McKinsey&Company

McKinsey on Government

Number 7
Autumn 2011

IT: Challenge and opportunity

4
More transparency, less complexity: How to boost federal IT yield

10
'Getting stuff done': A conversation with America's first CIO

18
Capturing value through IT consolidation and shared services

24
A city consolidates its data centers

28
Seven imperatives for success in IT megaprojects

36
Transforming IT: A German success story

42
Can you hack it? Managing the cybersecurity challenge

50
Getting ahead in the cloud

58
Better all the time: Continuous improvement in IT

McKinsey on Government is written by consultants in McKinsey & Company's global public sector practice along with other McKinsey colleagues.

To send comments or request copies, e-mail us: McKinsey_on_Government@McKinsey.com.

Editorial Board: Stephen Kelly, Cameron Kennedy, Nancy Killefer, Chandru Krishnamurthy, Anne Smith, Lawrence Wong

Editor: Monica Toriello

Contributing Editor: David Klein
Art Direction: Shoili Kanungo, Delilah Zak
Design: Shoili Kanungo
Editorial Production: Elizabeth Brown, Heather Byer, Nadia Davis, Torea Frey, John C. Sanchez, Venetia Simcock, Sneha Vats

McKinsey & Company
Industry Publications
Editor-in-Chief: Saul Rosenberg
Managing Editor: Lucia Rahilly

Cover artwork by Dieter Braun

Copyright © 2011 McKinsey & Company. All rights reserved.

This publication is not intended to be used as the basis for trading in the shares of any company or for undertaking any other complex or significant financial transaction without consulting with appropriate professional advisers.

No part of this publication may be copied or redistributed in any form without the prior written consent of McKinsey & Company.

McKinsey on Government
Number 7, Autumn 2011

2
Introduction

4
More transparency, less complexity: How to boost federal IT yield

To improve IT performance and productivity, federal CIOs must first develop a detailed understanding of IT investments and reduce complexity in the IT portfolio. Only by pulling these two levers can CIOs consistently deliver higher yield per IT dollar.

10
'Getting stuff done': A conversation with America's first CIO

During his last few weeks in office, Vivek Kundra, the first-ever federal chief information officer of the United States, reflects on his tenure.

18
Capturing value through IT consolidation and shared services

Agencies should look beyond data-center consolidation for opportunities to streamline IT assets. By pursuing a range of initiatives, agencies can boost effectiveness while cutting IT costs by up to 20 percent—without reducing head count.

24
A city consolidates its data centers

The experience of one US city provides lessons on how public-sector organizations can design and execute a data-center consolidation.

28
Seven imperatives for success in IT megaprojects

To implement public-sector IT megaprojects successfully, leaders must pay close attention to process, people, and governance. We discuss seven imperatives that, although not technically difficult, require dramatic changes in mind-sets and ways of working.

36
Transforming IT: A German success story

A once-underperforming IT function has become one of Europe's leading public-sector IT providers—due in large part to the leadership of Klaus Vitt, chief information officer of the German Federal Employment Agency. In this interview, Vitt reflects on the challenges of IT transformation and how to do it right.

42
Can you hack it? Managing the cybersecurity challenge

To secure cyberspace, technology alone is not enough. Strong management plays an equally important role.

50
Getting ahead in the cloud

The transition to cloud computing will be especially challenging for governments, given their myriad IT systems and their security, budgetary, and organizational constraints. We look at four critical actions they must take.

58
Better all the time: Continuous improvement in IT

By reorganizing its IT function and applying lean IT principles, the Netherlands' largest public-sector agency has drastically improved its performance and reputation. The agency's leaders talk about what they've done—and what still remains to be done—in their pursuit of IT excellence.

Introduction

This issue of *McKinsey on Government* is devoted to the challenge and the opportunity represented by IT. Pervasive and indispensible, IT is no longer exclusively the concern of chief information officers (CIOs); it must be on the agenda of the most senior leaders in government. Countries' public budgets are under great pressure at exactly the moment their populations want and need more from public services. Governments must deliver more while spending less—and IT, managed well, can help them do both.

We begin this edition with the challenge most starkly put. According to the authors of "More transparency, less complexity: How to boost federal IT yield," the fundamental goal of federal CIOs is to "ensure that every dollar spent on IT delivers the maximum benefit to taxpayers"—a tall order in the face of budget cuts and expanding agency missions. The answer, as the title would suggest, is to take IT out of its black box and put it in a clear one, and to simplify wherever possible.

Indeed, greater transparency—along with greater accountability—was a top priority for Vivek Kundra, the first-ever federal CIO of the United States, who is interviewed in the second article in this issue. In appointing Kundra to the role, President Obama articulated a dual charge: the nation's CIO would be responsible for ensuring "that we are using the spirit of American innovation and the power of technology to improve performance and lower the cost of government operations." Kundra shares his perspectives on the need for speedy execution, the virtues of not knowing how things are "supposed to work," and the importance of relentless focus in the face of the 24-hour news cycle.

