THE COLLABORATION CHALLENGE

Balancing digital collaboration with information governance

In this era of digital transformation, there is an urgent and growing need for government agencies and regulated industries to work more collaboratively to deliver better outcomes for their stakeholders.

This 'collaboration imperative' is being driven by a range of factors including the growing need for cross-agency collaboration, the use of outsourced service providers and increasing digital engagement with customer and citizens. It is also being driven from the highest levels of government, including the Digital Transformation Agency.

> The key to our future prosperity is to be **faster, leaner, more productive, more innovative and more collaborative**
>
> **Malcolm Turnbull**
> Australian Prime Minister[+]

LOOKING FOR BALANCE

Expanding digital collaboration, however, presents serious challenges for government agencies and regulated industries that are the custodians of confidential personal records and highly sensitive information, and must manage a complex set of risks. For example, governments have access to personal information such as a citizen's tax file. This information can cause serious privacy breaches or financial loss if it were to get into the wrong hands. Government agencies and other regulated industries also hold highly sensitive information that informs policy decisions and large commercial investments.

To maintain the integrity of this sensitive information and to protect citizens, stakeholders and their own reputations, government agencies and regulated industries have developed and honed robust information governance frameworks over many years. This includes significant investments in document and record management systems that ensure there is a complete record of how the information is managed.

These systems not only track usage, but also enforce access permissions, life-cycle and archive (or destruction) policies, guaranteeing the security of the information and maintaining a 'single source of truth'. It is important to note that this is not just "best endeavours"; good information governance is something that government agencies and other regulated industries are benchmarked against.

For all of these reasons, information governance cannot and should not be sacrificed simply to facilitate working with people external to the organisation.

Herein lies the challenge for government agencies and regulated industries:

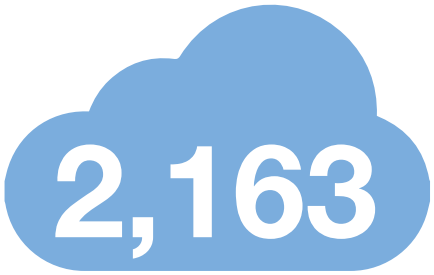
On the one hand, there is an imperative to be more flexible and collaborative with those outside their organisation.

On the other, they must maintain a secure regime of simple and cost effective information governance that manages the many legal, regulatory, privacy, intellectual property and security risks.

> Good governance increasingly depends on collaboration. [However], risks often manifest because the desire to 'do something' results in 'solutioneering' and expose their organisations to considerable risk.
>
> Professor Peter Shergold AC
> Board of Trustees, Western Sydney University

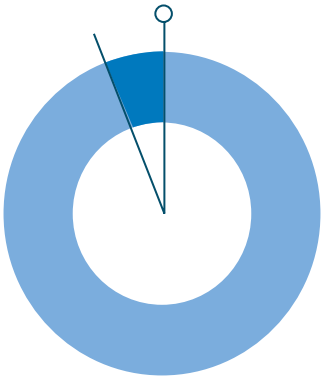
THE RISK OF INACTION

In the meantime, collaboration must and will go on – and if the CIO doesn't find a solution, the business users will. Unfortunately, in the absence of an easy to use and secure collaboration solution provided by the organisation, many are resorting to uncontrolled systems (or 'shadow IT') that erode information security and auditability – and expose their organisations to considerable risk.



INDIVIDUAL CLOUD SERVICES
IN USE BY THE QLD GOVERNMENT**

For example, when people take information out of controlled systems and share it via email, thumb drive or consumer- based file sharing systems, all transparency, visibility and auditability over that content is lost. It essentially bypasses information governance, meaning that security and regulatory compliance cannot be guaranteed. It creates multiple repositories of information, resulting in an absence of a 'single source of truth', making any sort of audit impossible and ultimately hampering the collaboration efforts.



81%
OF LINE-OF-BUSINESS
WORKERS ADMIT TO USING NON-APPROVED
SAAS APPS*

The risks of inaction are immense. In addition to the significant impacts on productivity and the integrity of the decision-making process, the privacy and security risks posed by this uncontrolled collaboration cannot be overstated. A solution that balances the need to collaborate externally while maintaining a secure regime of (cost effective) information governance is needed.

* McAffee Report 2013, By STratecast (a unit of Frost & Sullivan)
** Queensland Audit Office, 2016

APPROACHES TO SOLVING THE PROBLEM AREN'T WORKING

As organisations around the world grapple with this issue, a number of different approaches are being investigated, with limited success.

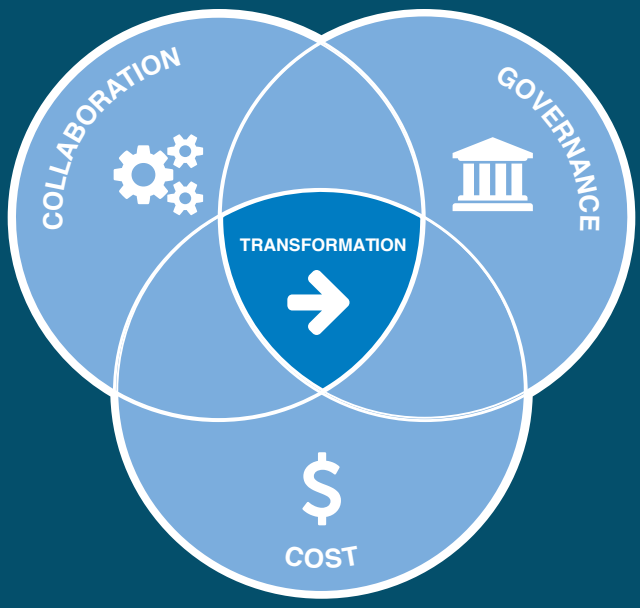
Standard Collaboration Tools are often 'consumer grade' file sharing applications that lack security required for sensitive data. They pose a massive risk, as there is no oversight and or administration capability. They also don't integrate with existing systems, meaning there is no transparency and accountability, and no 'single source of truth'.

