



Moving to the Cloud: Is Federal Financial Management Fair Game?

By: Robert E. Maitner Jr., CGFM, PMP

Cloud computing is suddenly all the rage. Turn on the television and you'll see commercial after commercial encouraging us to "move to the cloud." All the large technology companies are getting into the game, and smaller ones are also testing the waters. On June 6, Apple CEO Steve Jobs announced the company was launching its cloud music storage service called iCloud. It seems that you can either jump on the bandwagon or get out of the way because the move to the cloud is happening quickly. Now that we have seen the hype, do we really understand what it is and how it works, especially as it relates to public sector financial management?



Cloud Computing and the Federal Perspective

Not to be left behind, the federal government is planning to move in the direction of cloud computing. Late last year, the U.S. Chief Information Officer (CIO) outlined the government's vision for the future in a *25-Point Implementation Plan to Reform Federal Information Technology Management*, and it clearly includes cloud computing. Specifically, the plan declared "the federal government will shift to a 'Cloud First' policy. The government issued an implementation plan in May 2011, with the strategy to accelerate the safe and secure adoption of cloud computing."¹ And even in these days of federal austerity measures and budget battles, the government is not scaling back on this effort, with a plan to allocate \$20 billion of the total \$80 billion federal IT budget to cloud computing.

What is Cloud Computing?

A little background on cloud computing would help, especially for those of us whose world involves accounting transactions, accounts receivable, payables, PP&E, etc. If you do some research, on Wikipedia you will find:

Cloud computing refers to the provision of computational resources on demand via a *computer network*. In the traditional model of computing, both data and software are fully contained on the user's computer. In cloud computing, the user's computer may contain almost no software or data (perhaps

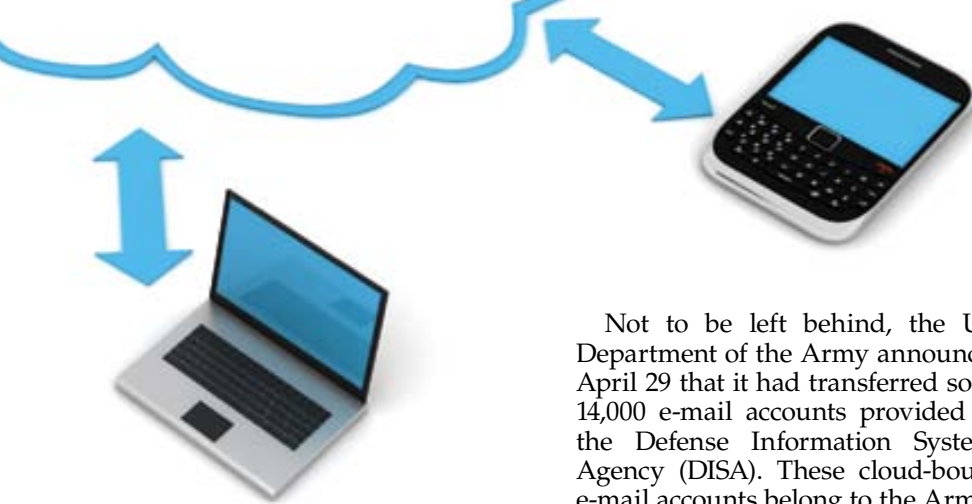
a minimal *operating system* and *web browser* only), serving as little more than a display terminal for processes occurring on a network of computers far away. A common shorthand for a provider's cloud computing service, or even an aggregation of all existing cloud services, is "the cloud."²

The National Institute of Standards and Technology (NIST) is charged with leading the initiative, and describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."³

The U.S. CIO, Vivek Kundra, who recently left government to enroll in a fellowship program at Harvard University, envisioned a future in which the government is more efficient, agile and innovative through more effective use of IT investments and by applying innovations developed in the private sector—hence, the emphasis on moving to the cloud.

A variety of cloud solutions are available. For example, we have seen different types of "services" associated with the cloud, such as Software-as-a-Service (SaaS), meaning that a local PC accesses software applications from the cloud servers rather than locally installed software. There is also Infrastructure-as-a-Service (IaaS), which delivers a computer infrastructure—typically a platform virtualization environment—as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service.⁴ Recent pictures of Apple's new enormous iCloud network center demonstrate the largess associated with the IaaS part of the cloud. Email-as-a-Service (EaaS) is where cloud (web-based) e-mail resides.

