InformationWeek
analytics

Analytics.InformationWeek.com

October 2011
$99

Analytics Report

Presented in conjunction with
InformationWeek Government

2011 Federal Government IT Priorities

Cybersecurity ranks as the top priority among federal IT professionals, according to our third annual survey. Data center consolidation rose in importance, while the Open Government Initiative fell. Our survey also reveals gaps between key White House initiatives and their implementation by federal agencies.

By Michael Biddick

Report ID: R3191011

TABLE OF CONTENTS

TABLE OF CONTENTS

Michael Biddick
InformationWeek Analytics

Michael Biddick is president and CTO of Fusion PPT and an *InformationWeek Analytics* contributor. He has worked with hundreds of government and telecommunications service providers in the development of operational management solutions. Most recently he has supported the Department of Homeland Security and the U.S. Department of Defense in the deployment of ITIL-based processes that are utilized to make their organizations more transparent and cost effective. Certified in several ITIL lifecycle service areas, Michael is also able to leverage more than a decade of operational tool design and implementation experience with service desks, network management systems and consolidated management portals in making enterprise architecture decisions.

Prior to joining Fusion PPT, Michael spent 10 years with Windward IT Solutions and also worked with Booz Allen Hamilton in its Enterprise Network Services group, developing network management solutions for a wide variety of both government and commercial clients. He also served on the academic staff of the University of Wisconsin Law School as the Director of Technology, heading up all aspects of IT management for the organization. Michael earned a Master of Science degree from Johns Hopkins University and a dual Bachelor's degree in political science and history from the University of Wisconsin-Madison. As a contributing technology editor to *InformationWeek* and *Network Computing*, he has authored more than 50 articles, including reports on cloud computing, government IT strategies, SaaS and IT process improvement.

InformationWeek Government

Executive Summary

To gauge how federal IT teams are managing the Obama administration's technology mandates and the many other projects on their plates, *InformationWeek* conducted its third annual Federal Government IT Priorities Survey. The survey was completed in July by 131 federal IT pros. IT security and cybersecurity were ranked the No. 1 priority. Data center consolidation moved up a few notches on the list, while the Open Government Initiative moved down.

One of the big changes in federal IT this year was the resignation of federal CIO Vivek Kundra, who was replaced by Steven VanRoekel, the former managing director of the FCC. One of VanRoekel's first actions was to announce new responsibilities for agency CIOs in the areas of governance, commodity IT, program management and information security.

Federal IT teams have a lot of their plates. The top five priorities, according to our survey, are cybersecurity, disaster recovery, data center consolidation, data records management and virtualization.

OMB's 25-point IT reform plan requires agency CIOs to lead internal IT project reviews that are based on the TechStat model used by OMB to assess big-ticket federal IT projects. The goal is to terminate or turn around one-third of all underperforming IT Investments by June 2012.

NIST gives agencies guidelines for implementing continuous monitoring, including both network and system-level monitoring, in their IT environments. While 21% of survey respondents have implemented continuous monitoring, a surprising 48% were not familiar with the requirements.

A key component of OMB's reform plan is applying IT to become more efficient. Eliminating duplicative "commodity services" and rationalizing IT investments are key tenets of the plan.

Federal IT teams must develop strategies for new types of computing devices. As more federal workers use tablets and smartphones, agencies must recognize that some of their apps will be running on employee-owned devices. This has implications for agencies that don't have policies in place and the security infrastructure to deal with this trend.

Research Synopsis

Survey Name: *InformationWeek* 2011 Federal Government IT Priorities Survey
Survey Date: July 2011
Region: United States
Number of Respondents: 131

Purpose:
To determine IT priorities for federal government technology professionals and contractors.

Methodology:
InformationWeek surveyed 131 federal government technology decision-makers. The survey was conducted online, and respondents were recruited via an email invitation containing an embedded link to the survey. The email invitation was sent to qualified *InformationWeek* and *InformationWeek Government* subscribers.

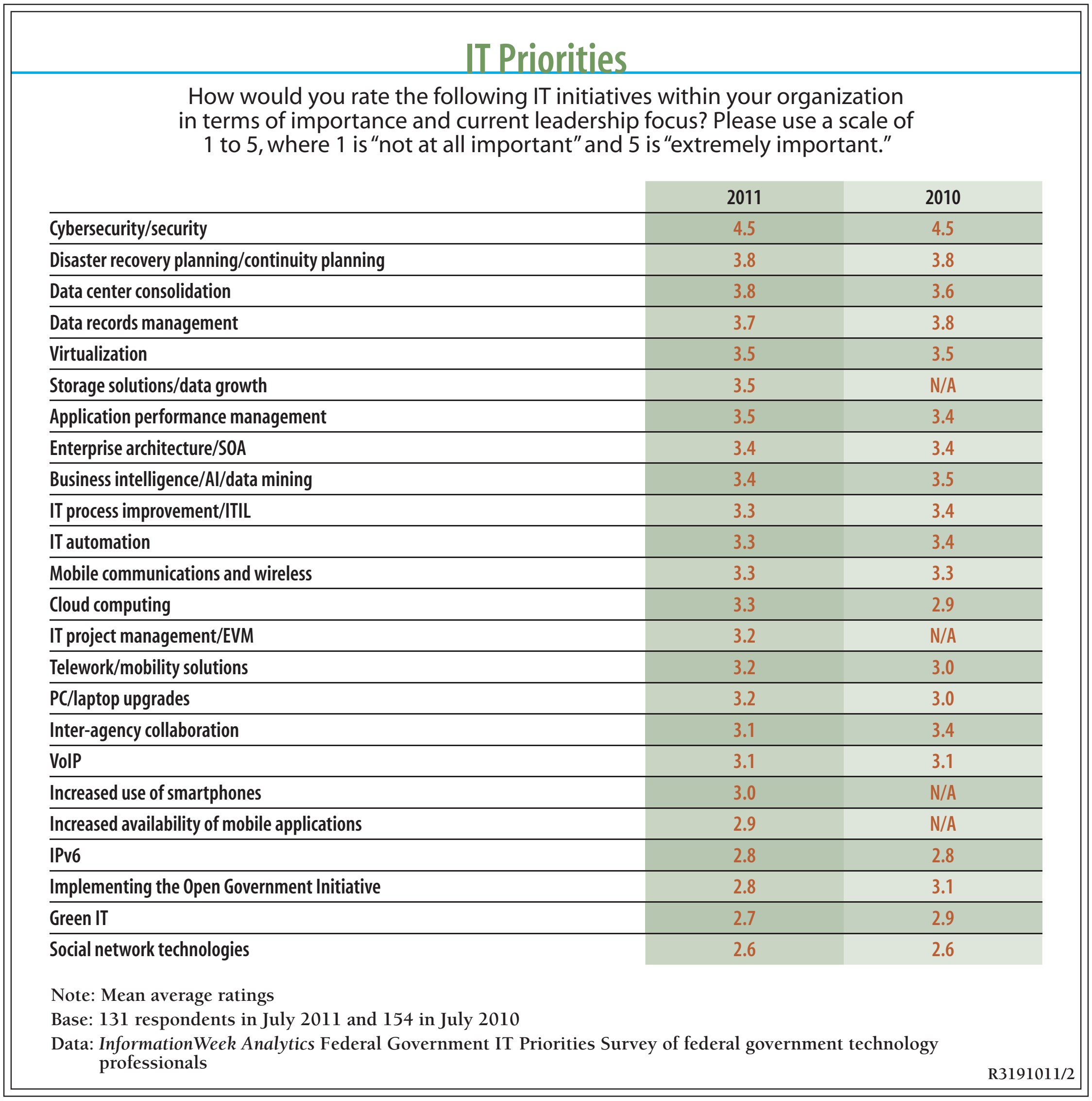
ABOUT US | ***InformationWeek Analytics'*** experienced analysts arm business technology decision-makers with real-world perspective based on a combination of qualitative and quantitative research, business and technology assessment and planning tools, and technology adoption best practices gleaned from experience.

If you'd like to contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com,* content director **Lorna Garey** at *lgarey@techweb.com* and research managing editor **Heather Vallis** at *hvallis@techweb.com*. Find all of our reports at *www.analytics.informationweek.com.*

Government IT Priorities

In the face of an uncertain economy and amid ongoing debate over federal spending and debt, it's difficult to know if we're entering a period of government austerity or one of additional spending aimed at boosting the economy. Either way, one thing is clear: The only way the U.S. government can deliver improved services, more efficiently and on the scale required, is by

Figure 1



IT Priorities

How would you rate the following IT initiatives within your organization in terms of importance and current leadership focus? Please use a scale of 1 to 5, where 1 is "not at all important" and 5 is "extremely important."

	2011	2010
Cybersecurity/security	4.5	4.5
Disaster recovery planning/continuity planning	3.8	3.8
Data center consolidation	3.8	3.6
Data records management	3.7	3.8
Virtualization	3.5	3.5
Storage solutions/data growth	3.5	N/A
Application performance management	3.5	3.4
Enterprise architecture/SOA	3.4	3.4
Business intelligence/AI/data mining	3.4	3.5
IT process improvement/ITIL	3.3	3.4
IT automation	3.3	3.4
Mobile communications and wireless	3.3	3.3
Cloud computing	3.3	2.9
IT project management/EVM	3.2	N/A
Telework/mobility solutions	3.2	3.0
PC/laptop upgrades	3.2	3.0
Inter-agency collaboration	3.1	3.4
VoIP	3.1	3.1
Increased use of smartphones	3.0	N/A
Increased availability of mobile applications	2.9	N/A
IPv6	2.8	2.8
Implementing the Open Government Initiative	2.8	3.1
Green IT	2.7	2.9
Social network technologies	2.6	2.6

Note: Mean average ratings
Base: 131 respondents in July 2011 and 154 in July 2010
Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals

R3191011/2

leveraging its huge investment in IT more effectively. The Office of Management and Budget has been pushing a series of initiatives with that in mind.

To gauge how federal IT teams are managing OMB's mandates and the many other projects on their plates, *InformationWeek* conducted its third annual Federal Government IT Priorities Survey. The survey was completed in July by 131 federal IT pros. We asked respondents to rate the importance of two dozen technology initiatives, to identify the factors driving their priorities and to assess barriers to execution, among other questions.

IT security and cybersecurity were ranked the No. 1 priority by survey respondents, by a wide margin. That's consistent with our 2010 survey findings and reflects the harsh reality of ever-present threats, both internal (WikiLeaks) and external (Operation Shady RAT). Data center consolidation moved up a few notches on the priority list, while the White House's Open Government Initiative moved down. Here too, the changes have a pragmatic explanation: Federal IT teams are under the gun to close data centers according to a plan that's being closely monitored by OMB. Meanwhile, their first- and second-round open government projects have already passed muster, so that work is deemed less urgent.

For the first time this year, we asked respondents to rate the importance of smartphones and mobile applications. Surprisingly, both ended up well down the priority list. Perhaps this is because employees are increasingly bringing their own mobile devices and apps to the office, with or without the approval of central IT. There should be no doubt, however, that this trend has policy and security implications that federal IT managers can't ignore.

Our survey revealed gaps between certain OMB initiatives and respondents' awareness of those initiatives. More than half of respondents were unfamiliar with OMB's TechStat project-review program, and nearly half were unaware of the National Institute of Standards and Technology's requirements around continuous-monitoring systems. This report examines these and many other issues that came to light in the survey results. (See Figure 1, page 8.)

