

# SECURE GOVERNMENT COLLABORATION FROM THE CLOUD >>

## Driving positive business transformation

Collaboration as a service is emerging as a transformational model for business IT. Government departments and institutions need to collaborate to increase their productivity and more easily meet targets.

Well-designed collaboration can facilitate agility, productivity and business innovation, offering opportunities for efficient, integrated teamwork with other government institutions, suppliers and partners, far more powerfully than before. When such collaboration is provided from a secure cloud environment, IT management, maintenance and support burdens are removed, whilst the most appropriate versions of applications are made available through the evergreen nature of the service. 'Cloud' and 'Collaboration' are better together.

# 'CLOUD' AND 'COLLABORATION' ARE BETTER TOGETHER

# COLLABORATION. DRIVING POSITIVE BUSINESS TRANSFORMATION IN LARGE ORGANISATIONS.

With more collaboration comes more shared data, and it is vital that this data is secured, and available for reading, storing and publishing only by those with explicit authority to do so. Can this level of security be achieved, from the cloud? If so, are there immediate significant transformational opportunities and how might these be exploited?

As a method of working, collaboration aligns closely with a key aspiration of modern business; that of bringing together, across sectors, the diverse talents, knowledge and resources available; bringing them to bear efficiently where and when needed, unhindered by boundaries.

The Software as a Service (SaaS) model, sometimes called “cloud computing”, is an obvious means to achieve this. Applications and data are hosted at a highly secure remote location and can be accessed by accredited people using any fixed or mobile device, alleviating the need to install or maintain software or infrastructure anywhere except in the service provider’s data centre. This offers technical and operational simplification throughout the application life cycle and has the potential to remove many of the costs and boundaries that impede collaboration between organisations and people.

However, boundaries have often been put in place deliberately to achieve compliance, protect privacy, intellectual property and provide traceability. Some boundaries were created not by design but by incidental physical, political or technical realities – for example the absence of connection between private networks – and whose integrity is assumed by governance, especially in the formulation and implementation of IT security policy. Such boundaries must not be compromised and the innovation promised by the cloud service must offer clarity, control and predictability at the edge.

## CONTROLLING WHO SHARES

A series of general purpose cloud computing services have proliferated but questions remain over their ability to support industrial strength secure applications, for which passwords and directories are not sufficient. Such systems are designed primarily for ease of use, based on the assumption that responsibility for access security, and impact if it is compromised, is borne by the individual account holder. This fails to address the needs of groups, teams and organisations responsible for sensitive digital information, where privacy breaches or security leaks are often only one mistake or misdemeanour away from reality. Of course, such systems must also be protected from sophisticated attack, with serious, possibly life threatening, consequences if undetected.

So organisations considering the adoption of cloud services must focus first on the authentication methods used. Public web-based collaboration tools are often affected by online identity theft, and miscreants, human or automated, often glean information from one system for use in penetrating another, such as illegitimate “lost” password retrieval.

For that reason higher-integrity web applications such as those provided by banks, which bear at least partial responsibility for their customer’s losses, cannot rely solely on the online channel for authentication, for example in changing passwords. Such a manual approach can be expensive and tends to undermine effective, efficient business: those procedures become a bottleneck.

The solution, already familiar to many online banking customers, is two-factor authentication, which requires the user to both know things (PINs, passwords) and have physical things (smartcards, tokens), and this forms the linchpin of the strategy to share regulated data using cloud services in Government. When there is confidence that the true identity of all users is known at all times, they can be allowed to access the specific information for which they have legitimate need with minimum hindrance and, (if tasked to do so) to amend, add or remove specific information with immediate effect: all in compliance with prevailing policy, assured by a reliable audit trail.



**Controlling what is shared.** Proven, advanced asset control and configuration management is built into collaboration platforms such as Microsoft SharePoint™ and its associated tools, so that in transforming current practices, existing information security policies can be implemented easily with no need to reformulate them or reclassify information.

## **CONTROLLING WHAT IS SHARED AND HOW**

Proven, advanced asset control and configuration management is built into collaboration platforms such as Microsoft SharePoint™ and its associated tools, so that in transforming current practices, existing information security policies can be implemented easily with no need to reformulate them or reclassify information. However, authentication and good practice does not in itself enforce those policies. An organisation's information governance and compliance strategy is reliant, in part, on the trust it has in its people. Internal training, culture and professional and personal relationships create an environment of trust, but how can that trust be offered to outsiders without diluting the efficacy of the security strategy? How can a department be sure its policies will continue to be applied diligently to the information for which it is originally responsible?

