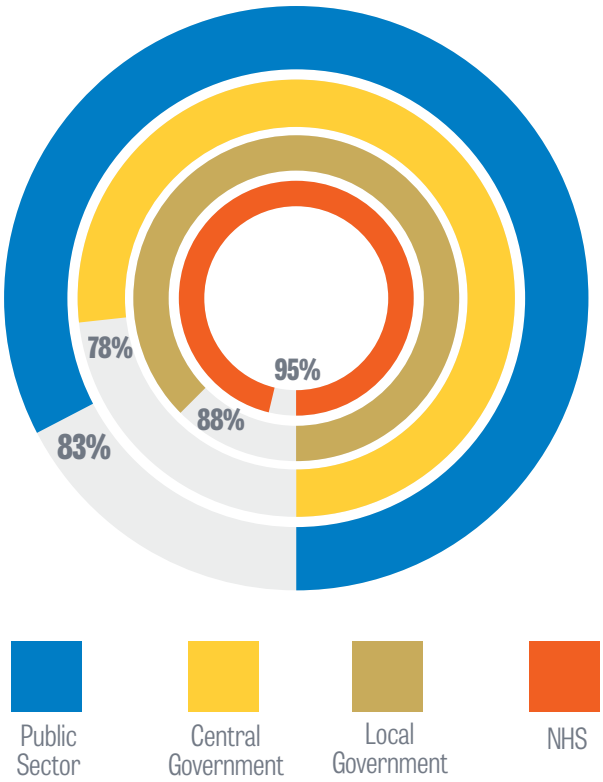
Public Sector Overview

Over the past few years, the G-Cloud procurement process has come under much criticism. Analysis of lacklustre spend through G-cloud, negative reports from suppliers and freedom of information requests have highlighted shortcomings in what is an excellent and welcome initiative. Unfortunately, this report supports many of them.

83% of public sector employees don't have a grasp on a flagship government-mandated procurement framework, G-cloud.

Awareness and usage are the two most common criticisms of G-cloud. In this survey, nearly three quarters (73%) of public sector respondents said they are unaware of the G-cloud framework. A further 10% say they have heard of it but are unsure what it is or how to use it. That's 83% of public sector employees that don't have a grasp on a flagship government-mandated procurement framework (78% central government, 88% local government and 95% NHS).

Understanding of G-Cloud in the Public Sector
(% don't understand)



It could be argued that knowledge and understanding of G-cloud is irrelevant to many public sector staff. The same cannot be said for IT departments, and again the research raises concerns, as only 50% of public sector IT staff have a working knowledge of the framework. 13% have actually purchased through the framework, but this is heavily influenced by behaviour in central government IT departments where the number stands at 22% (12% in local government, 5% NHS).

Another government-mandated commitment – successfully realised - was to ensure that 25% of government spend went to SMEs by the end of the last parliament. The survey asked public sector employees why they thought so few government contracts had been awarded to SMEs in the past. 62% confessed to not knowing why the situation existed. However, the biggest current barrier for SMEs was identified as in-built inertia – 20% feel that the public sector is simply used to dealing with large, outsourced ICT suppliers and feels more comfortable working with them.
Three concerns about working with SMEs gained equal footing from public sector employees (16% each) and they were:

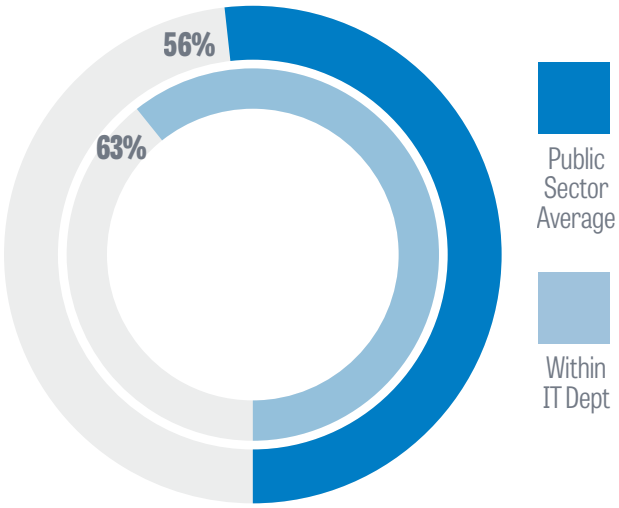
- The procurement process is too time consuming for SMEs
- SMEs might not have the correct security requirements in place
- The procurement process is cost-prohibitive for SMEs

There's a lot to deal with for SMEs in here – and bias differs by sector – but the fundamental issue is that public sector employees have a range of assumptions about SMEs that need to be challenged head on.

