

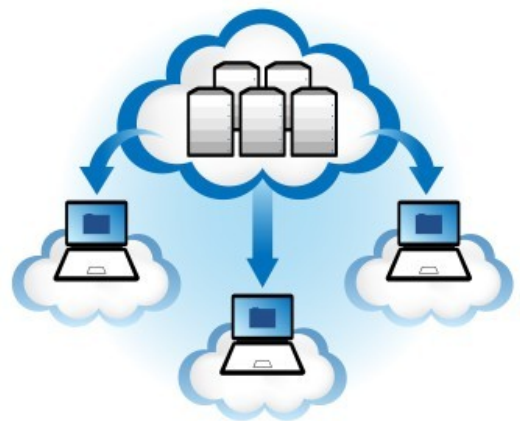
# Government Community Cloud

Driving cost reduction through Shared Service  
Cloud Centres

A Government Community Cloud is an implementation of the NIST Cloud reference model '[Community Cloud](#)', applied specifically within the public sector.

It's a technology program that is ideal to underpin cost-cutting initiatives, in particular establishing [Shared Service](#) organizations, as the fundamental purpose is to provide a platform which makes sharing IT infrastructure easier between multiple organizations, for reasons of creating cost and other efficiencies.

<http://GovernmentCommunityCloud.com>



## Executive Summary

The Canadian Federal Government [recently announced](#) plans to create a single IT department ‘Shared Services’ that will save \$100-200m a year through consolidation-driven efficiencies. As highlighted in this [fact sheet](#) there is lots of ‘low hanging fruit’ for cost savings due to a spread of many different email systems, networks and data-centres.

Huge cost savings will be achieved through standardizing on single systems for functions like email, and by reducing the number of data-centres from over 300 to less than 20.

Cloud computing, specifically the Community Cloud model, is a key design architecture for achieving these goals.



## Problem statement

The first painful irony to understand is that the fragmentation that needs joined up is actually man-made.

Like most large organizations Governments are organized hierarchically, with different departments for each of their main functions, like Education, Welfare, Tourism and so on, and the head of each department, the Deputy Minister, is directly responsible for the privacy and security controls of the information they process.

This means that typically each operates as a ringfenced ‘fiefdom’, because the simplest and most absolute method of achieving this information security is simply to purchase and operate your own IT estate: You buy your own servers and business applications and keep them entirely separate from any others.

Yes this does provide the means for the Minister to ensure their data privacy compliance, but it comes at a very high price – **For the taxpayer.**

This provides a local solution to their own needs but creates two key global issues: 1) A huge amount of under-utilized IT server hardware, meaning highly inefficient use of taxpayers monies, and 2) a lack of ‘joined up working’ across agencies, resulting in poor customer service for citizens.

- **Under-utilization expense** - The current TCO (Total Cost of Ownership) of just one cabinet of servers includes \$200k capital cost and another \$200k in operating costs for cooling and HR. Considering utilization rates can be as low as 5-15% that’s over \$300k in wasted monies, **per rack**. In Canada the Federal Government operates over 300 data-centres meaning thousands of racks, so the scale of waste is quite staggering.
- **Multiple layers of disjointed Government** - There is further fracturing because most governments are then further delineated by Municipal, Provincial and Federal levels of bureaucracy. Each then operates its own data-centres, IT organizations, .... etc., multiplying this cost another magnitude.
- **Application complexity** - There are hundreds of different business applications being used in this mix, meaning customer identify and other data is equally duplicated thousands of times creating yet more cost-inducing complexity.

# Government Cloud Computing

Cloud computing will be the technology that's key to the success of this initiative. It provides the means to reduce data-centres and consolidate applications this way, and Canada is following the lead of the USA where this same approach is being proven successful.

Under the leadership of Vivek Kundra the USA launched a 'Cloud-first' procurement policy to lead their own efficiency drive, under the umbrella of President Obama's overall [Campaign to Cut Waste](#). This was detailed in a '[25-Point Implementation Plan](#)' (40-page PDF).

They're achieving great progress. As highlighted in [this Whitehouse update](#) they're already closing many data-centres and are on track to save \$ 3 BILLION of taxpayer monies. This [recent survey](#) by NetApp reported American CIO's have already reduced data center counts by 31% and saved 20% of their IT budgets based on consolidation thus far.

## 5-Point Cloud Consolidation Plan



Cloud Computing is the key mechanic for a shared service initiative because in simple terms it is literally a technology for enabling shared services – It provides the means for many different organizations to share the same infrastructure, for purposes of IT and cost efficiencies.