From the perspective of a federal financial manager, an agency could be accessing finance and accounting software (provided by the vendor) through the cloud, accessing a virtual platform in the cloud and responding to e-mails that reside in the cloud, linking the SaaS, IaaS and EaaS models. The U.S. General Services Administration (GSA) has recently announced plans to solicit contractor support for Platform-as-a-Service



(PaaS). Apparently, many things can be performed “as a service.”

Kundra’s implementation plan called for agencies to identify three “must move” services, create a plan for migration to cloud solutions and retire legacy systems. One must be fully migrated within 12 months and the remaining two in 18 months. Instead of running personal computers encumbered with loads of data and software, the government plans to embrace the SaaS model, and has established working groups to identify and develop a set of baseline functional and technical requirements for a government-wide cloud solution. One of the frontrunners for this new approach is e-mail. Many people already rely on cloud-based e-mail providers, such as Yahoo, Google and Hotmail.

In early May, the Obama administration began to move e-mail to the cloud, when the General Services Administration released a Request for Proposal (RFP) valued at \$2.5 billion to move 950,000 e-mail boxes to the EaaS model.⁵ GSA anticipates it will realize a 44 percent savings for e-mail services.⁶

The federal government on April 27 announced its intention to conduct a major consolidation of its data centers, with plans to close 137 of 2,100 centers across government. Then-CIO Kundra said that the government is “cracking down on duplicative, underutilized assets across the federal government.”⁷ A third of the closed data centers belong to the National Aeronautics and Space Administration (NASA), which moved to a shared services model of doing business in the early 2000s. This is all in conjunction with the plan to move at least three functions for each agency to the cloud within 18 months.

Not to be left behind, the U.S. Department of the Army announced April 29 that it had transferred some 14,000 e-mail accounts provided by the Defense Information Systems Agency (DISA). These cloud-bound e-mail accounts belong to the Army’s CIO organization and other communications units, such as the Network Enterprise Technology Command and the Ninth Signal Command. The Army is also planning to merge some 10,000 e-mail accounts belonging to Army headquarters by June of this year. The Army predicts it will save more than \$100 million a year though the efficiencies gained from the enterprise e-mail system, starting in 2013.⁸

Challenges With the Cloud

It may not be smooth flying to the cloud. In late April, Amazon’s Elastic Compute Cloud (EC-2) experienced a widespread outage that went on for several days and severely diminished access to thousands of its clients’ websites, including Netflix and other large online businesses. While it is positive that customers did not lose any significant data through a crash on a local, personal computer, this situation does highlight concerns about a user’s inability to control the disposition of data that is being hosted by third-party “cloud” providers, such as Amazon. This is only one example of a few recent news stories, and certainly there are more that never made it to the press.

These important considerations need to be included in any implementation plan to move federal financial management functions to the cloud computing model.

Another lesson highlighted from the Amazon EC-2 meltdown revolves around diversification of networks and servers. When considering where and how to store critical customer information, it is important to consider contingency planning, disaster recovery and diversification of location. In other words, don’t put all your data on one cloud. If data is stored in networks that are clustered together in a single “cloud” loca-

tion, like some of Amazon’s clients, chances increase that an IT event or natural disaster could cause the loss of all or most of the data. Those clients of Amazon’s, including Netflix, who had spread out their data into different physical locations fared better in the recovery process, suffering only partial outages.

As recently as May 24, Amazon experienced another cloud-related setback, when its servers linked to its much-touted Cloud Player program crashed due to an overload of users purchasing the newest Lady Gaga album at a highly discounted 99 cents.

If the cloud cannot support overzealous Lady Gaga fans, can it handle the droves of data belonging to the federal government?

All these considerations need to be factored into the federal cloud equation. Given the fact that federal officials would not want to store sensitive information in certain countries, such as Iran, China and Venezuela, for example, location becomes an important consideration for purposes of system and data security.

Federal Financial Management Functions—Moving to the Cloud?

So what does all this mean to the federal CFO and other senior agency financial managers? Will financial management and accounting activities be strong candidates for functions to be migrated to the cloud? What are some of the risks involved, particularly surrounding assurance of data and security concerns? These questions merit further exploration and assessment.

