NTT DATA
Global IT Innovator

Issue 1

Strategy and Tactics for Federal IT Modernization

Tactical myopia in the rush to modernize and reach the cloud is limiting broad, deep and expandable success

Introduction: The rush to the cloud

The United States federal government faces many related, pressing information technology (IT) issues and modernization challenges:

- Obsolete and old applications and infrastructure (legacy systems)
- Diverse IT portfolios
- Numerous data centers (consolidation)
- Cloud First mandate[1]

Nat Bongiovanni
Chief Technology Officer,
NTT DATA Federal Services, Inc.

Many obsolete legacy systems are past due for replacement or retirement, and many aging systems are ripe for rework or upgrade. The proposition may be daunting: Legacy systems cost so much to maintain that just keeping the proverbial lights on consumes nearly all the IT budgets of government agencies. Civilian agencies, for instance, spend approximately three quarters of their IT budgets on legacy systems[2]. Sustainment allocation is broadly dislocating modernization.

Some agencies have even had to stop paying annual maintenance on select commercial, off-the-shelf (COTS) software and hardware because they simply do not have the budget to fund maintenance contracts for all their systems. Money that should be spent to modernize and move *away from* legacy systems is instead spent on inflexible mainframes, vintage code, proprietary architectures and no longer supported technologies to maintain service commensurate with user/customer demand. It is a vicious cycle of spiraling maintenance costs and limited innovation.

In haste, or even out of desperation, government agencies are moving rapidly but not necessarily effectively (i.e., doing the right things) and/or efficiently (i.e., doing things right) to the cloud.

This newsletter is not meant to make the case for modernization. If you're reading it, you likely already

[1]Kundra, Vivek. "Federal Cloud Computing Strategy." The White House, February 2011.
[2]Miller, Jason. "Agencies spending more on IT modernization efforts than they think." Federal News Radio, January 2016.

Gartner

realize that your legacy systems stand in the way of progress and efficiency. Instead, I will discuss the intricacies of modernization, as well as a *potential* cloud transition strategy to follow — one that is non-disruptive, quicker and more affordable.

Organizations need to understand the hard work to be done, beyond the proverbial low-hanging fruit, to match reality to the rhetoric. NTT DATA's efforts on behalf of its public and private sector clients have, in some cases, resulted in up to 30% gains in process and operational efficiency, 50% reductions in development costs, 10% to 15% savings in support costs resulting from retired applications, 30% to 50% savings in application support and up to 30% reductions in total cost of operations.

I hope this newsletter, featuring research from Gartner, informs and guides you as you explore the possibilities for modernizing your organization and migrating successfully to the cloud. If you would like to discuss your agency's specific requirements, contact us at: INFO@nttdatafed.com.

Nat Bongiovanni
Chief Technology Officer,
NTT DATA Federal Services, Inc.

Strategic forethought: Overcoming tactical myopia

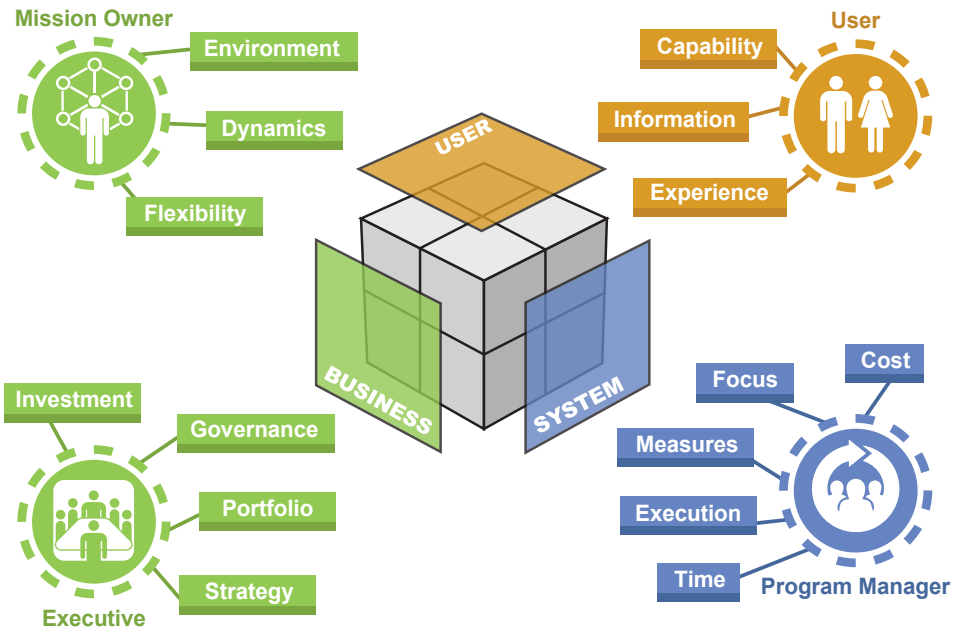
Strategic forethought, or planning, for modernization and cloud migration is essential to realize the conceptual, presumed benefits. Modernization is not just about technology; it's about an organization's purpose or mission. It is important to understand the things the organization must accomplish from *user, business* (operational, in the government space) and *system* perspectives. Doing so offers a true understanding of anticipated, real-world look, feel, purpose and performance of the deliverable(s); for example, how the form factor of the user interface impacts productivity.

At NTT DATA, we use the holistic, tailorable Surveyor framework to effect strategic forethought. It aligns business/operational goals, user needs and technology capabilities, and it balances the interests of the client hierarchy — from the user through the executives. There are many questions to answer; for instance: Is the environment dynamic or static? How much time is available? How much money?

The Surveyor framework enables clients to evaluate and reform their existing IT strategies or to build new, transformational strategies that are both completely aligned with business (or government operational) priorities and driven by empirical evidence. Ultimately, an effective strategy enables the business/operation and, conversely, a non-existent/poor strategy is a hindrance. It is important to understand the current IT assets as a total portfolio. Only then will you be able to determine, and possibly develop, suitable modernization options *before* creating a target-state architecture that balances business needs, technical debt (i.e., eventual consequences, the work that needs to be done) and skills. The modernization effort should be a tailored affair that follows a thorough analysis of an agency's legacy systems to reveal the most suitable modernization approach(es).

Inputs and insights must be synthesized into emerging hypotheses that are validated, prioritized and transformed into future-state requirements.

FIGURE 1 The Surveyor framework considers user, business and system perspectives for strategic alignment



Source: NTT DATA

Strategic forethought can eliminate inefficiencies in systems and drive continuous process improvements, freeing up funding to invest in modernization and technology enhancements.