CIO's can leverage Cloud computing to quickly drive cost savings in 5 key impact areas:

- **Infrastructure consolidation** - As the Whitehouse news report highlights the principle challenge is that these vast numbers of data-centres typically only operate at hardware utilization levels as low as 25%, but they still consume all the associated real-estate and power costs. This means that as much as 75% of these costs is wasteful spending, and can be eliminated by migrating the applications to Cloud computing which manages utilization much more efficiently. By doing so many of these data-centres can then be closed.
- **Application maintenance costs** - Migrating older applications from their coal-fired hardware on to new Cloud platforms is known as 'Legacy Modernization', and it reduces costs in many ways. In addition to the above physical consolidation it can also reduce the staff costs associated with maintaining the applications in these older environments, one of the biggest costs. Migrating many applications into a single Cloud environment reduces the overall support burden for all of them.
- **Shared Services Architecture** - These new approaches to designing how applications work in these new environments offers further IT efficiencies. Indeed the 'Community Cloud' model is key because it is literally a 'Shared Services architecture', meaning that rather than having many agencies each run a separate and different instance of their own application for the same purpose, they can all instead reuse the same code base. This reduces software costs even further.
- **SaaS contract consolidation** - This approach offers an equivalent, very simple and very powerful commercial model. The Government of Canada will find that they have multiple different software licence agreements, with vendors like Microsoft, and by consolidating these all into one will be able to negotiate bigger overall discounts and lower the associated administration costs. Furthermore by moving to Cloud systems they can leverage SaaS contract approaches, which streamline costs into a per-seat, utility model.

- **Integrated Service Delivery** - Costs also arise due to other complexities in the IT environment. Every domain like servers, storage, applications and networks each has their own management systems, help desk and support teams, and furthermore even different suppliers each have their own web portals for managing their services. This multitude of service management systems not only creates unnecessary costs but also causes the complexities which hamper quick and efficient service.

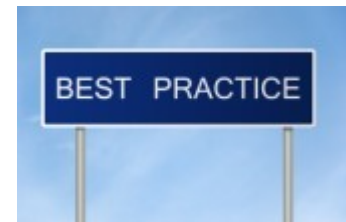
In short as large organizations grow over many years they inevitably accumulate excess and unnecessary capacities in a variety of areas.

Utilizing Cloud computing and best practices like [ITIL](#) to create Shared Service Centres leverages modern technology to achieve the large-scale consolidation required to trim these inefficiencies, simplifying and standardizing processes across infrastructure support areas, reducing costs, raising efficiency and responsiveness, and increases elasticity to handle future changes.

## Make MiCloud Your Cloud

A headline example of how these business benefits are being achieved is demonstrated by the State of Michigan.

Their '[MiCloud](#)' strategy is a comprehensive framework for adoption of Cloud Computing by a government agency for purposes of Service Delivery Transformation, one that can act as a best practice blueprint for others to emulate.



They define their own role as a full-service solution provider for their clients, and handle all the supplier negotiations and in a manner that enables cross-provider switching and avoids vendor lock-in.

Ultimately this is enabling them to transform the role of IT and how they deliver services, headlined by a punchy theme: *“The Cloud Computing paradigm says “The client can have something simple, proven and cheap immediately, or they can have something complex, unproven and expensive in six months.”*

Michigan sets themselves a top-level priority of **securing tangible benefits for citizens and businesses**, achieved through a number of specific business transformation benefits:

- **Imperative to maximize efficiency** - Government is under fierce pressure to reduce staff, capital and operating budgets. In categories like storage Michigan have delivered options at 90% cheaper rates.
- **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.
- **User empowerment** - Through self-service catalogues and Process Automation tools they are empowering users to embrace and benefit from IT without their direct involvement. 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.
- **Cloud sourcing** - 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.

They offer a 'Cloud Service Catalogue' – A “apps store” that includes virtual servers, storage, and hosting for web, apps and development, as well as a framework for integrating external SaaS applications, building an SOA (Service Oriented Architecture) Enterprise Services bus to integrate the applications.

## UberGlobal - Government Community Cloud provider

At the heart of the MiCloud strategy is the recognition that “*the Cloud Computing paradigm is a startling shift in the thought process behind ICT sourcing methods*”.