Built for purpose solutions are expensive to develop and maintain and are often difficult to scale to external stakeholders, other divisions or processes. In addition, licensing costs, staff training and the need to involve IT regularly cause bottlenecks for those looking to collaborate.

'Universal Systems' designed to facilitate collaboration between related agencies miss the need to collaborate now. These are often abandoned in planning because of the cost and the time to implement. Those waiting for a perfect, 'whole of Government" system, for example, will be waiting a long time.

A FRAMEWORK FOR BALANCING COMPETING IMPERATIVES

When working with anyone outside of their organisation a government agency or regulated organisation must find a solution that effectively balances the three competing imperatives of collaboration, governance and cost.



COLLABORATION

Collaboration can be a highly complex, fragmented process. Any solution must support all aspects of the collaborative process, providing complete context and transparency in a single secure location – more than just simply sharing files. A collaboration solution must be easy to use and minimise training requirements, as stakeholders, internal and external, are included in the collaborative process. It must also have the ability to scale multiple processes.

INFORMATION GOVERNANCE

The problem for government and other regulated industries is that during the current uncontrolled collaboration process there is no information governance. If audited, there is no way to prove that the collaboration process was secure and compliant with regulatory requirements. It is therefore vital that any collaboration platform used by government agencies or regulated industries is not only secure, but also integrates with the existing information governance framework. This integration must facilitate the synchronisation of documents with the existing document and records management system, updating both the content and audit trails.

The collaboration solution must also inherit, rather than replicate the access permissions, life-cycle and destruction policies that are governed by the existing document and records management system. Without this integration, the information governance that today provides auditability and transparency is lost.

COST TO PROVISION

The cost of implementation is also a major factor to be considered when delivering a collaboration platform. The licensing model of the platform must support the 'fluid' nature of the collaboration process, whereby new stakeholders, internally and externally are constantly added and removed without additional cost or restriction.

The human costs must be also taken into account. Any solution must be simple to use and cost effective to provision. Each instance where collaboration is required, should be initiated by the user, rather than IT.

CASE STUDY

National Blood Authority

The National Blood Authority (NBA) manages and coordinates arrangements for the supply of blood and blood products and services on behalf of all Australian Governments. Critical to its role is guaranteeing that strict information governance protocols are adhered to whenever sensitive health information is exchanged.

"Working across nine governments and over 400 hospitals, sharing information and collaborating with external parties in a secure and auditable way can be a nightmare," says Peter O'Halloran, Executive Director and Chief Information Officer of the NBA.

"Internally we had created a sound information framework that was controlled and compliant with legislation, government policy and best practice. However, as soon as we shared information outside the building we'd lose all of that transparency and traceability in an instant.

The NBA has addressed this challenge by utilising a simple, costeffective collaboration platform that empowers their team to collaborate externally, while maintaining their good governance practices.

"We knew we needed a collaboration platform that was secure, locally hosted and importantly, ensured complete auditability and traceability of information and activities. We also wanted something that would integrate into HP TRIM, gave us full audit trails and was IRAP assessed. Objective Connect was the only product that hit all those marks," O'Halloran says.

> Objective Connect is now used across the NBA whenever there's a need to work with anyone outside the organisation – and has meant the NBA can be more flexible with their working arrangements.

Peter O'Halloran
Executive Director and Chief Information Officer
National Blood Authority

"We have saved over $40,000 per annum in postage, courier and printing costs, but the most important saving is staff time. For our staff, using Objective Connect means that sharing files is now no different than sharing with someone in the office. Our responsiveness has improved massively and now we're collaborating."

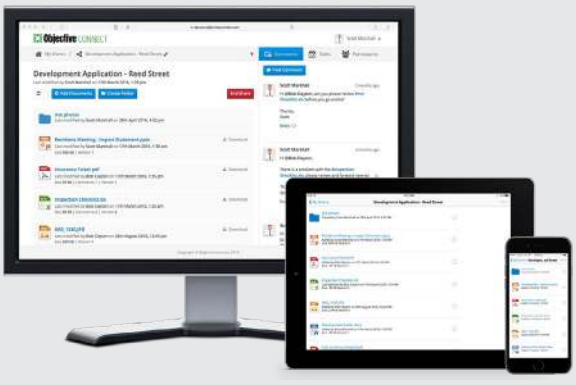
Work securely with anyone outside of your organisation

With government-grade security, Objective Connect creates a secure, private workspace to collaborate on documents, capture conversations and control tasks.

From cross-agency collaboration, working with outsourced service providers or simply digitally engaging with customers and citizens, Objective Connect can be used to manage any process involving external parties.

Information Governance can be maintained by integrating Objective Connect with an organisation's existing document and records management system, ensuring a 'single source of truth' is always maintained, even when working with external parties.

Because it can be used to manage any business process, Objective Connect enables digital transformation – removing the need for paper, email, thumb drives, DVD's and rogue or shadow IT.



OBJECTIVE CORPORATION LIMITED
Asia Pacific: +61 2 9955 2288 | Europe: +44 1628 640 460
www.objectiveconnect.com