GovCloud 2.0

Harnessing Cloud Computing for Digital Government Transformation

Cloud 2.0 refers to the intersection of Cloud Computing and web 2.0 social media, and when applied to the public sector is called GovCloud 2.0. This represents an evolution of e-government models that harness a powerful combination of the major advances in IT infrastructure “as a Service” with the collective intelligence business models known as “crowdsourcing” for radically transforming how government agencies serve the needs of their citizens while also dramatically reducing the costs required to do so.

GovCloud2.com
## Table of Contents

Executive Overview – The Cloud CIO ........................................................................................................ 3

How is this different from E-Government? ................................................................................................. 3

Section I - Digital Government: Citizen Service Transformation ............................................................. 4

  Wiki Government – Public Sector Crowdsourcing .................................................................................. 4

  Cloud 2.0 - Enabling peer to peer Citizen Communities ....................................................................... 5

  BPaaS – Standardizing shared best practices ......................................................................................... 7

Section II - Cloud Migration Management ................................................................................................. 8

  Cloud First – Portfolio Migration ............................................................................................................ 8

  Cloud PMO – Buying IT as a Service ....................................................................................................... 9

  Procurement Frameworks: Enabling Trusted Cloud Providers ............................................................... 10

  Cloud Service Brokerage ....................................................................................................................... 13

Section III - Enterprise Architecture ......................................................................................................... 16

  Federal Government Cloud – Shared Services Architecture ............................................................... 16

  Web Oriented Architecture .................................................................................................................... 18

  Cloud Identity Ecosystem ....................................................................................................................... 20

  Conclusion – Always On Digital Government ..................................................................................... 25

About the Author ........................................................................................................................................ 25
Executive Overview – The Cloud CIO

Cloud Computing is often described in entirely technical terms, and while there are certainly technical benefits the overall business case can be headlined first by business process transformation.

This larger scope is key for IT leaders looking to master becoming a “Cloud CIO”, as they will be able to explain the benefits of the technology in a form that will result in significant improvements, benefits that are clearly visible to the senior executive team.

This paper describes how these can be achieved across three main work streams:

- Citizen Service Transformation
- Portfolio Migration
- Technical Architecture

This provides a holistic framework to drive Cloud adoption, from business transformation through the application estate and enabling technical design.

How is this different from E-Government?

As the name suggests ‘Cloud 2.0’ represents a second generation of online enablement, so in what ways is this different from the first generation of e-government?

Fundamentally the most significant differences are:

- **Multiple integrated systems** – Traditional e-commerce mainly focused on adding a web front-end to one single legacy system, for example providing online access to the status of welfare claims from one department. In contrast Cloud 2.0 is about the same online citizen service but where multiple back-end systems will be dynamically joined together to achieve a more sophisticated business process.

- **Social web** – When e-commerce first emerged it was a long time before blogs, Facebook and other social web features. Or at least the trend was in its infancy, where it was very simplistic and used by a small minority. Today the technology is advanced, ubiquitous and used by billions of people, and this will further envelope legacy applications.

These two factors are going hand in hand to power a next generation ‘Web 3.0’ approach to enterprise IT, a model that will radically transform service delivery for citizens and also the cost base for implementing the required technologies.
Section I - Digital Government: Citizen Service Transformation

With this focus on citizen service the headline programs driving this transformation include the USA’s ‘Digital Government’ initiative.

Following on from their Cloud First initiative that launched the main wave of Government Cloud Computing, the Whitehouse CIO team then also published a strategy for Digital Government.

This describes the imperative to better enable more online service delivery through key technologies such as mobile applications, Open Data and Cloud computing.

Wiki Government – Public Sector Crowdsourcing

As highlighted this isn’t simply E-Government by another name. The scope includes integrating multiple back-end systems and “socializing” web applications.

Furthermore transformation isn’t limited only to technical aspects of social but also changes in how the business process itself is conducted. In short the adoption of “Crowdsourcing” techniques that enable multiple online users to participate in conducting a workflow, not just a linear progression from one person to the next, internally within an organization.

For the public sector this even has its own unique brand idea, called ‘Wiki Government’.

The term was coined by Beth Noveck, one of the architects of Open Government initiative for the Whitehouse, in her book of the same name (you can download a free chapter), which explains the principles of the concept prototyping work of the Peer to Patent Portal.
This Peer to Patent project illustrates the key principles of how Open Government is about far more than simply being more open with how information is published.