As US CIO, Kundra published a detailed plan for reforming government IT. One element of that plan entailed the closure of at least 800 federal data centers. Like many government agencies worldwide, US agencies have too many IT facilities, share best practices too rarely, and suffer enormous legacy-technology issues. The third article in this edition, "Capturing value through IT consolidation and shared services," describes how agencies can boost effectiveness through consolidation while cutting costs by up to 20 percent. A short piece that follows discusses the experience of one large US city consolidating its dozens of data centers into just two.

Another core element of Kundra's plan is better management of IT megaprojects. IT programs with enormous ambitions, long time frames, and grand budgets have a long history of disappointing their sponsors. The authors of the next article discuss the seven imperatives for success in implementing large-scale IT projects. The imperatives are not technically difficult, but they require a dramatic change in the way IT is managed and the way people think and work together. It's not rocket science—it's harder.

CIOs struggling with the thorny tasks of IT consolidation and megaproject management can

take inspiration from the achievements of Klaus Vitt, CIO of the 90,000-employee German Federal Employment Agency. Vitt, in an interview, reflects on how he led the transformation of an underperforming function into one of Europe's leading public-sector IT providers. He talks about the success factors of a large-scale transformation—among them, a comprehensive IT strategy, clear management structures, and a transparent system of IT targets that all employees can identify with and commit to. Vitt's place among the top 10 CIOs two years in a row, in the annual ranking by German magazine *CIO*, testifies to his success.

The next two articles tackle new and growing issues that require both technical and management expertise: cybersecurity and cloud technologies. The authors of "Can you hack it? Managing the cybersecurity challenge" argue that governments have yet to come to terms with the real military and economic risks posed to their countries by the openness and interconnectedness of modern-day computing. The authors propose a taxonomy to help government leaders understand the cybersecurity landscape, and a "value at risk" framework leaders can use to identify the most serious threats. Cybersecurity, they assert, is not just a matter of protecting technology against technology with technology; management matters just as much.

No treatment of the IT issues facing governments would be complete without a discussion of "the cloud," the remarkable trend toward provisioning IT "as a service" and transforming it into a utility, like water or electricity, that users can access as, when, and where they need—without creating infrastructure or "power stations" of their own. The opportunities for efficiency are massive, but so are the challenges. "Getting ahead in the cloud" looks at four actions agencies should take if they wish to benefit from this powerful new technology trend.

We close on an optimistic note, suggesting that public-sector IT can get "better all the time." The leaders of the Netherlands' largest public-sector agency, the Dutch Tax and Customs Administration, discuss the drastic improvement in performance and reputation the agency has achieved—and continues to strive for—through the discipline of lean IT transformation.

We hope these essays and interviews will inspire you on your journey toward IT excellence. As always, we invite comments at McKinsey_on_Government@McKinsey.com.

Stephen Kelly
Director, McKinsey & Company

Nancy Killefer
Director, McKinsey & Company

Chandru Krishnamurthy
Director, McKinsey & Company

More transparency, less complexity: How to boost federal IT yield

To improve IT performance and productivity, federal CIOs must first develop a detailed understanding of IT investments and reduce complexity in the IT portfolio. Only by pulling these two levers can CIOs consistently deliver higher yield per IT dollar.

Aamer Baig, Stephen Kelly, and Chandru Krishnamurthy

Faced with the hard reality of budget cuts, the pressing need for more robust IT security, and greater taxpayer expectations in a fast-changing technology landscape, chief information officers (CIOs) within the US federal government are under unprecedented pressure to increase IT productivity. This is a tall order; tomes have been written deploring the lack of productivity in federal IT spending and dissecting the structural and organizational challenges that hinder greater public-sector IT yield.

The US government's Office of Management and Budget has set out sensible guidelines and policies for reforming federal IT management that begin to address the fundamental challenge: ensuring that every dollar spent on IT delivers the maximum benefit for US taxpayers. These policies will take time to achieve optimal scale. Meanwhile, as federal CIOs go about their daily work, they must constantly keep in mind the twin mandates to deliver more but spend less.

Many levers can be pulled to deliver higher IT yield per dollar. Two, however, enable the effectiveness of virtually all the others. The first is increasing transparency into the performance and health of IT investments—that is, the short- and long-term strength of these investments. Transparency is crucial; after all, it is impossible to govern or manage what one cannot see. The second lever is reducing complexity: of IT investments, programs, and execution. In our experience, agencies pay too little attention

to these levers, and thus diminish the impact of the other actions they may take. The result is a failure to achieve sustainable improvements in IT productivity and performance.