New Leadership

One of the big changes in federal IT this year was the resignation of federal CIO Vivek Kundra, the architect of OMB's government-wide IT initiatives. In August, Kundra was replaced by Steven VanRoekel, the former managing director of the FCC, who spent 15 years at Microsoft before joining the public sector. When VanRoekel took over as federal CIO, he gave no indication of any changes in direction in federal IT strategy or policies, but federal IT pros shouldn't be surprised if VanRoekel comes up with his own ideas about how things should be done.

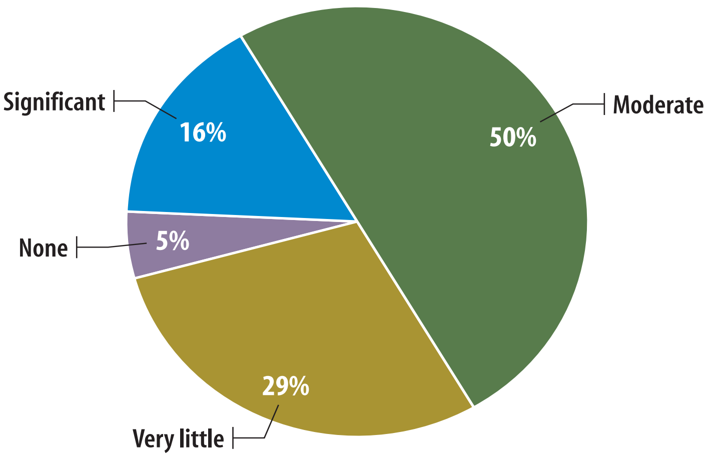
In July, a few weeks before he left OMB, Kundra said in a briefing that federal agencies tend to focus on policy more than execution. "So one of the things we did from day one is set specific timelines," he added. Yet, belt tightening in Washington could have an impact on how well agencies are able to meet such deadlines. If funding dries up, the timeframe for deliverables often gets pushed out.

Kundra spent much of his tenure as federal CIO trying to narrow the tech gap that separates federal agencies from companies in the private sector. He sought increased innovation in the form of cloud computing, software as a service, and mobile devices and applications.

Figure 2

Agency Innovation

What is the level of IT innovation that occurs within your agency?



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/19

Despite this emphasis, only 16% of survey respondents said they saw significant innovation in their agencies and 29% saw very little.

On the other hand, we see growing evidence of iPhones, iPads and other popular technologies across federal government, including places like the Pentagon. In fact, half of respondents reported a moderate level of innovation occurring within their agencies. We'll call that progress, albeit with lots of room for continued improvement. (See Figure 2, page 10.)

Kundra's policy initiatives culminated in the 25-point reform plan, published in December 2010. The plan notes that despite spending more than $600 billion on IT over the past decade, the federal government has achieved little of the productivity improvements that private industry has reaped. The plan sets deadlines for specific objectives over the next 18 months, but broad reform will likely take years to implement.

VanRoekel, the new federal CIO, picked up where Kundra left off. Upon taking office, one of his first actions was to announce new responsibilities for agency CIOs. In an Aug. 8 memo, VanRoekel laid out four key areas of focus for agency CIOs: governance, commodity IT, program management and information security. The goals include lowering operational costs, terminating or turning around troubled IT projects, and delivering meaningful functionality more quickly while enhancing security. During the next year, agency CIOs will be required to provide a progress report to the President's Management Council and the CIO Council.

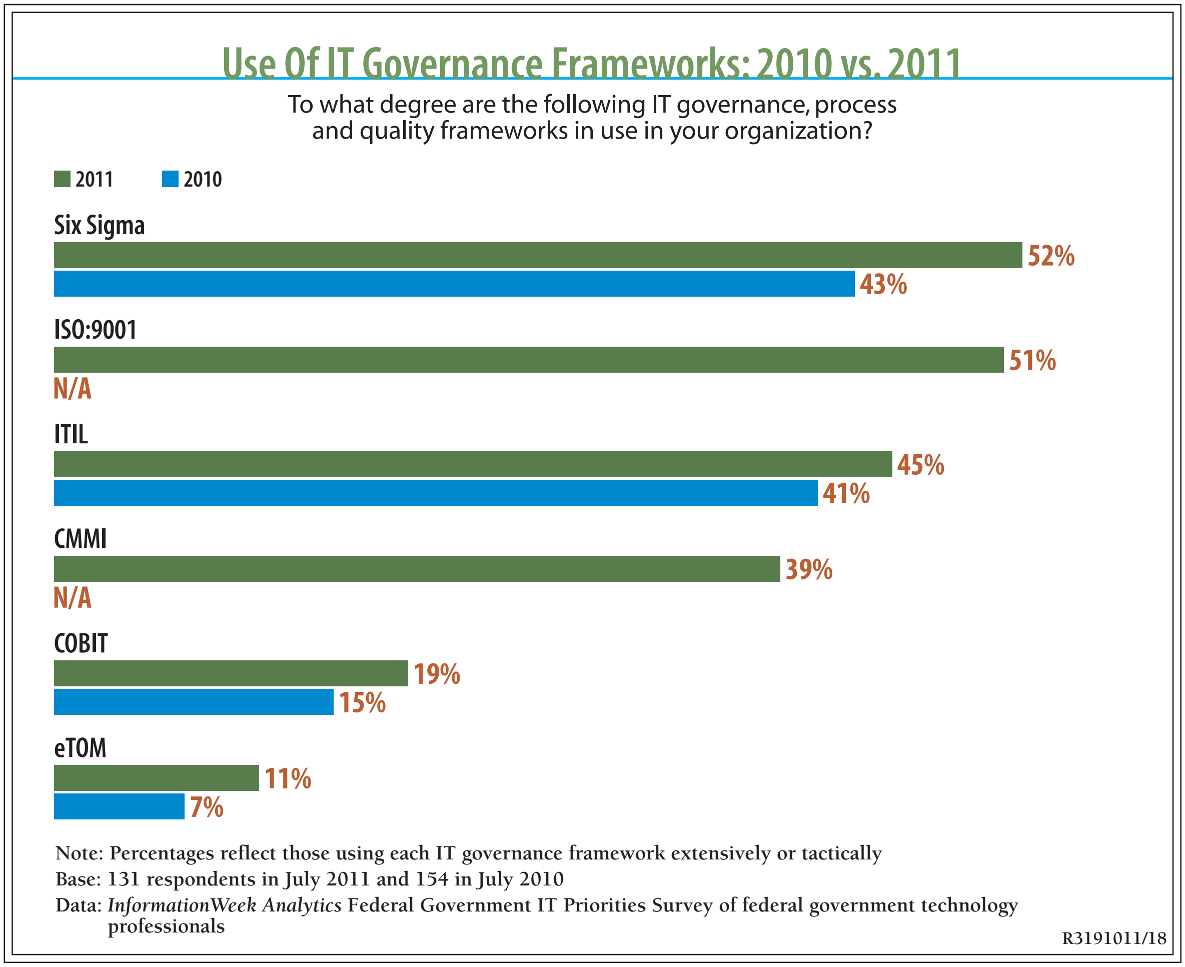
Prior to being appointed federal CIO, VanRoekel had a hand in the FCC's modernization efforts. He helped drive systems interoperability at the agency, and he worked with its social media team. We're still learning how the new federal CIO will tackle problems that span government and get agencies to move from policy to execution.

VanRoekel quickly learned that federal IT teams have a lot of their plates. The top five priorities, according to our survey, are cybersecurity, disaster recovery, data center consolidation, data records management and virtualization. Data center consolidation moved up from last year, no doubt as a result of the continued press from OMB and the Government Accountability Office on this program. Yet, our survey also revealed a disconnect with other OMB policy directives, as respondents put project management, cloud computing and process improvement lower on the IT priority list. These gaps must be closed, or at least narrowed, if the government is to make progress with its many IT challenges.

Governance

Agency CIOs have statutory responsibilities through the Clinger-Cohen Act and related laws for governance that drive the IT investment review process. Agency CIOs hold responsibility over the agency's IT portfolio, and a critical component of this is formal IT portfolio analysis as part of the yearly budget process. OMB's IT reform plan restructured the investment review boards by requiring agency CIOs to lead project review sessions called TechStat reviews (more on those later). The outcomes from those sessions are specific steps to put projects on the right track through completion, with a goal of terminating or turning

Figure 3


Use Of IT Governance Frameworks: 2010 vs. 2011

To what degree are the following IT governance, process and quality frameworks in use in your organization?

Note: Percentages reflect those using each IT governance framework extensively or tactically
Base: 131 respondents in July 2011 and 154 in July 2010
Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals

R3191011/18

around one-third of all underperforming IT investments by June 2012, according to OMB.

IT management starts with governance. From a high level, this means aligning the strategy of the agency with the IT priorities in the organization, then ensuring that the execution follows a well-defined process. Our survey found a few methodologies in use, increasing from our 2010 poll. Leading the governance frameworks in use was Six Sigma, ISO:9001, ITIL and CMMI. While the frameworks differ slightly depending on what they're trying to accomplish, the critical step for agencies is to begin using a governance approach to meet IT challenges. (See Figure 3, page 12.)

As an example, ITIL establishes a process to define service strategy and all of the tech components required to deliver IT services. Next, ITIL defines a process to design, transition and operate the service. Finally, ITIL introduces a mechanism to continually improve the service and evaluate the effectiveness for users. While these frameworks will not meet federal agencies needs completely, they can significantly reduce the time to establish these core process areas.

Once good practices are established, there should be occasional internal and peer reviews of IT projects. In January 2010, OMB launched its TechStat program to serve that purpose. Here, OMB officials, agency CIOs and other managers discuss the status of ongoing IT projects and, where needed, specify remedial steps. The National Science Foundation used TechStat to review the performance of FastLane, a public-facing Web portal that's part of NSF's mission-critical, legacy grants management system. Andrea Norris, acting CIO at NSF, credits TechStat with helping to improve governance of the investment, resulting from better prioritization of change requests.

TechStat sessions are a key element of IT governance and should be conducted at lower levels within agencies. OMB last year issued a TechStat toolkit with templates, guidance and other components designed to help agencies conduct their own, internal IT project reviews. Agencies must get better at identifying and tracking program risks well before they're put under OMB's spotlight. That requires establishing local governance at the department level and below.

That's the approach taken by the Department of State, which conducted an internal TechStat review of its messaging systems, including its Telegram Legacy System, which supports the preparation and delivery of State telegrams. That review session resulted in a decision to retire the Telegram Legacy System and integrate the agency's other messaging systems, according to

State CIO Susan Swart. The internal review "will also improve insight into investment performance and improve the acquisition lifecycle to enable comprehensive, integrated system development and transparent performance measurement reporting," said Swart.

Lack of awareness continues to hamper efforts to improve IT governance. In our 2010 Federal Government IT Priorities Survey, 56% of respondents were unaware of the TechStat program. A year later, we're not seeing much improvement; 55% were still unaware that the program exists. As a step in the right direction, 14% noted that they conduct their own internal TechStat-style project reviews and 4% were aware of stopped or redirected IT projects based on TechStat reviews. (See Figure 4, page 15.)

Nitin Pradhan, CIO of the Department of Transportation, said TechStat reviews are improving governance and accelerating delivery of IT investments at his agency. Pradhan called TechStat "an opportunity to review the entire IT portfolio and provide strategy direction and guidance."

Frank Baitman, the former CIO at the Social Security Administration (he resigned in August), said TechStat uncovered issues with SSA's Disability Case Processing System and created a framework to address them. The agency also provided training to the project manager involved and gave attention to issues created by a delayed contract award. Those steps were expected to put the project back on track and lead to a green rating on OMB's IT Dashboard.

