WHITE PAPER

EFFICIENT I.T. IN THE TIGHT BUDGET ERA

Focusing on key areas, such as virtualization, mobile computing and document management, to inexpensively modernize IT systems

Executive Summary

CIOs, technology managers and program executives in the public sector face the challenge of modernizing systems, enterprise applications and mission delivery in the face of tight or declining budgets. Few state and local governments have returned to their pre-2008 status quo of steadily growing revenue and expanding budgets.

The federal government, with its record deficits, is choosing to find savings in discretionary agency budgets. Managers in federal agencies will contend with flat or slightly declining IT budgets for at least the next two years.

Yet pressure to improve government services never abates. Agencies at all levels need funds to invest in state-of-the-art web services, for example. They need creative solutions to cybersecurity threats, to free workers from time and location constraints through mobile computing, and to modernize core enterprise applications.

TWEET THIS!

Table of Contents

2 Tight Public Administration Budgets

3 Data Center Efficiency

6 Mobility

7 Document Management

None of those improvements can happen if outdated IT facilities and processes consume ever-larger portions of fixed annual budgets. So CIOs are turning to investments in technologies that pay for themselves through greater efficiency, not only in the data center, but also in how the enterprise operates. Once amortized, these investments yield savings that are then available to invest in greater productivity, agility and functionality.

Tight Public Administration Budgets

There is no way around it. Government budgets at the federal, state and local levels remain hampered by a weak economy. State and local governments must live within their year-to-year means, with no deficit spending. At the federal level, Congress and the administration are trying to control deficit growth by limiting discretionary budgets — that is, the budgets for operating departments and agencies.

Among the items that managers are asked to rein in is spending on IT. In fact, for the first time, the federal IT budget is set to drop next year. Not by much — slightly more than 1.2 percent.

But in the context of 25 years of rising IT expenditures, any reduction signals a new environment. Congress and legislatures remain committed to improving access to public services using IT, but agencies must find ways to do this with the budget they have.

State IT spending also trends flat or down. Fiscal restraint has been compounded by the winding down of funds flowing from the federal government as part of the American Recovery and Reinvestment Act of 2009.

Yet at all levels, government CIOs and program managers strive to work around these budgetary barriers through innovative approaches to cost-cutting. They can then apply the money they save to new developments, such as mobile services, and investments in modernized financial, enterprise resource planning, human resources and other core applications.

The CDW·G *Efficient Agency Report* (see URL link in the *Finding Those Efficiencies* sidebar) that state CIOs' top priorities for 2012 focus on the consolidation and optimization of data centers, as well as other parts of their infrastructures. The list of priorities also includes cloud computing, broadband and more mobile services.

Government agencies have reached the point where, in order to move ahead with urgent IT modernization plans, they must free up operations and maintenance dollars by updating processes and infrastructure. They must wring out the inefficiencies in data centers to make them more agile and responsive to future requirements.

What Is FedRAMP? Is It Only for Feds?

For two years, the federal Office of Management and Budget, together with several other executive branch agencies, has been working on a project to speed up the process of certifying that commercial cloud-service providers can guarantee a sufficient level of cybersecurity. The project is the Federal Risk and Authorization Management Program (FedRAMP), and it applies to data of medium and low sensitivity.

FedRAMP's goal is to create a single certification process that all federal agencies can use for cloud-service providers. Such a process would save time and effort for both the agency and the cloud provider.

In February 2012, the government released the concept of operations for FedRAMP and chartered the FedRAMP Joint Authorization Board, consisting of CIOs from the Homeland Security and Defense departments and the General Services Administration. This group will approve contractors to certify third-party cloud providers, part of a complex apparatus that's scheduled to begin operation later this year but will not be fully operational until mid-2013.

In the meantime, federal agencies can reference the security controls that FedRAMP will eventually use to vet cloud providers. The standards were developed in conjunction with the National Institute of Standards and Technology (NIST) and are applicable to any agency — federal, state or local — looking for assurance that its unclassified data will be safe in the cloud.

Luckily, government IT managers have several potent tools at their disposal to make technology budgets go further. CDW·G asked several hundred CIOs at all levels of government how they were identifying savings without cutting into the muscle of programs.