Increasing transparency

The first order of business for a government CIO should be to dig down to the bedrock facts about IT performance and health. Agency leaders must understand the sources, uses, effectiveness, and efficiency of IT funds in enough detail to be able to make informed decisions about strategy, operations, and governance.

This is challenging, given the public sector's labyrinthine appropriations, budgeting, acquisition, and organizational processes and structures. One agency, for example, invested six months in developing an elaborate governance process, only to realize that the process addressed less than 10 percent of the agency's total technology spending. Much of the IT spending was not visible to agency leadership because it was not managed in a consolidated pool; units within the agency had direct lines of appropriation, and most IT spending was hidden in individual program budgets. Consequently, agency leaders were governing only the tip of the IT iceberg.

In another example, a government department's IT spending was dispersed across about a dozen organizational silos, each of which spent at least $30 million on IT annually. Very few of the department's senior leaders realized that its total spending on IT amounted to more than $1 billion. The department's scale qualified it as one of the world's largest IT shops, yet it was effectively operating as a set of much smaller organizations, leaving on the table efficiency improvements on the order of 30 to 40 percent. The same assessment that revealed these facts also brought to light huge variations in the prices that the department's agencies paid for comparable products and services (Exhibit 1).

The aggregated data were revelatory to senior executives. Equally eye-opening was the fact that most of the inefficiency was driven not by the IT community but by each organizational silo's need for control and by the lack of cross-agency visibility into performance.

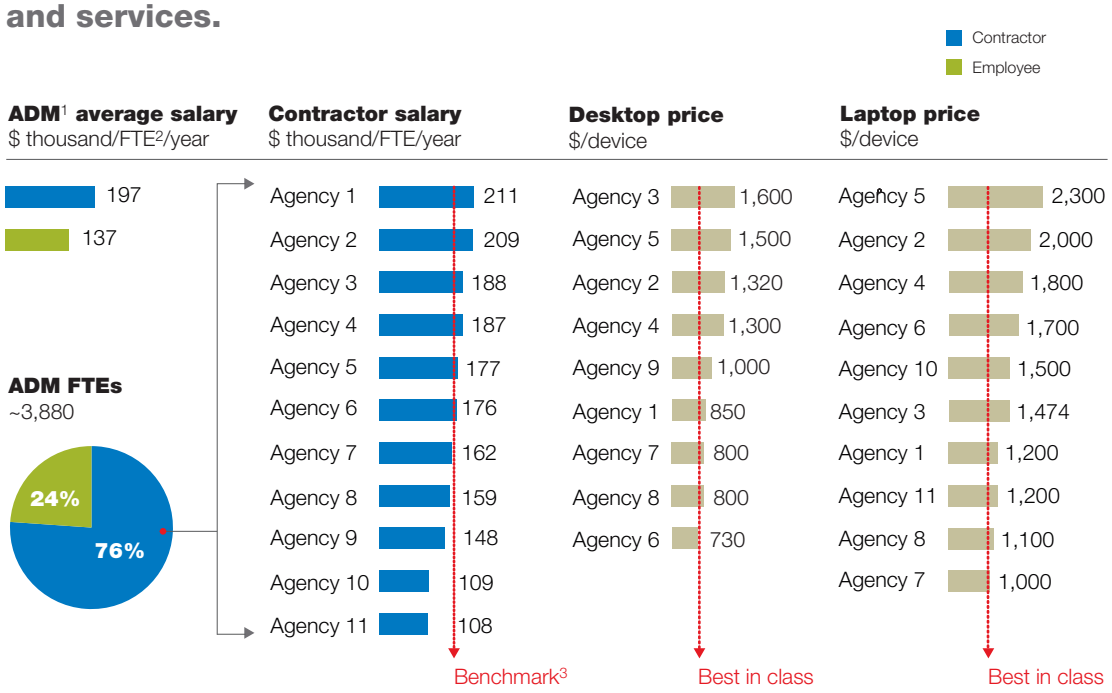
The department's investment in transparency more than paid off. Once the potential for efficiency improvements became clear, the department was able to take steps to capture it—for example, by shifting to best pricing for laptops and desktops, developing a product catalog to minimize unnecessary customization and increase the organization's buying power, and creating standardized rate cards to help agencies evaluate contractor labor wages. These actions have put the department on track to save approximately $100 million per year.

Transparency begets trust, and trust begets effective governance. It is remarkable how much effort the government spends on audits and "checkers checking checkers," yet how little is actually learned about true return on IT investments. Ironically, the current inspection-oriented mind-set puts people on the defensive, creating less incentive for transparency.

The right kind of transparency—focused on outcomes, ratios, yields, and quality, rather than on checking the box on inputs, budget and schedule adherence, due process, and forms and procedures—will greatly improve the level of trust within and across agency boundaries. Federal CIOs and agency leaders should regularly conduct a rigorous "IT transparency checkup." Often, such a checkup entails detailed, line-item-level

Exhibit 1

Agencies pay widely varying prices for similar products and services.



