

Canadian Government Cloud Computing

A Canadian Best Practices Guide to
Implementing Cloud services in the
Canadian Public Sector



An expert guide from the Cloud Best Practices Network

<http://CanadaCloud.info>

Table of Contents

Executive Summary.....	3
Harnessing ITaaS – The CIO's new role.....	3
Sharing best practices.....	3
Building GovCloud Services, Part 1 – Solutions Matrix Model.....	4
Solutions Matrix Model.....	4
Business Use Cases.....	4
GovCloud Best Practices.....	5
Cloud MRM.....	5
Digital Fuel for the 21st Century.....	6
Government Cloud Hubs – Shared Services Cloud Architecture.....	7
PaaS Best Practices : Platform for Hybrid SaaS.....	8
PaaS Catalogue – Standardization.....	8
Hybrid SaaS.....	9
Canadian Cloud Security Best Practices.....	10
PaaS and Cloud Security.....	10
Cloud Identity and Security Best Practices.....	11
Virtualization and Identity Security.....	11
VMware Horizon Application Manager.....	12
Smart Signin.....	12
Business Process Protection.....	13
Conclusion and next actions – Legacy Modernization.....	14
Authors.....	14

Executive Summary

Harnessing ITaaS – The CIO's new role

Recently Cisco published a white paper called [Enabling IT as a Service](#) (11-page PDF), which provided an executive level introduction to the main trends of Cloud Computing and how CIO's can harness them to great effect and summarizing its main business value.

Ultimately they focused on the core value of 'ItaaS' – IT as a Service, highlighting the fundamental shift from fixed, asset-based IT to one that is entirely service-centric, where they describe programs like ITIL have stipulated service processes but this is still based on fixed-asset IT.

Service-oriented IT is literally that, technology that you consume (and then internally supply) as a service. This offers huge benefits that the CIO can generate for the board not least streamlining cash flow requirements, and this new approach goes to the heart of the new transformational role for the CIO, in particular the alignment of IT agility to business process improvement.

“the CIO, who is gradually becoming a broker of IT services with a business-first mentality that guarantees a service will be delivered via the best method possible. In the future, a service could be delivered via IT internally or through an external cloud provider, depending on the needs of the business.”



MaaS – Municipality as a Service

We'll be explaining the effect by focusing on how one level of the public sector, Municipalities, can begin to adopt this new model in our upcoming 'MaaS' webinar.

Register [here](#).

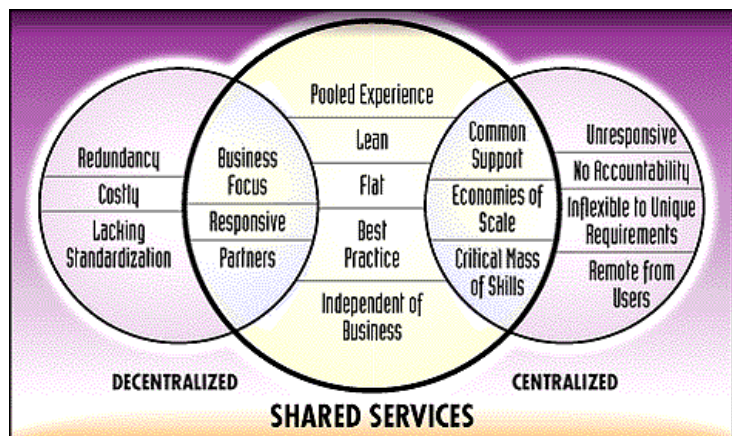
Sharing best practices

A critical feature of Cloud Computing is that it more easily enables sharing of best practices – Through virtualization and templates any configuration of IT can be packaged for re-deployment elsewhere.

This is important as Cisco's white paper highlights that one of the most important critical priorities for CIO's to invest in this new type of technology is '**business process enablement**'.

In short when one CIO masters a new technology and applies it to e-enable a new business process, this can be encoded into a template and made reusable for others to do the same.

Recently the Government announced the Shared Services Canada initiative, which is seeking savings of \$\$ hundreds of millions, through agencies consolidating data-centres, infrastructure and applications.



Our GovCloud program will provide a best practice sharing group to facilitate this.

Building GovCloud Services, Part 1 – Solutions Matrix Model

The objective of this guide is to introduce and explain Cloud Best Practices, as defined by the American standards organization NIST, and how these might be applied in Canada to recreate a Canadian version including aspects like security and privacy policies.