It demonstrates the huge potential for business transformation that Cloud 2.0 offers, that it's not just about migrating data-centre apps into a Cloud provider, connecting an existing IT system to a web interface or just publishing Open Data reporting data online, but rather utilizing the nature of the web to entirely re-invent the core process itself.

**It's about moving processes into the Cloud, not just IT.**

In [this 40 page Harvard white paper](#) Beth describes how the US Patent Office was building up a huge backlog of over one million patent applications due to a 'closed' approach where only staff from the USPTO could review, contribute and decide upon applications.

To address this bottleneck she migrated the process to an online, Open version where contributors from across multiple organizations could help move an application through the process via open participation web site features. Peer to Patent is a headline example of the power of Open Government, because it demonstrates its about far more than simply publishing reporting information online in an open manner, so that they public can inspect data like procurement spending numbers.

Rather it's about changing the core decision-making processes entirely, reinventing how Government itself works from the inside out, reinventing it from a centralized hierarchical monolith to an agile, distributed peer to peer network. In essence it transforms the process from ‘closed’ to ‘open’, in terms of who and how others can participate, utilizing the best practice of ‘Open Innovation’ to break the gridlock that had occurred due the constraints caused by private, traditional ways of working.

**Cloud 2.0 - Enabling peer to peer Citizen Communities**

This effect of Cloud-enabled social transformation of business processes is also recognized in the [Cloud computing strategy document](#) recently released by Canada Health Infoway, the Canadian E-Health standards authority.

“We see a logical and necessary fusion in the use of cloud to support mobile computing, social computing, analytics and consumer enablement.”
The paper covers all the related technology components – Privacy, encryption, et al, and also offers a strong vision for how these ideas could be turned into real-world implementation:

“Cloud-based implementations provide a flexible and readily scalable method for supporting the integration of social networking into e-health service delivery patterns and enabling consumers of health services to become active participants in their care.

This could include participating in communities of people with the same condition, becoming part of their own virtual care team, or simply allowing people to participate in the scheduling of their own appointments or review of results."

This last point highlights that in addition to the e-commerce 1.0 function of providing self-service access to online information, the fundamental design goal of Cloud 2.0 systems is the “peer to peer” model where a key aspect of how citizen value is achieved is that it is provided by another citizen.

In the same way the Peer 2 Patent portal expanded both the capacity and quality of how many patents could be processed, by opening up the workflow to a community outside the patent office, so the same effect can be applied to any public sector service the same way with the same benefits.

Kansas - Cloud-Powered Participative Democracy

The ultimate conclusion to how this transformation can be applied to government processes is demonstrated by the State of Kansas.

We showcased this case study for one of our Open Government webinars, where Sean McGrath of Propylon described how their technology had been used to apply this effect to the Kansas legislature, in his presentation ‘Re-inventing Participative Democracy, One Cloud At A Time’.

As described in Propylon’s own case study Kansas was experiencing the same issues that the Patent Office was, but for their law making procedures, and so they used a Cloud-based application to re-invent it to achieve a similar Peer to Patent transformation for how this works.
Social Impact Cloud Computing – Open sourcing best practices

This powerful transformation of how government works can be applied universally and offers considerable potential in areas where progress is especially difficult if being made at all.

‘Social Impact Cloud Computing’ is the view of the technology trend that links it to social innovation related policies, and by using open source software governments can share these best practices with others to do the same.

For example the Hackney CAB Crowd Map is a grass roots level project that uses an innovative web site to help draw attention to social housing issues in this part of London. This shows how social media tools can be used to better organize and share information to achieve helpful new business models, and it is achieved via simple and entirely free open source software. This means that it can be easily shared and run anywhere globally via the Cloud.

BPaaS – Standardizing shared best practices

What this also highlights is the potential to achieve much larger scale of social transformation by leveraging even more powerful software, and the new IT outsourcing models that can make this possible.

For example the Province of Ontario is using Microsoft Sharepoint FAST Search software to power a 'Service Location Finder', a search engine capability that can match a request for 'Drivers Licence' to nearby offices that provide this service.

One central installation of FAST software is configured to provide multiple service finders to different departments, an approach known as BPaaS – Business Process as a Service.

No Wrong Door - Critically this helps unify information from across multiple different agencies, making online service quicker and easier for citizens. A ‘No Wrong Door’ policy means that a citizen can search on any one of these different sites, but will always get a consistent answer then and there, not be shuttled between departments.