[1]Application development and maintenance.
[2]Full-time equivalent.
[3]Public-sector weighted average of like-for-like roles.

Source: Federal Data Center Consolidation Initiative (FDCCI) data; agency data; interviews

analyses of vendor contracts, as well as a thorough review of an agency's technical and managerial policies for every IT cost category. CIOs should also ask themselves a series of questions regarding both the current performance of IT and its long-term health.

IT performance: How efficient and effective are we?

- Are our IT assets and vendor contracts well utilized? Are we truly operating at scale? What efficiencies could we gain from consolidation and centralization of services and pooling of IT labor resources?
- How productive are our application development and maintenance (ADM) staff and third-party providers?
- If we deliver above-average to best-in-class efficiencies, how much of our budget could we free up to fund higher-value initiatives?

IT health: Are we investing in the right priorities and in the right proportions?

- How much of our IT budget directly supports mission-specific applications and processes, and how much is allocated to utility IT and basic enterprise support? Should we be allocating

our resources differently? Where should we invest more, and where should we reduce our expenditure?

- Where could IT play a truly transformative role in both improving our core business processes and innovating how we deliver on our mission?

- How effectively do we manage demand for IT dollars? Do we handle trade-offs well, or do we avoid conflicts and thus make sub-optimal decisions?

- Are we developing in-house talent in pivotal jobs and skill sets, or are we too dependent on contractors?

The upside of conducting a regular transparency checkup is significant: from 30 to 40 percent in yield improvements and, counterintuitively, license to invest more in IT.

Containing complexity

The second critical enabler in improving the federal government's yield per IT dollar is reducing *avoidable* complexity. Eliminating complexity in general is not the right goal; much of what the government undertakes is intrinsically complex, and often the IT required to support it is necessarily complex as well. For example, there is simply no parallel to the IT systems that enable the US Air Force's supply and logistics chain, which stretches across several hundred bases around the world, to deploy aircraft, personnel, and munitions at a few seconds' notice. Furthermore, unique government-appropriations and acquisitions regulations add legitimate complexity to both IT and non-IT investments.

That said, CIOs must make every effort to contain unnecessary complexity, because added complexity has an exponential rather than a linear effect on budget, schedule, and functionality risk. Reducing the complexity of large-scale projects is the subject of part of another article (see "Seven imperatives for success in IT megaprojects," p. 28); here we focus on three ways to contain complexity in all projects within an IT portfolio or in an enterprise.

Segment projects by complexity. The IT portfolios of most government agencies consist of three broad types of investments: a handful of complex, large-scale projects; a base load of utility services (such as end-user device management and data-center operations); and a steady, modest flow of low-complexity maintenance and enhancement projects. Because these projects have different levels of complexity, they should be treated differently. However, agencies often have a one-size-fits-all process for conceiving, approving, and executing projects of all kinds.

Some federal CIOs have started to create different "swim lanes" of process flow for investments, depending on their size and complexity. By simplifying the requirements, approval, and acquisition processes for smaller, less complex projects, they reduce cycle time by as much as 40 percent, deliver quick wins, and free up time to focus on larger, more complex projects.

Another major opportunity for CIOs is to create a catalog of services, with clear internal pricing and service-level agreements, for the core utility IT functions. A service catalog gives users clarity into what they are actually paying for. It also makes ordering, installing, servicing, and charging for IT products and services faster and easier. The focus here is on service levels, demand management, utilization, and unit-cost reduction; metrics for each of these can be communicated and managed using a simple

scorecard. By introducing a service catalog supported by industrial-strength delivery models, agencies can free up capacity that they can then devote to containing large-program complexity.

Plan and budget for interface complexity. There are three main types of interfaces that contribute to program complexity: interfaces to enable data transfer between systems; organizational interfaces, which are needed when a system requires funding, resources, people, or data inputs from multiple organizations; and end-user interfaces. Systems interfaces are usually reasonably well-handled by integrators. However, program designers typically underestimate the complexity in organizational and end-user interfaces.

Rarely do the priorities of two organizations align perfectly, and budgets and schedules almost never account for interorganizational delays. For example, one agency's inventory-management system required more than 50 systems interfaces that spanned 12 different organizations, each with its own IT priorities. The coordination of interoperability and data-integrity tests with the release schedules of each of the 12 different organizations caused a delay of nearly six months—and because the agency was carrying $4 million in monthly fixed costs for a program-management office, the delay cost almost $25 million. Had the agency designed the test modules in a way that would not require parallel testing in multiple organizations, it could have avoided or shortened this delay. Phenomena of this kind can be modeled to a significant degree, allowing an understanding of likely organizational complexity early enough to inform design, funding, and deployment decisions.