Via their 'GC Community Cloud' program the Canadian Government is defining their localization of these models. You can download the PPT and other materials from [this section](#).



It is also to showcase local expertise and vendor products who are available to enhance and implement these best practices. This provides them the ideal context to explain their innovations and value-add services.

Solutions Matrix Model

Fundamentally the NIST cloud models are based on two key design methods of 'Service Models' (IaaS, PaaS and SaaS) and Deployment Models (Private/Hybrid/Community/Public Cloud).

This makes this matrix of different options possible, that can be used by agencies to determine which specific configuration is correct for them, based on their information security requirements.

		CLOUD SERVICE MODELS		
DEPLOYMENT MODELS		Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)
	Private			
	Community	X	X	
	Public		X	
	Hybrid			

Business Use Cases

Then in addition to this matrix NIST is organizing a catalogue of '[Business Use Cases](#)'.

These package up these combinations and apply them to specific use case scenarios, such as Email hosting, E-Discovery and IT Service Management, amongst others, and are therefore forming a best practices library that other agencies can then reuse for procuring the same services.

The use case states what configuration of Service and Deployment models are needed. For example the E-Discovery scenario says that the service is required on a SaaS basis (Software as a Service) and implemented via a Community Cloud model.

GovCloud Best Practices

One of the most powerful features of Cloud Computing is the ability to share and implement best practices, both in terms of these NIST building blocks but also then how these can be used to implement more specific models, those specific to government.

For example our next webinar is [MaaS – Municipality as a Service](#), which is focused on the municipal level of government, and a best practice program for these folks includes the MRM from the Canadian municipal association ‘[MISA](#)’.

Cloud MRM

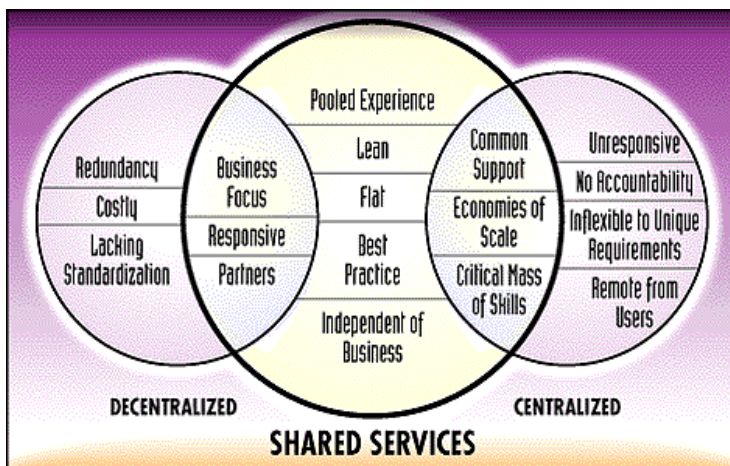
This stands for **Municipal Reference Model** which is a program to create repeatable best practices for how to operate a town or city. These is a framework that helps you quantify how to organize your resources and departments into Programs, Services and Processes, and you can then implement these structures on one set of technology products, currently the IBM suite.



The program includes a database of all the different processes and also templates for performance reporting, with all of this aligned to key goals, like improving service for citizens and how you can better achieve this while also improving your cash flow and other organizational benefits.

For further info here is a [detailed description of the MRM](#), and there is a [presentation here](#) from the principle designers that explains how it can implemented as well a discussion of using reference models for service mapping in general.

Therefore one of the most practical aspects for Municipal CIO’s to consider about Cloud Computing is the role it can play in making these best practices implementable within their IT environment.



This is an example of the **business process enablement** that Cisco describe.

The MRM stipulates the municipal operations best practices, and these can then be implemented on Cloud platforms, such as Salesforce.com for example.

Via 'application packaging' techniques these can then be encoded into a repeatable templates that then enables others to do the same.

Government Cloud Hubs – Shared Services Cloud Architecture



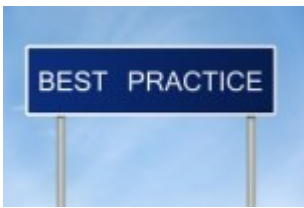
The previous section talked about Municipalities beginning to move into a mode where they not only buy in Cloud services, but they also become a seller of them too.