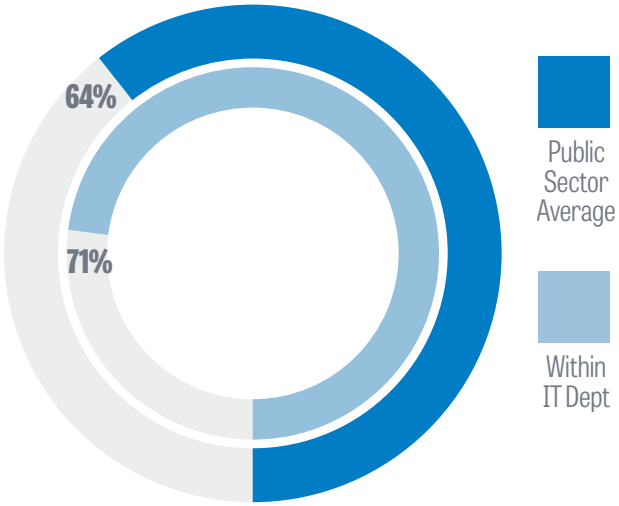
"When it comes to data residency, 64% of public sector employees prefer their data stored in the UK, increasing to 71% in the IT department."

One line of questioning that does provide hope for UK SMEs is a preference towards UK cloud vendors and storing data on British soil. 56% of public sector employees would feel more comfortable using cloud services provided by a UK cloud vendor – rising to 63% within IT departments. When it comes to data residency, 64% of public sector employees prefer their data stored in the UK, increasing to 71% in the IT department. This is one competitive factor that should buoy UK companies – whether SMEs or corporates.

UK cloud vendor preference (% comfortable)



Preference for UK data residency (% agree)



Overall, across the public sector there's patchy awareness of and adherence to government-mandated initiatives and commitments. It may be that G-cloud will never fully achieve its ambitions, but it's more likely that it's just taking longer – especially outside of central government – than anyone might have expected.

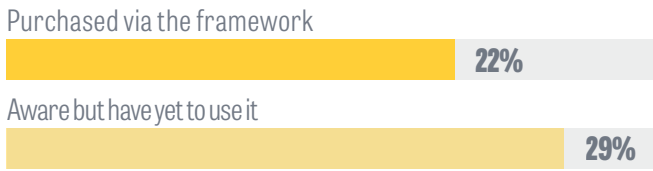
Central Government

If government communications professionals can congratulate themselves on awareness levels of security classification systems, then they have to accept there is work to be done where G-cloud is concerned. The initiative aimed at easing procurement has not entered the consciousness of, or been understood by, 78% of central government employees.

Only 6% of central government employees have purchased via the framework so far, and a further 14% are aware of G-cloud and have yet to use it.

Perhaps this is a little hard as it's not reasonable to expect everyone of every level in an organisation to be aware of a flagship procurement programme. So the survey dug into the IT community who should be using G-cloud regularly. Even so, of this group, 45% of employees are not aware of G-cloud, don't know if their department uses the framework or don't understand it. 22% of central government IT professionals have purchased via the framework and 29% are aware but have yet to use it.

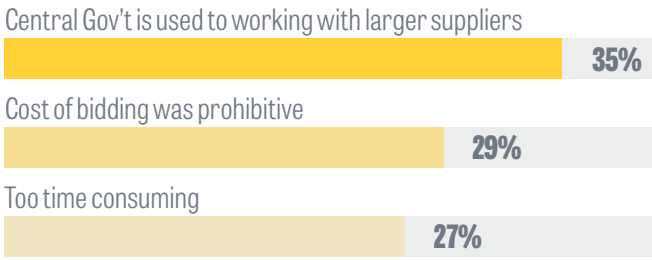
Central Gov't IT departments that have procured via G-Cloud



Even within central government IT departments, it seems challenging to drive understanding and use of G-cloud.