At the U.S. Agency for International Development, CIO Jerry Horton is incorporating TechStat into the agency's broader approach to IT governance. USAID conducted a TechStat review of its Enterprise Disaster Recovery investment in March. The review uncovered performance challenges and led to corrective actions such as weekly program oversight meetings that are used to communicate progress, opportunities and challenges to stakeholders, including the enterprise architecture team and agency executive management.

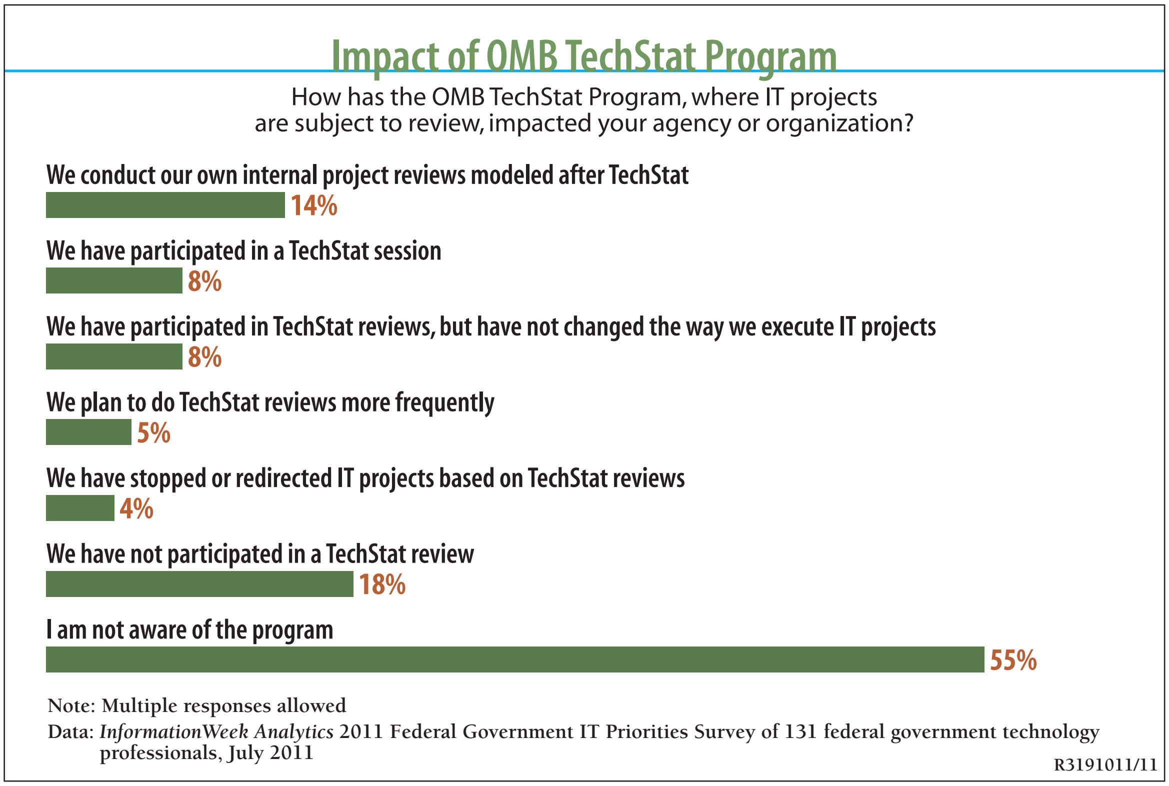
While TechStat is effective for keeping projects on track, it's important that IT leaders ensure that planned projects align with the agency's mission before they get funded. Projects must fit with the objectives contained in an agency's strategic plan. Only 36% of respondents to our survey follow their strategic plan closely, while 43% deviate from it regularly. Why the disconnect? While the honchos in headquarters typically devote considerable time and resources to the development of a strategic plan, the staffers and managers responsible for daily operations aren't as closely tied to it.

Without the guidance of a strategic plan, IT projects from operations and maintenance to new initiatives will be difficult to prioritize and budget. Instead, reactive decisions will be made that don't meet the needs of internal or external stakeholders. Although an elaborate IT strategy isn't necessary, governance does require a way to prioritize the choices that leaders make. Governance frameworks will also help establish a path so that checkpoints exist to keep programs on track. (See Figure 5, page 16.)

Information Security

The No. 1 priority among federal IT pros, as it was last year, is security, with 69% viewing it as extremely important. That reflects OMB's emphasis on "well-designed, well-managed continuous monitoring and standardized risk assessment processes," to be supported by CyberStat ses-

Figure 4



Note: Multiple responses allowed
Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011
R3191011/11

sions run by the Department of Homeland Security (DHS). CyberStat sessions are essentially TechStat-style reviews with a focus on IT security.

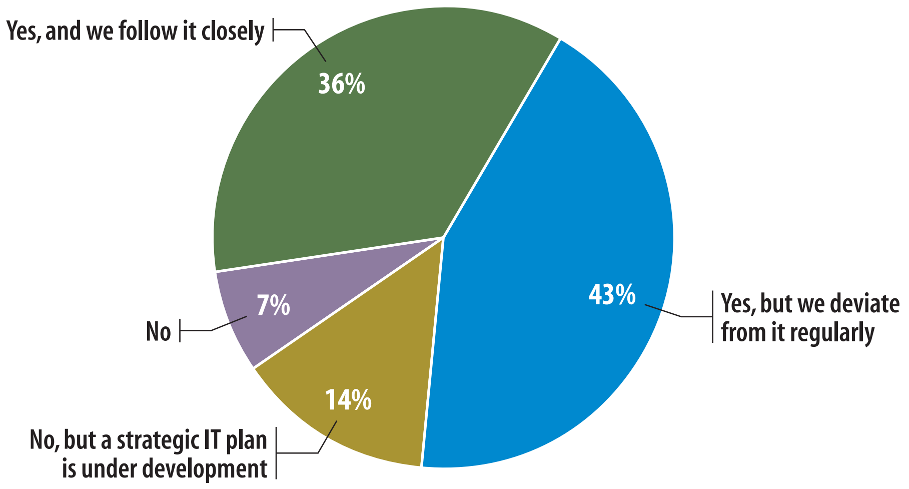
The goal is that continuous monitoring and CyberStat together will provide essential, near real-time security status information to agency officials, and allow for immediate remediation to address any vulnerabilities. The Department of Education piloted the CyberStat program earlier this year, and OMB concluded it led to concrete actions and outcomes.

As federal CIO, Kundra was critical of the government's certification and accreditation (C&A) process for verifying system security, saying it was too static for today's threats. In our survey, 23% of respondents still regard the C&A process as being very valuable, but that's the minority view. A majority, 62%, find C&A to be a mixed bag; sometimes helpful, sometimes not. (See Figure 6, page 17.)

Figure 5

Strategic IT Plan?

Does your organization have a strategic IT plan?



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

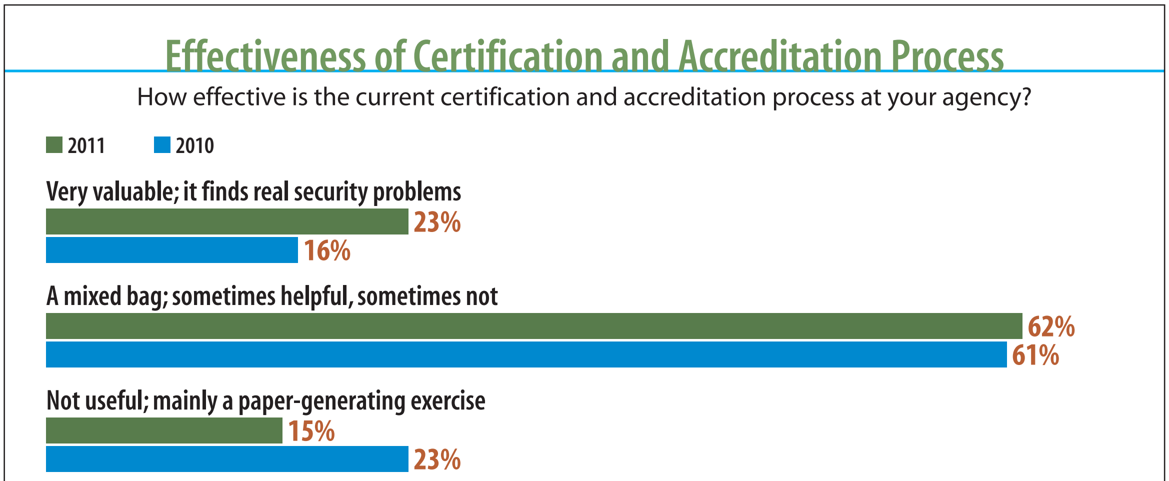
R3191011/9

NIST special publication 800-137 gives agencies guidelines for implementing continuous monitoring, including both network and system level monitoring, in their IT environments. While 21% of survey respondents have implemented continuous monitoring, a surprising 48% were not familiar with the requirements. While continuous monitoring solutions can add complexity and be difficult to implement, they also serve as a foundation for getting a comprehensive inventory of data center assets.

The key to effective security is to control access to applications, networks and, most importantly, data. The ability to link access control to specific data is key to doing that. The use of continuous data protection tools can prevent situations like the WikiLeaks breach by limiting who can transport data and help track data leaks if and when they do occur. The requirement to share information and collaborate need not be contrary to good security, but effective controls are needed.

The goal isn't to prevent every attack—that's impossible—but to rapidly detect threats and respond to them. Continuous monitoring is essential, but the real challenge is how to respond when you detect an attack. IT teams must develop the ability to rapidly switch hardware, net-

Figure 6



Base: 131 respondents in July 2011 and 154 in July 2010
Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals
R3191011/8

work paths, and servers to disrupt attacks and preserve capabilities. That's costly to do in small environments, but feasible in large, consolidated data centers. (See Figure 7, below.)

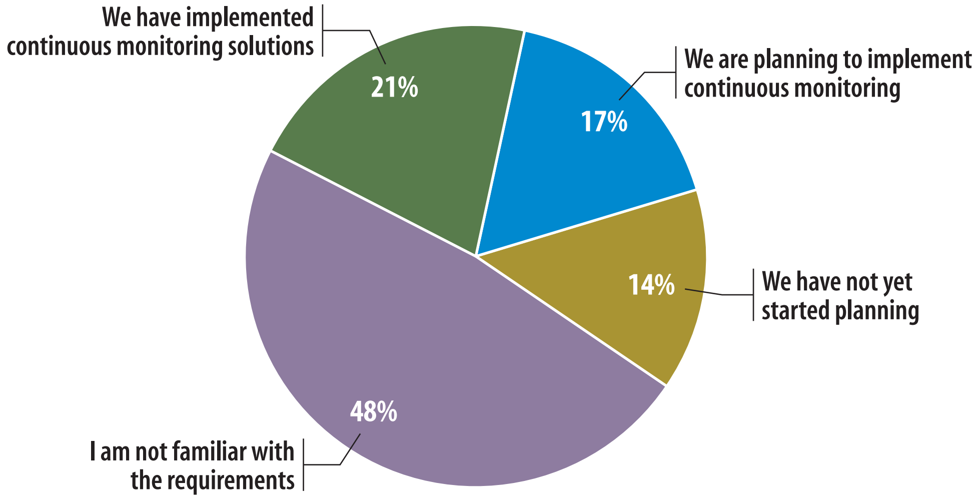
Nicole Drapeau Gillen, director of security firm Tailored Solutions, says IT pros need to have a holistic view of their enterprise and threats to their organizations' intellectual capital. That can be done by integrating data that's not typically combined, such as HR records, security system logs and open-source information. This approach is well beyond the server and network monitoring that most organizations do today, but given the ever-increasing threats, new approaches are in order.