Reality-based requirements drive the future-state vision and the supporting future-state architecture that, in turn, is translated into a prioritized list of projects leading to the desired end-state. Hence, *strategic approaches can leverage individual projects to address multiple issues — like modernization, data center consolidation and cloud migration — and spend scarce IT funding to advance on multiple fronts.*

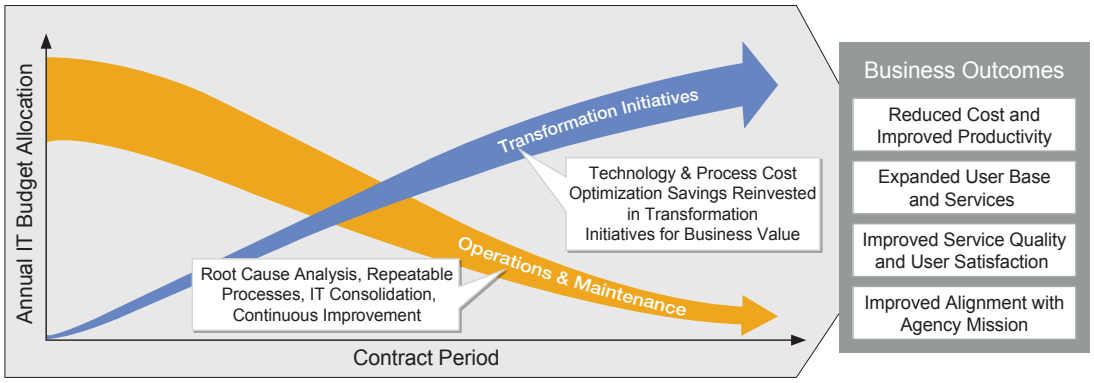
Assessments and strategy initiatives sometimes seem esoteric or vague from a client perspective. This enforces the sense of skeptics that such efforts involve clients providing all the input and prioritization. In actuality, worthwhile, meaningful strategic forethought challenges and informs client input with industry trends, best practices, cross-client experience and technology thought leadership to drive higher value results. The ultimate outcome is an actionable roadmap that is well informed by the client constituencies, defined as a series of interim states with an associated project list. Recommendations are highly specific and feasible, and they have a defined cost-benefit profile.

Strategic forethought can eliminate inefficiencies in systems and drive continuous process improvements, freeing up funding to invest in modernization and technology enhancements.

A properly structured modernization program or initiative has the potential to create enough budget space to reinvest in transformation projects and modernize a technology footprint without increasing overall budget size[3]. Modernization may become self-funding and self-sustaining; within a fiscal year, for example, if the right things are done (being effective), enough may be saved to fund the next year (greater efficiency). Voices in the U.S. federal government have also begun to promote the idea that it is possible and desirable to "harvest inefficiencies to reinvest in innovation."[4]

Just a few years ago, a large government agency faced a significant potential cost because of its use of expensive, proprietary computing platforms. NTT DATA led an evaluation that demonstrated the same capability could be achieved with commodity hardware using the Linux operating system for a fraction of the cost — millions of dollars that could be used for more urgent and important tasks.

FIGURE 2 Strategic forethought may create budget space for reinvestment



Source: NTT DATA

[3]Chharia, Ashwini. "Transformational Outsourcing: A Self-Funded Approach to Transforming an IT Organization." NTT DATA, December 2015.

[4]VanRoerkel, Steven. "Federal Information Technology FY 2014 Budget Priorities." Executive Office of the President of the United States, April 2013.

Transformational Outsourcing

A self-funded approach to transforming an IT organization

Many government organizations are burdened by aging IT environments that consume an increasing amount of the annual operating budget and may, in turn, lead to technological obsolescence. In many cases, these organizations recognize the need for a truly transformative modernization of IT systems and processes. However, most lack a funding source or the expertise to implement such a transformation. One innovative approach government agencies are considering is transformational outsourcing.

Download the perspective.

Acknowledging and moving beyond the limits of legacy systems

Enthusiasm often outpaces readiness in modernization and cloud migration initiatives. The fact of the matter is that most legacy systems:

- Are brittle
- Cannot run on or do not benefit from virtualized environments
- Are not cloud-ready
- Cannot adapt to new security requirements and vulnerabilities

So, rather than forcing technological upheaval and overly ambitious leaps for the cloud, it behooves organizations to follow defined processes for modernizing and transitioning systems. For instance, there are likely phases for a move from one hosting environment to another:

- **Rationalization** to determine the value and technology status of applications, as well as to identify where modernization efforts will have the best impact (and where modernization may not bring sufficient benefits)
- **Analysis and design** to define needed resources and the schedule for those applications that require rework, or even replacement, as well as to identify the technical work to be completed
- **Modernization** to perform the defined work to make an existing application cloud ready, as well as to test a reworked application(s) for production readiness
- **Transition** to perform the work necessary to prepare the cloud environment, test the cloud environment and test the process to transition to the cloud, as well as to perform back-out/rollback, if needed
- **Operations** to support the business with the application in the cloud environment, as well as to monitor resource utilization to identify and leverage areas where configuration changes can improve efficiency with no negative impact on the mission

Rationalizing diverse portfolios

Diverse enterprise IT portfolios — imagine numerous assorted applications and infrastructure components across a wide range of programming languages, operating systems, databases and devices — have significantly increased support costs and resource demands. Lack of strategic forethought while attempting to modernize, or what was earlier referred to as "tactical myopia," further aggravates the "portfolio spread" problem.

The ongoing impact of budget constraints and mandates to do more with less leaves a higher number of legacy systems outdated and less effective than ever before.

The ongoing impact of budget constraints and mandates to do more with less leaves a higher number of legacy systems outdated and less effective than ever before. Organizations can end up doing even less with less or more operations and maintenance (O&M) spending; of course, neither condition is desirable.

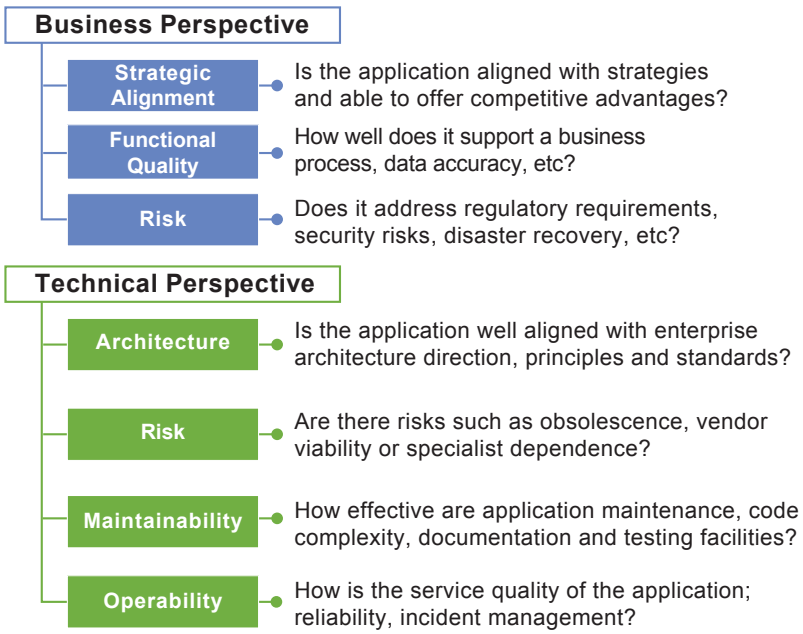
Rationalization is a fundamental activity to preclude the aforementioned hazards and to promote simplicity — more precisely, reducing accidental complexity through intentional simplification — and to improve both efficiency and data quality. NTT DATA's Application Portfolio Rationalization (APR) process and toolset has been applied with over 200 commercial and government clients. APR can be applied to many different types of systems commonly found in government, including government or commercial off-the-shelf and open-source or custom applications. APR methodically assesses each application to identify capability/deficiency in functional and technical areas, as well as to identify a path forward for modernization efforts.

The assessment evaluates the entire technology stack for each application and provides insight across the portfolio. This, in turn, enables the capability to further rationalize the underlying infrastructure, including determining valid approaches for cloud migration. Such a combination of expertise, methods and tools results in a broader view than just evaluating applications. One of the key aspects of this is a metrics-based assessment tool that can be configured to measure elements of value for each client.

APR has baseline business (functional) and technical evaluation criteria. We have a predefined base set of nearly two dozen criteria and scoring values that we tailor to the organization for which we are doing the evaluation. Some criteria are weighted more heavily than others, and the tool is designed to easily adjust the criteria, scoring and weighting.