The majority of respondents said they were pursuing a strategy of reinvesting the savings from efficiency initiatives into new technology that improves service delivery and produces yet more savings. In fact, nearly 80 percent said they had launched IT efficiency-improvement programs in the past couple of years.

Specifically, technology managers in the public sector are looking at five areas of technology to boost the efficiency of their IT infrastructures:

1. Server virtualization: An immediate efficiency boost can be delivered through server virtualization, which

reduces the number of physical servers an agency needs to do its work. A smaller server count also leads to other savings, such as smaller floor-space requirements and less electricity consumption to power servers, networking and cooling equipment.

2. Storage virtualization: This technology typically follows server virtualization. Storage needs continue to grow. And although the cost per unit of storage has fallen, the total cost has risen, in part because of agencies' underutilization of physical storage, and in part because of management complexity.

Storage virtualization hides the complexity, simplifies storage management and increases the utilization rates of physical disk drives. Coupled with data deduplication and thin clients, storage virtualization can slow the growth of (or even reduce) enterprise storage costs.

3. Cloud computing: This technology offers a source of IT efficiency through the use of shared online services. Vendors host varying levels of cloud services, accessed via secure networks that range from physical infrastructure to software as a service.

Cloud computing presents itself to government IT customers as an infinitely scalable utility, paid for with operational, not capital, funds. Similar to a utility, cloud computing is typically priced on a per-unit basis (per user, transaction or compute capacity), making its costs more predictable.

4. Mobile computing: Productivity increases for government staff by giving them access to data, applications and resources anywhere they happen to be via mobile devices. And with so many staff members buying their own notebooks, tablets and smartphones, there are ways that agencies can enable secure mobility while avoiding much of the cost of acquiring and provisioning mobile devices.

5. Document management: While this technology used to mean little more than scanning and tagging paper documents, it has evolved into enterprise content management. Social media and web applications lead to vastly more documents, most of which begin as digital files. Today's document management solutions enable faster and more efficient operational processes.

These technology approaches aren't free – at least not initially. They require upfront investment. For example, server virtualization software requires new skills and enterprise licenses. And it often affects the licensing of applications and operating systems.

Virtualization may also require new hardware. But CIOs find that these investments more than pay for themselves through increased efficiency. If implemented separately, server virtualization, storage virtualization, cloud computing and document management projects would cost an agency more than $1.1 million.

But if deployed in that order, and if the savings are used to fund additional investment in IT efficiency, those technology deployments would run less than $400,000. That savings can be used to pay for both new IT investments and new functionality for mission delivery.

Finding Those Efficiencies

CDW·G recently conducted a survey of government IT managers for its *Efficient Agency Report*. To learn how others are stretching dollars while enhancing services, access the report at:

CDWG.com/efficientITreport

Data Center Efficiency

Data centers have become the freight trucks of computing. They are big, expensive to operate and totally necessary. Even as government agencies' dependence on data and applications grows, they're using a variety of strategies to lower the cost of data center computing.

One approach is consolidating data centers (when a government body or department has several) and sharing the consolidated capacity across agencies. Another strategy is outsourcing data center functions to cloud service providers. Whether at the federal, state or local level, the drive to squeeze cost out of data centers, worthwhile in itself, is part of a larger effort to free up funds for innovative development.

The federal CIO, Steven VanRoekel, a former Microsoft executive, has stated explicitly that reducing operations and maintenance spending is a strategy for liberating developmental dollars. Federal IT spending may not be growing as it did in the 1980s and 1990s, but the revised spending mix will permit investments in application development, mobility and the better overall use and discovery of data, including unstructured data.

Server Virtualization

Server virtualization is a proven technology for boosting data center efficiency. This technology won't merely tweak IT efficiency – it will multiply it, increasing server utilization by a factor of up to 20. The direct benefit comes from reducing the number of physical machines required to

generate the same computing power. The indirect benefits include savings in power consumption, cooling and data center space.

Virtualization can also improve the availability and reliability of information systems and enhance continuity of operations.

Specifically, virtualization is a technique for abstracting all the software and hardware components of a server: applications, operating systems, memory and network interface devices. The result is what's called a virtual machine (VM), the basic building block of virtualized environments.