In addition to shifting investments to continuous monitoring, the Obama administration's fiscal 2012 budget called for investing $459 million in the operations of the National Cyber Security Division at DHS and government-wide Red and Blue teams for penetration testing. The lack of a federal budget has arguably made the country less secure, as agencies are in limbo with

Figure 7

Capability to Support the NIST SP 800-137 Requirements

How well equipped is your agency to support the NIST SP 800-137: Continuous Monitoring for Federal Information Systems and Organizations requirements?



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/12

regard to funding. Cybersecurity is a priority, but will there be funding to act on it?

The feds are also facing a shortage of workers with the cybersecurity skills needed. DOD CIO Teri Takai is leading a government-wide effort to update the Clinger-Cohen core competencies, which serve as a baseline for IT management skill requirements. Course work based on the competencies is used by the Federal CIO University consortium and the DOD's iCollege to provide graduate education, including in the areas of information assurance and cybersecurity.

Commodity IT

A key component of OMB's reform plan is applying IT to become more efficient. We continue to see all-too-many inefficient programs across government. A common example is building a network management center to monitor IT infrastructure instead of leveraging systems that are already in place. Redundant services might include email, data centers, networks, identity and access management, security, Web infrastructure, and finance and HR applications. Eliminating duplicative "commodity services" and rationalizing IT investments are key tenets of the reform plan.

CIOs can do that by pooling an agency's purchasing power as a way of driving down costs and improving services. (OMB says as much in its Aug. 8 memo detailing new responsibilities for agency CIOs.) A consolidation effort can integrate IT resources and eliminate duplicative systems and applications. In lieu of IT silos, CIOs should steer toward shared services, either as a provider of them or a consumer.

That shift will be difficult for many inside the organization to accept, but it's long overdue. We recently saw an IT manager struggle to build a back-up data center environment, even though his agency had a simple solution already deployed. He argued it would be more expensive to use the shared service, because money was already invested in infrastructure. However, his calculation didn't include the operations and maintenance costs associated with a back-up data center, or the management time involved.

To meet this shared-services objective, agencies are turning to cloud computing (multitenant, pay on demand) and hosted environments (dedicated, outsourced). The National Archives and Records Administration is using the cloud model in a variety of ways: in an email pilot; to streamline the agency's Security Clearance Tracking System; to manage and track Freedom of

Information Act requests; and for a Web portal created to accept FOIA submissions. With more than 500 FOIA cases in fiscal 2011, NARA expects the self-help portal to help address 10% to 15% of inquiries before requests are even made and reduce the average case time from 25 days to 15 days.

Consolidating data centers as planned under the FDCCI won't be easy. OMB wants to close 800, or 38%, of Uncle Sam's 2,094 data centers by 2015. As a first step, it asked the 24 participating agencies to submit data center inventories and consolidation plans by the end of August. However, a GAO report released in July at the request of Congress suggests the FDCCI is getting off to a slow start. Yet, GOA found that only one agency had submitted a complete inventory and none had delivered complete plans. What's more, OMB didn't require agencies to document the steps they took to verify inventory data.

Surprisingly, GAO also discovered that 20 agencies didn't reference a master schedule in their consolidation plans, 12 didn't provide cost-benefit calculations and nine neglected to address risk management. GAO cited cultural, funding-related, operational and technical issues in explaining the shortcomings. For example, 19 agencies reported difficulty obtaining power usage data.

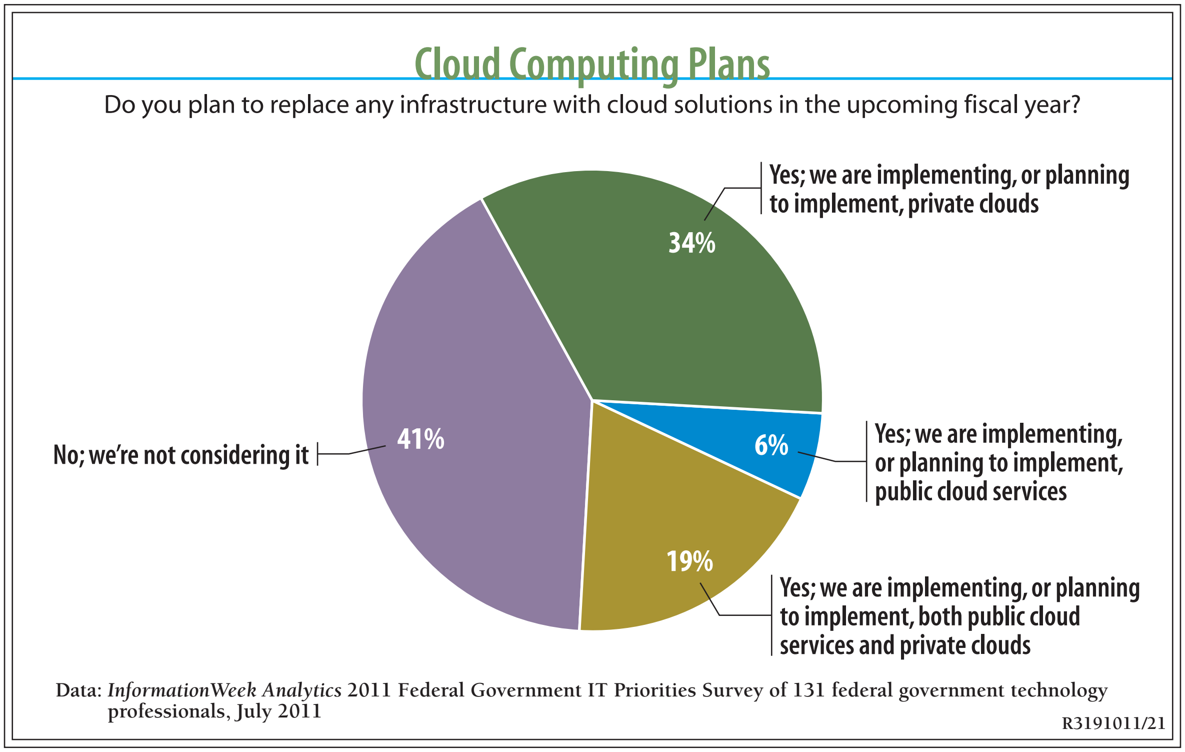
Data center consolidation ranked third among all IT priorities in our survey. Forty percent of respondents indicated that their agencies had consolidated one or more data centers, while 31% indicated their agencies were in the planning stages.

Another area of focus is the use of cloud environments for commodity IT platforms, infrastructure and services. OMB's cloud-first policy directed agencies to identify three "must move" services within three months, then move one of those to the cloud within 12 months and the remaining two within 18 months. Some agencies are looking to deploy private clouds. The goal is to take advantage of economies of scale and deliver services on demand to departments and end users, all with greater data center efficiency. Organizations building private clouds must make sure that their data center technologies—servers, storage, security, virtualization and network infrastructure—are ready for this new model. While much of the technology needed for the cloud is familiar, new investment and upgrades will be required. For example, one area for investment, currently lacking in many government environments, is true service management and automation.

In our survey, 53% have implemented or are planning to implement private clouds. That's a substantial number for a technology concept that just emerged in 2008. The shift to cloud computing and other types of shared services should result in substantial cost savings, allowing agencies to reallocate funding where most needed. Yet, developing a private cloud isn't a trivial undertaking, and they're not ideal for every situation. (See Figure 8, below.)

Paul Christy, CIO of the Small Business Administration, is moving his agency's new public-facing innovation portal to a cloud service. The decision was made to allow for greater scalability and uptime, at lower costs. The SBA is also preparing to move its HR training system to the cloud. Such moves are typical of agencies that seek to move some workloads into the cloud, but continue running their most critical systems in dedicated (non-cloud) environments. Migrating enterprise apps to the cloud isn't a trivial process, as we have seen from the large-scale migration of email underway at DoD.

Figure 8



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

GSA recently completed one of the most ambitious moves to the cloud. The agency transitioned its email to Google's Gmail service, at a projected cost savings of 50% over five years, or about $15 million.

Program Management

The IT reform plan also calls for improving the management of large federal IT projects by recruiting and hiring people with program management skills. Only recently did the Office of Personnel Management establish "project manager" as a formal job category in federal government. Annual performance reviews and accountability for project management are addressed in the reform plan. Likewise, OMB's IT Dashboard is intended to display progress—or lack of it.

In recognition of the fact that hiring experienced program management talent is challenging for federal agencies, OMB has created a career path for IT program managers. A priority for agencies is to identify IT program management competency gaps in the next Human Capital Management Report and develop plans to close those gaps. OPM is working with the departments of Treasury and Agriculture to pilot the IT program management career track.

Too often, agencies develop a program cost estimate, then rely on a contractor to do the work. If the program doesn't go well, the contractor gets blamed. While there's obviously an appropriate place for contractors in the execution of federal IT programs, agencies must not relinquish responsibility for the ultimate outcome. Thus, IT project management must be a priority whether agencies do the work with internal resources or via contract. (See Figure 9, page 23.)

In *InformationWeek*'s 2011 Federal Government IT Priorities Survey, 66% of respondents had a project management office (PMO), a 7-point increase from 2010. Nevertheless, many agencies still haven't mastered the art of IT project management. They often don't place enough authority with the PMO, but rather use it to create templates and other project management documents. Contractors are left to make decisions on how to move forward with implementation.

When we asked why IT projects go off track, 31% of survey respondents said lack of budget, 23% blamed conflicting or poorly defined requirements and 19% said they couldn't obtain skilled IT staff. The project management challenge is compounded by long procurement cycles and legacy development approaches that cause many of the technologies developed to be years behind the state of the market. (See Figure 10, page 24.)

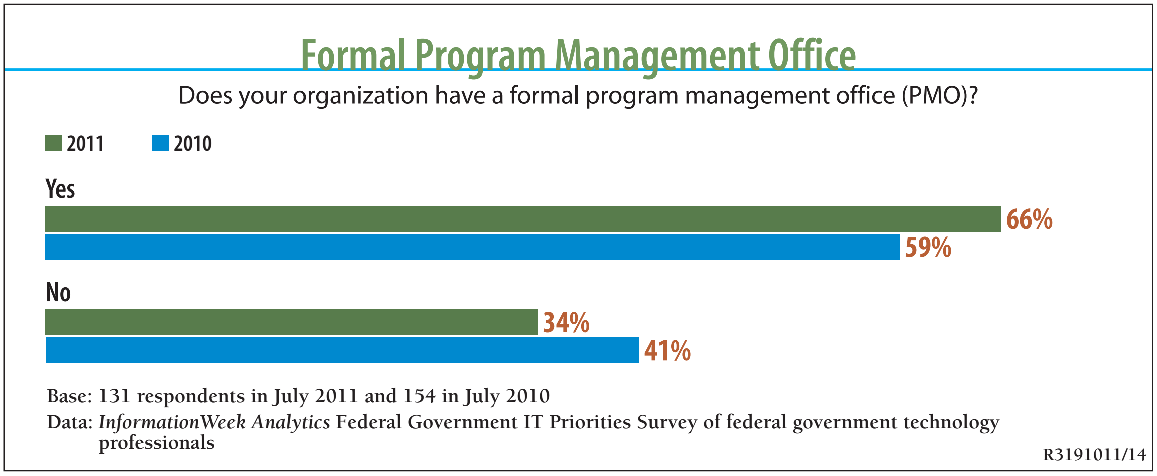
With the right focus, effective IT project management should be one of the easier priorities to master. Approaches like earned value management (EVM) can be used to monitor the health of projects, though few agencies are prepared to effectively use such measurements. OMB's IT Dashboard lets anyone drill down on hundreds of IT projects in federal government and examine their on-budget and on-schedule status, as well as an overall rating from the CIOs behind those projects. You can also see project milestones and the cost and schedule for each milestone.