For example searching for Drivers Licence on any number of different sites will link them to the relevant services such as applications, renewals and related processes that are spread across multiple sites. This type of capability can be made more easily accessible to other projects via this model.
Section II - Cloud Migration Management

Moving applications into this new Cloud model is a best practice we describe as ‘Cloud Migration Management.’

Cloud First – Portfolio Migration

This process was first headlined by the USA Government, the high profile focus led by the CIO at the time, Vivek Kundra.

Vivek sparked the GovCloud industry by proclaiming agencies would be mandated to adopt a 'Cloud First' policy, documented in a 25 point plan to reform federal IT spending, to deliver better Business Value to the American public for their $80 billion a year spending.

However as you might imagine this is by no means a simple exercise and is where the heart of the challenges for the CIO can be seen, in terms of achieving the Cloud First requirements. The issues that needs addressed were recently identified through an auditors analysis of the progress of the Cloud First program.

In the GAO report Progress Made but Future Cloud Computing Efforts Should Be Better Planned (26-page PDF) they reported that despite the hype about this pioneering initiative, the practical reality is that it has presented a number of tough challenges for the agencies to achieve the goals.

They identify that many of the submitted plans are missing key component parts, like estimated costs for the service, and major milestones and performance goals. Only one of the plans has the full set.

"all but 1 of the 20 plans submitted to OMB were missing one or more key required elements. In its 25-Point Plan, OMB required agencies to prepare a plan for implementing each cloud-based service and retiring the associated legacy system."

These challenges therefore describe the component parts of CMM, the services needed to effectively handle the full migration, with the fundamental value being:

- **Best practices knowledge and expertise** - Many government IT workers have little to no experience of Cloud systems, which requires them to learn a whole set of new tools and procedures, and furthermore found the NIST Cloud models initially confusing.
• **Project Portfolio Management** - PPM provides the skills and tools to better manage a portfolio of transformation projects like this - It can address the need to manage costings, state milestones and business benefits.

• **Certifying and accrediting vendors** - Agencies have no mechanisms to know who is appropriately approved to host government apps. Standards bodies like OASIS are defining frameworks for this requirement.

• **Data portability and interoperability** - Ensure the ability to smoothly exit and move between Cloud providers. Again standards bodies like OASIS are developing protocols like CAMP and TOSCA to meet this need.

Through this mix of skills, tools and standards, and within an overall ROI context of business transformation, CIOs can be empowered to leverage the Cloud to drive visible organizational benefit and cost reductions across their entire IT estate.

**Cloud PMO – Buying IT as a Service**

One of the first areas that presents challenges for newcomers to the Cloud field is actually the procurement rather than the technical aspects of using Cloud services. Many IT departments are built around buying hardware and software, installing and configuring IT, not ‘ITaaS’ – IT as a Service.

In their recent white paper Cisco describes this effect in detail. [Enabling IT as a Service](#) (11-page PDF) provides an executive overview of the ability to buy your technology in the form of a utility service.

For insights into the practical implementation of how one agency has tackled these challenges the case study for the state of Michigan is very helpful. Read our short review of this case study in ‘[Make MiCloud Your Cloud](#)’ to see how Michigan mastered the use of Cloud Computing and delivered the following transformation benefits:

• **Service Delivery Improvement**: As part of the review process, Michigan targets functions with cumbersome ordering processes and long fulfillment times for cloud transformation opportunities. Since clients value more granular delivery options, Michigan reviews opportunities to break up complex tiers into simpler options that may be managed and delivered by separate means.

• **Cloud Sourcing Cost Reduction**: Migrating commodity ICT functions, like messaging, to outsourcing providers. Government is under fierce pressure to
reduce staff, capital and operating budgets, and Michigan leverages Cloud services where appropriate to drive down IT costs. In categories like storage they have delivered options at 90% cheaper rates. Migrating commodity ICT functions, like messaging, to outsourcing providers, to free up staff to work on higher level activities that add real value. Not only does this reduce cost but it meets their need to provide staff with more innovative and challenging work.

- **Compliance and controls**: They have eliminated “rogue sourcing”, where consumers go around the IT department to order Cloud applications like Google directly, by offering their own in-house alternatives for lower costs, and through rapid, self-service tools. This improves cost-controls and reduces IM risk.