Where “*government once saw itself as a unique business domain demanding unique ICT functions and custom solution, but now these business processes are converging with those of industry. Workflows such as staff recruiting and the ICT functions that support them, are now becoming standardized commodities.*”

They’ve recognized that adding custom software and proprietary COTS applications greatly increases the complexities they have to manage, and so commodity ICT via the Cloud acts to reduce this, adapting common IT services to the needs of government.

Through a framework of Cloud sourcing methods like RFP and policy templates, what they call ‘MiDeal’, they are also acting as a Cloud Service Provider: Enabling other units of government to purchase using their contracts and maximize the cost savings that all parties enjoy.

An example of how this model of a Cloud Services Catalogue for internal and external commodity IT sourcing is detailed in [this 12-page PDF](#) from Australian Cloud provider [UberGlobal](#), which acts as a blueprint for how they have built a Federal Government Community Cloud service using [Parallels technology](#), which offers:

- A secured environment capable of hosting high security apps and data
- Implements Software as a Service (SaaS) and Cloud Infrastructure as a Service (IaaS) in line with NIST Definitions of Cloud Computing (SP 800-145).
- Offers a catalog of services like the Microsoft app suite, VMware based Virtual Dedicated Servers (VDS), and Cloud backup for workstations and laptops amongst others. They also include managed instances of open source applications, such as Drupal, Moodle and WordPress.

Over the next few release points Uber will add the remainder of the Microsoft Business Productivity Online Services Standard Suite (BPOS), including Microsoft Lync and Dynamics CRM. These products will generally be billed per month per seat or instance, with the ability to add or remove products at any time.

Additionally, the use of CDI and a separate instance of Active Directory and BPOS can allow a lead agency to achieve the benefits of cloud services while maintaining a unified identity management schema between its internal and cloud based applications.

As highlighted a key feature of a Government Community Cloud is an ‘Apps Store’ – A catalogue of new applications that the Cloud platform can run, and by using Parallels UberGlobal are implementing the [APS initiative](#). This is the type of technology ideal for [Sharing Cloud Best Practices](#).

This packages a number of popular applications for deployment via platforms like Parallels, who via their partnership with Microsoft have a particular specialism in delivering the MS suite, like Lync, Sharepoint and Dynamics, and tailoring these for specific Community Cloud scenarios, like the [Health Community Cloud Automation Partnership](#).

Importantly UberGlobal have aligned this platform to the business requirements of the Australian

Government, most notably:

- **Reducing Administrative Burden** - Make IT applications more easily accessible to a wider community of users, through automation which reduces manual workload too.
- **Reduced Cost** Uber's pricing is structured around a price per-seat per-month, resource usage, or licence fee-per-use. Agencies can have the flexibility to scale up or down as demands require, and will not be required to buy or maintain excess capacity.
- **Increased Agility**. Make it quick and easy to provision IaaS and SaaS.
- **Improved Security**. Centralize application management and apply better security practices.
- **Cost Recovery**. Using the reseller system to enable IT departments to act as service providers and cross-charge their 'customers'.

## Government Community Cloud

For very large organizations like Federal Governments they further require an overall strategy and enterprise architecture; one that also encompasses other essential technologies like their WAN (Wide Area Network) and security systems.

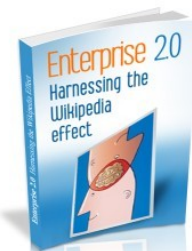


The '[Canada Cloud Roadmap](#)' plan developed by the Canadian Federal Government provides a best practice blueprint for such a requirement.

It provides a framework which builds on the NIST foundation and identifies how it can be applied to the Canadian IT estate, based on a design model with three main sections:

- [Community Cloud](#) Service Offering - 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. This is underpinned by a [Cloud OSS](#) to handle the automation of provisioning, delivery and cross-department billing.
- A [Cloud Security Model](#) - 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.
- An [Enterprise 2.0 Collaboration framework](#) - This technology platform enables staff to utilize a set of Web 2.0 collaboration tools and enable more interaction with the public.

This provides a complete blueprint for an Enterprise Cloud strategy, and specifically for the public sector a complete platform for [Open Government Cloud Computing](#).



## Securing Federated Services

Information security is a critical success factor for widespread adoption of Cloud Computing, and this is primarily addressed through 'Securing Federated Services'.

This refers to securely linking local IT systems with remote data-centres and applications, and is based on utilizing open standards and best practices provided by organizations such as [OASIS](#) and the [Kantara initiative](#).

These open standards are key to interconnecting the mix of in-house and Cloud based systems for identity, security and networks.