A VM communicates with physical hardware through an intermediary software layer called the hypervisor. Several leading software manufacturers offer highly developed hypervisors and an ecosystem of support products to go with them.

Once abstracted (or encapsulated), up to 20 VMs can run simultaneously on a single physical server. That moves the organization from a computing model of one application/OS/memory bank/network device per server to as many as 20. Much of virtualization technology centers on Intel x86 architecture servers, although VMs may encapsulate Windows, Linux, or even Mac OS X platforms.

Through virtualization, server utilization shoots up from an average of 5 percent to 80 percent, which is the practical limit. The hypervisor continuously allocates hardware resources (memory, CPU cycles and storage) to the VMs it supports.

The concomitant benefit of virtual machines, besides high server utilization, lies in their portability. As abstracted software units, VMs can move instantly from a failed or at-capacity server to another one in the same data center (or at a distant site via a wide area network) without users being aware of it.

VM portability means higher availability for applications and, therefore, more uptime. That translates to better data center efficiency because server maintenance or replacement won't interrupt operations. The IT staff can configure two or more VMs to back each other up at prescribed intervals, depending on the application's recovery time objective (RTO).

Some VM backup and replication utilities regularly "ping" the spare VMs to verify that they're problem-free and ready to run. Using such utilities, the IT department can recover an entire machine or a single file, making virtualization a highly efficient means of maintaining availability.

Server virtualization enhances data center efficiency by making it fast and easy to deploy new servers. Of course, it's important to avoid server sprawl — even of virtual servers —by establishing a governance process to "gate" requests for new VMs. But once approved, a new virtual machine takes only minutes to create and get running.

Storage Virtualization

Storage virtualization complements server virtualization by increasing the utilization rates of disk arrays. In government (as in industry), the past 10 years have brought exponential growth in data. The growth in government data has been driven in part by electronic records and documents, online deployment of services to the public, and the adoption of continuous monitoring in network operations and homeland security–related activities.

The resulting storage sprawl is expensive and tends to promote low utilization of storage resources. It also complicates the administration of those resources, robbing time from IT staff. Storage sprawl, like server sprawl, swells the physical space needed to house everything and puts extra demand on the electric grid.

Dedupe to Wring More from Storage Virtualization

When it comes to storage virtualization, data deduplication improves efficiency for both storage and network traffic. Deduplication software identifies multiple instances of identical data across files and removes them, replacing them with markers to the copy that remains.

Deduplication, in some respects a form of data compression, reduces storage requirements. For example, several people may be working on a spreadsheet, but with deduplication, a single copy serves everyone. Some deduplication solutions also reduce network bandwidth by prestaging unchanged file sections or blocks locally, so that only dynamic elements move across the network.

There are two types of data deduplication, each with its pros and cons. The first is in-line deduplication, which is analogous to in-band storage virtualization. It runs deduplication algorithms serially, while data blocks are in motion and before they're committed to a storage disk. An appliance detects and prevents multiple copies from being stored.

The second is post-process deduplication, which occurs after the data has been written to disk. Initially, it requires more storage; therefore, post-process deduplication won't free up disk space as much as in-line. But post-process dedup also won't affect application performance the way in-line deduplication might.

Storage virtualization abstracts data at either the file or block level. It presents data to applications and users logically, so that the physical location of that data becomes irrelevant. A virtualization layer of software underneath the data handles the task of allocating physical disk space to the virtualized data blocks. A logical data unit might exist physically on different storage arrays, but through storage virtualization, the IT group can avoid much of the complexity of partitioning disks, allocating storage and assigning logical unit numbers.

Typical storage virtualization architectures employ a controller that intercepts user requests and data, mapping the data to a physical disk. This is known as in-band virtualization. It removes a processing load from the host and is simpler to implement.

With out-of-band virtualization solutions, data requests are adjudicated by a separate server that holds metadata, which also takes some of the burden off the host processor. Once that server approves the request, the data itself moves directly to and from the storage device. This approach is more complicated, but it also uses network bandwidth more efficiently.

Both in-band and out-of-band storage virtualization come in solutions that support multivendor or heterogeneous storage environments. This is important because it helps the organization avoid lock-in with a single storage vendor.