- **User empowerment**: Through self-service catalogues and Process Automation tools they are empowering users to embrace and benefit from IT without their direct involvement, to free up staff to work on higher level activities that add real value. Not only does this reduce cost but it meets their need to provide staff with more innovative and challenging work.

- **Process transformation**: A process orchestrator function that enables business users, regardless of ICT skill level, to create process definitions which are published to the service catalogue. This serves as a foundation for process transformation.

- **Green IT**: Reducing the carbon footprint through closing many 'coal-fired' data-centres and consolidating around a smaller number of more modern, Green-energy environments.

**Procurement Frameworks: Enabling Trusted Cloud Providers**

In addition to these best practices for individual IT departments to follow, central shared service units can also establish broader procurement frameworks for wholesale ITaaS across the organization. A high profile example is the UK’s [G-Cloud program](https://www.gov.uk/government/programmes/g-cloud).

These programs cater for two primary functions:

- **Assessment and Certification**: Providers are audited to ensure compliance with procurement and technical policies.

- **Services Catalogue**: “Apps stores” of supplier services.
These frameworks are the backbone to Cloud transformation initiatives, as they enable a ‘approve once, use many’ approach to ICT procurement.

In short the key area where governments experience considerable inefficiency is not in the technologies themselves but rather in their procurement and project management, the organizational structures and procedures. Here there is considerable complexity that forms an expensive overhead of time and cost that greatly slows the ‘rate of innovation throughput’ that IT departments can deliver.

This refers to how much and how quickly IT units can respond to the needs and requests of the end-user business departments they support. Typically this is via detailed requirements analysis projects that output RFP procurements and then procurement implementations. End-to-end this can take months and years, cost millions and on many occasions fail entirely; the net result is very slow, very poor innovation throughput.

In contrast the apps store approach enables this to be avoided, putting self-service IT into the hands of the end-users at the coal face, and where it can be continually improved through a process and system of sharing best practices. For example imagine the earlier case study of the Hackney CAB scenario was uploaded so that other social housing projects could simply reuse it straight off the shelf.

Not only does this improve service delivery for agency buyers, but it also acts as an economic stimulus, enabling more small businesses to participate in Government procurement. (Read more in issue one of our TRANSFORM e-magazine, which focuses on this innovation-enabling aspect of the G-Cloud program).

**Apps Store – Open sourcing best practices**

Establishing an Apps Store is achieved through contracted Cloud Providers populating a catalogue with their service offerings for agencies to buy via this framework agreement, and can provide the ideal way for IT teams to proactively meet the needs of their users.

For example the GSA Cloud First review document also lists all of the apps that the various agencies plan to migrate, which therefore lines up a set of services for Cloud Providers to adopt and make available, so that migration services have target environments to move the retired functions to. This included:

- Email
- Sharepoint
- CRM
- Grants Management
• Correspondence Tracking
• Audit Resolution
• Web Site Hosting
• BPM Document Management
• Electronic Library
• Offsite Vaulting
• Program Management

Similarly in the Canada Health Infoway Cloud strategy the document lays out a suite of new EHealth applications they plan to procure via a SaaS approach.

**Cloud Provider Assurance**

For governments the security and privacy of data is of paramount importance, and so the second required foundation is a program to audit and Cloud providers and certify that they are implementing the required standards for information security.

There are numerous standards to consider, ranging from the global bodies such as ISO through to national initiatives, such as CIO.gov publishing recommendations for US agencies: “**Best Practices for Acquiring IT as a Service**” (44-page PDF)

This describes their recommendations for a number of building blocks that provide the foundation for safe Cloud Computing in the public sector, such as:

• Contracting and billing
• FedRAMP Security
• IDaaS standards – Identity as a Service
• Privacy and Compliance
• Data Location
• E-Discovery and FOIA access

These are still general enough to be considered best practices for any public sector body and so can be reused to support implementations elsewhere.

Organizations such as the [Cloud Security Alliance](https://cloudsecurityalliance.org) stipulate a menu of technical security practices that can be implemented to achieve this level of information compliance requirement.

As an example of how these types of steps can be implemented by a Cloud Provider this [Amazon white paper](https://aws.amazon.com) (24 page PDF) describes their mix of technologies and procedures they implement to achieve this.
Cloud Providers should be able to provide details on security controls, specifically as they relate to hosted VMs. Key security concerns around privacy, compliance, segregation of VMs in public clouds (inter-VM security risks such as hypervisor breach or vulnerabilities), and interoperability and litigation hold should be addressed in the SLA.