Research analyst IDC calls these ‘Cloud Hubs’ in [new insights they are revealing](#) about how this effect is already occurring in the USA, with municipalities buying from ‘upstream’ State-level providers, and also selling to them too.

It’s clear there is a very powerful story about the potential for new revenue sources and local economic development, as well as a new mode of IT.

The fundamental building blocks of the type of platform required for this strategy include:

- **Self-service portals and platform automation** - For example Cisco has just made two acquisitions to fill out their products here, for their [Cisco Cloud Portal](#), part of their [Cisco Intelligent Automation for the Cloud](#) program.
- **Cloud Brokers** - As highlighted in their blog, [Gravitant were recently profiled by Gartner](#), who described the key features of what constitutes as a ‘Cloud Broker’, basically being that you buy from someone else, package it and sell it on. Gravitant provides the platform for enabling this marketplace.
- **The NIST Models Catalogue** - The actual services being bought and sold need to be defined via a common language to enable these catalogues to be defined and then populated.



To explain this last part in more detail you can see in the article about the IDC research that the different types of Cloud installation can be a little confusing – All the Private/Public/Hybrid models plus SaaS, IaaS, MaaS, etc.

They’re initial confusing but are actually well thought out and most importantly they’ll be “baked into” the above Cloud Portal type

technology, so there’s no need to master them only understand what role they will play in **facilitating procurement**.

Fundamentally they regulate security and privacy policies, and also the scope of commercial services, like what the Cloud Provider is and isn’t responsible for. This clarifies the service itself and associated SLAs and other product management can then be built around them.

These are the foundations that the NIST Business Use Cases are based on, which cater for users needs at the level they experience, for example they want hosted email or e-discovery, as a Cloud service.

The ability to provision and deliver Cloud services against these specifications therefore means agencies are in a position of being able to not only service their internal staff needs but also those of other organizations – An interesting opportunity to consider.

PaaS Best Practices : Platform for Hybrid SaaS



The [GC Community Cloud ITSS](#)

[documentation](#) stipulates the Cloud service specifications that the Government of Canada plans to deploy, and can be used by external commercial providers as well as internally by Shared Services Canada users.

They provide technical design blueprints for security configurations to ensure Cloud environments are compliant with Government of Canada standards.

Primarily they can be used as industry-wide product specifications because they're based on the NIST models that are now universally recognized as the default Cloud Best Practices, and relate to how service providers define and deliver their services.

The four primary categories are:

- Colocation
- IaaS – Infrastructure as a Service
- PaaS – Platform as a Service
- SaaS – Software as a Service

NIST calls these Service Models and they do indeed define product specifications, in that they regulate what the service provider is and isn't responsible for, in terms of up to what 'layer' do they provide technical support for.

For example PaaS includes elements like Databases, and so the Cloud provider therefore agrees to support that application.

PaaS Catalogue – Standardization

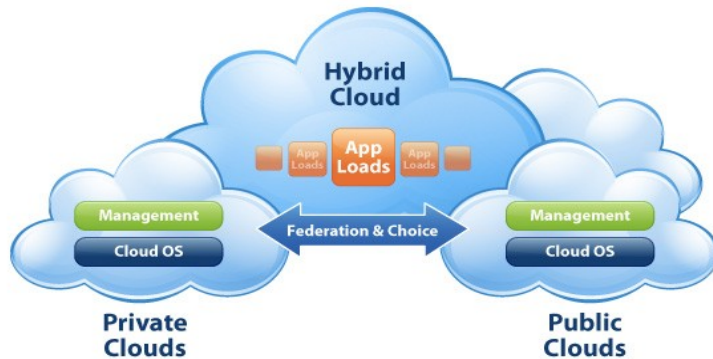
IaaS refers to virtual servers and storage, whereas PaaS is about the middleware between this layer and the applications that make use of them – such as Operating Systems, web servers, middleware and database software, and so forth.

A PaaS strategy builds these into self-service portals to maximize the productivity of software developers and also to better enforce Enterprise Architecture standards. A proliferation of multiple different software platforms can be tightened back to just a few, while also reducing delivery times from weeks to hours and minutes.

In the GC Community Cloud Canada begins to define their PaaS catalogue items, as well as increasingly ITaaS-centric, such as single tier web hosting, three tier application hosting, database hosting (DBaaS) and Virtual Desktop (vDaaS).