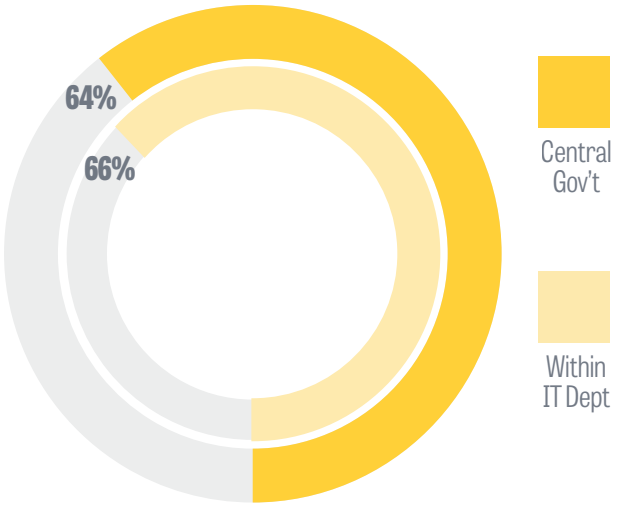
When asked why so few government ICT contracts had been awarded to SMEs in the past, central government employees point to historic difficulties that have led to a kind of inertia. 35% believe SMEs have lost out because central government is used to working with larger suppliers, 29% felt the cost of bidding was prohibitive for SMEs and 27% felt it was too time consuming for SMEs.

Why SMEs have lost out on public sector ICT contracts



Linked to working with SMEs, there is a surprising strength of feeling linked to data sovereignty and residency in the public sector. Hosting data on UK soil is important to 64% of central government employees – 66% to IT employees. This is a potentially useful USP for SMEs trying to win central government ICT contracts, as many of the international ICT bidders do not or cannot host data solely in the UK.

Data sovereignty for Central Gov't

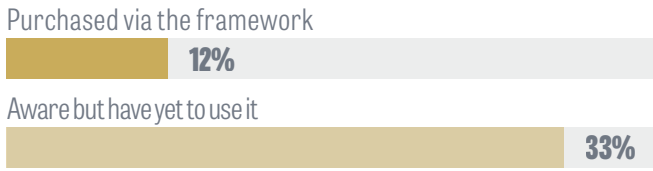


Local Government

The G-cloud initiative – the government's flagship ICT purchasing programme – suffers from a lack of awareness in the local government sector. Only 12% of local government employees are aware of G-cloud and understand it. Much has been written about the problems involved in rolling out G-cloud beyond central government and these statistics add fuel to that fire.

Only 3% of local government employees have purchased via the framework to-date, and only 7% are aware and yet to use it. In the IT department, things are a little more positive – but there is still plenty of room for improvement. Just over half (51%) of local government IT professionals are aware of G-cloud. 12% have purchased via the framework – roughly half the number in central government, and double that in the NHS. 33% are aware, but have yet to use G-cloud.

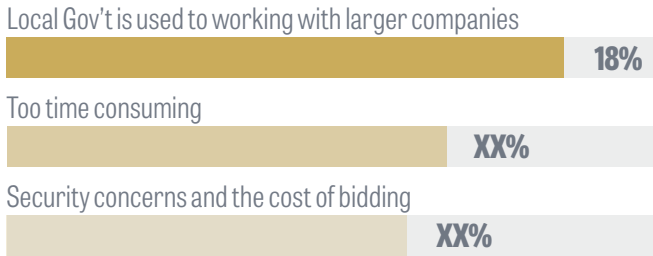
Local Gov't IT departments that have procured via G-Cloud



There are reasons to be positive about the future of G-cloud in local government ICT procurement, but it's clear there is a lot of work to do.