For example the Government of Canada is utilizing Kantara for their roll out of an enterprise-wide credential management application. This will provide single sign-on for users to the many enterprise applications they operate, and then Cloud applications too.



## Cloud Security

The ubiquity of software solutions delivered over the internet as services (SaaS) to all manner of end user devices drives a growing demand from users for login simplicity across many sources, commonly referred to as single sign-on. The corollary concern of users is of course protection of privacy when personal and financial data is shared across service suppliers. Those suppliers of services view the same issues from the point-of-view of collaboration with peers and partners in various forms of federated identity assurance.

From the simplest social network application to highly regulated industry sectors there is money to be made, savings and agility to be achieved, and greater utility to be delivered when a collection of service providers (private or public) can join an ecosystem delivering cloud computing services, and even further benefits for cross-service assurance of identity (each others identity as well as that of common users). In the days of castles-and-moat datacenters, CIO's protected their information technology with guards, guns, and glass, and limited network access to locked down networks.

Now factor in cloud computing.

Cloud computing, (private, public, or hybrid) is now the accepted solution for optimizing IT resources by leveraging automation, virtualization, and multi-tenancy. But, with the benefits of new cost models and greater agility come a loss of control and new risk surfaces and vectors.

## Open Standards for Cloud Identity and Security

The Kantara Initiative's Identity Assurance Work Group (IAWG) has defined common ground around the policies and procedures required to create trustable services. This work dovetails with the spreading adoption of the various SaaS delivery models, and the transition to cloud IaaS platform choices across both public and private sectors. To grasp the context and solicitation, see:

1. Guidelines for federated identity services (see [Kantara Federation Operator Guidelines](#)).
2. Identity Assurance Framework Assurance Levels (see [Kantara Identity Assurance Framework v2.0](#)).
3. Assurance Framework Service Assessment Criteria (see [Kantara Identity Assurance Certification Program](#)).

Similarly, the OASIS Standards body has established the [Identity in the Cloud Technical Committee](#). And, the US has formed NSTIC, the [National Strategy for Trusted Identities in Cyberspace](#), and the list of involved organizations, regulators, and governments goes on and on.

International Standards for Assurance Engagements ([ISAE](#)) No. 3402 for third-party reporting for service organizations similarly outlines the process auditors now take to attest to the controls and security measures taken by companies who provide outsourced information technology services.

At the heart of all the evolving solutions are five basic concepts:

- **Frameworks:** Best practices, standards, policies, regulations, and laws establishing how credibility is created and maintained locally as well as in broader federated community.
- **Responsibility:** The organizations and management who are accountable and liable for properly implementing the various frameworks.
- **Platforms:** The software, hardware, networks, and facilities built and purchased by responsible organizations to deliver trusted technology solutions.
- **Accreditation:** The who or what that certifies an entity's compliance at various risk levels of the frameworks.
- **Trust:** Reliance backed by audit, compliance, enforcement, indemnification, insurance, and brand.

No matter how complicated the world of information technology becomes, it always leads back to the CIO and the IT organizations willingness and ability to faithfully implement frameworks, their skillful use of IT platform choices, and prudently awarded credentials. No matter how complicated our high tech society becomes, CIO's cannot outsource accountability.

The fundamental need to build network firewalls around use-case specific sets of applications, geographies, and/or security clearance levels has not changed. It has simply become more fine grained and virtual. More fine grained in the sense that ubiquity of devices, mobility, 3rd party SaaS, and role based access have all made AD and LDAP risk groupings smaller and smaller. Virtual because server hardware is no longer dedicated to applications, rather VMs serving different security realms can reside on the same physical server.

For example, consider a few of the standards from Kantara's Identity Assurance Framework.

**Example:** Kantara CO\_OPN#060 [Secure Remote Communications](#) stipulates:

*“If the specific service components are located remotely from and communicate over a public or unsecured network with other service components or other CSPs it services, the communications must be cryptographically authenticated...”*

This is an example of a key best practice they stipulate, that acts to ensure the safety and integrity of using Cloud-based systems.

Consider an in-house or 3rd party SaaS offering that runs on virtual servers in yet a different 3rd party environment (ex. CIO "A" deploys a CRM service from ISV "B," who in turn runs the service at cloud provider "C").