Many government agencies use cost and schedule models that do not sufficiently account for the nonlinear effects of interface complexity. These flawed models lead to unrealistic investment cases; programs are predestined to "fail" because ingoing assumptions are fed into linear models that underestimate the true cost of complexity. Programs that overrun their budgets and schedules are labeled "failures" because they miss the modeled expectations, which were unrealistic from the outset. Many of these programs would still be sound investments because the business value offsets the costs and complexity risks.

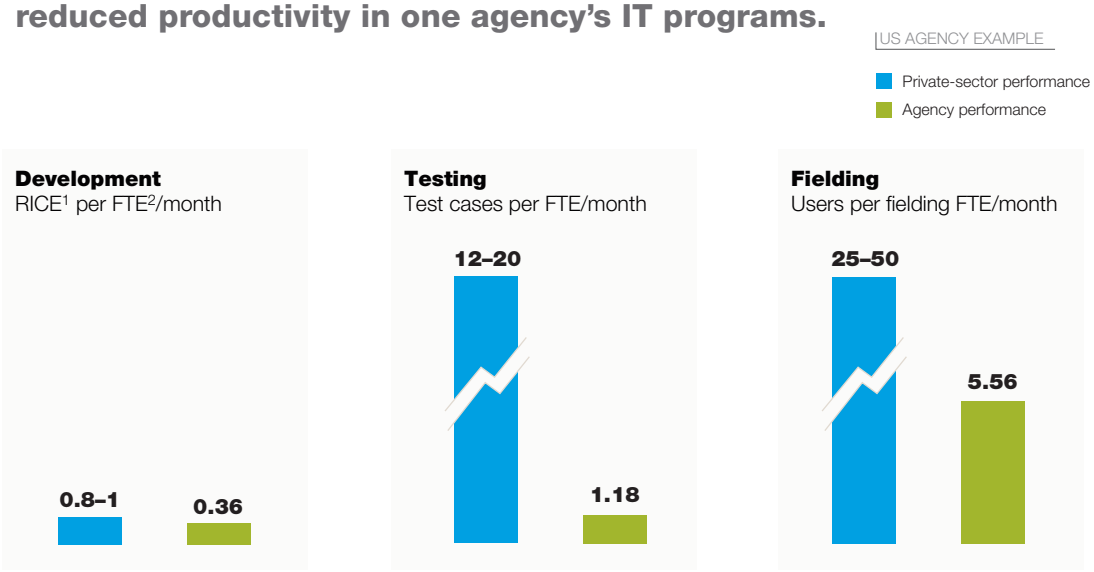
Design vendor contracts to match program complexity. Government agencies negotiate different types of vendor contracts, the three most common of which are fixed-price, cost-plus, and time-and-materials contracts. Many agencies believe a fixed-price contract shifts risk to the vendor, but in reality IT vendors are quite sophisticated: they protect themselves either with requirements-change or customer-delay clauses, or by charging a premium to cover the risk. Poor vendor management is one reason that many government programs are one-third to one-tenth as productive as private-sector programs (Exhibit 2).

Few complex IT programs are well suited to monolithic fixed-price or cost-plus contracts. Program elements are not all the same; therefore, contract elements should not be all the same. The art is in designing and negotiating different contract elements for modules within the same program.

Because the battle against complexity can be won or lost at a program's inception, it is vital that

Exhibit 2

Poor vendor management contributes to considerably reduced productivity in one agency's IT programs.



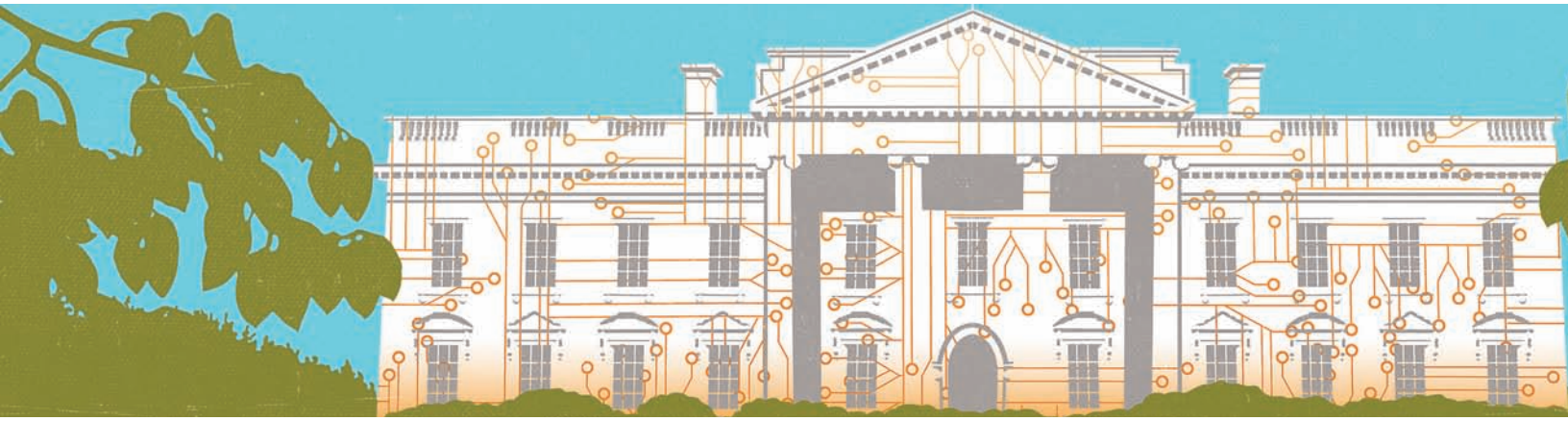
[1]Reports, interfaces, conversions, extensions.
[2]Full-time equivalent.