**Cloud Service Brokerage**

Furthermore, the supplier landscape will evolve such that ITaaS will become available from ‘Cloud Service Brokers’.

As [Gartner explains](#) a Cloud Service Broker creates an e-marketplace of Cloud services, bringing efficiencies to buyers who can access an aggregated community of suppliers, with automated Cloud management processes implemented across them.

CSBs help drive IT efficiencies through features such as:

- Aggregating a catalogue of many 000’s of applications and IaaS.
- Technical integration across their application suite, such as Identity single sign-on for secure user access across all of them, achieving compliance.
- Ordering automation, IT administration and reporting features to better manage utilization.

Automation of IT administration is the key process to leverage to drive cost efficiencies through Cloud Computing, and the CSB model extends this across multiple providers to create a marketplace of services to automate this way.

[Gravitant](#), one of the early startups pioneering this trend, offer a case study that documents lessons learned from their pilot work with the State of Texas ([13 page PDF](#)).

Implementing the Texas Cloud Self-Service Portal they established:

- What applications are suitable for Cloud hosting and which aren’t
- Agility and diversity – How the CSB model is ideal for accelerating deployment of projects needing to be up and running quickly, like a mobile voting portal
- Standardizing the complexity of the multitude of different supplier service options
- Cost control – Harnessing these benefits to better control IT costs

**Cloud Portability & Open standards – TOSCA**

A key technical architecture that will yield both IT and business benefit is ‘Cloud Portability’, the ability to easily move applications between different underlying IaaS providers.
Being able to ‘shop around’ will drive down costs across suppliers, and also enable improved resilience and performance, where applications can be easily moved in the event of emergency or slowing capacity.

Open standards are essential to this interoperability, highlighting early initiatives such as the OASIS TOSCA standard.

TOSCA is important to government organizations because governments are likely to rely on many different vendors in the private sector to provide cloud platforms for strategic government services. The requirements and preferred providers will no-doubt change over time, as evolving regulatory and business issues change, however a constant for cloud services will be "no vendor lock-in," driven by standards for portability and lifecycle management such as TOSCA. In particular, TOSCA’s applicability to challenges such as deployment and other lifecycle stages such as scaling, patching, etc. across all services models such as IaaS, PaaS, and SaaS will be foundational.

The portable, declarative descriptions of a service enabled by TOSCA will become even more important as the number of cloud vendors and offered services increases and those providers increase in their diversification advanced capabilities because services will be able to be deployed in a fashion that takes optimal advantage of those advanced platform capabilities, rather than just supporting a lowest-common denominator.

Lastly, TOSCA will also enable easier deployment, failover, and lifecycle management of mission-critical services, such as for disaster response, national defense and other government services.

**GovCloud Hubs**

There are different variations of the CSB model possible, where it can be either supply or buyer-driven, meaning it is a very fertile area for innovative new e-market scenarios, such as:

- **End-user IT organizations** – A large organization can deploy a CSB platform to automate their own internal Private Cloud resources, and then also to source resources from external providers.

- **GovCloud Hubs** – A specific industry example of this effect is the concept of ‘GovCloud Hubs’, Cloud computing e-markets for the public sector by the public sector.
As described on ReadWriteWeb "Government Cloud Hubs" are where different levels of Government collaborate to maximize cost-savings for taxpayers, such as municipalities buying from ‘upstream’ State-level providers.

This model offers yet more potential for addressing inefficiency issues that government experiences at the organizational and process level, most notably those associated with how IT budgets are defined and rolled down through organizational hierarchies.

In short some departments receive too much funding, but knowing they have to spend it to keep it they therefore spend on excessive hardware and other technologies that largely go unused, whereas others receive too little, and struggle to meet the demands of their citizens due to inefficient scale.

The ReadWrite article is a great example – Small municipalities still have a relatively equal demand for IT but are too small to have the skills or resources required for a minimum level of IT capability, whereas the province or state they are within often has considerable levels of resources.