Hybrid SaaS

The GC Community Cloud also defines two different PaaS implementation models – A (Dedicated PaaS) and a (Shared PaaS), again referring to whether the PaaS itself is in a virtualized, shared environment or operating its own single hardware.



Critically this is described as the foundation for their SaaS strategy too, and ultimately defines a new category of Delivery Model, a ‘**Hybrid SaaS**’ scenario.

Typically SaaS is entirely remotely hosted, but as the Government of Canada stipulates, they are looking for SaaS but delivered via a more localized version, based on a Hybrid Cloud approach – Therefore Hybrid SaaS.

They describe this as:

“In addition to the IaaS and PaaS services, shared applications will also be provided as part of a Software as a Service (SaaS) set of offerings. Examples include a shared eMail service or a shared Collaboration service. These applications will reside within the same shared domain as the shared PaaS set of services. This will enable SaaS applications to leverage the shared PaaS services to the greatest extent possible (ie. for SaaS applications to be hosted on the PaaS services.”

This is part of a broader ‘GC Community Cloud’ program which defines an overall multi-tenant ‘Federal Cloud’ architecture, to encompass **Shared Corporate Applications** -

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. As described they are starting to see these as PaaS layer items, setting them up for SaaS delivery scenarios for these major applications too.

This approach is also appearing in the USA too. The [NIST Business Case Use cases](#) also stipulate these same combination, where the E-Discovery service is also asked for via this Hybrid SaaS model.

This is reflected in the USA Government having a [procurement program for IaaS](#), a blanket purchase agreement that enables agencies to buy Cloud services from a pre-approved list of suppliers.

NIST also defines additional Service Models including PaaS and SaaS – Platform and Software as a Service, and so we’re equally likely to see purchasing programs emerge for them too.

Canadian Cloud Security Best Practices

Naturally the security of information hosted in Cloud systems is of paramount importance, and luckily the Cloud best practices in these areas are now fully maturing to cope the wide array of areas that need covered.



There are various industry authorities in this area including NIST, such as the [Cloud Security Alliance](#), which stipulates a program of best practices.

Canada is also active in the development of key Cloud resources relevant to this trend.



Recently they published their ‘**ITSS Security Domains & Zones**’ documentation that stipulates the security models required to implement their ‘GC Community Cloud’ program, as we have documented [here](#).

PaaS and Cloud Security

The roles of both PaaS and Cloud Security are explained through their overlap, in that security is often an area that an organization expects to be enforced in a common and standardized manner.

PaaS also has an objective of this common standardization, which includes but is not limited to security, also encompassing application servers and middleware.

Cloud	Enterprise
SaaS	Applications (SAP, Oracle BS)
PaaS	Middleware (DB, ESB, App Srvr)
IaaS	Virtualization / Hardware / OS

This is explained through analyzing the NIST ‘[Business Use Cases](#)’.

In these documents they describe the need for a set of ‘common building blocks’ that correspond with the PaaS layer of the Cloud stack, what NIST describe as ‘[cross-cutting](#)’. These are described in the following way in the use cases:

“In addition, the initial public platforms will benefit from being able to operate on the community cloud infrastructure, and visa-versa. To that end, the following interoperability requirements are needed:

- 1. Authentication and identity management interoperability will be required so that users of multiple target clouds can maintain consistent identity and role based access across multiple cloud implementations.*
- 2. Virtual machine management interoperability will be required so that platforms running in multiple cloud implementations can be stopped, started, terminated and otherwise operated through a consistent interface.*
- 3. Billing and reporting interoperability will be helpful to allow for meaningful comparisons of costs and benefits across multiple cloud implementations.*

8.3. Portability

Static virtual machine portability is required so that the maintained platform images can be freely migrated between cloud implementations without the need for parallel development or maintenance. Dynamic VM portability, where running machines are migrated in flight is not required.”

Cloud Identity and Security Best Practices



A key backbone to our program is the combination of 'Cloud Identity and Security Best Practices', referring to the intersection between Cloud Computing and Identity Management technologies.

The importance of this is illustrated through the NIST Business Use Cases. For example the E-Discovery use case describes both a need for common Identity Management as well as data sharing between different Cloud-hosted applications, like the e-discovery application being able to audit another providers hosted email. These secure data sharing mechanisms will be facilitated by common, standards-based PaaS layer components, and it also achieves compliance with multiple government mandates.

