What Should You Move to the Cloud, and How Do You Protect It?

Dan Lohrmann
Chief Technology Officer
State of Michigan

Today's Focus

- Today's Headlines
- The National View
- Michigan's Approach
- Three Point Security Strategy
- Challenges to Consider

Before we begin

A few headlines

What's happening around the country?

- Oregon, Colorado, Utah and Montana announced this week an RFI to obtain information on the economic and technical feasibility of government GIS services being sourced by Cloud Computing Providers.

- The Department of Veterans Affairs (VA) plans to move 600,000 of its employees to a cloud-based email and collaboration system in a comprehensive migration project it's calling the "Big 4."

- The cities of Chicago, Andover, Minnesota, Virginia Beach, Virginia, and Carlsbad, California were among the local governments Microsoft recently signed up for its cloud services, while agencies in Colorado and Idaho were among state government wins.

- Vivek Kundra releases federal cloud computing strategy February 2011 and a $ 3 – 5 billion cloud RFP, with the possibility of the states being involved.

And there are more initiatives announced every day……

FedRAMP

Federal Risk and Authorization Management Program

- FedRAMP was designed to solve the security authorization programs of cloud computing. It enables agencies to either use or leverage authorizations with:
  - An interagency vetted approach using common security requirements
  - A consistent application of federal security requirements
  - Consolidated risk management
  - Increased effectiveness and management cost savings

Michigan's IT Landscape

17 Agencies

47,000 State Employees

IT support provided for:

- 800+ critical business applications
- Over 56,000 desktops and 3,900 Servers
- Over 1,300 telecom locations
- A private Government Cloud Storage Service deployed
- A private Government Cloud Development Environment available

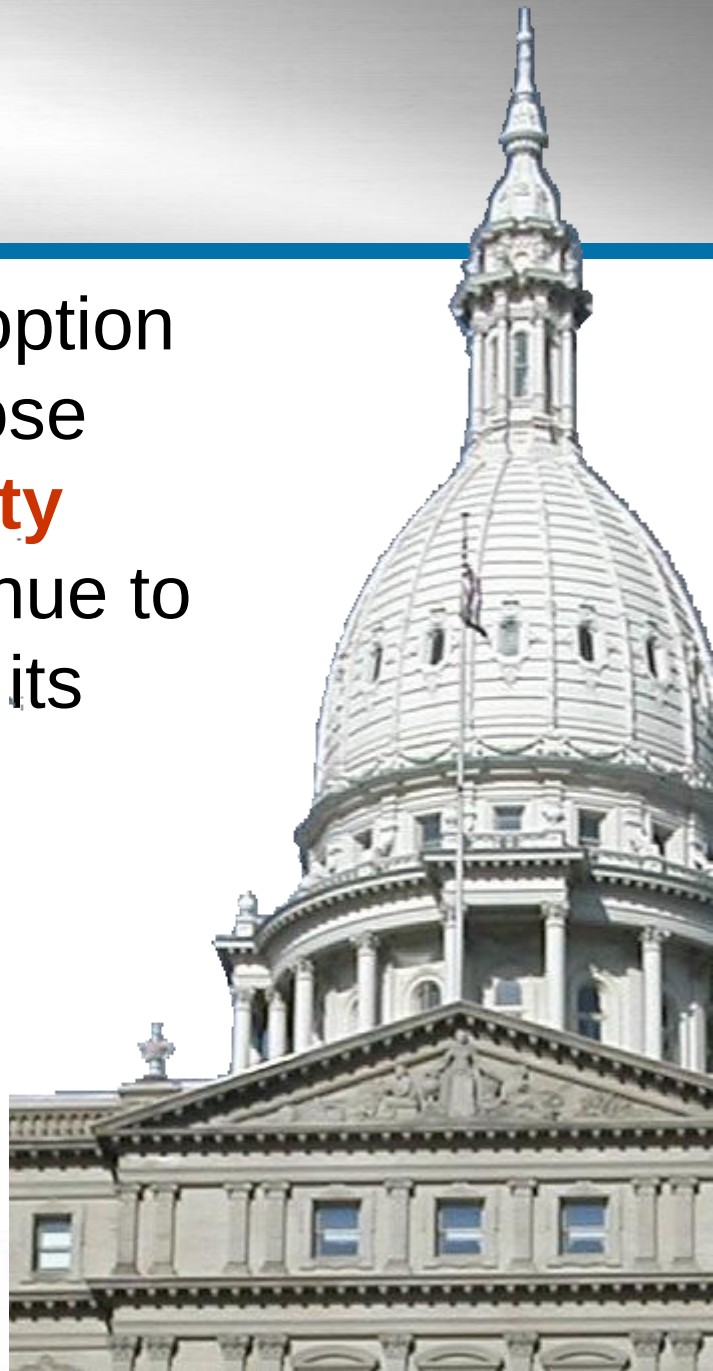
Michigan's Cloud Vision

Manage **primary** and **secondary** functions through a strategic tiered approach based on the criticality of the function.

