Advancing governance practices and driving thought leadership

Moving to the Cloud? The Time for Information Governance is Now

Assessment, Curation, and Insight Are Essential When Migrating Data to the Cloud

CGOC
THE COUNCIL

The benefits of moving data to the cloud are touted everywhere, but doing so without an information governance plan in place can cause more problems than it solves.

A cloud infrastructure allows businesses to focus on their core mission, not their IT shop. The cloud is relatively secure, easy to manage, and cost-effective—you can switch it on and off, pay for more or less, and usually pay by usage. You can use the cloud for all kinds of applications. It increases data connectivity and accessibility. And it's a critical platform for both managing the tsunami of data organizations now face and for powering analytics initiatives.

Moving to the cloud is also easier than it has ever been. As a result, key decision-makers throughout the enterprise are considering a major shift to a cloud-first strategy. For example:

- **Chief Information Officers,** who dealt with a halt in infrastructure spending during the recession, are now deciding how to address their aging infrastructures. Moving to the cloud seems like a more practical and faster option than replacing outdated software and hardware.
- **Chief Security Officers,** observing the current rise in the number and severity of data breaches, are determined to avoid such a nightmare at their organizations. They are encouraged by the superior data protection and access management rights offered by today's cloud service providers and are eager to take advantage.
- **Chief Operating Officers** are attracted to the business continuity and efficiency that the cloud provides in the face of a natural disaster or a potentially rebellious or noncompliant mobile workforce.

These benefits and more are making some a bit starry-eyed at the prospect of forklifting their data over the firewall and having someone else shoulder the burden for a fraction of the cost.

But not so fast. While there is certainly a powerful and exciting new frontier to explore, before you can realize the promises of moving to the cloud, you must put a transition methodology or plan in place. Otherwise, there may be a high cost to your organization's bottom line or reputation.

Consider what typically happens when a family moves from one home to another. Most people don't pack the moving van with each scrap from the far recesses of every closet and the basement. Instead, they park a rental dumpster at the curb for a few days and elatedly pitch in all sorts of old and unusable belongings. While this purging activity is necessary and healthy, it must be done carefully and with some thoughtfulness. What if they unknowingly toss out a dusty box of important tax documents or even an aunt's shabby but prized antique desk? What's to be done if there's suddenly a tax audit or the aunt comes to collect the desk? The only way to avoid a crisis is to have more foresight and put a better plan in place before the move.

The same should be true of a move to the cloud. It is crucial that this move be well-thought-out and planned. It makes little sense to move all of your data. According to a joint CGOC and EDRM survey,[1] you may be able to defensibly dispose of as much as 70 percent of what you currently store. This can be done by process of elimination. Understand what you plan to keep and protect—mission-critical data, sensitive and private data, and data retained according to legal or regulatory mandates—and delete the rest.

Any problems accessing or defensibly deleting data will be compounded when moving data from corporate premises to a cloud provider. This makes it vital to have a governance practice in place before your data moves from your direct control. In addition, clarify your potential cloud vendor's policies regarding time limit and method of retrieval for data needed for eDiscovery and governance purposes. It's imperative that you don't get locked into a long-term contract that doesn't meet those essential needs.

Note that the shift to the cloud will take time, so there will be a period during which your data will live on a hybrid infrastructure of on-premises and cloud solutions. While this hybrid infrastructure may be a necessary and limited transition state, it may also exist for other reasons, such as specific long-term needs of various stakeholders. Legal and financial documents and records may need to be maintained in more secure content repositories than general cloud collaboration. It may also stem from "rogue IT" or departments taking it upon themselves to meet their own needs without abiding by IT mandates. Whatever the reason, make sure your governance strategy and solutions support this reality.

Executives "need the cloud because it gives analytics a powerful punch. The cloud provides an agile, scalable foundation for managing and pulling more insights out of the tsunami of data crashing over companies."

– James Kobielus, "Five Ways to Move Your Data into the Cloud," Wired.com, www.wired.com/insights/2014/10/move-big-data-projects-cloud/

[1] CGOC, "Information Governance Benchmark Report in Global 1000 Companies," October 2011, www.cgoc.com/2012/resource/

The Solution

Information governance (IG) is increasingly cited as one of the top five initiatives for companies to tackle over the next two years. There is no better time to consider your governance plans and policies than when you are planning a move to the cloud.

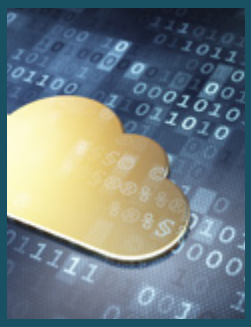
The approach to IG has significantly evolved over the last few years. Historically, IG projects involved collecting handfuls of data and segregating it for analysis. The amount of data in today's enterprise, however, is enormous and grows larger every day. With the addition of new sources and types such as unstructured and structured, the mountain of data presents an ever-increasing challenge. As a result, IG is essential in understanding all of your data—no matter where it resides—and helps put into place the necessary practices and processes to meet business and compliance needs.