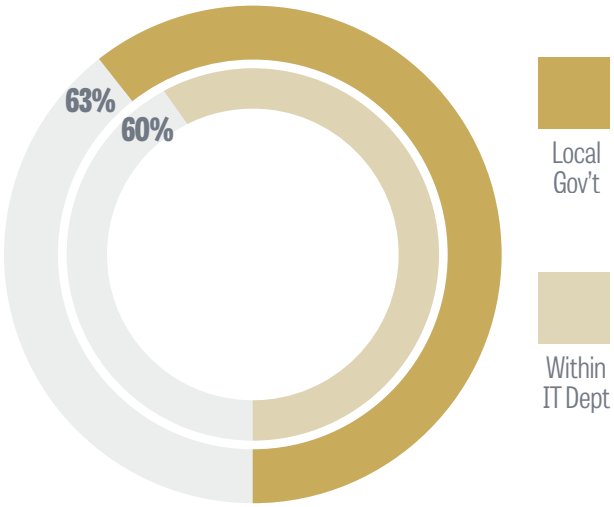
The government made much of its target of driving 25% of spend to SMEs by the end of the last parliament. While 66% of respondents couldn't put their fingers on why so few public sector contracts were traditionally awarded to SMEs, there are a number of embedded concerns around working with SMEs in local government. The biggest is around the fact that the sector was used to working with larger companies (18%). The second concerns the ability of SMEs to spend the time on long bidding processes. At joint third, security concerns and the cost of bidding for projects were highlighted as reasons for lack of SME opportunity.

Why SMEs have lost out on public sector ICT contracts



But there are glimmers of hope for UK-based cloud SMEs wanting to serve the local government sector. 63% of local government employees were more comfortable with their data being stored in the UK, 60% in IT departments. And roughly half of employees and their IT colleagues would prefer to work with UK cloud vendors.

Data sovereignty for Local Gov't



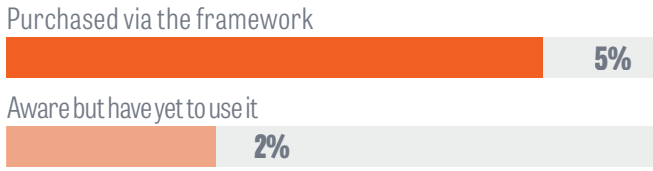
NHS

Senior public service officials charged with driving G-cloud should look away now. 95% of NHS employees are not aware of G-cloud, don't know if their organisation uses it, or don't know what it is.

1% of NHS employees are aware of the G-cloud framework and have purchased through it, 3% are aware but have yet to use it.

Shifting focus to the more relevant NHS IT departments, 79% of NHS IT staff are not aware of G-cloud, don't know if their organisation uses it, or don't know what it is. 5% have purchased via the framework, but 2% have actively purchased outside G-cloud – more than twice the average.

NHS IT departments that have procured via G-Cloud



As a government-run entity, the NHS will be encouraged to ensure that a reasonable proportion of its spend goes to SMEs. But when asked, NHS employees were the least likely of public sector staff to have a view on why the NHS has typically done less business with SMEs than large companies. Almost three quarters did not know why SMEs had not traditionally won NHS contracts.
The remaining quarter of respondents listed concerns over SMEs having security requirements in place, that the organisation was more comfortable working with larger suppliers and a feeling that the procurement process would be too onerous for SMEs.

Across the public sector, it was NHS employees who were most keen on data being stored in the UK. 69% expressed a preference for data residency, versus a public sector average of 64% - though NHS IT departments were actually the least likely at 57%. Allied to this, more NHS staff preferred UK-based cloud vendors – providing a shot in the arm for British SMEs targeting the NHS with cloud services.

Action Plan for Public Sector Executives and IT Leaders

The public sector is clearly at the beginning of a long journey. The destination is a new way of working, underpinned and enabled by cloud computing platforms. But it is a journey filled with obstacles, challenges and crossroads. So how can public sector executives and IT leaders drive their organisations forward? What practical steps can they take?

Building awareness and confidence in cloud computing

The awareness issue is really one of terminology. Where the government has publicly evangelised 'the cloud', many public sector workers do not understand the term – and why should they? Many employees are probably blissfully unaware that they use cloud services every single day in their private lives. When introducing new platforms and services, executives and IT leaders should focus on the benefits of cloud computing as they relate to public sector employees' real challenges.

When it comes to boosting confidence in cloud computing, time will be a healer. Different parts of the public sector are at different developmental stages in their IT infrastructure, levels of connectivity and devices used. Confidence comes from positive user experiences, so be careful. Don't advocate cloud services if your IT architecture, bandwidth or hardware cannot support a decent user experience from the beginning. Executives and IT leaders can also boost confidence in cloud platforms by emphasising the use of UK cloud vendors and commitment to maintaining UK data residency.