But this type of project management deals with data that may be outdated. In order to achieve more effective project management, accurate task and timekeeping are needed at the contractor level. Real-time data on project status could be used to identify and mitigate potential problems before they occur. Unfortunately, few agencies have the tools to make this type of project management a reality.

Agencies must ensure that all aspects of an IT project can be managed and that leaders have full visibility into its health. At the Department of Education, CIO Danny Harris implemented enhanced change management and improved verification procedures to help get the sought-after business value.

At SBA, Christy formed a "tiger team" to oversee the first round of deliverables for an identity

Figure 9



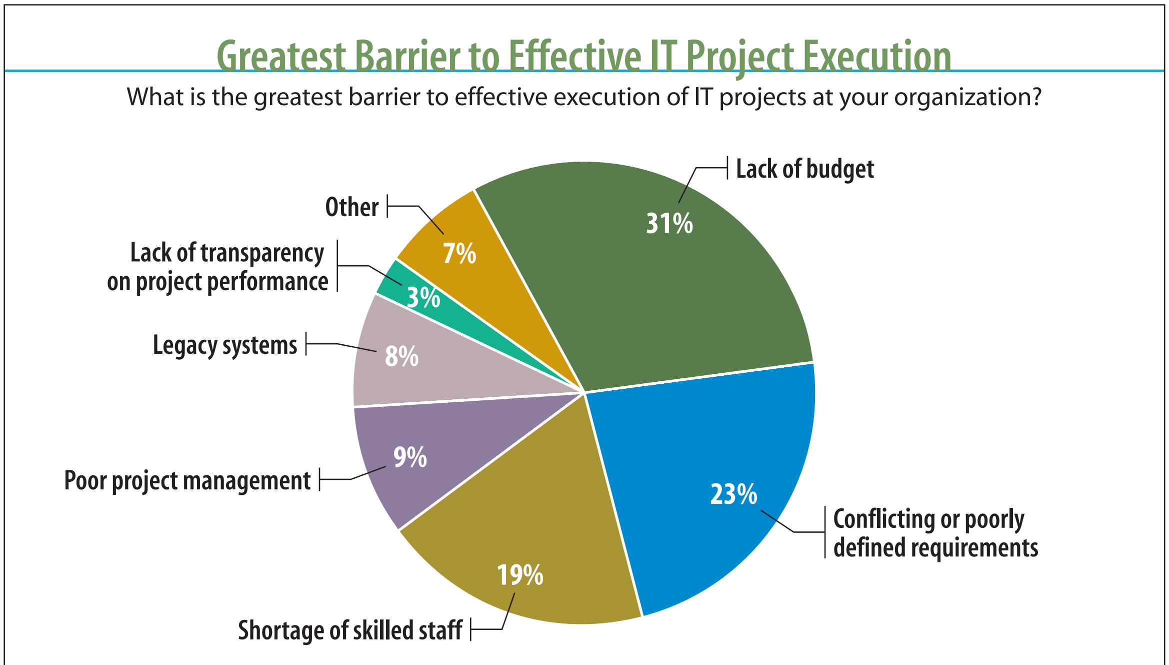
Base: 131 respondents in July 2011 and 154 in July 2010
Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals
R3191011/14

and access management project. Such a triage approach, while effective for small projects, wouldn't be an effective way to manage a broad portfolio of IT programs. Instead, CIOs need more sophisticated project and program management, including the organizational skills and management tools to support that.

Next Steps

Our survey found disaster recovery planning/continuity planning, data records management, business intelligence/AI/data mining and application performance management near the top of the government IT priorities list. In Kundra's final presentation to the House Oversight and Government Reform Committee's Technology, Information Policy, Intergovernmental Relations and Procurement Reform Subcommittee in June, the outgoing federal CIO shared 10 lessons learned. They included the need to tap into the "golden sources" of data instead of creating derivative databases, as well as employing common data standards. Such steps are

Figure 10



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/10

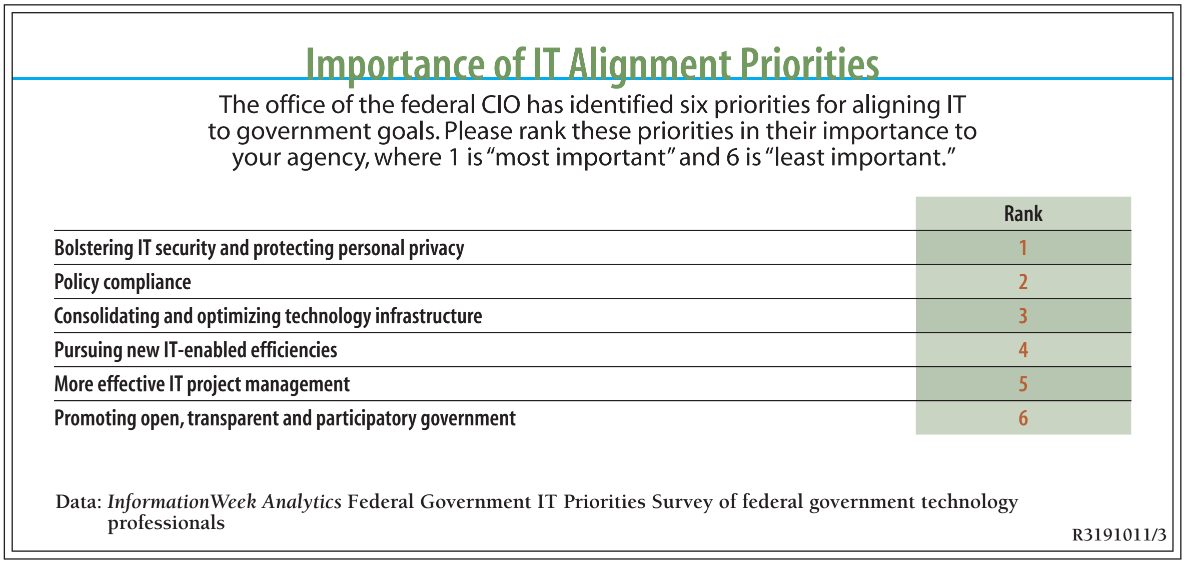
prerequisites if initiatives such as data records management and BI are to succeed.

Federal IT teams will also have to develop strategies for new types of computing devices. In August, Hewlett-Packard revealed it was looking to sell its PC business, causing some to question how much longer PCs will remain relevant as tablets and other new form factors rise in popularity. While I heard laughter from one government contracting officer, who sees no slowdown in PC purchases, the post-PC era is clearly on the horizon. As more federal workers use tablets and smartphones, agencies must recognize that some of their apps will be running on untrusted devices that may be employee-owned. This has implications for agencies that don't have the security infrastructure to deal with this type of enterprise architecture. The need to support mobility and consumer devices will also drive cloud adoption.

A critical shift will be a move away from perimeter-centric security to application- and data-driven security. Expect to see more government applications that need to incorporate security into the app itself and monitor the profile of users. (See Figure 11, below.)

Agencies need help prioritizing these and the other mandates competing for their limited resources and developing plans for what are, in many cases, interrelated challenges. With so much to do, they must look for situations where one initiative helps drive forward another, so-

Figure 11



Importance of IT Alignment Priorities

The office of the federal CIO has identified six priorities for aligning IT to government goals. Please rank these priorities in their importance to your agency, where 1 is "most important" and 6 is "least important."

	Rank
Bolstering IT security and protecting personal privacy	1
Policy compliance	2
Consolidating and optimizing technology infrastructure	3
Pursuing new IT-enabled efficiencies	4
More effective IT project management	5
Promoting open, transparent and participatory government	6

Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals

R3191011/3

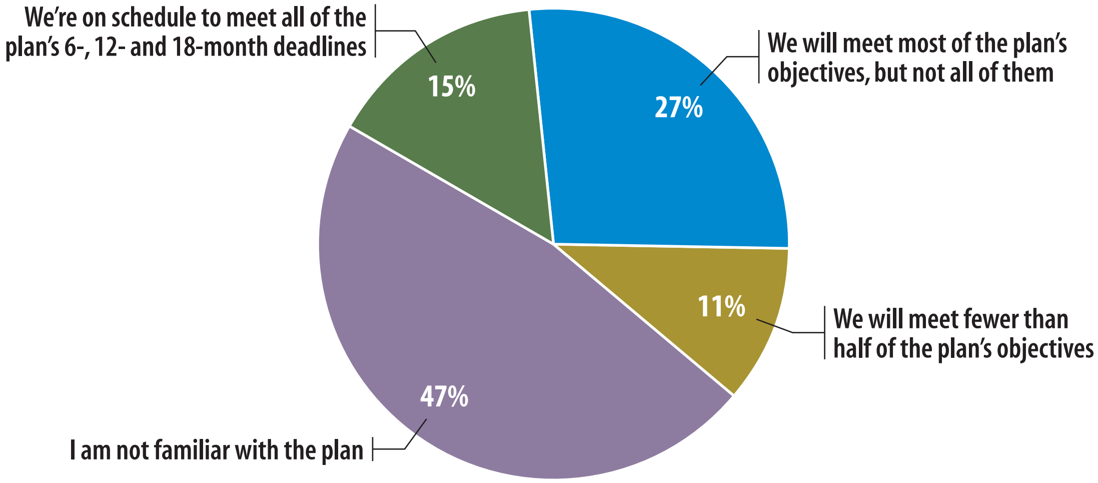
called "win-win" scenarios. As an example, data center consolidation and the adoption of cloud computing may centralize critical resources, and once those things are done, it will be easier to apply consistent security policies. Likewise, if we don't tighten cybersecurity, agencies won't embrace open government.

Notably, the White House's Open Government Initiative lost the most steam in our survey, dropping to the bottom of the priority list, with only 7% seeing this as extremely important. This may reflect that many agencies have completed the first set of requirements around open government—completing and publishing organizational plans, establishing websites, and releasing some data sets—so they can ease up a bit on the gas pedal. The risk is that the open government movement isn't deemed as important as it once was, which would be a setback. Agency officials must be attentive to ensure that doesn't happen.

Figure 12

Progress in Meeting OMB's IT Reform Plan

What is your agency's progress in meeting OMB's 25-point IT reform plan?