A great example is [this recent press release](#) from NASA, about their use of 'PIV' technologies to secure their move to Google apps.

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.

It also demonstrates healthy portions of political compliance too. By adopting Google they are demonstrating progress against their Cloud First requirements, and simultaneously doing the same for [this Whitehouse directive](#) requiring agencies to begin accepting sign-in credentials from external sites, a principle known as 'federated identity'.



This federation is achieved through best practice frameworks such as the [Kantara Initiative](#), which provides a means of stipulating differing user security levels ranging from 1 through 4, referring to the number of factors used in the authentication process, and also to build 'Trusted Services', a network of providers to then accept these credentials and provide access to the user.

As well as their own in-house standards for identity authentication [ITSG-31 here](#) the Government of Canada has also standardized on (and contributed to) Kantara. Their specific implementation is defined in [this document](#). (53-page PDF).

Virtualization and Identity Security



As highlighted recently the Canadian Government published their 'ITSS Security Domains & Zones' documentation that stipulates the security models required to implement their 'GC Community Cloud' program, as we have documented [here](#).

It builds on their previous reference documents, [ITSG-22, Baseline Security Requirements for Network Security Zones](#) and [ITSG-38, Network Security Zoning](#), which describe WAN (Wide Area Network) level approaches to sharing networks the same way.

This same principle is applied higher up the stack, across virtualization, servers and storage, and hence in essence describes best practices 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.

Fundamentally this defines the required **Virtualization Security**, meaning the separation of Virtual Machine environments in the same way vLANs separate networks, so that agency customers can be

ensure their applications are logically entirely separate from those of other agencies. Only then will they move to multi-tenant Cloud environments.

VMware Horizon Application Manager

An example of a vendor technology that can be used to implement Cloud Identity and Security Best Practices is the [Horizon Application Manager](#) from VMware.

As [this article](#) explains the Cloud itself has a user authentication process, for users and admin to sign on to the actual environment, such as vCloud in this case and it may not be as robust as you need or as compliance dictates.

Therefore the principles of Identity Management, increasing the security of these user authentication procedures, can be applied to Clouds too, both internally and importantly externally. It will likely become a key mechanic required for “secure Cloud outsourcing”, especially to government.

Hence Cloud Identity Management includes this sign-on process, and then the role it plays as a secured single sign-on across the applications that the Cloud is used to run. This function of interconnecting different systems this way is known as ‘Federation’, as described in the diagram above.



Smart Signin

Other similar solutions include [SmartSignin](#), an example of a home-grown Canadian venture specializing in this field.

SmartSignin is based on a joint venture with the University of Toronto, to leverage a unique new security algorithm to make online user security more robust while also easier to use.

SmartSignin offers a platform to implement Cloud and Identity security best practices through:

- A “cookie-less” approach to web security.
- Support for multiple devices and multi-factor authentication modes
- Cloud SaaS sign-in to any web based application
- Hybrid IDaaS model for enterprise single sign-on to apps like SAP and Oracle

Business Process Protection

Achieving and maintaining the security of Cloud systems isn't limited to only security technologies. Ensuring the safety of the information also includes protecting against disasters through business continuity best practices.

This highlights another local Canadian startup firm. [Data Gardens](#), based in Edmonton, is another venture being developed within this incubating context of Canadian Government Cloud Best Practices.



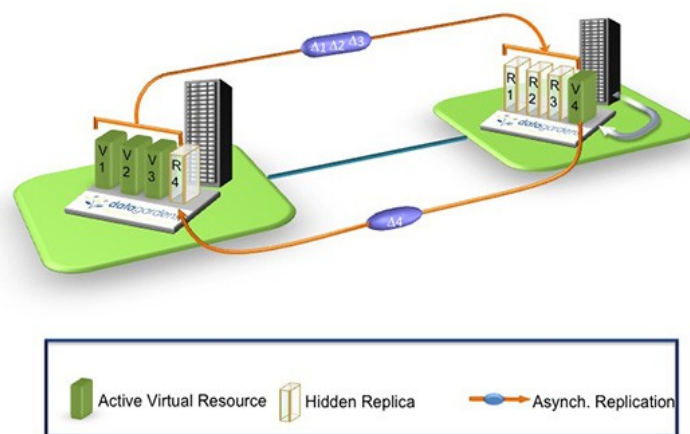
In contrast to traditional approaches to BCP, Data Gardens does not force the customer to design, script and maintain his own custom recovery plans - Instead WAVE non-disruptively embeds live IT systems into distributed virtual structures that are intrinsically resilient to site failures, using its own data replication and VM protection systems to move live processes between sites.