Source: Agency data; commercial ERP experts; McKinsey analysis

agencies maintain control of a program's scope and requirements. Unfortunately, agencies often outsource the scoping and requirements-gathering process to vendors, which typically have little incentive, perspective, or power to limit a project's scope and requirements. A clear scope, frugal requirements, and aligned sponsorship make it easier to more sharply define modules of functionality within a program: standard or semistandard use cases (such as basic data cleanup or encoding) can be negotiated at a fixed price, while more complex elements (such as interoperability tests) might be better suited to time-and-materials contracts.

We have too often heard government leaders say, "We keep funding IT, but we don't know what we're getting in return." Making the performance of IT transparent and easily understood is the first step in the journey toward higher yield per IT dollar. Agencies must then eliminate unnecessary IT complexity, putting into practice the gist of Albert Einstein's method, "Make things as simple as possible, but no simpler." Through greater transparency and reduced complexity, IT can better play a transformational role in the efficiency and effectiveness of every government agency.

Aamer Baig is a principal in McKinsey's Chicago office, **Stephen Kelly** is a director in the Philadelphia office, and **Chandru Krishnamurthy** is a director in the Atlanta office. Copyright © 2011 McKinsey & Company. All rights reserved.



'Getting stuff done': A conversation with America's first CIO

During his last few weeks in office, Vivek Kundra, the first-ever federal chief information officer of the United States, reflects on his tenure.

Nancy Killefer and Kreg Nichols

When President Obama appointed a federal chief information officer (CIO) in March 2009, he said that the nation's CIO would be responsible for ensuring "that we are using the spirit of American innovation and the power of technology to improve performance and lower the cost of government operations." The CIO would also "play a key role in making sure our government is running in the most secure, open, and efficient way possible." The individual he chose to occupy that role was Vivek Kundra, who at the time was the 34-year-old chief technology officer for the city of Washington, DC.

Kundra, who came to the United States in 1985 after having spent most of his childhood in Tanzania, has experience in state government—he had served as Virginia's assistant secretary of commerce and technology—as well as in the private sector. He had also been a technology adviser on President Obama's transition team. As federal CIO, among his first initiatives were Data.gov, a Web site that gives the public access to government-held data sets, and the IT Dashboard, an online tool that tracks the performance of federal IT programs. More recently, he published a 25-point plan for reforming federal IT management and a cloud-computing strategy for the US government.

In June, Kundra announced that he would be leaving his post for a joint fellowship at Harvard University, where he will be splitting his time between the Joan Shorenstein Center

on the Press, Politics and Public Policy and the Berkman Center for Internet & Society. In July, with just a few weeks left in his tenure as CIO, Kundra spoke with McKinsey's Nancy Killefer and Kreg Nichols in Washington, DC.

McKinsey on Government: *You stepped into a big new role with no prior experience in federal government. What were your thoughts and expectations coming into the job?*

Vivek Kundra: During the transition, everything was very exciting. I was fueled with all these ideas and dreams about remaking the federal government. And I remember walking into the office on my first day, seeing the technology in the White House, and feeling like I had gone back a decade in time. I thought, "This is the most powerful city in the most powerful country on the planet, and this is the technology we have access to?"

Looking back, what I think helped me the most was the fact that I was naïve—I didn't know how things were "supposed to work." Very shortly after I started, at my first Senate hearing, I was asked, "What are you going to do differently from previous administrations in managing the $80 billion IT budget?" I said I'd launch an IT dashboard—I'd put cost and schedule information about every major federal IT project online—and I would do it in 60 days. Everyone told me, "You're crazy! Nothing in the federal government gets done in 60 days. You're so naïve."