Inputs are collected through multiple channels, including technology discovery using simple network management protocols, as well as via a questionnaire and interviews with client stakeholders. The same rules and scoring are applied across the full set of applications being

FIGURE 3 Sample business and technical evaluation criteria of NTT DATA Application Portfolio Rationalization



Source: NTT DATA

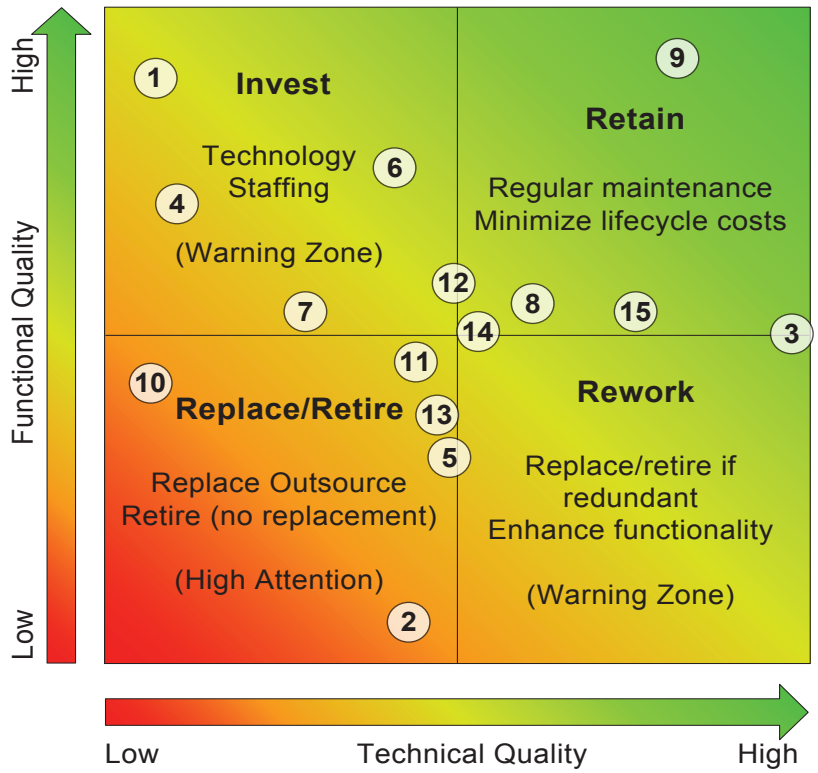
assessed. This assures fair scoring is applied, while also removing the emotional or "conventional wisdom" aspects of lesser assessments.

With the configurability of our APR tools, we include data quality along with application rationalization. It is common that as an application ages, the way in which it is used evolves. As a result, portions of the older data are less valuable, sometimes misleading or even incorrect. More recent data within the system is better aligned with the current mission paradigm and generally holds more reliable data. The rationalization process identifies data that no longer brings value to the mission (or even detracts from mission success) and supports recommendations to improve or eliminate those data sources, thus improving data quality.

The output for a portfolio assessment identifies functional/mission value and technology drag. Where the categorization of actions has not already been determined, we use our tool to categorize applications in four quadrants as shown in Figure 4:

- **Retain** applications (circled numbers in the upper right quadrant) that are serving the organization well.
- **Invest** in applications (upper left) that support the organization and mission well but would benefit immensely from corrections to technical deficiencies, such as a platform upgrade.
- **Rework** applications (bottom right) that, while of good technical quality, are weak mission supporters. These applications may be redundant with retain applications. Thus, with some rework on the retained applications, redundant applications can be retired.
- **Replace**/**Retire** applications (lower left) that exhibit both mission and technology issues and that do not bring sufficient value to the organization. Equivalent/comparable functionality often already exists in retain or invest applications, so retiring the application is prudent.

FIGURE 4 Categorizing applications for action using NTT DATA's APR tools



Source: NTT DATA

There are many more scoring tables and graphs such as more detailed scatter plots and heat maps that offer significant detail behind this type of summary display which are standard APR outputs.

Once the scoring is completed and validated by our staff and with our client stakeholders, we develop a roadmap to define the approach that will be used to modernize the applications and migrate them to the cloud.

Once rationalization is complete, analysis and design begins. Multiple parameters can be addressed concurrently. Parameters might include establishing the security baseline, determining the to-be architecture for applications and/or establishing cloud-based server size.

Data center consolidation and Cloud First

The federal government is moving ahead with major initiatives such as data center consolidation and Cloud First. Without strategic planning, however, these efforts seldom yield desired cost savings and could jeopardize mission success, regardless of tactics. Not all systems can, or even should, be migrated to the cloud. Following APR, and with a view of the applications that can be consolidated or moved to the cloud, you need to have a reasonable idea of the effort necessary to modernize the applications. That work helps drive data center consolidation and cloud migration.

The federal government is moving ahead with major initiatives such as data center consolidation and Cloud First.

Immediate, tactical steps (if well planned and executed) can drive strategic goals while impacting the mission and cost in the near term. The related challenges all center on the problem of legacy migration. Looking holistically (strategically) instead of discretely (tactically) can enable one investment to address multiple problems.

Incorporating commercial best practices and tools

Unsurprisingly, IT solution and service providers can quite easily become proverbial hammers looking for nails. Affecting success is predicated on bringing the right "tool" for the given problem. Last year's (or last customer's) answer is not the prescription for all.

The federal government can benefit greatly from IT modernization and cloud migration experiences in other sectors, such as industrial, commercial and academic. Multi-sector experience provides exposure to best practices and the latest and most practical technologies. For government to truly develop and operate with the efficacy and efficiency often credited to the private sector, best-of-breed solutions must be brought into the federal space; these are often discussed, occasionally heard, but less often embraced "outside the box" lines of thought. The best practices need to be recognized, chosen as appropriate for the federal client and environment, and then tailored or right-sized.

To briefly discuss the need to understand the impact of right-sizing and a set of applications, we need only consider the very nature of the cloud. In all cloud deployment models (private, community, public, hybrid), workloads are consolidated through some form of resource virtualization. This is the primary, and an often significant, source of cost savings over on-premises solutions that are not currently virtualized. Planning for workload consolidation is critical for success. At the beginning of a transition phase, current applications are assessed to determine runtime statistics, patterns and cycles that are inherent in the function of the application. It is most efficient to size servers based in a public cloud at a capacity that handles spikes within specific time periods. For instance, if a server runs at 10% CPU utilization most of the time and spikes to 25% CPU utilization once a week, with no other patterns, then the size of the compute metric for the cloud server should be approximately 25% of the current physical server. Other metrics, such as memory, storage and network, can be similarly sized and configured. In essence, knowing the application runtime metrics is necessary to effectively plan a cloud deployment — or at least have a sense of how it should be accomplished.

As a starting point during analysis and design of the best practice cloud migration, all the utilization statistics for all the servers within the "as is" environment are analyzed and the new environment is designed to meet minimum compute, memory, network and storage requirements. In the cloud, starting small does not introduce significant risk, because the organization can conveniently and immediately resize the environment after transition. Also, in the cloud, starting with the minimum requirements reduces the operating costs of the environment. Once the application has been transitioned to the public cloud environment, performance statistics can be evaluated on an ongoing basis and sizing based on actual usage can be periodically adjusted. Of course, most cloud-ready applications take advantage of the native elasticity of the cloud to resize themselves within set parameters. Across an IT portfolio, this process significantly reduces compute, memory, network and storage costs.

Global research and innovation

At NTT DATA, we benefit as a subsidiary of the NTT Group. We have both a diverse client base and access to the work of the NTT Innovation Institute, Inc., known as NTT i³, "i cubed." NTT i³ is a world-class open innovation and applied research and development center that contemplates and cultivates thought leadership, innovative strategies and practices, and technological breakthroughs.