The Cloud Brokerage model would offer a new model for more efficiently matching demand to budgeted resources that would address these types of issues.
Section III - Enterprise Architecture

To support this portfolio transformation agencies will require an enterprise-wide IT architecture, comprising foundations such as:

- Shared service Cloud models
- Web oriented architecture
- Cloud Identity Ecosystem

Federal Government Cloud – Shared Services Architecture

The GSA defines this overall best practices framework for implementing Federal Government Cloud Computing. In this Vision and Strategy presentation they set out the overall designs for setting up design and procurement of GovCloud services, including industry governance models and this headline technical design blueprint.

See this image fully expanded here.

GC Community Cloud – Platform for Shared Services Canada

Similarly in June 2010 the Canadian Federal Government Public Works CIO described their GC Community Cloud program, in this 18 page PDF presentation.

It describes a roadmap plan for their adoption of Cloud Computing, acting as a template blueprint for an overall enterprise architecture and strategy for Cloud computing.
It provides a framework that builds on the NIST foundation of the Community Cloud design, and identifies how it can be localized to the Canadian IT estate, defining a taxonomy including:

- **Private and Community Clouds**: A multi-tenant application environment for their breadth of enterprise applications, like Oracle, SAP and Microsoft, used for their core business processes like PAY, and also their common IT requirements, like email and collaboration.

- **Platform as a Service**: Database Solutions, Virtual Firewalls, Process Automation, Cloud Provisioning Services, Cloud Peering, Virtual Storage Service, Virtual Compute Service.

- **Virtual Office**: A set of shared applications for automating modern office working including Cloud Desktop, Document Management, Web 2.0 collaboration both internally with staff & partners, and externally with citizens via a multitude of social media channels.

- **Network and security architectures**: A logical architecture for segregating 'Cloud Security Zones', linking each Cloud area (IaaS, PaaS, SaaS) to a security infrastructure component, and describing how the computing environments will be integrated with their wide area networks and access control systems, through a Cloud Services Access Layer and a Cloud Peering Layer.

This model is discussed in detail in our white paper [Government Community Cloud](#) (22-page PDF). This covers:

- Case studies and best practices in Government Cloud Computing
- Moving to Agile practices through DevOps and PaaS
- Open Data innovations
- Migrating legacy environments like Lotus Notes
- Cloud Security Model
- Data interoperability across multiple providers
Web Oriented Architecture

As highlighted earlier in this document these shared computing environments are only part of the equation. They certainly do improve the cost efficiency of IT, however they don`t enable a transformation of the business process itself, so the visible benefits to the organization are minimal.

Instead achieving this impact requires a new approach for the data and user models too, one that can be described as a ‘Web Oriented Architecture’ (WOA).

This is an evolution of the SOA (Service Oriented Architecture), which keeps the same architectural principles but expands the scope to a larger ecosystem that reflects the exploding social media world we now live in, encompassing facets such as:

- RESTful integration methods
- Open Data
- Semantic Web and Linked Data
- Federated Identity

This combination yields a greatly increased capability for secure information sharing across different agency systems.

An example of where and how this can applied is described in the Canada Health Infoway Cloud Computing in Health strategy document.

This provides a reference model for important aspects of a Cloud strategy, especially for Healthcare but also in a broader sense.

In particular it provides a focus for defining 'Cloud SOA', the intersection of Cloud computing and the SOA.

The document builds on the NIST Cloud Computing foundations of the service models like IaaS (Infrastructure as a Service) and PaaS (Platform as a Service), and describes how these can be combined with the SOA to accelerate deployment of E-Health systems:

"This could include establishing cloud implementations to service common software applications used by multiple facilities in a region or jurisdiction, provisioning EMR and CIS application capabilities through cloud. In addition, jurisdictions may wish to deploy multiple HIALs, or they may wish to improve scaling and extensibility of a single HIAL
through virtualization of services. The SOA upon which the Blueprint for EHR solutions is based is well suited to transition to a cloud-based IT model.”

That's a very powerful and very explicit linkage between the primary value of Cloud migrations and the recommended EHR standards that CHI sets for EHealth across all of Canada.

**Open Data**

Governments, and now also Healthcare organizations, are increasingly publishing their data in an open and reusable format, 'Open Data', referring to the use of licences that frees the information to be used by developers in new applications.

This has spawned an extensive spectrum of innovative new applications and models for developing them, increasingly being adopted in the public sector. For example as this [press release describes](#) the NHS are replacing their Secondary Use System with an Open Data platform.

These developments are part of a broader evolution of the Cloud as a universal 'programmable web'.