But I figured an IT dashboard was straightforward: we could get the smartest developers, leverage a vehicle at the General Services Administration, and just get it done. I blocked out from 7:00 p.m. to midnight every day for 60 days. Everybody was shocked that I would show up and bring dinner, and I would sit in a room with the developers and a whiteboard, and we'd work on it. During the day I met with people and got feedback—chief executive officers of major companies that had contracts with the federal government, members of Congress, open-government groups like the Sunlight Foundation—and at night I would do the development. And we launched the IT Dashboard in 60 days.

So I decided to continue being naïve, to push the envelope and focus on execution. I realized that's how I would make the biggest difference in federal government—not by issuing a policy memo or publishing a framework, but just by getting stuff done.

McKinsey on Government: *So you got a very early win.*

Vivek Kundra: It wasn't just an early win; it was a big win. Soon after the dashboard went live, agencies started killing IT projects themselves. I realized how powerful sheer transparency was. I took a picture of every CIO and put it right next to the projects they were responsible for.

McKinsey on Government: *How did the CIOs react to that?*

Vivek Kundra: Initially they were skeptical and not happy. Their view was, "We don't know if the data on the dashboard are accurate, we haven't really looked at it, we need more time," and so on. But as soon as they saw that the president cared, and that their cabinet secretaries and deputy secretaries cared, they got on the train. There were some who were resistant and continue to be resistant to this day, but then we started the TechStat accountability sessions,[1] which created enough of a pressure point that everybody had to participate. So I

[1] Launched in January 2010, TechStat accountability sessions are regular reviews of federal IT programs, conducted by the Office of Management and Budget (OMB) and agency leadership. According to the OMB, the sessions have enabled the government to turn around or terminate at-risk IT programs, leading to $3 billion in savings.

Accountability and transparency served as our platform for highlighting that IT was a problem worth solving

wouldn't say everybody was madly in love with the launch of this product, because it did create a lot of pain—but if someone is going to give you $80 billion, why wouldn't they hold you accountable? There was a culture of faceless accountability in federal IT, and I wanted to change that.

McKinsey on Government: *How did you get President Obama's buy-in?*

Vivek Kundra: The president recognized that IT was important. During the transition, he had formed the Technology, Innovation, and Government Reform team. Transitions have historically had teams focused on defense or the economy or health care—but this was the first time there was a team focusing on technology. On his first full day in office, the president issued a memorandum on open government and transparency, which are things he feels very strongly about.

Accountability and transparency served as our platform for highlighting that IT was a problem worthy of solving. Before that, IT was a sleepy little issue; senior people in the government didn't see IT as important. Why does IT have to be better than finance or human resources? Their view was that essentially it should be a race to the bottom. But my view was that we should race to the top. We should build one thing after another. We were very aggressive early on in making sure that, with each iteration, the IT Dashboard kept improving.

McKinsey on Government: *So every day you'd work from early morning until midnight. Looking back, would you have spent your time differently? Would you have slept more? Or do you think you could have used more support?*

Vivek Kundra: I've thought about that question a lot. Would it have helped if I had delegated more? But I knew coming into the job that I could make one of two decisions: I could either treat my job as a marathon—over the course of four years, or eight years if I were being presumptuous, spread things out slowly and have a sane life—or I could accept the fact that I would have no life and double down on everything. I chose the latter, because one lesson I'd learned working in government is that the beginning is where you can make the biggest mark. If I started strong and proved value in the first 45 days, I'd have the credibility to sit down with agencies and say, "This is our game plan; let's go execute it."

I also recognized that if I wasn't on the battleground, agencies would say, "Well, he's delegated it to some other person." It's not the same. My

personal presence was important. I spent a lot of time with people at the agencies—the career folks who have been around for a long time and who will carry this change forward. I also spent time with senators and a number of congressmen and their staff, and even with people who have left government—former senators, ex-CIOs, ex–program managers. I wanted to make sure I was getting the best ideas, no matter where they came from.

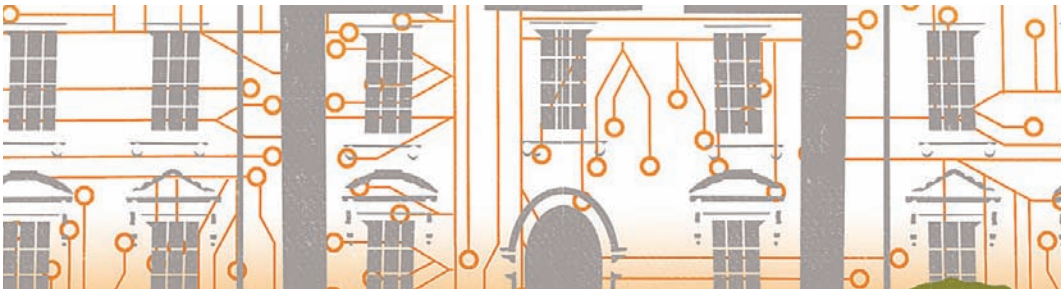
Vivek Kundra

McKinsey on Government: *What's the best idea you got from someone outside government?*