Cloud Computing

Cloud computing has become an important efficiency initiative for government agencies. The federal approach has evolved along two paths.

Cloud first: A cloud-first policy requires agencies contemplating an expansion in data center capacity to look to a cloud provider first rather than build new, government-owned capacity. Simultaneously, authorities are trying to establish an internal marketplace for unused, government-owned data center capacity that can be bundled together logically and offered to other agencies.

Gradual migration: The Office of Management and Budget is asking agencies to move two services or applications to the cloud this year, presumably the start of a steady migration of HR, financial, e-mail and enterprise applications.

Fulfillment of these policies has been slower than hoped, but the trend is clear. In February 2012, the federal CIO Council advanced another milestone in its plan to enable universal security certification for cloud computing. This was followed by a user's guide to selecting and deploying cloud services.

At the state and local government level, cloud computing initiatives date back a decade. Efforts range from outsourcing platforms to hosting mission-critical applications in the cloud. Cloud computing can lead to greater data center efficiency, but it takes understanding.

The Information Technology Laboratory at the National Institute of Standards and Technology (NIST) has produced the most flexible, inclusive definition of cloud computing: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Variations on the definition exist, but NIST's is the one that defines cloud activity in the public sector.

As a practical matter, NIST's definition translates into three basic levels of cloud service.

Software as a service: SaaS refers to applications hosted remotely. The application may be the agency's own, but more often it is a vendor's commercial application. Several categories of applications exist as SaaS, including e-mail, HR, customer/contact relationship management, group collaboration and communication technologies. Some vendors are cloud-only and don't even offer customer-hosted versions of their programs.

Platform as a service: PaaS is often used for software development. The cloud vendor hosts the data center, operating systems and development environments. The Defense Information Systems Agency (DISA) operates a cloud of this nature called Rapid Access Computing Environment (RACE). Developers buy space in DISA's cloud in order to store virtual machines that they use to code and test applications or modules.

Infrastructure as a service: IaaS provides the "bare metal" on which customer organizations load their software. It frees them of purchasing or leasing servers, storage and networks, as well as infrastructure maintenance and administration.

Keep in mind, a cloud is a data center. It just happens to be owned and operated by someone other than the agency and made available to clients on a per-capacity unit or per-user basis. And in most cases, any IT department, government or otherwise, can use it.

In some cases, government agencies have special requests for cloud providers. For example, they might ask the provider to dedicate servers and hardware in the cloud for their specific use. While this is doable, if the agency's goal is

maximum efficiency, it's wise to restrict such requirements to classified or secret information.

For unclassified or merely sensitive computing, so-called multitenant clouds yield the most savings. The cloud operator moves data and virtual servers dynamically within its own data centers to maximize efficiency and meet service-level agreements (SLAs). From the tenant's standpoint, a cloud functions as if it were an unlimited utility.

When a department or other organization includes multiple agencies or components, it may consider operating its data centers as a cloud. In this case, the department or other umbrella organization is the cloud provider and the agencies or components are the tenants.

This is known as a private cloud and, like public clouds, this setup involves housing multiple tenants, dynamically allocating capacity based on demand and using a chargeback financial model to cover the cloud's costs. Operating a data center as a private cloud results in higher utilization rates and yields a higher return on investment.

Some agencies use a hybrid approach, with commercial public and governmental private clouds harnessed together and presented as a single utility to users and organizational components. But whether private or hybrid, adopting cloud principles can boost the efficiency of an organization's own data center and offer cost-effective computing resources to other agencies that want to outsource data center operations.

Using a cloud leads to more predictable costs and the ability to quickly add or subtract resources as needed, which lowers administration costs. The cloud provider supplies computing at uptime and redundancy levels specified in the SLA.

IT staff is free to pursue other tasks, such as application development. Consulting company Booz Allen Hamilton has said that cloud computing can reduce operations and maintenance lifecycle costs by up to two-thirds, compared with acquiring and running an agency's own infrastructure.

Mobility

Teleworking and portable computers with modems (of one kind or another) have been around for years. Yet government organizations, like their commercial counterparts, are now seeing an explosion of interest in mobile computing. Two factors drive this growth: the latest generation of smartphones and tablets, and the ubiquity of reliable 3G, 4G and Wi-Fi mobile bandwidth.