---

"Options to make enterprise data more open, consumable, and Web-like"
Cloud Identity Ecosystem

One of the keystone foundations of Web Oriented Architecture is the emerging “Cloud Identity Ecosystem”.

The Identity Ecosystem is a term coined by the USA Government and their NSTIC ‘Trusted Identities in Cyberspace’ program. It refers to the futuristic environment that will be created through ‘federated identity’ being used better interconnect previously isolated systems, which they describe as:

"a user-centric online environment, a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value. Key attributes of the Identity Ecosystem include privacy, convenience, efficiency, ease-of-use, security, confidence, innovation, and choice."

The term Cloud Identity Ecosystem then refers to the combination of i) the role Cloud Providers will play in implementing this system, and also (ii) how the Identity Ecosystem will enable the evolution of 'the Cloud' itself, as a singular data sharing Internet environment rather than just individual Cloud services like Amazon.

Federated Identity – Foundation for Transformational Digital Government

As the name suggests this is an evolution based on the foundation of systems used for Identity Management, those that are used to streamline the username & password procedures for accessing applications, that now encompass Cloud resources as well.

For example as this NASA press release explains their Identity security technologies enabled their move to Google apps, providing staff with new collaboration apps while also ensuring compliance with the USA Government ID Management standards.

By securing the user authentication process to Cloud apps like Google they are putting in place one key foundation for ensuring ultra-robust Cloud Security, demonstrating one part of the relationship between the Cloud and Identity Management.

This is only the starting point of the benefits, as once previously isolated applications are connected at this Identity level then it opens up a gateway for the flow of personal information, engendering the Identity Ecosystem.
The Ecosystem will provide a keystone foundation for Digital Government.

As introduced at the beginning of this paper we defined one of the differences of Cloud 2.0 vs first generation e-commerce being multiple back-end systems, united together via this Identity federation approach.

Government services are a great demonstration of the value of this approach, as multiple agencies must exchange a variety of citizen information like births, deaths and other events to be able to fulfil their own individual processes, much of which happens via manual, expensive paper-based methods.

The UK Government calls these ‘Trusteed Transactions’, and have taken steps such as joining the OIX to implement the required interchange open standards.

As they explain this means a community of participants adopting the same standards for sharing Identity data in a common and secure manner, so that transactions like smartphone e-commerce can be easier and quicker, while also more secure.

It is a trend also being pioneered in Canada. As described in this press release the Canadian Government selected SecureKey for the first building blocks of federated identity methods, where government users can sign in to web sites via login credentials provided to other organizations, such as banks.

The Government of Canada has also published best practice white papers on this topic, including Federated Identity Management in the Government of Canada and Trusting Identities, the IMSC Pan-Canadian Approach, which includes an Assurance Model.

They also describe the role these will play in Trusted Transactions, publishing Going Digital: Transitioning to Online Payments.
The role these integrated Identity systems will play in transforming government service models is defined in the [OASIS TGF](https://www.oasis-open.org/committees/tgf/) (Transformational Government Framework), where they describe:

- "Have a business architecture based on federation between a wide range of trusted organizations (the Government, banks, employers etc.), and a clear model for cross-trust between these organizations.

- Use a supporting technology architecture which does not rely on monolithic and potentially vulnerable large databases but which, in line with the SOA paradigm, uses Internet-based gateway services to act as a broker between the different databases and IT systems of participants in the federated trust model.

- Put people directly in control of their own data, able to manage their own relationship with government - whether on their own behalf as individual citizens or in another identity relationship or intermediate role - and with clearly visible controls to reassure them that this is the case."

The academic sector has long been a pioneer of federated identity systems. By developing the [Shibboleth](https://www.shib.org) framework they enabled federations like InCommon, which works to link Identity Providers with service providers. As they explain "Federated Identity management is the practice of using identifying credentials in one domain or organization to access assets in a different domain or organization."

This combination provides a foundation for integrated digital commerce across this community of users and service providers, where they describe:

*For example, in 2006, the University of California Office of the President implemented UCTrust. By having the individual institutions of the University of California system join InCommon, the University of California system office could deploy, across the entire system, an application that provided employees with access to retirement information. Also in 2006, the Virtual Library of Virginia (VIVA) licensed content from the Public Broadcasting System (PBS) and used these three elements to support distribution to close to 400,000 students.*

**IDaaS – “Real Me-as-a-Service”**

Governments will be able to implement these systems in-house, or like any other application, outsource them to a Cloud provider, a model known as `IDaaS` - Identity-as-a-Service.
IDaaS refers to implementing these Identity Management capabilities as a hosted service, that can be tailored for the unique compliance requirements of different industries.