Moving the federal government to cloud computing has not been without its vociferous critics. For example, Linda E. Brooks, the CEO of a public sector human capital solutions platform provider, and a regular contributor to the *Huffington Post*, wrote a highly critical piece, saying, “The administration has not clearly identified the cloud solution it wants. The Federal Cloud Computing Initiative (FCCI) did not provide clear definition and direction. The ‘cloud’ is a metaphor for the Internet. It is a style of computing in which IT-related capabilities are provided through SaaS, allowing users to access technology-enabled services

from the Internet without having to demonstrate knowledge or expertise with the technology infrastructure that supports them or the computing code that allows it to function. But not all cloud solutions are created equal.”⁹ In particular, Brooks is critical of companies that claim to understand true cloud computing, when in reality they are merely specialists in moving activities to the Internet. She also points to the administration’s policy mandating that agencies move to the cloud, while allowing the U.S. Departments of Veterans Affairs and Homeland Security as well as the Office of Personnel Management to continue to waste billions of dollars on non-cloud IT projects.¹⁰

So given a program that is lacking clear direction and has inconsistent enforcement, how can federal financial managers determine if cloud computing makes sense for them?

Financial Management Activities—Determining Candidates for the Cloud

The CFO organization within any federal agency performs several financial management-related activities daily—from the simple (posting a transaction to the accounting system), to the complex (reconciling large amounts of financial data and accounting cleanup). And with Enterprise Resource Planning (ERP) solutions up and running at some agencies, the intricacies of ERP systems have to be part of the equation.

In any scenario, work surrounding core financial management tasks—accounts receivable, accounts payable, invoicing, cost accruals, grants management, reconciliations and financial reporting—could all potentially be moved to the cloud environment. But what assessments would be needed to determine the best candidates?

The benefit to the CFO organization would need to be balanced against costs. And how would a move to the cloud affect large ERP solutions that are already running or currently being implemented? Again, these are areas that need to be kept in mind before declaring an all-out move to the cloud.

Case Study: U.S. Department of Labor

Any discussion about the move to financial management performed in the cloud environment should also include shared services. After all, what is the cloud but one large shared services center? Within the federal government, a fairly early example of this is the U.S. Department of Labor.

In early 2010, Labor was replacing its 20-year-old financial management system, and decided then that a system that could be integrated across 22 organizations was the way to go. This laid the groundwork for an eventual cloud-based solution, whereby Labor implemented a financial management system through Shared Service Provider (SSP) Appliance, which is based on Oracle Financials Release 12, and owned by a private contractor, Global Computer Enterprises (GCE).

The department decided to move to a pre-built solution that would save considerable time, money and risk, as well as introduce change simultaneously to users in all its agencies.¹¹ According to Labor and its provider, the system was running in 18 months, and under a cost of \$10 million. If this is true and can be replicated at other federal agencies, one would expect the cumulative cost savings to be significant.

Labor is not limiting itself to financial management in its migration to the cloud. The department released a May 26 Request for Information soliciting industry feedback on a planned migration of its 21,469 e-mail users to a cloud system. E-mail is one of three services the department has told the Office of Management and Budget it will migrate to the cloud.¹²

Now, more than a year later, how is Labor doing under the new shared services model? Opinions differ regarding the example at Labor, with some questioning the true cost of the program given the re-work and corrective actions that resulted from the migration.

Jim Taylor became chief financial officer at Labor in June 2010. He describes a legacy financial management environment that was plagued by a 20-year-old, nonintegrated system of batch programs characterized by poorly defined processes, few controls and reliant on data

calls to perform financial reporting. The department also had a history of failed financial modernization initiatives, at a cost of more than \$35 million, which resulted in no improvements to financial management and accountability.

Taylor has served for years in senior financial management positions while at both the U.S. Department of Commerce and the Federal Emergency Management Agency. He favors the move to integrated, shared services for financial management operations. He notes, “I have been through this process several times before, from the stand-alone systems, custom systems, and I believe in this model.”