Learn more about NTT i³ and its latest innovations.

As described in the previous paragraphs, incorporating or integrating commercial best practices and tools is very much a strategic issue, because strategic business and operational decisions (or lack of) will either promote and support or dissuade and obstruct desired outcomes and end-states. There are evolutionary and revolutionary innovations, some sustaining and others disruptive[5], in or coming to the marketplace that may or may not be appropriate in the federal space. Good, well-informed strategic consultation and consideration will identify potential solution paths and synergistic opportunities.

Approaches: Modernization tactics

Tactical considerations are better reserved for after thorough strategic assessments. The assessment determines what needs action but does not prescribe the specific approach or options for enhancing business value. There are different modernization tactics, such as:

- **Migration**
  - Translates (converts) existing code from one programming language to another
  - The most common migrations are from COBOL to other programming languages, such as Java or .NET
  - Business value: Reduce mission risk and costs by moving away from older technologies where sustainment resources are dwindling
- **Augmentation**
  - Applies to applications that are operational and meet mission objectives but cannot accomplish a specific, requisite organizational function(s)
  - An example is the creation of a data warehouse or a big data store to provide analytics or extended search capabilities to an existing enterprise system
  - Business value: Reuse components that provide mission needs with acceptable technologies, thereby reducing the risk and cost of unnecessary change
- **Replacement**
  - Preferred when the application cannot be migrated for technical, legal or functional reasons
  - Examples include replacing a heavily modified COTS program with a low-code solution or replacing major sub-components of a custom application so that it can be transitioned to a cloud environment
  - Business value: Eliminate applications that may not fully meet the mission, or technology that has introduced unacceptable cost or mission risk

[5]Christensen, Clayton and Michael E. Raynor. The Innovator's Solution: Creating and Sustaining Successful Growth Boston, MA: Harvard Business School Press, 2003.

- **Improvement**
  - Use when an application meets functional criteria and has minimal technical risk but can be made more efficient or more effective
  - For example, a legacy client-server application might be improved
  - Business value: Reuse components that provide mission needs with acceptable technologies, thereby reducing the risk and cost of unnecessary change
- **Encapsulation**
  - Isolates an aging technology that is difficult to migrate from all modern systems
  - An example is moving all the interfaces of an aging mainframe to an enterprise service bus (ESB), thereby making the connection to other systems more reliable and less brittle
  - Business value: Reuse components that provide mission needs with acceptable technologies, thereby reducing the risk and cost of unnecessary change

Determining which modernization path to follow — a tactical choice — is predicated on the results of the APR — which is consistent with the strategic view. We assess the current solutions first, and then use that assessment to define the most efficient approach to modernize and enhance business value. The following examples show how these approaches play out in the real world.

Mainframe encapsulation and migration

NTT DATA has done work for a government customer with a very complex mainframe environment that required a two-step approach to modernization. The first step involved the encapsulation approach, isolating the mainframe connection by creating an ESB layer between the mainframe and all other applications. This masked underlying changes and minimized disruption to users in the second step, which migrated COBOL code to a modern Java environment in a relatively short time.

Legacy client-server augmentation

NTT DATA recently completed the augmentation of a legacy client-server application, making it a cloud-ready application that is much more stable and scalable. A significant part of the augmentation involved removing unnecessary technical complexity and introducing coarse-grained web services. This enabled significant changes in the underlying support technology that both decreased cost and increased reliability.

For many legacy client-server applications, the capability to augment or improve the relatively recent n-tier architectures makes them more efficient for the cloud. This is especially true where the architecture uses the very common model of a web tier, combined with an application tier, and then a data tier. In most cases, the web tier and the application tier can be readily augmented to allow for high elasticity, thereby gaining significant efficiencies in the cloud. Also, because major cloud service providers (CSPs) offer database services, it is possible to migrate a COTS database to a CSP database and gain further efficiencies.

Analysis and (re)design of a given application might include some significant changes; for instance, moving the business logic from the database to a middle application tier or restructuring the "client," perhaps a web server, to appropriately leverage the application layer. An architectural aspect could be web tier and application tier elasticity — automatically expanding and contracting to minimize operational costs while always maintaining adequate response time for the capability owner — in a public cloud environment.

The redesigned architecture could be configured to have three tiers:

- A data tier that leverages existing database functionality in the cloud
- An application tier that uses an application server image and load balancing combined with auto scaling to correctly size the application tier at all times
- A web tier that utilizes a web server image that is also designed to load balance and auto scale

Cloud transition

Transition to the cloud starts with defining the configuration of the cloud environment that will support migrated applications. Establishing and testing several sample configurations will identify an efficient, scalable, reliable and cost-minimized configuration. Automated scripts can be created to perform the transition, and they can be repeatedly tested and refined to account for

the many variables that can occur in the transition process. Developing a back-out/rollback plan and processes is highly advisable.

Application analysis

In the context of transition, an *application analysis* identifies the most efficient, scalable, cost-effective configuration of the cloud environment. At NTT DATA, we evaluate all the performance metrics for compute, memory, network and storage to determine the actual statistics and usage on all tiers for all servers. Using the data collected in that process, we establish initial configurations, and then test them to measure the results. We also establish the initial cloud configuration based on the best results of the testing. It's important to review the tests and recommended cloud configuration with clients.

Security requirements analysis

Security requirements analysis for the transition of applications to new environments, be it a cloud or a physical server environment, should include a consistent set of starting steps, and then additional validation steps as required.

Our analyses often include a review of the Federal Information Processing Standards (FIPS) environment requirements (high/medium/low) for the current operational authorization(s). This provides a baseline for security controls testing validation in the target environment. Any identified gaps are remediated and validated in advance of application transitions, and the authority to operate (ATO) is then potentially extended to the new environment, if applicable. Variables between applications may require additional steps; for example, applications that use Active Directory for authentication inherit previously validated/approved security controls. Applications that use separate authentication must be reviewed to determine if they can inherit existing controls or if they will require separate testing for their authentication, including steps to validate variables such as password strength, password change cycle, incorrect password lockout thresholds or grace logins provided.

The planning process is not significantly different for transition from a physical colocation environment to a public cloud environment. It still requires the same analytical steps, including a review of the prior assessments (e.g., FedRAMP) completed for that cloud environment and any potential weaknesses. Public clouds with, for instance, FedRAMP and Department of Defense Impact Level certifications likely meet many required security controls. However, an analysis will check to see if transitioned applications rely on an area that may have been a weak point in the last assessment of the public cloud.

Other system-level controls can be created to fully satisfy testing for ATO for the migrated application in the new environment. During security requirements analysis, existing baseline plans can be tailored for establishing and testing security controls that are not met in the application and the cloud platform. The plan can define the IT security requirements that must be met in the target cloud environment. Necessary technologies can then be added to the plan to fulfill each requirement and position the government to pass the ATO for the migrated application. Wherever possible, existing solutions should be used to meet requirements, especially when adding a migrated application to an existing private or public cloud environment. In-place identity and access management solutions, intrusion protection and prevention, data encryption, security monitoring and other system-level IT security elements are referenced, as available, to satisfy the related requirements.

At NTT DATA, we often have insights that prompt us to look beyond stated requirements. We take extra steps, starting when we create our security transition plan, to implement and use in actual operations all industry best practices — like security patching of images and applications, closing unnecessary ports on all servers, only allowing relevant applications and services to run on those servers, and installing and integrating a continuous monitoring solution such as a security information and event management (SIEM) agent on servers to monitor logs.