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

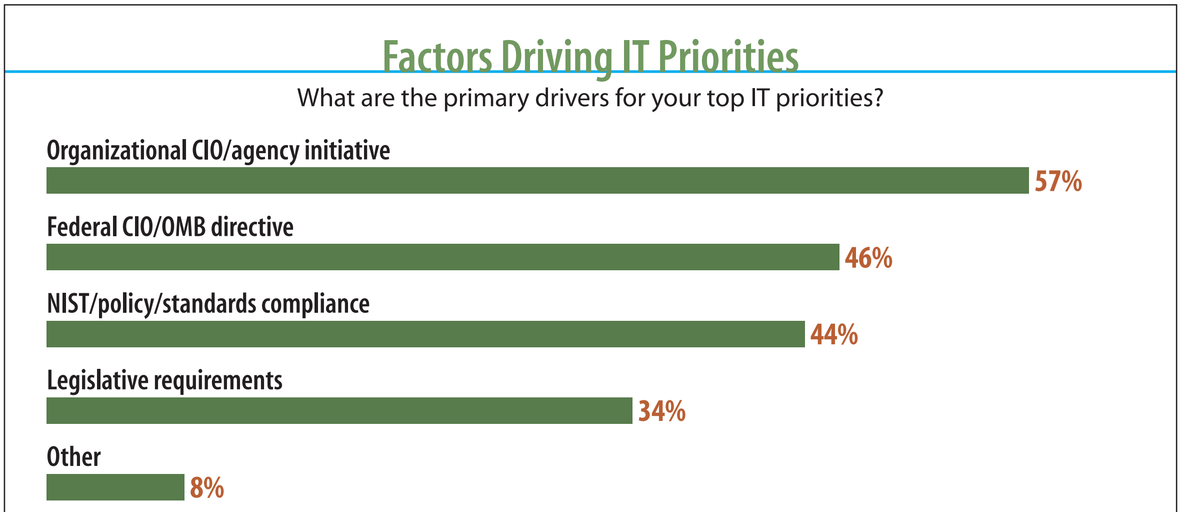
R3191011/5

Failure to do a better job at IT project management is another potential risk—one that would hamper efforts to modernize government through adoption of new technologies. Only when challenges are addressed in a coordinated fashion will we be able to really make progress on key priorities.

Our survey identified areas for improvement in executing on policy initiatives. While 23% said bolstering IT security and protecting personal privacy were being executed extremely well in their agencies, the numbers in other areas dropped off quickly. How well are agencies meeting the objectives in the IT reform plan? Only 15% indicated that they're on schedule to meet all of the plan's six-, 12- and 18-month milestones. (See Figure 12, page 26.) More than half (57%) were of the opinion that their own agencies' initiatives were more important than those set by OMB. That should be a point of concern given efforts by OMB and the federal CIO to align goals and communicate them to rank and file federal IT employees. (See Figure 13, below.)

The jury is still out on how well agencies will satisfy key IT initiatives such as open government, cloud first and data center consolidation. Change in government, as with any large enterprise in the private sector, isn't easy. While there have been pockets of progress and

Figure 13



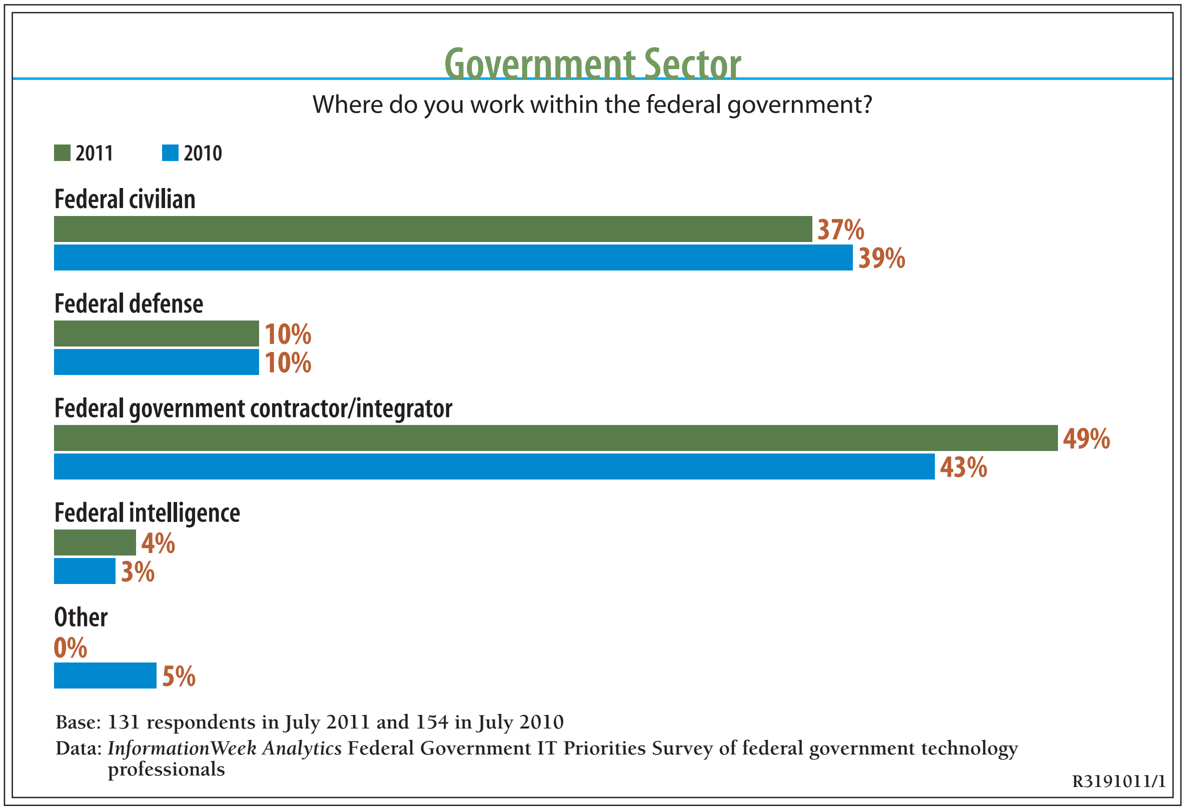
Note: Multiple responses allowed
Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/6

innovation, most of the work required for improved IT performance lies ahead.

The federal government's ability to leverage IT and set priorities will be a defining factor in its ability to reduce costs, lower debt and improve services. That's why IT reform must be more than a "plan." For agency CIOs and their IT teams, progress hinges on continued execution.

Figure 14



Government Sector

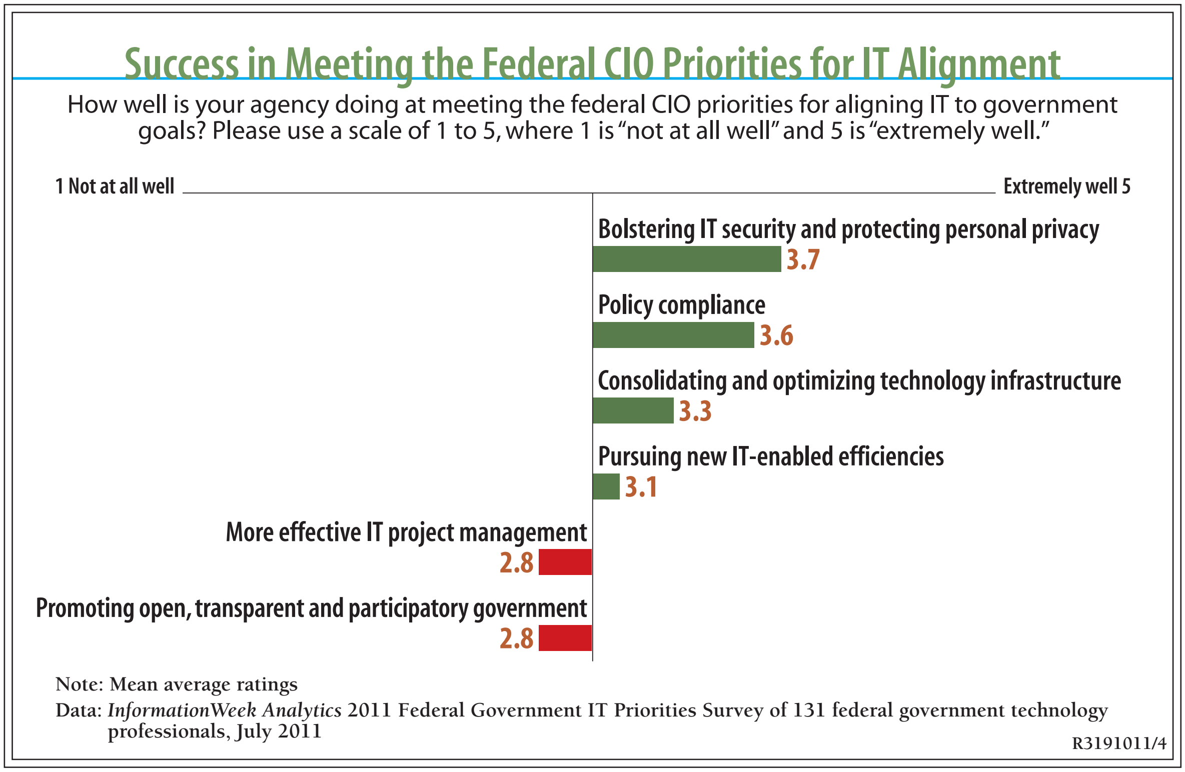
Where do you work within the federal government?