He is familiar with the model at Labor, having started in the early planning stages in October 2009, as a special detail to the secretary, then more recently as the CFO, although the planning for the financial system actually occurred before 2008. The contract for the project was signed in June 2008. Taylor was on detail to help the system go live, which it did in January 2010. The department is not going solo on this effort, however, with OMB closely involved and monitoring performance at Labor.

Taylor believes the successes at Labor can be replicated across other federal agencies, given proper considerations of scale and planning. “One of the early challenges we had occurred when we were hit with a significant increase in scale, resulting from a four-fold increase in the number of users compared with the legacy system. This had not been anticipated in the original project scope, and in the end, it cost us in money and effort.”

Labor has experienced its share of challenges with its move to a cloud environment. In addition to the “sizing” issue—going from a legacy, batch system to a “real time” system—issues related to training and process changes arose and became more critical. And these business process changes ran the spectrum of financial management activities, to include human resources, travel, procurement, invoicing, etc. A symptom of these process changes was a tripling of fees related to Prompt Payment Act requirements, and what Taylor refers to as “huge training issues.”

Labor also experienced problems related to data conversion, testing, operational issues and financial reporting. These resulted in additional efforts and added cost in the fourth quarter 2010. Ultimately, Labor went through a major effort to correct data errors and discrepancies, while keeping the grants management program moving. When the dust settled, the department's auditor, KPMG, issued a disclaimer on Labor's 2010 financial statements, after more than a decade of unqualified opinions. KPMG cited large discrepancies related to the department's liabilities, which appeared to be linked to the new financial management system, New Core Financial Management System (NCFMS). Since then, KPMG has upgraded its audit opinion to "unqualified" based on the department's major cleanup and reconciliation efforts.

Overall, Taylor is optimistic about the state of financial affairs at Labor and pointed to automated processes (such as invoice processing and approval), increased efficiencies in financial reporting and a normalization of business operations. Taylor said Labor is now able to send the right performance and financial data to key managers in vastly less time. Additionally, these gains will be reported by the Obama Administration as it rolls out its Performance.gov accountability tool.

And the gains are not only operational, but financial as well. Labor reports that the cloud initiative ended up costing less than \$10 million because it was a pre-configured, scalable system with no infrastructure. In fact, the provider for the SSP-

Appliance owns the hardware that is used across the department for this system.

In response to skeptics who claim the solution at Labor is not a true cloud implementation, Taylor said he does "not lose sleep over the definition. If it walks like a cloud, looks like a cloud, then it's a cloud." From the CFO's perspective, he is more concerned about operational efficiency, accountability and gains in financial reporting. Whatever people may want to call it, according to the CFO, it works for the department.

Taylor said the one piece of advice he would give to financial managers at the beginning stages of rolling out a cloud-based solution would be to focus on the "business processes" that result from a new system. The end users should be fully involved in the implementation to ensure they understand the implications to changes in business processes and both the "as is" and "to be" environments that result from this type of system change. Again, training considerations must be part of the equation.

Taylor said cloud computing is certainly not a "magic bullet" and all implementations struggle with similar issues—business process changes, data cleanup and conversion, and the risk of losing clean audit opinions due to these types of challenges. To assess the true cost of this type of program, factor in the re-work that is associated with the effort during and after implementation. Some argue, for example, that the true costs to Labor are significantly higher than the \$10 million reported when all efforts are factored into the equation, and could be closer to \$50 million.

Equal Employment Opportunity Commission (EEOC), Looking at the Cloud

The Equal Employment Opportunity Commission (EEOC), a comparatively small independent federal agency, announced in March that it is also moving to a cloud-based solution for its financial management operations. The EEOC signed a five-year contract with a local service provider, which has a base period of 20 months with four one-year options.

The contract is worth up to \$10 million if all options are exercised. In addition to supplying all necessary hardware, software and communications for hosting, the contractor is expected to perform full-service accounting operations and transaction processing for the commission, including invoice processing and travel management. The goal is for the new system to comply with federal accounting and system standards as well as improve financial management performance and cost controls.¹³