Although the phenomenon has been termed the "consumerization" of IT, that characterization is only partly accurate. Many people have become familiar with tablets in their personal lives, but smartphones have been in corporate use for a decade. What's changed is that new mobile devices can run more data-intensive applications.

Moreover, thanks in part to government demands, organizations now have a choice of solutions to secure tablets and smartphones. Considering all that, combined with extreme portability (most are light weight and possess a six- or seven-hour battery life), it's easy to understand why workers have clamored for their employers to adopt smartphones and tablets into their workday toolsets.

Two recent announcements demonstrate how this latest incarnation of mobility is taking root in government: The Air Force recently awarded a contract to buy up to 18,000 Apple iPads to replace paper manuals in flight kits; the Department of Veterans Affairs announced it would begin to allow Apple iOS and Google Android devices on its enterprise network.

More important, the federal government has launched a mobile strategy to unify its approach to using mobile devices and to consolidate requirements. It realizes that mobility can help remove some of the friction in processes in which government engages.

State and local governments are also going mobile, deploying mobile applications both for staff and for an increasingly mobile public. For instance, emergency response agencies are examining smartphones on 4G networks as an answer to the long-elusive challenge of interoperable communications. Such an application brings voice, video and other data together in a way that radio systems have not.

For government at all levels, mobility enhances the value of unified communications networks by combining communication and collaboration tools, as well as productivity and enterprise applications, on a single device. Single-device mobility benefits users by freeing them from carrying two or more discrete devices. And it can cut down the number of devices the IT department has to manage.

A mobility strategy should be designed to improve organizational efficiency. These efficiency gains can accrue in a number of ways. First (and perhaps most obvious), mobile devices as computing clients can be less expensive to acquire than traditional machines.

Second, effective mobility can boost employee productivity by allowing supporting telework and work in the field. As a result, mobility can lead to reductions in office

and real estate costs. Some agencies lease space with fewer workspaces than staff, anticipating greater mobility.

Furthermore, a mobility strategy can extend an agency's other IT initiatives. Lightweight, always-on devices, as part of a secure, virtualized infrastructure, enable collaboration through built-in video conferencing and other enterprise applications. It all adds up to greater productivity, which is equivalent to getting more out of an existing infrastructure and its fixed costs.

Bring Your Own Device

Managing mobile devices requires careful planning, especially when agencies consider how to get those devices into the hands of users. As mobile computing has grown in importance, a spinoff development, known as "bring your own device," has taken root in government.

Loosely defined, BYOD effectively means that workers buy their own devices of choice, and the agency's IT department manages how those devices can access resources, what data they're allowed to carry, what happens if they're lost, and more.

BYOD opens the door to the advantages of mobility while saving money on device procurement. It can present challenges to the IT team, given the array of hardware architectures and operating systems available, but it's usually policy that presents the most daunting challenges.

Before Deploying BYOD

Given the growth in security options for enterprise mobile devices, data and intellectual property loss pose a far less significant problem for the IT group than it did just a few years ago.

But when embarking on a bring-your-own-device mobile strategy, in which staff use their personal devices for government work, the IT department faces a list of questions, among them:

- Does the security configuration include a provision for the remote destruction of data if the device is lost or stolen? Who has authority to carry this out?
- Which services and products are eligible for reimbursement?
- BYOD policies should never cover any and all devices. How wide a range of devices will the agency allow in terms of both hardware and supported operating systems?
- What personal apps will the IT group allow users to have on their devices? And what policies will apply to the use of location-based information associated with many apps?

For example, worker-owned devices will contain both enterprise and personal information. This can complicate the IT team's administration and control of such devices. For instance, how does the IT department approach wiping clean a personal device when it's lost or stolen?

Still, BYOD can increase mobile efficiency if the program is designed to have predictable costs and if the enterprise supports only one device per staffer.

Document Management

Ultimately, data centers support operational processes and strategies. Much of the critical information that people access rests in documents, such as written text, spreadsheets, presentations, forms and contracts.