Base: 131 respondents in July 2011 and 154 in July 2010

Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals

R3191011/1

Figure 15

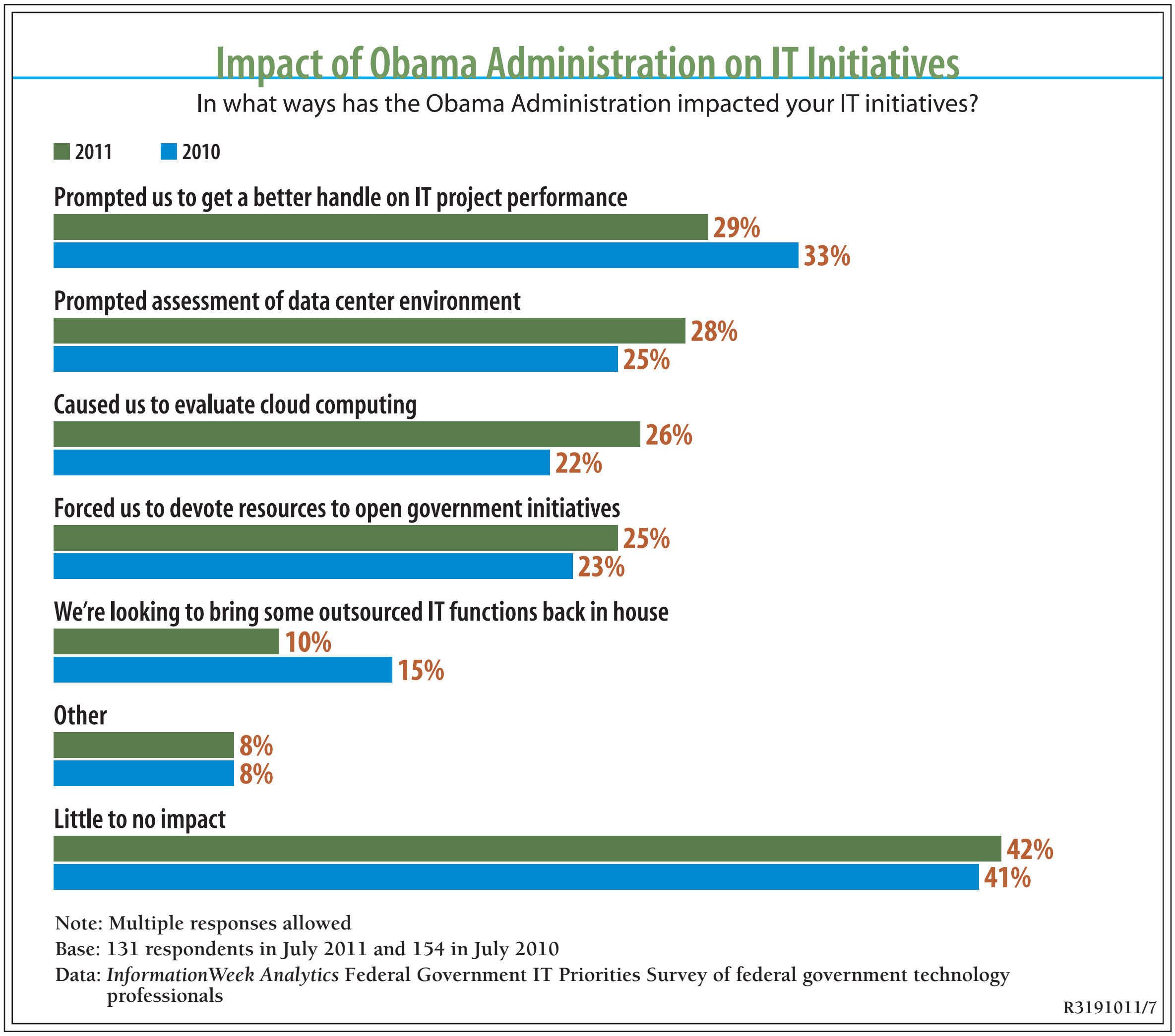


Note: Mean average ratings

Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/4

Figure 16



Note: Multiple responses allowed

Base: 131 respondents in July 2011 and 154 in July 2010

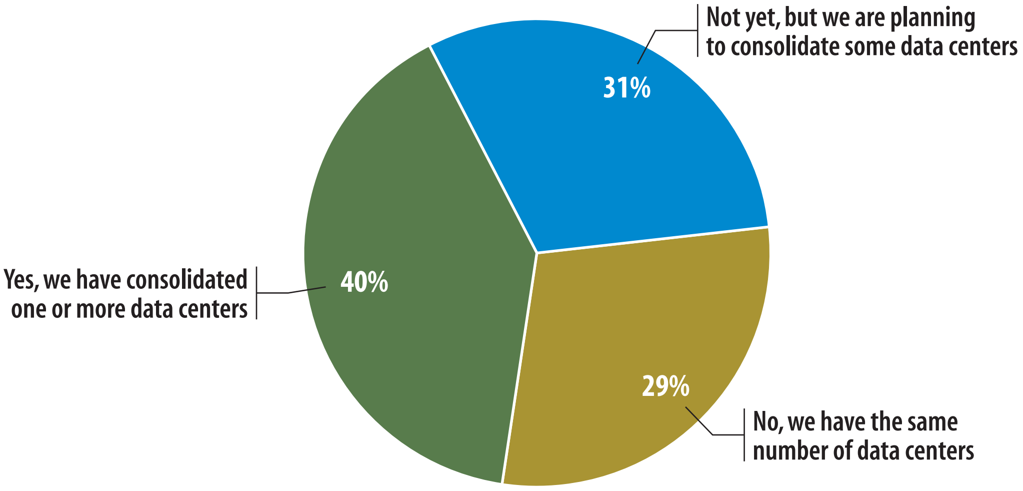
Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals

R3191011/7

Figure 17

Data Center Consolidation

Has your agency consolidated data centers over the past 12 months?



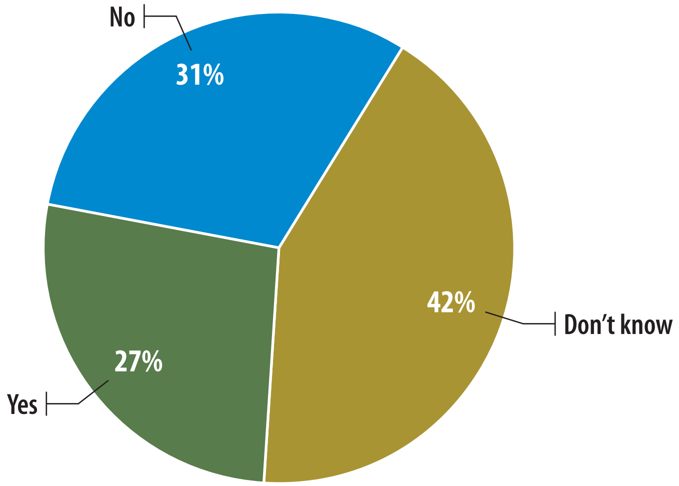
Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/13

Figure 18

Implementation of the Open Government Initiative

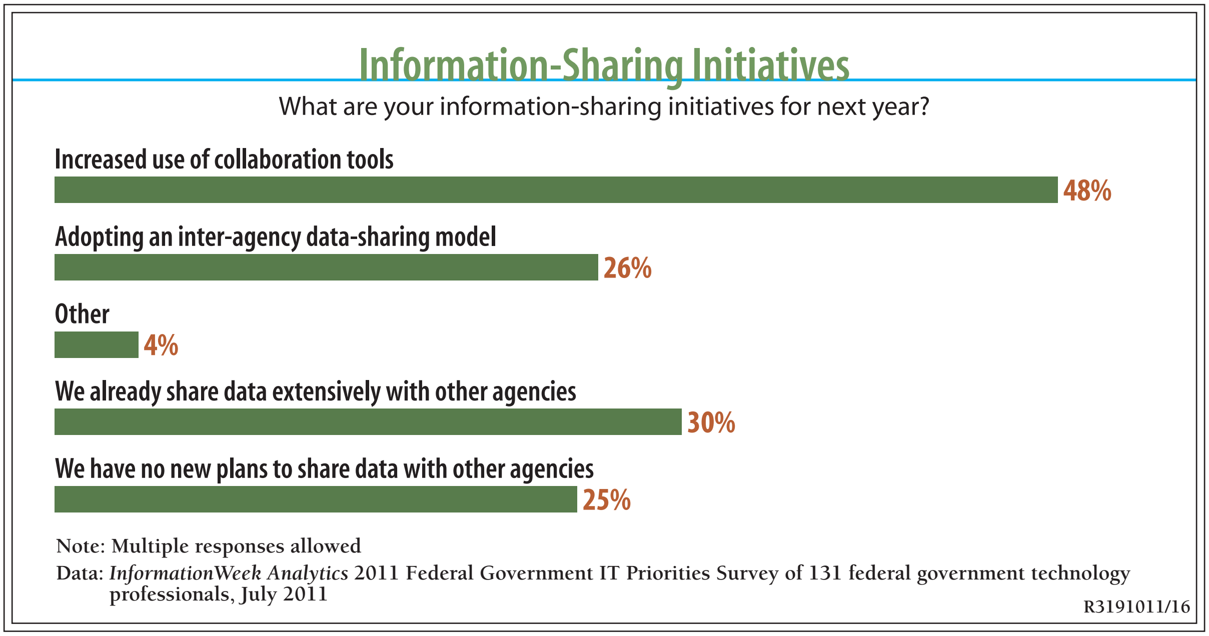
Has your agency implemented the open government initiative by providing data on data.gov or on its website (e.g., www.agency.gov/open)?



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/15

Figure 19

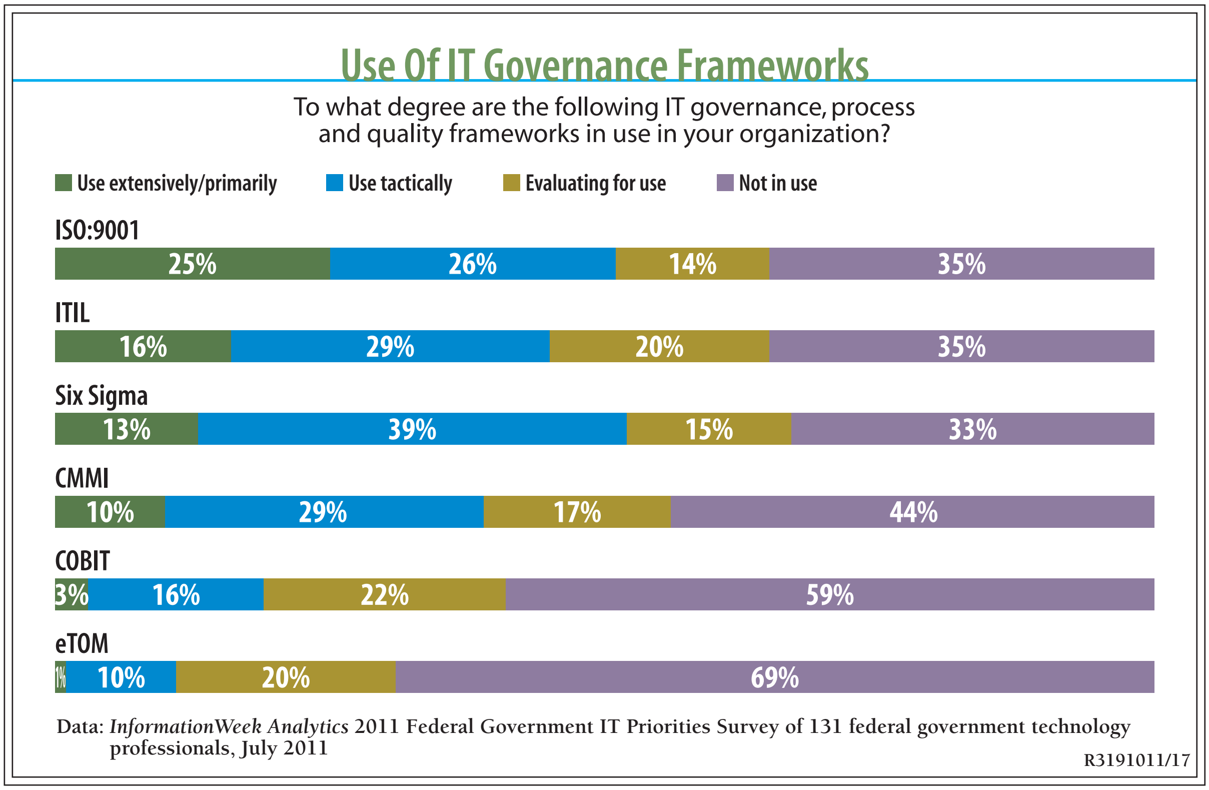


Note: Multiple responses allowed

Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/16

Figure 20



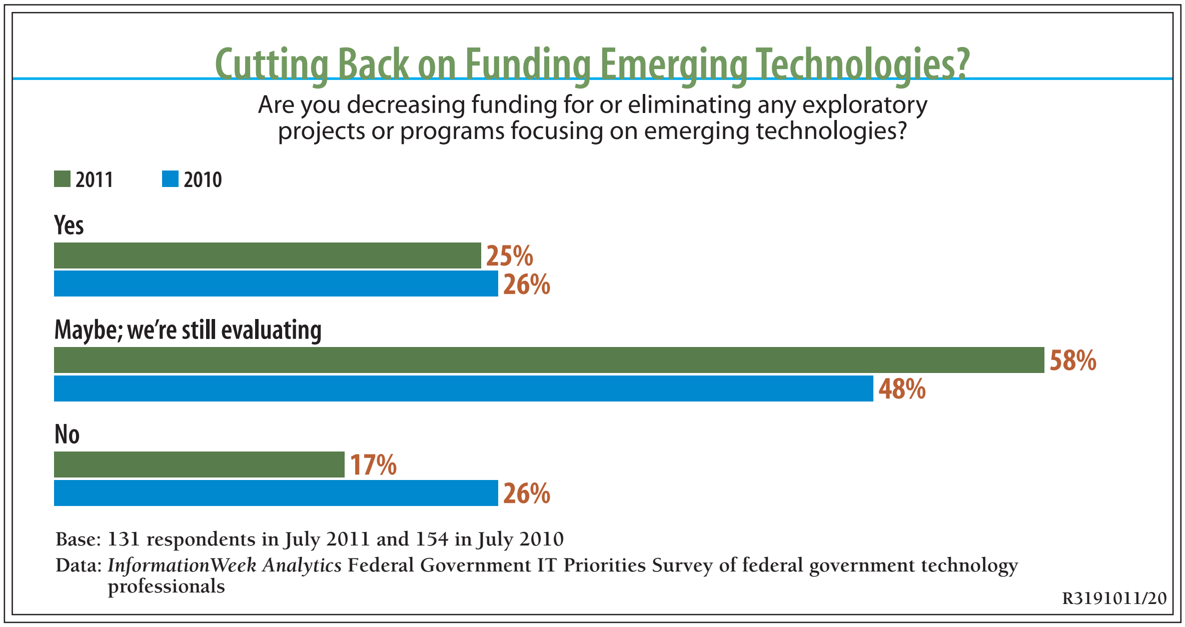
Use Of IT Governance Frameworks

To what degree are the following IT governance, process and quality frameworks in use in your organization?

Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/17

Figure 21



Base: 131 respondents in July 2011 and 154 in July 2010

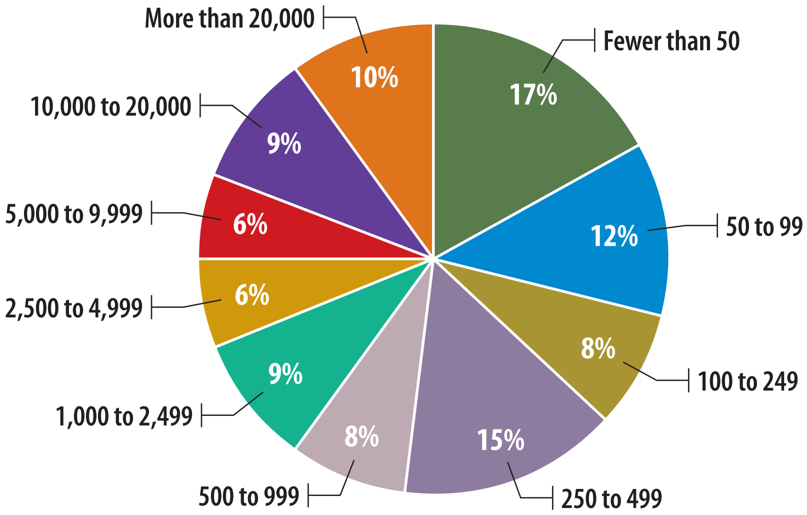
Data: *InformationWeek Analytics* Federal Government IT Priorities Survey of federal government technology professionals

R3191011/20

Figure 22

Size of IT Organization

How many individuals are employed within your IT organization?



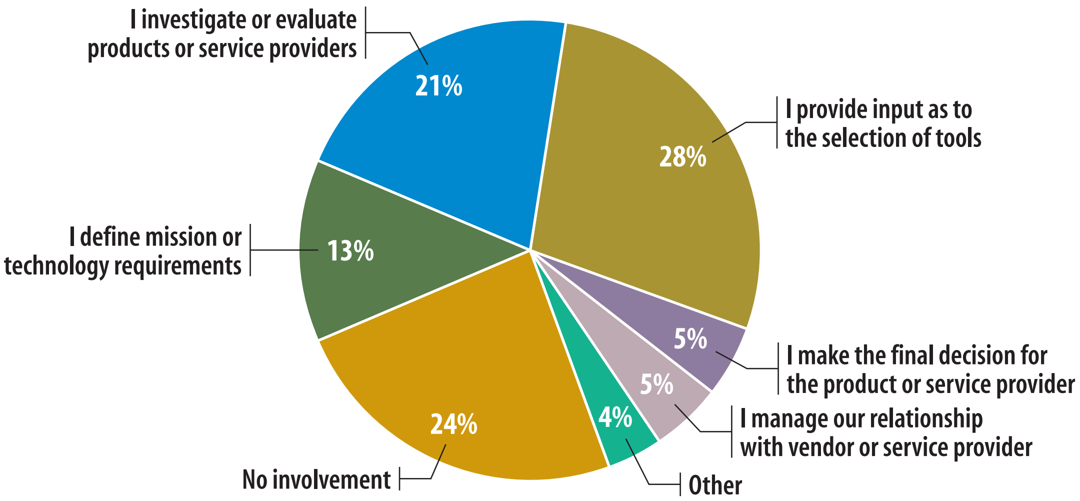
Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/22

Figure 23

Primary Role in the Selection and Use of Technologies

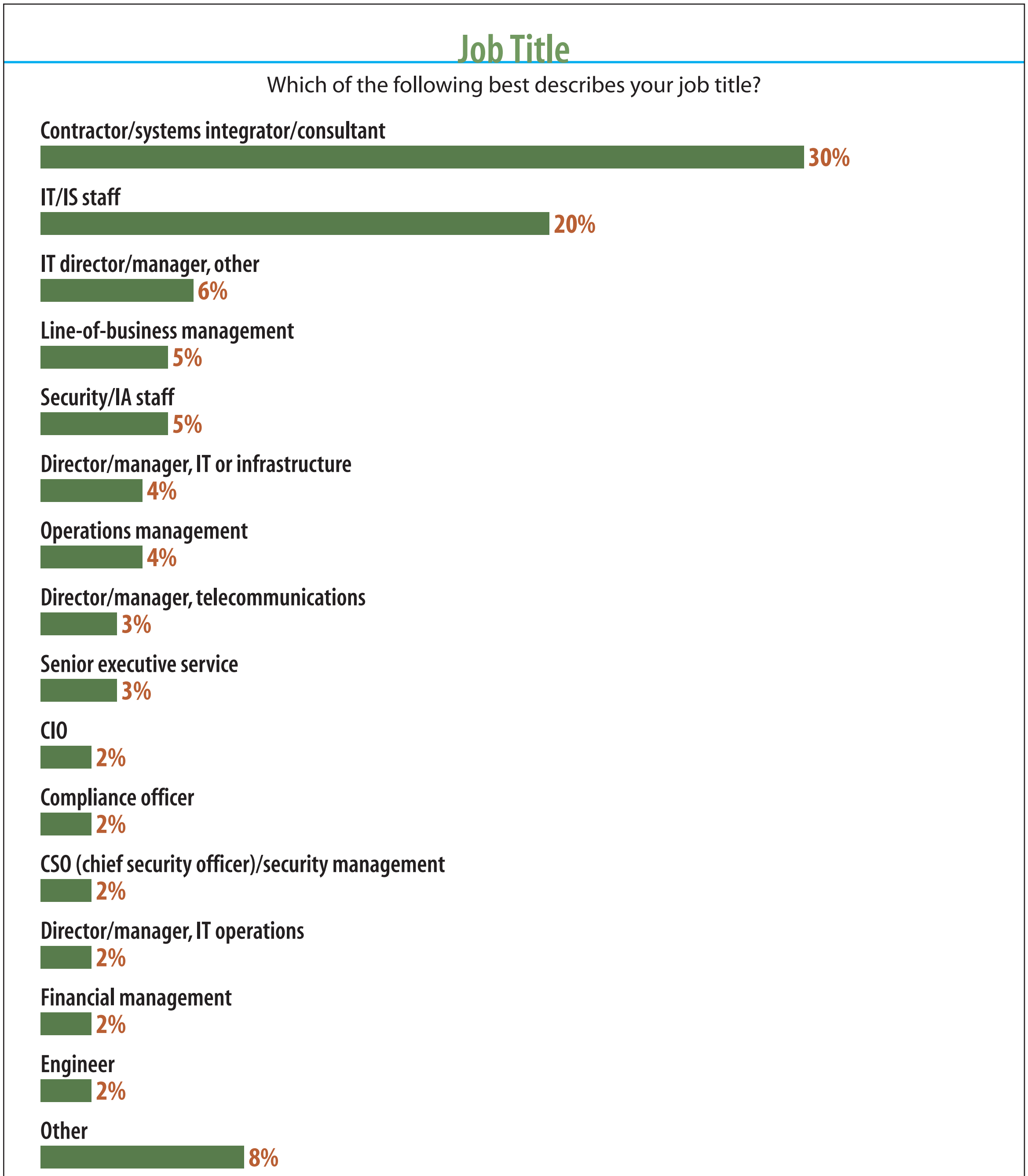
What is your primary role in the selection or use of technologies?



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/23

Figure 24



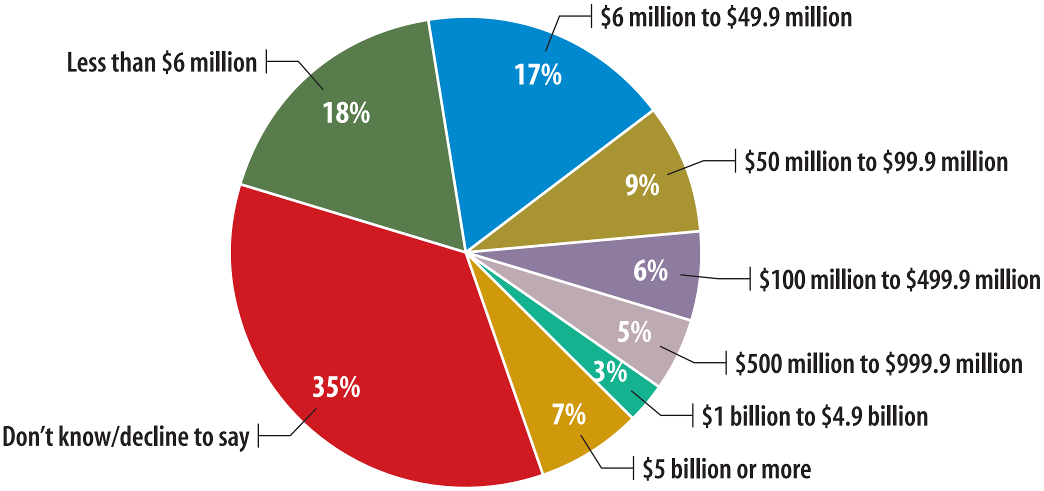
Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/24

Figure 25

Annual Budget

Which of the following dollar ranges includes the annual budget of your entire organization?



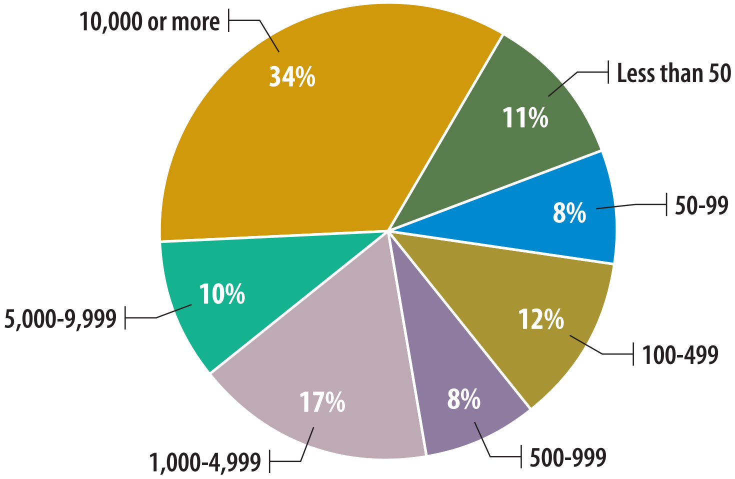
Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/25

Figure 26

Size of Organization

Approximately how many employees are in your organization?



Data: *InformationWeek Analytics* 2011 Federal Government IT Priorities Survey of 131 federal government technology professionals, July 2011

R3191011/26