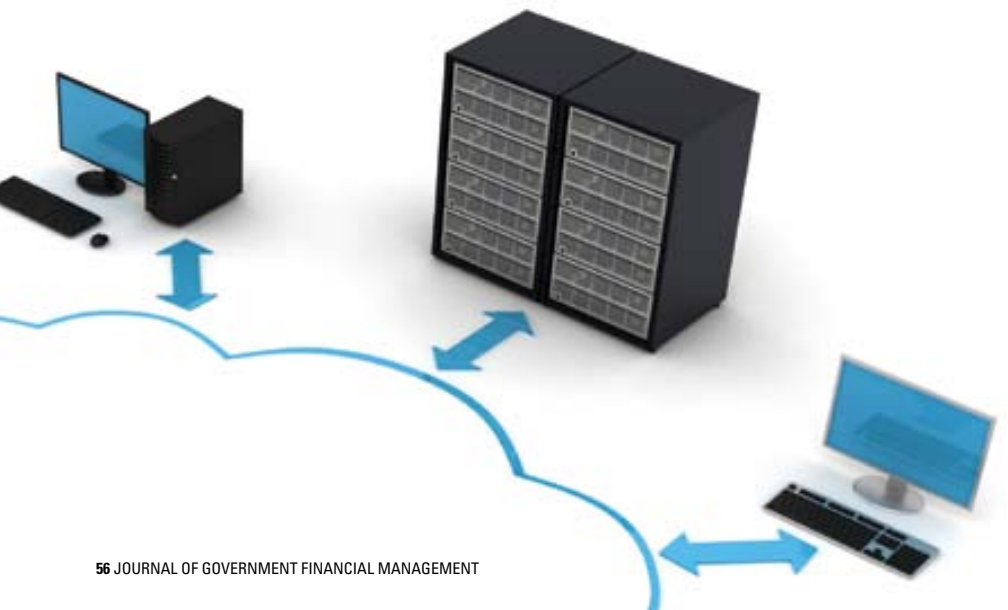
Jeffrey Smith, EEOC chief financial officer, is leading the project, and he explained that the EEOC has been operating in a shared services environment for about 10 years, provided by the National Business Center (NBC). EEOC will be transitioning from Momentum to the new solution. A major EEOC goal was to reduce its operating and maintenance (O&M) costs, and the new system would result in a 40 percent reduction in cost compared with what is being paid to the NBC.

Currently, EEOC receives clean audit opinions and has carefully planned its total user licenses to avoid related challenges down the road. Smith said the commission has no issues related to data integrity and cleanup. All in all, the EEOC is predicting a smooth, on-budget transition to its go-live date of October 3.

Naturally, since it is very early in the process for the EEOC, potential challenges and ultimate lessons learned remain to be seen.

Security Considerations, Information Assurance and Audit Considerations

Security concerns have always been and will continue to pose challenges for federal IT managers, and the move to the cloud will be no different. Questions about access to sensitive government data and unauthorized breaches into



federal systems surround the debate over cloud computing. According to a panel of federal technology leaders that convened in early May, "The greatest hurdle to moving vital government data and programs into the cloud is federal executives' confidence in outside security systems."¹⁴ To address security concerns, the Obama administration is developing a program called Federal Risk and Authorization Management Program (FedRAMP), with the goal of establishing a standardized government review of private sector information technology so individual companies' offerings will not have to be reviewed and approved by multiple departments and agencies.¹⁵

Although promising, FedRAMP, which will be run by GSA, has not alleviated all concern over data security in the cloud, and some federal leaders remain apprehensive about turning over large volumes of sensitive data that will reside in remote cloud clusters of networks. As seen with recent problems in Amazon's cloud network, these concerns are not insignificant.

The real question revolves around security of federal systems and data as a whole, and is certainly not specific to cloud computing alone. In today's federal IT environment, security remains a major issue particularly as it relates to access to sensitive systems and classified information. Moving to the cloud will not necessarily elevate security concerns to new highs, but will rather keep the same focus on them as they exist in the current environment. In the end, they will not be going away.

Any thought of handing over large amounts of federal government-owned data to another party elicits concerns about assuring data integrity, continuity of operations and disaster recovery. Again, the Amazon example demonstrates that a cloud solution is not without risks.

In assessing whether a cloud solution makes sense, considerations need to include how to defend applications and data from potential malicious attacks, and providers need to prepare and undergo all the required certifications and accreditations for a cloud infrastructure. These types of tasks require highly skilled and certified staff in addition to meticulous planning.