The best practice: "A" should insist that message traffic is encrypted all the way to the dedicated virtual servers at "C's" remote location. "A" is accountable for message traffic to/from the

topology of virtual server running at "C" location, but "C" is outside of "A's" span of control. If "A's" message traffic is decrypted at "C's" edge router and travels in plain text on "C's" cloud network, "A" has an unprotected liability. Rather the message should be encrypted to the firewall in the virtual machine itself, subsequent traffic between virtual servers in the cloud should also be encrypted, and the end-to-end secure communication should be in the control of "A".

Even when "B" or "C" have provided assurance of compliance with SAS 70 and or ISAE 3402, CIO "A" is accountable for the security of the message, is liable, and has little or no contractual recourse for damages real or implied from either provider (read your contracts). And, of course should data leak or be corrupted the brand of the accountable CIO is likely to be damaged far more than that of the various technology providers. In today's pop culture the fall-out from data breaches, often reach as high as the CEO (e.g. Sony 2011, BoA/Citi - 2011).

Best practices dictate that "A" should require his message traffic is secure using an overlay network with no clear text messages moving over segments shared with other tenants at "B" or "C," or over segments administered by provider staff.

To be accredited, CIO "A" must regularly sign certifications presented to "A's" auditors stating that messages are encrypted and fully within "A's" span of control for the entire trip. Or, the trust ecosystem has to have matured to the point that "A's" liability is eliminated. A Kantara like ecosystem that will pass liability through a trust network is projected, by the US White House, to be more than a few years into the future.

All of this can be summarized in the old adage of, "The security of a chain is only as strong as it's weakest link." In context, "The security of an enterprise network utilizing any semblance of outsourced or hosted environments is only as strong as the protection of the data in transit and data at rest from external and internal threat vectors. All attack surfaces must be protected."

## Vendor profile – CohesiveFT

CohesiveFT's VPN-Cubed® is a virtual 'Overlay Networking' appliance. VPN-Cubed is the first commercial solution which enables customer controlled networking in a cloud, across multiple clouds, and between private infrastructure and the clouds.

VPN-Cubed provides an overlay network that allows control of addressing, topology, protocols, authentication, and particularly encrypted communications for application, data and security infrastructures deployed to virtual and cloud computing environments. When using the cloud messages move into and across internal networks of 3rd party controlled infrastructures, external networks of 3<sup>rd</sup> party controlled infrastructures, as well as brink 'n mortar datacenters many times outsource to 3<sup>rd</sup> party controllers. VPN-Cubed provides completed end to end encryption of these messages in all of these environments.

How does it do this?

VPN-Cubed Managers are virtual appliances deployed in the cloud (any virtualized environment)



and peered together to form a resilient load balanced mesh overlay network. The VPN-Cubed Managers are hybrid devices; they are virtual routers, virtual switches, SSL VPN concentrators, IPsec VPN concentrators,

firewalls, and protocol re-distributors, configurable in a mesh organized in virtual containers, each container providing a specific enterprise or application function. These secure virtual containers can be used to run key business computing topologies that have been moved to a cloud environment, including secure access to and extension of the corporate datacenter. Multiple peered VPN-Cubed Managers across cloud regions and zones offer fault tolerance and can be

used to provision development or operational infrastructures on the fly, eg - allowing "N" identical copies of virtual server topologies to be run simultaneously, these can be identical down to their IP address.

VPN-Cubed can be easily integrated with existing edge and DMZ equipment running standards based security such as IPSec extranet boxes, intrusion prevention, intrusion detection and stateful inspection, VPN-Cubed doesn't require new knowledge or training to implement. Enterprise application topologies can be easily deployed in a controlled global network, accessible by staff, customers and partners alike, all under the application owner's control, all in complete security.

VPN-Cubed is part of CohesiveFT's 'Secure Application Container' allowing you to migrate to/deploy you application to any virtual/cloud infrastructure without the application topology knowing or caring where it is running.

## About the authors

**Neil McEvoy** - Neil McEvoy is the Founder and President of the Cloud Best Practices Network, and inventor of the Enterprise Cloud Business Transformation program. Neil is a Cloud computing entrepreneur, with a 15+ year track record of launching new products and businesses across the spectrum of ASPs, SaaS and Cloud computing trends.

Neil can be reached on [neil.mcevoy@15consulting.net](mailto:neil.mcevoy@15consulting.net)

**Dwight Koop** – Dwight is the COO of CohesiveFT (and was COO of RabbitMQ Services which was recently acquired by VMware). He has 30 years in high tech investment banking and software technology, including senior management with Borland and The Swiss Bank Corp. One of the founders of the Chicago Board Options Exchange (CBOE). Founder of several early stage software tools and cryptography companies.