For example in 2011 Verizon launched a service compliant to Level 3 of the USA Government requirements, and that this Cloud model offers a cost model 20-70% cheaper than trying to run it in-house. As explained in this NextGov article this enables agencies to implement important Identity life-cycle processes, like certifying online identities. (Learn more in this presentation).

Obtaining compliance with the USA Governments Level 3 requirement is achieved through certification by a ‘Trust Framework Provider’, such as Cloud Identity standards organizations like the Kantara Initiative.

Kantara provides a certification framework to assess and approve IDaaS implementations against these government requirements, and also helps organize the required technical innovations.

For example this includes a telco working group which focuses on extending federated identity systems across mobile and other telco networks. For example this white paper Bridging IMS and Internet Identity describes how integration can be achieved between open Internet identity standards like OpenID, with the proprietary ones of cell phone networks like IMSI.

When used in conjunction with the same mechanisms on Cloud hosted applications, then an end-to-end Trusted Transaction model is possible, ideal for the new mobile applications that the Digital Government initiative is seeking.

Being able to offer secured identities as a service will open up a whole range of new and innovative ways where they can be used as a building block for new services.

The role and value of these trusted transactions can be seen by the problems they will solve, and how they will solve them.

For example in the GAO document GAO-12-893: Drivers Licence Security, they report on the Identity security weaknesses associated with the issuing of Drivers Licences, given the central role they play in establishing and proving identity for individuals in a wide variety of business processes.
This review includes a focus on the REAL ID Act, a framework intended to help address this weakness in the systems of government process, as the central root factor is the ability to assure a person’s identity is who they say are.

This highlights the role and value of federated identity, as a suitable example to show in action in response is called the ‘Real Me’ service, being pioneered by the New Zealand government.

Developed in conjunction with their national postal service they have deployed a novel service for online identity authentication and related access, with over 40 different government service providers unified into delivery for half a million users.

This implements an 'iCMS' - Extended Authentication Consent Management Service, that utilizes a security token service based on WS-Trust Messaging and SAML tokens, Identity open standards from OASIS, enabling:

- Pseudonymous Authentication, via 'federated sharing tags'
- Two-factor authentication through text message to cell phone
- Verified Data - A secure, privacy-centric data exchange
- A clear consent model - An extensible data across multiple providers
- Government Cloud attribute provider: Drivers licence information

These trends will have uniquely dramatic changes to how software architecture is designed and implements, as 'Cloud SOA' will emerge by utilizing this plumbing, features the NZL Government have designed such as a "privacy domain bus" for managing exchanges of data between applications.

This core design can be reused universally by other agencies for the same purposes.

For example on page 29 of the Canada Health Infoway Cloud computing strategy document they describe the need for a SaaS option for this same Consent Management function.

With these standardized authentications as part of a Cloud environment developers will be enabled to create a higher order class of application, a ‘government approved’ secure SaaS, which could incorporate features like age verification at point of sale, voice identification via telephone, mobile e-commerce and other Trusted Transaction scenarios.
Conclusion – Always On Digital Government

Cloud Computing represents far more than simply “lifting and shifting” existing applications from an internal data centre to an external one, and enjoying some degree of cost efficiency on the underlying hardware.

Instead the trend represents a number of major evolutions of how software is deployed and used to deliver business processes, and how those processes themselves can be transformed to harness a new world of collaborative social media.

This abstraction of software away from a single unit of underlying hardware, brings with it multiple levels of benefit including also significant improvement in associated high availability.

The availability weaknesses of the traditional approach of locating systems in a single data centre were highlighted by this outage in Calgary.

The impact was severe, knocking out a variety of important government systems and preventing a number of critical healthcare treatments, emphasizing just how critical it is for the public sector to achieve 24x7 availability.

In our white paper Always On Digital Government, we describe how technology from ZeroNines can achieve this through a “Multi-Cloud architecture”, where applications run across multiple data centres not just one.

This concludes the paper, where we can see the major characteristics that define GovCloud 2.0 are the socialization of legacy applications, and in a form that operates across multiple Clouds achieving always on Digital Government.

About the Author


Connect on Linkedin or send an email.

Tune into our regular schedule of GovCloud webinars.