Virtualization

Of course, transitioning to the cloud involves *virtualization* of as many aspects of the applications and system as possible. In a hybrid or private cloud environment it is possible to mix non-virtualized and virtualized capabilities. In the public cloud, however, everything is either virtualized or provided as a service. When transitioning applications to the cloud, and especially to the public cloud, understanding how to reduce the overall size of the environment can reap significant cost benefits. Determining what

can be turned off, as well as when and how, scales servers based on necessity with as little excess capacity as possible. As a result, the application owner can significantly reduce cost while maintaining operational readiness.

The transition of an application and its related environments to the cloud starts with the use of virtual machines, provided the images are as close to optimal at the start. This includes a database server image that is sized based on normal usage and accounts for expected spikes, a single application server that can automatically scale to multiple application servers, a load balance across those servers and a web server that operates similarly. As the application is modernized, it can be deployed to the cloud environment — first in the development environment (only running when in use), which is easily replicated to the testing environment (only running when in use), and then replicated to the production environment. The virtualization can be nearly invisible if the concept of using virtual machines is inherent in the entire process.

As public cloud providers have proven, virtualization at every level of the IT stack is valuable and enables maximum flexibility in providing IT services to internal and external consumers. Virtualization of network communication and storage, as well as servers, enables deployment of resources on very short notice. It is equally valuable to be able to add resources to existing configurations to support increasing loads, even when those loads were not projected. Public cloud providers offer GUI-based tools to add these resources quickly, and many are automated based on configurable parameters.

Schedule

When considering a transition *schedule*, project activities should minimize impact on the mission supported by the application, the time frame for transition to avoid peak periods such as fiscal year-end, the users of the application and the organization(s) affected or using the application. All aspects must be considered, not just requisite technical tasks or tactical maneuvers to place an application in the cloud. For instance, consider the impact schedule has on the various stakeholders performing O&M for an application. Use off-hours/weekends or other periods of downtime to perform transition activities whenever possible.

Proper schedule steps include a planning process that identifies the events and dependencies required to complete the transition. Planning should occur in conjunction with the client's subject-matter experts on the application being transitioned. Schedule time is allocated to defining, configuring, testing and reconfiguring the cloud model/environment (whether private, community, public or hybrid) necessary to support the application. Sufficient time must be afforded to test new applications in the cloud environment, as well as the processes of deploying the application into the cloud environment and rolling back the deployment. Moreover, schedule time must also be allocated for reviewing the outcomes of each step, and then adjusting based on those results. Clients should be included in all transition activities, as their schedules permit, and encouraged to participate in and review the results of preparations for deploying an application to a cloud environment.

Data preparation

Data preparation is highly dependent on the age of the legacy application, the technologies used in that application and the efficiency of current data structures. In most cases, data restructuring is required and should be part of the application assessment.

If data is held in outdated technologies and must be migrated to current solutions, we prepare it for transition by applying tools to the existing data stores to perform automated data conversion to the greatest extent possible. We have been successful at significant automated conversion with minimal manual efforts. For example, our current work for a federal client entails converting from an antiquated Unisys® database to an Oracle® database. Automated mapping tools did a significant portion of the work, and a small number of data architects completed the data conversion. This is one way, as mentioned earlier regarding strategic forethought, to eliminate inefficiencies in systems, drive continuous process improvements and thus free up funding to invest in modernization and technology enhancements.

When preparing for data transitions, it is wise to pursue a practical conversion instead of an ideal conversion. Data migration efforts are often viewed as an opportunity to get everything 100% correct in the perfect taxonomy; in reality, that rarely happens, and then only with very significant resources and elongated schedules. Small

compromises made with clear understanding can significantly reduce the cost and schedule of data migration. Reasonable and valuable compromises deliver solutions quickly, with little loss of fidelity.

In many data stores, there are data elements that are known to be unreliable, corrupt or unused. During data preparation, those data stores can be identified. *Not* trying to correct or clean the data or *not* importing it can save significant costs and control a scheduled transition.

After analysis is complete, data must be migrated to the target solution. In many cases, data volumes are significant and the data continues to evolve as the existing systems continue to run to support the mission. Data preparation can take a point-in-time data capture, including the vast majority of the data placed in the target solution. The data can be converted as needed and loaded into the target solution. From the point of data capture forward, all data changes should be captured as the existing system continues to run. Changes can be applied to the migrated data store incrementally, in much smaller bulk conversions. As cutover dates for new systems approach, bulk loads can be reduced in time span until the last bulk conversion is merely a few hours' to a few days' worth of data that can be converted and loaded as the new system is brought into the production environment.

Interfaces

Retaining *interfaces* to other systems avoids upgrades becoming required for other systems throughout an enterprise. During an analysis and design phase, interface transition planning should identify every system-to-system interface and determine the level of effort needed to upgrade them.

System-to-system interfaces enable data exchange. The portion of the interface that faces another system should remain unchanged, with rare exception. In interface transition planning, the outward portion of an interface can be recreated in the new technologies of the transitioned system. In some cases, adapters are needed as a bridge between older technologies and modern ones. Eventually, the adapter can be eliminated.

Considering human-machine interfaces in the user experience is another factor for successfully transitioning systems. In some cases, clients desire minimal changes in the user interface to avoid retraining the (potentially large) user base. Although this approach is well understood, it must be carefully weighed against the importance of providing an excellent user experience. There is no substitute for collaborating with the client to create the right user interface in the migrated application.

With new interfaces in place, planning for testing and organized cutover for each interfaced system must occur. This involves creating a schedule for transitioning to the new interfaces, considering dependencies and impacts, as well as bringing up the new interfaces one-by-one until all interfaces with other systems are proven to work properly.

Service transition planning, cutover and rollback

Planning the transition of an existing application from its current environment to a cloud environment usually includes a modernized version of that application, and that plan is critical for mission continuity with minimal interruption. Good *service transition planning* starts in analysis and design, working with the client to identify the best window for the transition to occur — this typically means targeting lower utilization of the application as a primary time for transition. The many aspects of service transition should be considered, including user training, technical staff training, impact to other systems, staffing and supporting the new environment immediately after the transition is complete. This planning is significant and should occur as the application is being modernized and the new application and environment are being tested.

To minimize and manage the inherent *cutover* risks, you must create a detailed cutover plan. This plan results in an ordered punch list of the activities necessary to take the existing application out of service and place the migrated application in service in the cloud. Process automation should be maximized, and those automated processes should be tested repeatedly prior to the live cutover event. Inherent in cutover planning is a quality control function to assess potential deficiencies or defects. We create scripts of the cutover and perform checks along the way, repeatedly, until those scripts run flawlessly. Performing multiple mock cutovers demonstrates the viability of the tools. Intentionally creating error conditions during mock cutovers proves the viability of the scripted events and demonstrates that staff are ready should automated processes fail to meet expectations.

In some cases, a few days is sufficient. In other cases, it may require a month to fully cut over. Following configuration management processes and documentation for any required changes maintains the integrity of the new solution. It also enables sufficient governance and oversight, even in a critical stage of the effort.

Although a back-out/*rollback* plan will vary for each application, in our experience, keeping the existing system fully operational for a specified number of hours/days/weeks is a good risk-mitigation step. Data changes can be logged in the new system and applied to the existing system if rollback is required. Inexperienced providers may downplay or overlook rollback, but it is an important — arguably critical — element of transition.

NTT DATA Success story: Re-hosting a disaster recovery site

Recently, NTT DATA Federal Services, Inc., chose to re-host our disaster recovery (DR) site to the Amazon Web Services (AWS) GovCloud. In the move from a physical machine environment to a cloud environment, we used the augmentation approach so that all capabilities were met in the cloud environment. We also replaced some applications with COTS alternatives that were better suited to the AWS GovCloud environment.