Primary Functions
Mi Cloud

External clouds are not a viable option for every function, particularly those that are **critical** or have a **security requirement**. Michigan will continue to securely house such functions in its government cloud.

Examples: health records, taxes, criminal justice



Secondary Functions External clouds

Key targets for external clouds are vast and provide exciting opportunities for the delivery of **non-critical** functions.

Examples: Human resources, email, messaging

When it comes to managing external clouds, there are two extremes …

One extreme is blind trust

- Adopt a commodity cloud function as-is (cloud sets the rules)
- BUT: Provider accountability is low while risks are high

…Opposite extreme is all about control

- Dictate the standards, terms & conditions, etc.
- BUT: No longer a commodity (and no longer cheap!)

State of Michigan IT Services

DTMB delivers a range of options:

- Highly performant, highly redundant, highly available
- High value business at a high cost
- DTMB is **great** at this
- Options: Gold – Silver – Bronze

We needed to add Aluminum and Tin options

- The **good-enough** service options
- New tiers that are aligned with business value

Why did Michigan embrace the cloud?

What were we trying to fix?

- Automation: Human touches cost money
- Recruiting & retention:
  - Automate routine work
  - Focus staff on challenging, **satisfying** work
- Speed to deliver: cloud and non-cloud
  - Positive impact on **non-cloud** service delivery
- Simplicity: complexity kills
  - Complexity imposes risk and cost **on the entire enterprise**

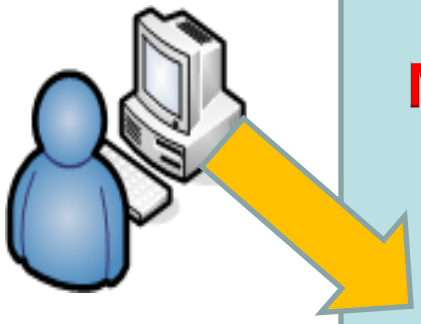
Why internal cloud first?

- Legal: Unconstitutional to indemnify a provider
  - Virtually all commercial cloud **Ts&Cs are DOA**
- Security: Internet threats removed
- Performance: Intranet speed, not internet
- Focus: Michigan business is paramount
- Market: DTMB matures as the market matures
- **Cost**: Making an external service compliant destroys the cost benefit

What did Michigan do?

- On-demand **file storage service**
- Users submit an on-line request
- Users receive a new network file share within 10 minutes
- Optionally, users map as a drive
- Permissions managed with an on-line wizard
- Usage based billing at a daily rate

How does MiCloud work?



State of Michigan

Service Interface

Process Automation

Shared by all cloud services

Service A
- DTMB Internal
- Vendor

Service B
- DTMB Internal
- Vendor

Service C
- DTMB Internal
- Vendor

Service + provider specific

State of Michigan

Usage Metrics

Billing

Shared by all

Security Strategy 1:
Internal Cloud First

SOM MiCloud Storage

- Delivered 99% faster
- Fully automated
- 85% cheaper
- Intranet speeds
- Threat surface collapsed

SOM MiCloud Hosting

- Delivered 99.995% faster
- Fully automated
- 75% cheaper (running)
- 97 % cheaper (suspended)
- Intranet speeds
- Threat surface collapsed

Security Strategy 2:

Govern and secure a single touch point

- Single contract for enterprise
- Single “service interface” for enterprise
- All services consumed through standard service interface = single touch point to secure
- Security requirements are constantly changing, apply mitigation at a single touch point rather vs an enterprise wide search

Security Strategy 3:
Involve Third Parties

- ***Third Party Data Replication***
  - Protect your data from loss if the vendor runs into legal trouble or closes shop
  - Replicate data hosted with Vendor A to Vendor B or internal storage
- ***Third Party Certification of Compliance***
  - Make sure your vendor doesn't allow anyone other than third party auditors to view security details
  - If you can view a cloud vendor's security details, the bad guys can, too!

Three remaining challenges

Things to consider:

- Legal Issues
- Compliance
- Can You Get Out?