In addition, if the escalating number and scope of data breaches has taught us anything, it should be that the walls we continue to build around our enterprises will continue to fail. We need to try something new to fully protect and govern the sensitive and private data our clients and stakeholders entrust to us.

With an effective IG program, you can gain the knowledge and insight you need to make smarter decisions about what to move, where to move it, and how to secure the sensitive and private data you have, whether on premises, in the cloud, or a combination of both. You can also begin confidently identifying the information you don't need, enabling you to dump it without fear that the deletion will come back to haunt you. Deleting this information will save you time and money, and reduce the risk of breaches and damage to your reputation.

At a practioners meeting, a CGOC member made this humorous comment: "Governance is about making you compliant despite the fact that you have users on your system." It is difficult to maintain the proper, prudent, and mandated level of controls on your data given the pace, location, and agility we see in today's economy. It is no longer feasible to lock down your user's email and file systems and throw up walls between your company and the social or digital world. For an organization to comply, users need to comply.

This is a monumental challenge. In recent rulings, courts have made clear they consider your data to be your data, and they don't stipulate or make allowances for your technical challenges.[2] They don't care where you have the data hosted—you are responsible for it, period. This makes a comprehensive IG program an imperative.



Any problems accessing or defensibly deleting data will be compounded when moving data from corporate premises to a cloud provider. This makes it vital to have a governance practice in place before your data moves from your direct control.

[2] Andra Grp. LP v. JDA Software Grp., LLC, No. 3:15-mc-K-BN, 2015 WL 1636602 (N.D. Tex. April 13, 2015), Brown v. Tellermate Holdings, Ltd., No. 2:11-cv-112, 2014 WL 2987051 (S.D. Ohio July 1, 2014).

A Better Plan: Five Steps to Take Now

Given that every shift to the cloud should be done with great caution and care, here are the top five steps every transition plan should include:

1. **Create a steering committee comprised of decision-makers from legal, IT, records, business, and privacy/security.** The best resource for understanding how to develop this committee is the Information Governance Reference Model (IGRM).[3] The steering committee will be responsible for driving IG policies and procedures and for acquiring tools as needed to accomplish the next three steps.
2. **Map your existing information.** What are the different sources of data? How does data flow into a usable format? How is this information maintained and deleted? Who is the owner of that repository or data type?
3. **Assess the content of the data.** What information is records and must be retained? What can be—or needs to be—disposed of in accordance with legal and regulatory requirements and business needs? What information requires higher security levels or special authorizations or permissions?
4. **Assess the value of your data to stakeholders.** What information hasn't been touched in eons? Could the data contain information that could return business value in the future?
5. **Evaluate potential cloud providers.** Each provider has different capabilities, especially in the areas of security and accessibility. Match the data you want to move to the cloud with the appropriate cloud provider. Many organizations find they need to utilize multiple cloud providers to satisfy various requirements.

Only after taking these steps should you begin moving your data to the cloud—and then only the data that is necessary and valuable, which is likely to be as little as 20 percent of your current data.[4] And this final fact is important: by moving only valuable information to the cloud and deleting the rest, your cloud initiative will deliver a financial reward to your organization while also reducing risk.

[3] Information Governance Reference Model (IGRM), www.edrm.net/projects/igrm

[4] "Automating Information Governance: AIIM Research Findings and Industry Trends," AIIM webinar, June 10, 2014, www.aiim.org/Events/Webinars/Archived/20140610-webinar

About CGOC

CGOC (Compliance, Governance and Oversight Council) is a forum of over 3,300 legal, compliance, privacy/security, and records management professionals. Established in 2004, it fills the critical practitioners' gap between the EDRM and The Sedona Conference. Its charter is to create a forum in which executives can get the insight, interaction, and information they need to make good business decisions.

CGOC conducts primary research, has dedicated practice groups on challenging topics, and hosts meetings throughout the U.S. and Europe where practice leaders convene to discuss discovery, analytics, privacy, and governance. Members gain insight from diverse industry perspectives and harness the collective experience of the breadth of practitioners required to solve today's complex legal, IT, and business challenges. Nearly a third of CGOC members attend events throughout the year, highlighting dedication to advancing their corporate practices and demonstrating the value of the in-person gatherings. **For more information, go to** www.cgoc.com.

Courtesy of IBM

IBM | CGOC THE COUNCIL

For inquiries please contact us at cgoc@cgoc.com or go to www.cgoc.com for more information.
Printed in the U.S.A. 011516V2