The DR rehosting process began with an application portfolio rationalization to identify candidate applications that would benefit from a move to the cloud. Next, we analyzed and documented the specific applications we planned to move to the cloud. This determined whether the cloud environment met all requirements (availability, security, economy, etc.), as well as the optimal cloud configuration. We then identified how we could use capabilities such as a virtual private cloud, Amazon virtual machine images for the web, application and database tiers (EC2), and simple storage services (S3). Minor modernization efforts on the application stack we intended to move followed, including virtualizing physical environments and right-sizing compute, memory, network and storage metrics to achieve optimal results from both performance and efficiency perspectives. After the modernization phase, we developed a schedule for the transition that included multiple live tests at convenient times for the business and mitigated any risk of loss of data or capability. Finally, we created and executed a detailed cutover plan, completed the transition to the cloud and began operating the DR site from AWS GovCloud.

While we were operating the new DR site, we continued our transition activities by decommissioning our previous collocation site and repurposing or retiring the hardware that was no longer needed. In the end, we reduced our disaster recovery costs by nearly 80% and increased our ability to provide solutions to our customers by establishing a Solution Lab Environment that uses repurposed equipment.

Source: NTT DATA

Research from Gartner

Government CIOs See Expected Cloud Cost Savings Evaporate

Government business leaders are pushing agency CIOs to increase responsiveness and deliver savings by making rapid moves to cloud. However, evidence is mounting that these expectations may be overly simplistic and unrealistic.

Impacts

- Government CIOs are making quick, tactical choices to achieve compliance with cloud-first directives and, consequently, are compromising the opportunity to maximize the potential savings or realize other benefits from cloud computing.
- Government CIOs' and business leaders' failure to establish appropriate operational and investment practices creates an environment that complicates their ability to make more considered and strategic decisions, ultimately inhibiting broader support for cloud adoption.
- Weak or absent cloud adoption strategies relevant to the agencies' context hinder CIOs' ability to leverage cloud computing to deliver benefits to the overall organization and, as a result, promote the ad hoc procurement of stand-alone solutions by business units.

Recommendations

Government CIOs:

- Implement cloud-first directives as part of their enterprise IT strategy.
- Examine the business case for any move to cloud and identify all internal dependencies and actions necessary to deliver intended benefits.
- Explore the wider range of attributes associated with cloud such as self-provisioning, scalability and elasticity to determine where these may help meet workloads or support greater organizational agility.
- Engage the wider organizational workforce (such as legal, procurement and risk management), while conducting a capability assessment highlighting the skills, training and culture needed to support the effective use of cloud computing.
- Consider the most appropriate cloud model (private, community, public or hybrid) that will meet compliance requirements, while also delivering the required operational outcomes and anticipated benefits.

Analysis

Agency business leaders and senior executives clearly perceive cloud computing as providing the means to lower costs and improve service — often choosing to proceed without the need to seek approval or even involvement from the internal IT department. Vendors, claiming to be able to deliver significant savings, have successfully targeted the CFO and business leaders by offering cloud as a potential solution to budget problems through reduced IT expenditure. This is, after all, what clients want to hear during periods of severe fiscal constraint. Gartner has seen cases where financial managers, acting on advice from vendors and others, applied immediate budget reductions of 15% and more to total IT budgets. Such expectations are rarely achieved, and transitioning to the new environment and/or decommissioning existing/legacy services may, in fact, cause costs to rise. Such actions, founded as they are on hearsay and marketing hype, have the potential to create enormous risk to government services.

Cost savings remains the No. 1 reason that organizations cite in regards to a desire to move to the cloud (see Figure 1).

There is mounting evidence (see Note 1) particularly emanating from the U.S. following numerous audits, that government agencies following cloud-first policies have not delivered the expected cost savings, nor have they adopted cloud at the expected speed. The most recent and detailed of these audits is that published by the U.S. Government Accountability Office (GAO)[1] in late 2014. It is possible that agencies with significant on-premises portfolios will find themselves in a situation where vendors in search of higher margins are pushing them to transition to the cloud and leave clients to face the more difficult savings opportunities, such as head-count reduction, in order to meet their own commitments.

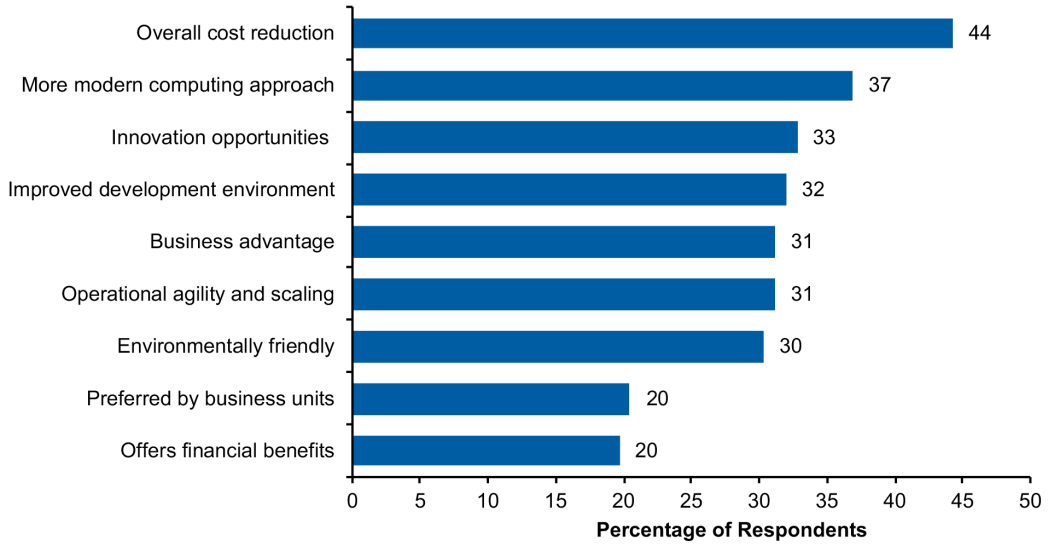
Cloud Benefits Are Bigger Than Savings

While considerable focus has been on the potential savings achievable from cloud computing, the real benefits are arguably in other areas, such as time to deploy new solutions (innovation and agility), scalability that can be exploited to avoid costs by preventing the over provisioning of capacity, and elasticity to meet fluctuating workloads.

However, where budget savings are still required, data center consolidation, which is being undertaken in countries such as Holland and Finland, is most likely to yield savings. It can also facilitate valuable, early cooperation between government departments. Applications that are migrated, instead, directly to the cloud and have not been specifically architected to be cloud-ready/native will not be able to take advantage of the resources (compute and storage, for example) available to them.

Both cost avoidance and cost reduction represent potential savings to the organization, but only the latter can truly deliver a smaller IT budget, while the former is often used to boost savings figures in support of new initiatives.

FIGURE 1 Gartner 2014 Cloud Adoption Survey



N = 122

Source: Gartner (February 2015)

Many governments have initiatives explicitly designed to achieve savings by implementing cloud computing. Processes such as catalog-based procurement solutions have also been utilized to make procurement easier by preselecting suppliers (see Note 2). These approaches do not take into account those SaaS purchases by business departments that can be made now without involving the IT department.