Recently, the Information Security and Identity Management Committee (ISIMC) of the federal CIO Council released its strategy and guidelines

for the use of cloud computing. Specifically, the ISIMC outlined a series of measures and controls to be put into place for any federal cloud solution, to include:

- ➔ The cloud environment must have verified, auditable controls to provide assurances to users that it will not cause them harm.
- ➔ The cloud environment must be robust and complete in its defensible architecture and controls.
- ➔ The cloud environment must provide rapid and automated defense and response, such as malware detection, audit, identification and access controls.
- ➔ The cloud environment must be able to address the intellectual capability of the attacker, and include robust architecture, standardization, risk assessment and policy training for human defenders.¹⁶

Typically, shared service providers are required to produce annual audited assurance statements to its users and federal clients. Similar statements need to be included as part of a shared services solution based in the cloud. And what about the response from the audit community? Federal cloud computing is so new that the audit community has yet to weigh in with its thoughts.

Concluding Thoughts on Moving Forward with Cloud Computing

Whether it is simply another version of shared services, or a new concept, it appears that cloud computing is here to stay, at least for the foreseeable future. And it is clear that the potential gains in operational efficiency and cost savings are significant, and that it makes overall good business sense for the federal government to adopt proven best practices from the commercial world. While the potential exists for major savings, during the early phases of this movement, they are difficult to quantify given the challenges of security, business processes, data cleanup, etc. Like any good thing, important considerations must be part of the equation. It will be important to assess those activities that are best served to move to the cloud, analyze the costs versus benefits, and ensure that security and information assurance concerns are an integral part of the planning.

End Notes

1. U.S. Chief Information Officer (CIO), *25-Point Plan to Reform Federal Information Technology Management*, December 2010.
2. Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing.
3. U.S. Chief Information Officer (CIO), *25-Point Implementation Plan to Reform Federal IT*, December 2010.
4. Wikipedia, definition of Cloud Computing and IaaS, http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure.
5. "GSA to boost cloud computing with new RFP," *Federalnewsradio.com*, April 28, 2011, www.federalnewsradio.com/?sid=2362341&nid=35.
6. "IT Reform: GSA Issues RFQ for Cloud Email Services," *CIO.gov*, May 11, 2011, www.cio.gov/pages-nonnews.cfm/page/IT-Reform-GSA-Issues-RFQ-for-Cloud-Email-Services.
7. *The Washington Post*, "Government Closing Down Data Centers of part of IT overhaul," Majorie Censer, April 27, 2011, www.washingtonpost.com/business/capitalbusiness/government-closing-data-centers-as-part-of-federal-it-overhaul/2011/04/26/AF7Bpb0E_story.html.
8. "Army completes first stage of cloud email move," *nextgov.com*, April 20, 2011, www.nextgov.com/nextgov/ng_20110429_6654.php.
9. "Cloud Illusions and Confusion: The Fog of Wasteful Government Spending," *Huffington Post*, April 13, 2011, www.huffingtonpost.com/linda-e-brooks-rix/cloud-illusions-and-confu_b_848647.html
10. *Ibid.*
11. "Labor Department takes financial management to the clouds," *Government Computing News*, February 2, 2010, <http://gcn.com/articles/2010/02/01/department-of-labor-financial-management-system-cloud-computing.aspx>.
12. DOL Releases RFI on Cloud Email," *FierceGovernmentIT.com*, May 30, 2011, www.fierceregovernmentit.com/story/dol-releases-rfi-cloud-email/2011-05-30.
13. "EEOC Takes Financial Management to the Cloud," *Government Computing News*, March 8, 2011, <http://gcn.com/articles/2011/03/08/eec-financial-management-cloud.aspx>.
14. "Security remains the biggest hurdle for agencies moving operations to the cloud, federal IT officials say," *Nextgov*, May 5, 2011, www.nextgov.com/nextgov/ng_20110504_5517.php.
15. *Ibid.*
16. Federal Cloud Computing Strategy, May 2011, www.us-cert.gov/GFIRST/presentations/Federal_CIO_Council_ISIMC_Guidelines_for_the_Secure_Use_of_Cloud_Computing.pdf.



Robert E. Maitner Jr., CGFM, PMP, a member of AGA's Washington, D.C. Chapter, is a senior manager with Baker Tilly Virchow Krause, LLP.