Challenge 1:
Legal Issues

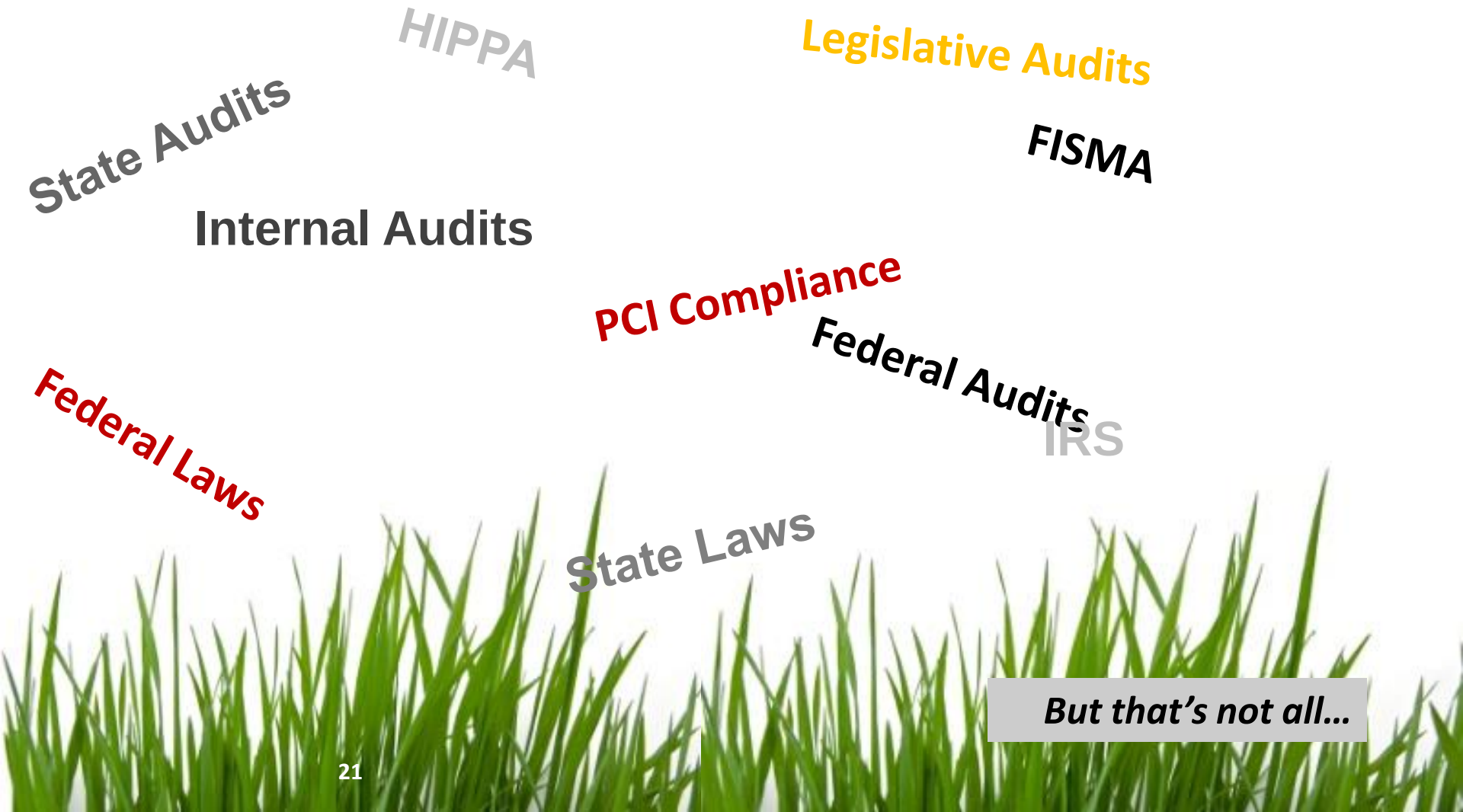
Based on our research, there are no legal issues or constraints for Cloud Computing that are not present in 3rd party hosting agreements – but do your homework before putting your applications into the Cloud.

- Understand AND document the business application's compliancy requirements – HIPPA, PCI etc.
- Guarantee that your Agency/State will own and control all access to your business data, configuration data, and business processes.
- Stipulate that the provider will replicate **your** business data to **your** designated data repository at a designated interval of time.
- Insure compliance with your Identify and access Management processes.

If your Cloud provider is not willing to comply with your security and business requirements – then don't risk your information in their cloud offering.

Challenge 2:

The Compliance Jungle, which apps to choose?



But that's not all…

Challenge 3:
Getting Out of the Cloud

- Can you get out?
  - Vendor interoperability isn't here yet
  - Interfaces are a challenge
  - Service offerings are coming

Questions

Contact Information

Dan Lohrmann,
Chief Technology Officer
lohrmannd@michigan.gov