IT Management Practices Need to Be Cloud-Ready

Despite these initiatives, adoption is poor, and few government cloud customers seem to be able to report long-term cost savings. Indeed, vendors such as Skyscape and Eduserv have attempted to help clients do better by advising them of inefficient usage patterns and failure to leverage cloud capabilities or minimize their costs. The same vendors report that some customers seem unwilling to change their operational procedures to switch off compute power when not needed. This lack of willingness to change operational practices or failure to exert adequate management oversight and control over the new landscape helps explain some of the disparity between the expectations and the reality.

Evaluating the benefits of cloud programs can be difficult due to inadequate asset management and a lack of understanding of the true extent of cloud services being deployed within an organization (see Note 3). An organizational strategy, an inventory of cloud services and a capable asset management process are needed; otherwise, it is impossible to ensure that the number of monthly per user charges does not inexorably rise over time. Indeed, poor management and operational practices may well see any savings erased, and in a worse case, cloud could actually represent a higher-cost platform in comparison to more traditional technology solutions. The inventory must utilize existing cloud definitions[2] to avoid confusion caused by the use of "cloud washing" terms. This is critical in order to assess actual progress, in contrast to those situations where either the vendor or the agency chooses to describe the solution in vague cloud terms, largely as a consequence of their desire to demonstrate compliance with policy goals.

Impacts and Recommendations

Government CIOs are making quick, tactical choices to achieve compliance with cloud-first directives and, consequently, are compromising the opportunity to maximize the potential savings or realize other benefits from cloud computing

Any CIO pressed to adopt the cloud must ensure that those making such demands are aware of the policy, procedural and culture changes necessary and the resources required to make the move efficiently and effectively. Invariably, there will be compromises that the business will need to accept. Failure to consider these can lead to delays in establishing procurement policy, staff training and new operational process and procedures, which may lead to delays in cloud adoption, such as experienced by the U.S. Department of Defense.[3]

The GAO report is consistent with Gartner's client feedback and earlier research. The most prevalent myth about the cloud is that it always saves money. While this is sometimes the case, it is by no means certain. The GAO report, for example, showed that only 20% of the cloud initiatives were associated with any savings. There are many other reasons cited for migrating to the cloud, such as increased agility. However, a long and/or complex procurement process will equally erode the agility benefit as much as any cost savings.

Despite cloud vendors' recommendations for change in operational practice, some customers do not accept or trust cloud's ability to automatically provision additional compute power when needed. This often results in architectures with excess capacity to prevent the possibility of end-user complaints. Those CIOs who have moved an application to IaaS and PaaS, in particular, should have in place a feedback mechanism where vendor-supplied performance and utilization reports are acted on in order to eliminate wasteful operational practices and reduce expenditure to the minimum, without accepting additional risk.

FIGURE 2 Impacts and Top Recommendations for Government CIOs

Impacts	Top Recommendations
CIOs are making quick, tactical cloud choices to achieve compliance and, consequently, are compromising the opportunity to maximize the potential savings from cloud computing.	• Look beyond simple cost savings in developing a cloud-based business case, and understand what benefits are sought. • Subject business cases that claim to deliver substantial cost savings to an independent review.
Failure to establish appropriate operational and investment practices complicates CIOs' ability to make more considered and strategic decisions.	• Engage the workforce in adopting behaviors and thinking that support more effective use of cloud computing. • Assess business practices and consider opportunities to use cloud technology to exploit attributes such as scalability, elasticity and time to innovate.
Weak or absent cloud adoption strategies hinder CIOs' ability to leverage cloud computing to deliver benefits and promote the ad hoc procurement of stand-alone solutions by business units.	• Establish a cloud strategy that can be understood and agreed to by the business and leadership. • Use policy frameworks to control unnecessary duplicated purchasing and to monitor utilization rates of cloud solutions.

Source: Gartner (February 2015)

Recommendations

Government CIOs should:

- Look beyond simple cost savings in developing their cloud-based strategy to ensure that potential benefits align closely with corporate strategic objectives.
- Subject business cases that claim to deliver substantial cost savings to an independent review that the CFO will accept.
- Understand the vendors' performance (solution/system monitoring) reports and act accordingly to manage risks more cost-effectively.

Government CIOs' and business leaders' failure to establish appropriate operational and investment practices creates an environment that complicates their ability to make more considered and strategic decisions, ultimately inhibiting broader support for cloud adoption

Complex compliance regimes and approval processes often exist in government, and CIOs are expected to follow routine operations in order to ensure that the outcomes do not deviate from the stated government policy or practice. Risk management, auditing, finance, legal and emergency planning departments all seek to devise and influence policy decisions to cover all potential aspects and eliminate risks wherever possible. This wins the approval of elected officials who want to maintain the confidence of voters by minimizing any project or policy failure. However, this is unrealistic, and it slows down the innovation needed by governments and their agencies in their digital journey.

Government CIOs developing a cloud strategy should, therefore, consider how to bring these groups on board. They are vital to reducing the overall complexity of the implementation of cloud and must be encouraged to adopt a pragmatic approach to risk management rather than risk elimination. In this way, CIOs can exploit such cloud advantages as speed to deploy, which are necessary to support the introduction of new business practices, products, services or operating models.

A continued risk-averse approach hampers the efficient introduction of cloud computing. CIOs must begin to understand the issues and engage others in finding the answers to questions about deployment model (private, public or hybrid), data residency and application migration. Some requirements, and hence some of the answers, may be dependent on other government agencies, especially when it comes to security compliance and data protection issues. The government CIO is then dependent on guidance and procedures being made available in a timely manner to allow him or her to proceed. This guidance is often not given.[3] The result is that when government CIOs are tasked to move to the cloud, they are likely to look for the path of least resistance and lower risk, such as test and development platforms, which can be at the sole discretion, and in the control, of the CIO.

Those CIOs who have not already done so will need to include in staff appraisals metrics measuring the efficient use of these new classes of resource for system utilization. CIOs should also monitor workloads and make recommendations to the business when either a change of practice or a move to a new or different cloud platform is appropriate. This strategic approach to determining cloud migrations should form part of an overall decision framework that the business leaders of any government or agency understands and actively takes part in.

Recommendations

Government CIOs should:

- Engage the wider workforce across the government/agency in adopting changed operational behaviors and thinking that supports more effective use of cloud computing, using cultural as well as technical training.
- Monitor and assess existing business practices and their capacity to evolve, considering the opportunity to use cloud technology to exploit the attributes such as scalability and elasticity.

Weak or absent cloud adoption strategies relevant to the agencies' context hinder CIOs' ability to leverage cloud computing to deliver benefits to the overall organization and, as a result, promote the ad hoc procurement of stand-alone solutions by business units

The ability for any part of the organization to procure cloud computing (see Note 4) and the lack of enterprise[4] control or strategy will, over time, lead to increasing organizational inefficiency. Technical architectures become stretched, information architecture becomes more problematic, and costs increase due to the larger number of applications having to be integrated, often at short notice. It is, therefore, vital that CIOs raise this issue and gain the understanding and support of business leaders in order to prevent the lack of strategy leading to a failure to consider the impact on legacy applications.

CIOs and procurement professionals must agree on a cloud service procurement policy or framework as part of an overall cloud strategy. Use this framework to create a constructive, ongoing dialogue with business units to demonstrate that IT is there to help them achieve their business goals rather than just to say no. In this way, a win-win scenario can be achieved for the business unit, the IT department and the overall organization. This allows the IT department to act as a cloud service broker, using a cloud management platform (CMP) to enforce policies and governance over the introduction of cloud services. The CMP seeks to control access management (for example, identity access management), service management (third-party service aggregation into a service catalog), service optimization (orchestration for provisioning and billing) and service selection (cost and SLA comparison across cloud providers).