The traditional approach to BCP is reflected in products like VMware Site Recovery Manager which is a scenario of two linked data-centres with big, dedicated equipment replicating data between them, rather than the use of shared multi-tenant Cloud environments. This is often expensive and requires a scripted shut-down of the failing site and then a scripted re-boot of the new one, a process fraught with potential for error that often doesn't achieve the primary recovery goals.

In contrast 'Cloud BCP' leverages the distributed nature and low-cost commodity base of Cloud Computing to operate more of a continuous availability. WAVE technologies can protect both physical and virtual infrastructure.

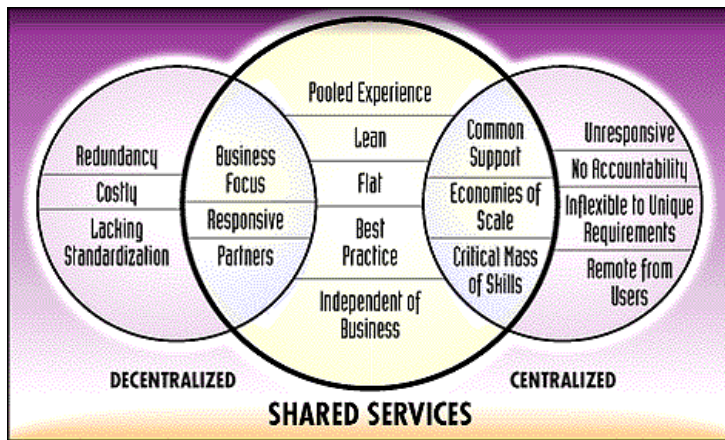
WAVE protects more than just IT infrastructure, instead it protects live processes as well so literally it is the business process itself that is kept live across multiple sites, providing "cloud-class business continuity" although not limited to emergencies. WAVE is an agile system that is used proactively to avoid all forms of planned and unplanned downtime, and can even redistribute workload non-disruptively between sites to help better utilize multi-site architecture.

In short WAVE builds automated high availability style protection directly into the multi-site cloud environment it protects.



Conclusion and next actions – Legacy Modernization

One of the motivations for the Shared Services Canada initiative was the commentary from Auditor General Sheila Fraser about the risk to government presented by the [aged nature of many of their IT systems](#).



This challenge is magnified by the fact that many of the staff who support these systems are baby boomers due for retirement within the next ten years or so.

Therefore there is an escalating risk with legacy systems. Not only are they already aged but once the only staff who know them move on then the processes they run become locked in to obsolete platforms, unsupported and most importantly cannot be easily modified or improved.

As applications are virtualized it becomes easier then to manage them with various systems management tools and automation platforms. Not only can this platform be used to manage the virtual apps but also to automate the manual labor associated with maintaining the applications itself like SAP or Oracle. For example it can automate functions like SAP System Copy.

Encoding this human knowledge into repeatable software services therefore protects against this aged workforce risk while also creating IT operational efficiencies and cost savings. Therefore the key point is that there is a wide range of organizational and strategic benefits derived from moving apps to the Cloud, not just ones of a technical nature.

Overall government agencies can look to Cloud services for business solutions to immediate pain points they are experiencing, such as IT systems without a DR failover option or cost and time savings for key users in the accounting department running month-end closings.

Ultimately Cloud services can be applied to existing legacy IT scenarios to maximize the overall ROI achieved from the original investment.

Authors

Neil McEvoy, Founder, Cloud Best Practices Network

Neil McEvoy is a senior executive, consultant and communicator specializing in adoption of innovative new technologies for enhanced business effectiveness and accelerated social change. He is a subject matter expert in cutting edge technologies such as Identity 2.0, Cloud Computing, Big Data and the Semantic Web, and as the Founder of the Cloud Best Practices Network (cloudbestpractices.net) works to organize a community of industry pioneers, experts and consultants and communicators to help distil these into easily repeatable business models.

Contact Neil: neil.mcevoy@15consulting.net