Adherence to policies can be enforced by automated policy management, interfaces and applications can be made to enforce policy depending on the user's identity, or employing organisation. Organisations can choose what to collaborate on and who with, depending on the candidate partner's own policies and security strategy, and place in the public sector network. Organisations might start by comparing existing policies and selecting the most rigorous elements from each, so that each party sees its general policy either adopted or extended and strengthened, but never downgraded. Some rules will be organisation specific and some will be subject to standard governance models such as the Data Protection Act.

## **CONTAINMENT**

Trust-based strategies to protect and manage assets shared via cloud services will work only when those assets are appropriately restricted within the cloud. Any chance of sensitive documents being misappropriated or maliciously amended would remove the trust required to collaborate at all with partner departments. If out-of-date versions of documents could continue to be circulated within the cloud, trust in the accuracy of the data would be lost.

One solution is Digital Rights Management (DRM), which offers sophisticated rules-based access restriction and encryption of data and documents to prevent use or amendment by unauthorised persons. When integrated with collaboration platforms such a solution should make the rogue distribution of material very difficult indeed. Strong blanket encryption of data at network level is highly effective because without decrypting a document, an unauthorised person has no knowledge of the information it contains, however this doesn't lend itself to collaboration platforms where personal productivity and system performance will be affected. At document level DRM can effectively eliminate casual or opportunist abuse and therefore is suitable as a measure to protect sensitive data in a collaboration environment. It is effective in restricting the ability to break security by forwarding, saving, printing, copying, taking a screen-shot, saving onto CD, memory stick etc.



## IS CLOUD-BASED COLLABORATION SECURE COMPARED TO OTHER PRACTICES AND ARCHITECTURES?

Traditional methods of sharing data between sites tend to have points of risk. High-profile security failures have occurred, for example where portable storage devices or unencrypted email has been used. Secure cloud-based collaboration can obviate that risk and reduces the number of points of potential security failure, whilst maintaining compliance and audibility.

The cloud itself needs to be industrial strength in terms of failover and avoidance of points of failure. Technically, the data centre is the most critical component. Confidence in the compliance, reliability, redundancy and, especially, the security measures applied must be very high before committing regulated data to it.

Even when that is the case, the implications for any given group of organisations of moving towards collaborative working and centralised infrastructure, require consideration, especially the human factors.

## CONCLUSION: CLOUD AND SECURE COLLABORATION. NOW IS THE TIME TO PILOT.

Collaboration, provided as a service, can drive real business transformation in the public sector. Until now there have been good reasons to be cautious whilst the pressures to collaborate from policy makers have been building. Departmental heads are looking for secure, functionally complete ways to accelerate collaboration, CIOs are looking to provide this type of functionality within decreasing capital budgets, CFOs are looking for flexible, demand-based utility pricing, while users in organisations are asking why their collaboration experience at work compares so poorly with that which their family uses every day at home. Meanwhile, the press are circling, looking for high-profile examples of business failure by departments that haven't shared information.

The next step change in government efficiencies through IT is not process automation – much of this work has already been attempted – rather it is through enabling people to perform their jobs more effectively through access to other people and knowledge. Every pound invested in user centric and collaborative computing is a pound invested in improving worker and thus departmental efficiency.

The benefits of collaboration are likely to prove irresistible and the cost of implementing it will continue to fall, but collaboration comes with security and governance responsibilities, but now is the time to pilot cloud-based secure collaboration in public sector.

## ABOUT ATOS ORIGIN

Atos Origin has contributed security-critical components and services to the Government Gateway since its inception in 2001, worked closely with Microsoft to provide best-of-breed solutions to major international organisations across all sectors for over 10 years, and recently formed a further accredited alliance to provide and support Microsoft's Business Productivity Online Services. This experience and achievement make Atos Origin uniquely able to help its customers gain the most from the new generation of business technologies.

Atos Origin is an international information technology services company. Its business is turning client vision into results through the application of Consulting, Systems Integration and Managed Operations. The Company's annual revenue is EUR 5.5 billion and it employs 50,000 professionals in 40 countries. Atos Origin is the Worldwide Information Technology Partner for the Olympic Games and has a client base of international blue-chip companies across all sectors. Atos Origin is quoted on the Paris Eurolist Market and trades as Atos Origin, Atos Worldline and Atos Consulting.

## CONTACT US

4 Triton Square  
Regent's Place  
London  
NW1 3HG  
United Kingdom  
Tel: 020 7830 4444  
[www.atosorigin.co.uk](http://www.atosorigin.co.uk)