This approach reduces risk as control is improved over data, security and information flows. Senior management must be made aware of the risks posed to any agency of ill-informed or uncoordinated procurement of cloud solutions. The CIO should be quite explicit in stating that IT takes no responsibility for the consequences of

business unit buying that takes place without their involvement and will not be held accountable for any risks or costs that result.

The conversion of legacy systems to cloud should not be assumed to be simple. For example, USDA officials stated that "they would need to consider redesigning their network topology to accommodate new cloud service bandwidth requirements and traffic streams" (see Note 4). And indeed, the GAO report failed to identify a single example of a legacy system converted or replaced by cloud in any of the agencies reviewed.

In many cases, it is likely that the business benefits will not justify the cost and risks associated with the transition. "If it ain't broke, don't fix it!" is a mantra to which most CIOs would subscribe. In other cases, the implications to the existing enterprise or application architectural models of introducing cloud may create a "ripple effect" that adds levels of complexity beyond what can be sustained and entirely negates any savings being anticipated. Nevertheless, existing architectural patterns, on which most legacy systems are based, are indeed being threatened by cloud, and CIOs would be well-advised to prepare for this future transition (see Note 5).

Recommendations

Government CIOs should:

- Establish a cloud strategy, including how to use a CMP to exert control over the government/agency, and the reasons this must be understood and agreed to by the business departments and senior leadership.

- Ensure that the senior leadership and business leaders understand and actively manage the risks associated with cloud usage, including continued use of legacy applications.

Evidence

[1] Cloud Computing Additional Opportunities and Savings Need to Be Pursued

[2] The NIST Definition of Cloud Computing

[3] DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process

[4] Audit Report The Department of Energy's Management of Cloud Computing Activities

[5] $307 million (2012) + $529 million (2014) + estimated $418 million (2013 no official figure supplied) = $1.25 billion.

[6] Fiscal-year expenditure in report shows $20.7 billion for 2012 and $21.3 billion for 2014, so extrapolated figure for 2013 used is $21 billion to reach total of $63 billion for the three years.

Note 1
U.S. Government Cloud First Policy

The U.S. Government Accountability Office (GAO) published the results of the second examination into the progress of the government's Cloud First policy in September 2014. Based on a sample of seven agencies, representing over 25% of the total information and communications technology (ICT) budget, this showed savings attributable to cloud of less than 0.5% over three years. In particular, of the 101 cloud-based projects undertaken by these agencies over three years, only 22 of these delivered any measurable reduction in costs. This is in contrast to the often-hyped examples of greater than 50% savings that find their way into the public domain. It would seem that either these claims are based on a fallacy or that government agencies are unable to achieve such savings. Government CIOs need to better understand why the failure of cloud projects to deliver meaningful savings appears to be so prominent in government.

In June 2014, the GAO provided a 25-page statement as testimony to the U.S. Senate on reform initiatives that could improve efficiency and effectiveness in information technology. In that statement, the word "cloud" did not feature.

The GAO report highlights savings being generated for the seven agencies by only 22 out of the 101 projects undertaken over three years. Against expenditures of approximately $1.25 billion5 by these agencies on cloud services, savings of just $95.95 million were recorded. Cloud projects therefore generated less than 7% of savings on their related investment. In reality, however, the situation is actually far bleaker. When considered against the estimated total IT expenditure of $63 billion6 for these agencies, savings from cloud represent less than 0.5%. It is also worth noting that the IT expenditure for these agencies shows a year-on-year increase over the period when many governments are showing real cuts in expenditure.

Note 2
Cloud Procurement Initiatives

The U.S. Government has sought to help realize savings through its Cloud First initiative, while aiming to concurrently minimize risks by implementing certification programs such as FedRAMP. In the U.S., states such as California and Hawaii have implemented their own community cloud offerings as a different approach to achieving cloud benefits, while minimizing risks associated with the public cloud. Frameworks such as the U.K.'s CloudStore (GDS G-Cloud) and the Australian Government's Data Centre as a Service panel are examples here. In both cases, the intent is to allow agencies at all tiers of government to quickly contract with cloud providers to deliver packaged services.

Note 3
U.S. Government Department Audits

A report from the Department of Labor highlights the department self-declaring 44 cloud initiatives, while audit discovered 130 cloud initiatives being undertaken.

A further report by the U.S. Department of Energy, Office of Inspector General, also highlighting the challenges faced in extracting value from cloud states, that "Absent approval of cloud computing services, the Department may not meet FedRAMP's primary objective of providing a cost-effective, risk-based approach to cloud services by leveraging cloud service assessment and authorization activities." This underlines some of the practical issues that can emerge when seeking to pursue a cloud-first policy quickly and measuring departments' performance or acceptance of the policy against how quickly, rather than how well, they implement their strategies. Comprehensive strategies and business and implementation plans are needed to procure, control, coordinate and monitor cloud programs effectively if savings will be achieved at all. A more recent audit report by the Inspector General for the U.S. Department of Defense states in its findings that "...DoD may not realize the full benefits of cloud computing. In addition, DoD was at greater risk of not preserving the security of DoD information against cyber threats."

Note 4
Cloud Enables the Rise of Shadow IT

This lack of control can be seen within the U.S. Department of Energy report, which shows that the CIO reported against 44 initiatives, whereas 130 were actively running. This exemplifies the rise of shadow IT and demonstrates the scale of the difficulty for the IT department to have overall responsibility for the deployment of technology within any given agency.

Note 5
Legacy Applications Languish

Despite agencies being obliged to comply with OMB's Federal Cloud Computing Strategy and explicitly required to "assess readiness for migration to a cloud service by determining the suitability of the existing legacy application...," the GAO report found that "most of their investments had not been evaluated for cloud services." Agencies stated that they "only planned to consider cloud options for these investments when they were to be modernized or replaced," thus leaving legacy applications untouched until replacements were due.

Gartner Research Note G00272823,
Neville Cannon, Glenn Archer,
2 June 2016

About the Author

Nat Bongiovanni, Chief Technology Officer, NTT DATA Federal Services, Inc.

Nat Bongiovanni is the chief technology officer at NTT DATA Federal Services, Inc. He is a veteran of the United States Navy and has nearly 35 years' experience in the public and private sectors. Mr. Bongiovanni has worked as an analyst, architect, consultant and manager of information technology, systems and operations. He is a project management professional (PMP)® and an Amazon Web Services (AWS) certified solutions architect - associate.

Mr. Bongiovanni has managed everything from short, high-intensity efforts to large programs with multiple subcontractors. As an architect, he has many highly successful implementations of his vision and design. Over his career, Mr. Bongiovanni has made major contributions in data warehousing and enterprise architecture for business and analytics systems. He has produced total solution architectures within multiple team environments. His responsibilities have included project planning, estimating, budgeting, testing and implementation management. Mr. Bongiovanni's management background includes full system development lifecycles, mentoring employees and managing integrated project teams of employees, subcontractors and vendors. He has used his technical expertise and knowledge to advise clients on the effective selection and implementation of technology, as well as on strategies to overcome the obstacles related to implementation.

His diverse clients and employers include the Defense Intelligence Agency, the U.S. Securities and Exchange Commission, Blue Cross Blue Shield and Enterprise Rent-A-Car.

About NTT DATA

NTT DATA partners with clients to navigate and simplify the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. We deliver tangible business results by combining deep industry expertise with applied innovations in digital, cloud and automation across a comprehensive portfolio of consulting, applications, infrastructure and business process services.

NTT DATA is a top 10 global business and IT services provider with 100,000+ professionals in more than 50 countries, and is part of NTT Group, a partner to 85 percent of the Fortune 100.

nttdata.com/americas

NTT DATA
Global IT Innovator