One area public sector executives and IT leaders will need to work hard on is an inherent inertia towards cloud computing driven by protectionism. Across the public sector, the number of IT staff has grown dramatically in the last decade and cloud computing offers an opportunity to streamline this huge cost base. These 'empires', and continued attempts to maintain and grow them, represent the biggest practical barrier to the public sector realising the clear advantages of cloud platforms:

- **Speed – cloud-based platforms can be deployed instantly, negating the need for IT support or infrastructure procurement**
- **Security – more secure than current collaboration methods, far more efficient and completely auditable**
- **Flexible – simple and quick to scale services up/down; no more lock in to long term agreements**
- **User friendly – designed with ease of use in mind, for anybody to use**

Understanding and complying with the new security classification system

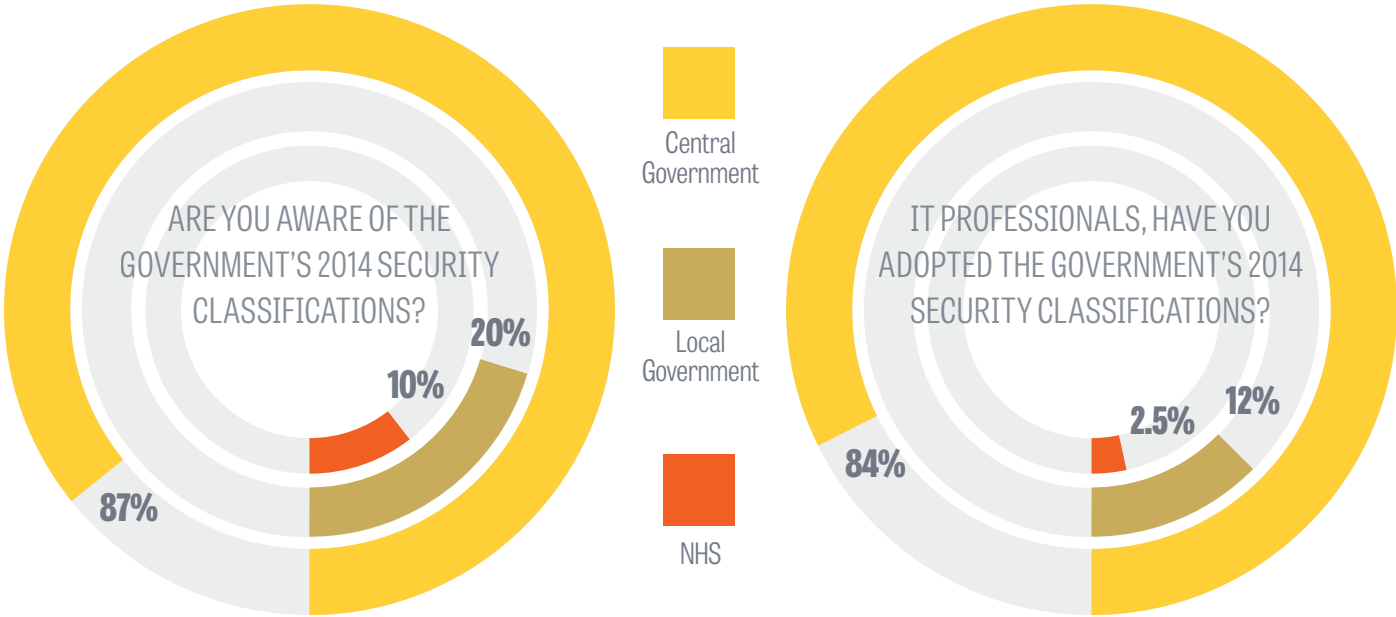
The government's new security classification system is not especially difficult to understand. However, the system represents a seismic cultural change. No longer is information security enforced from above – public sector organisations and their SIROs (Senior Information Risk Owners) are responsible for the interpretation and application of the guidelines. Effectively, something that was once objective and rigid has become subjective and flexible.

Further complication arises as the government does not currently certify commercially-available solutions against the new security classification system as it did with its predecessor. With the Impact Level system companies like Huddle were certified to securely store information categorised as being between IL0 to IL4. While most SIROs and industry watchers would agree that information identified as 'Official' or 'Official Sensitive' (roughly 90% of all public sector documents) effectively mirror up to IL3 categorisation, the lack of matching certification is unhelpful. The PSN (Public Sector Network) generally accredits organisation-specific services rather than a cloud service as a whole. There are, however, some alternatives to help people gauge the security credentials of suppliers.