Government agencies can realize significant efficiencies using better document management solutions. The CDW·G *Efficient Agency Report* found that more than half of state and local agencies are implementing document management solutions. CIOs commented that, on average, investments in document management technologies returned 139 percent.

Document management has evolved as the information industry has evolved. What qualifies as a document has broadened substantially in the past decade, from paper files to any piece of information relevant to the operation of an organization. In fact, document management has its roots in paper-intensive procedures in which volumes of printed pages and images were scanned and filed.

Banks built vertical, stovepiped systems for capturing images of checks and statements at high speed. The systems tagged the documents for quick retrieval from, typically, optical storage. Such systems in the public sector help manage processes for criminal investigations, tax and revenue administration, and social case management.

Vendors now integrate these systems with solutions that tag, store and retrieve documents that are born in the digital-only world. This can include Microsoft Word files, e-mail messages and more. For example, government agencies routinely use social media platforms to solicit comments on rules, regulations and proposed initiatives. Plus, agencies generate large quantities of their own digital information in all formats.

Document management has, in some respects, evolved into enterprise content management, a discipline seeking to organize structured and unstructured data in both physical and digital formats for efficient storage and retrieval. Today, agencies are trying to get a handle on everything from video clips to text chats.

Functionally, modern document management systems comprise a number of serial steps, starting with capture and tagging. Document tags, in aggregate, are referred to as metadata and describe everything from the contents to the location of documents.

Although document capture can still mean scanning, an integrated solution may also allow an employee to tag and file away a copy of an e-mail attachment, for instance, from within the client software. When the employee files an electronic document in the document management system, this step can trigger workflow, security and distribution-control engines.

In this way, the system grants rights, according to the profile of the user, to view or edit documents. It can also route documents to appropriate people as part of a specified process.

Agencies store electronic documents in a hierarchical storage management system, which assigns the documents to the most appropriate type of storage for the expected frequency of retrieval. That is, documents in active use will head to solid-state or first-line spinning-disk media. Archival material will come to rest in optical or tape media. Depending on the controlling regulations, archival material may eventually be destroyed.

Complete document/content management solutions can be vital to complying with government rules and regulations. For example, at the federal level, the National Archives and Records Administration maintains a library of detailed regulations governing documents, all of which are defined by statute.

So the most effective document management systems will have pertinent rules and regulations built into their workflow. And they will log the movement and disposition of electronics files so that management has an audit trail proving that documents received proper treatment.

Document management systems automate lifecycle management of documents and records, whether they end up stored in electronic archives or destroyed according to policy. Such a system, by enforcing rules and policies, increases the efficiency of staff who create, handle, evaluate or publish documents, while reducing legal risk to the agency.

By making documents of all types instantly retrievable, government agencies can improve collaboration, especially if the document management solution integrates with collaboration environments such as Microsoft SharePoint or Lotus Notes.

Finally, an up-to-date solution integrates document management with important government functions, such as online publishing and Freedom of Information Act requests. These help agencies respond more efficiently, meet their goals for government transparency, and improve service to the citizen.

A Checklist for Document Management

Document management systems can be as complex as an agency's own processes. Here are some points to consider when embarking on a new or upgraded document/enterprise content management project.

- **Does the system comply with relevant statutes, regulations and standards?** Several publications from the International Organization for Standardization (ISO) cover document and record management. ISO 15489 applies to information and documentation. ISO 23081 covers the management of metadata. Agencies will find federal records management requirements in numerous sections of the U.S. Code.
- **Does the software include a robust search function?** Users shouldn't have to navigate various complex tools to find documents in a particular repository.
- **Can the system securely support mobile users while minimizing the danger of data leakage?** Two basic architectures aim to protect information on mobile devices. One allows enterprise information to be stored on smartphones or tablets but creates a virtual "sandbox" on the device to separate that information from personal data. The other keeps files behind the enterprise firewall, giving mobile read-only access.
- **Will the solution support multiple processes across domains within the organization?** That is, can one product support document management functions as disparate as, for example, accounts payable and case management? Although the organization's processes might require tweaking to fit the strengths of such a solution, the resulting efficiency can outweigh the cost of buying individual document management solutions for various functions.

TWEET THIS!

CDW·G PEOPLE WHO GET IT™