Public sector executives and IT leaders should consider ISO a good benchmark for security, but that's very much 'table stakes' for people who are serious about security. Those looking for the 'gold standard' should take a look at the US government's FedRAMP certification. The Federal Risk and Authorization Management Program is a new US government-wide program that provides a rigorous, challenging and standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services.

Based on discussions with the Cabinet Office, Huddle has produced an infographic to help clarify the implementation options for SIROs considering the new security classification system. Public sector executives must work together to ensure that that their file storage, sharing and collaboration systems are secure, and can be trusted to carry information under the new guidelines.

Awareness of Government Security Classifications (2014) is limited outside of central government
(% aware)



G-Cloud and working with SMEs

"The impact of G-cloud in central government departments is impressive, but there is a long way to go in establishing awareness and regular usage in local government and the NHS"

G-cloud is a very strong purchasing framework that will drive fundamental cultural change in the way in which the public sector procures IT services. It's an incredibly ambitious programme that should be celebrated, rather than derided – which is far too often the case.

While this survey highlights there is a long way to go in establishing awareness and regular usage of G-cloud in local government and the NHS, the impact it has had in central government departments is impressive. Awareness and usage will improve as large, multi-year IT contracts conclude and more vendors leverage the framework. Public sector executives and IT departments should embrace G-cloud and give it the support it deserves.

SMEs are also set to benefit as the monolithic public sector IT contracts of yesteryear come to a close in the next two to three years. As a result of the G-cloud framework, public sector executives and IT leaders will find that they are able to use SMEs without having to invest additional time and resources – tackling the major reported barriers to working with SMEs. When factoring in public sector employee preferences for UK cloud vendors and keeping data in the UK, working with UK SMEs could provide a win-win for all.

Conclusion

The public sector is in the early stages of a seismic change in working culture. It's an evolution predicated on closer collaboration between public sector organisations and external stakeholders. Cloud technologies – specifically collaboration platforms – are key enablers. However, issues of adaptation (specifically confidence), of security (where theory and practice are at odds) and of meeting government mandates (where awareness and conformity differ) are impeding progress.

"Moving to the cloud is a cultural, not a technological evolution."

But the conclusions of this research are more positive and more optimistic than much written on the subject of public sector evolution. Public sector executives and IT leaders can drive usage of the platforms upon which collaborative working cultures can be built, but need to bear in mind three key takeaways:

Change management is critical: moving to the cloud is a cultural, not a technological evolution. Employees need to understand how collaboration platforms can practically help them. IT teams need to let go of the 'bigger is better' mentality when it comes to resources. Everyone needs to be patient and only launch services when the underpinning connectivity and device infrastructure is in place. Training – both initial and ongoing – will prove invaluable.

Information security is complicated: the new classification system is difficult to master, with its change in emphasis and responsibility. Public sector executives and IT leaders must decide how they will implement the system in their organisations, what commercial platforms they will deploy to ease implementation and compliance and how they will approach the issue of certification.

Digital government is a certainty: it's easy to point to missed milestones and poor awareness of mandates, but these are minor set-backs in a bigger, more important plan. With hindsight, the objectives were overly ambitious – but rather that than the alternative. Public sector executives and IT leaders must embrace G cloud and the 25% SME target and drive their organisations forward in achieving their worth aims.

The UK public sector is at a key point in its evolution and, while timescales are lengthening, the foundations for a more efficient, more productive and more valuable service are there for all to see – with the caveat of some fundamental lessons are yet to be learned.

About Huddle

Huddle is a secure cloud collaboration service that enables enterprise and government organisations worldwide to securely store, access, share, sync and work on files with everyone they need to -- regardless of whether they are inside or outside of an organisation's firewall. Co-headquartered in London and San Francisco and with offices in New York City and Washington D.C., Huddle's customers include 80 percent of Fortune 500 and 80 percent of UK government departments, as well as companies such as Kia Motors, Williams Lea, Driscoll's, Unilever and P&G. The company is privately held and backed by leading venture capital firms in the US and Europe.

For more information visit www.huddle.com
or follow us on Twitter @huddle.

To view our use cases for healthcare visit https://www.huddle.com/customers/collaboration-case-studies/

To activate your free trial, visit huddle.com

"Moving to the cloud is a cultural, not a technological evolution."

huddle™