Vivek Kundra: There were so many. One is in IT procurement. The government procures things in two ways: the traditional procurement process and a grants process. I was looking for a third way, and I'd done some work for Washington, DC, on issuing challenges and prizes as a way to procure new IT. I met with some innovative people, including a group called TopCoder, which gets armies of developers to convene spontaneously and work on software challenges. For too long, we thought you could do that for Web applications but not major projects. I spent a lot of time thinking through this and talking to people, and I realized that it could work for multimillion-dollar projects. I worked with Congress to get special prize authority, and now every agency in the US government can spend up to $50 million on competitions and prizes. NASA and the Department of Defense have been using apps competitions; the next frontier is major projects. I think it's going to be one of the biggest game changers in government IT procurement.

McKinsey on Government: *IT procurement is one of the main topics in your 25-point plan for reforming federal IT management, which the White House released in December. It's not the first-ever plan for government IT reform. What makes your plan unique?*

Vivek Kundra: I would say three things make it unique. First, it has deadlines. It's not a theoretical framework or a report that sits in one of the countless metal cabinets you find throughout Washington. Second, its development was neither top-down nor bottom-up but a combination of both—we had a co-creation mentality. We brought in CIOs, chief financial officers, chief administrative officers, the White House, external experts. Third and most important, there's a sustained focus. At every CIO Council meeting it's on the agenda. I've got a team, and I took everything else off their plates—all we do is the 25-point plan. We have daily updates, I personally call people



when they miss deadlines, I escalate issues to the chief of staff and the Office of Management and Budget director as necessary. You could have a great 25-point plan, deadlines, and co-creation, but if people aren't relentlessly focusing on it, things won't happen.

McKinsey on Government: *In Washington, with the 24-hour news cycle, sustained focus seems extremely difficult to achieve. How have you kept your focus?*

Vivek Kundra: I've been ruthless when it comes to my calendar. From day one, I decided to focus on only four big things. The first is effectively managing the $80 billion budget, and in that category I would put the work that we've done on the IT Dashboard, the TechStat sessions, and the 25-point plan. The second is the efficiency and the effectiveness of federal IT, and on that front I went after data-center consolidation and the $20 billion shift to cloud computing. The third is cybersecurity. The only reason we were able to send model legislation to Congress—on everything from rationalizing privacy laws in 50 states on personally identifiable information to making sure that we have a four-star general focused on command-and-control infrastructure—was because we really went heads down on cybersecurity. The fourth is open, transparent, and participatory government. In that category are the launch of Data.gov and getting the legislation on challenges and prizes. So those are the four things, and I didn't take any meeting that didn't tie to one of the four. It's tempting—in the White House you can be like a kid in a candy store, people are always wanting you to fly out to some event and it all sounds fun—but I didn't want to be just flying all over the country giving speeches. I really wanted to get stuff done.

McKinsey on Government: *It's interesting that one of your priorities is cybersecurity and another is openness. Is there any tension between those two?*

Vivek Kundra: I think the tension between security and openness is overdramatized. The tension is really between privacy and openness. Take Medicare/Medicaid transactions. One of the things I pushed hard on was making government data accessible: for example, making transparent how much a knee replacement would cost in Washington versus Houston versus New York. Everyone's default position was, "We're not going to release any data." But the real question was at what level should you not release data? You could issue data at the state level but not at the Zip Code level because if you're in a rural part of a state, there might be only one person in a Zip Code that has that particular health condition. So these kinds of privacy problems require a lot of thought.

But on the security front, my experience has been that CIOs in agencies are themselves the number-one reason for cybersecurity incidents. They're the biggest villains because their default stance is to ban everything. And what do most users do? They use the banned tools anyway. There's shadow IT everywhere and therefore less security.

In the 1960s, the greatest innovation in IT was happening in government. In the 1980s, it was in corporate enterprise. Today all the action is in the consumer space, and because most CIOs are not willing to accept that, they are making IT less secure. Let me give you an example: I don't believe individuals should have to carry multiple devices, and I don't believe the federal government should be in the business of negotiating major contracts with telecommunications providers. When I say that, everybody is up in arms—"Vivek doesn't understand security!" But today when I travel, I don't fly United States of America Airlines and I don't rent a car from the United States of America Car Fleet. I book a flight, I rent a car, and the government reimburses me. In the same way, why aren't we letting people bring their own mobile devices or laptops and building all the security we need in the cloud? We would save billions of dollars if we did something that simple. Right now we spend all this money managing contracts, putting out bids, and provisioning and deprovisioning.

McKinsey on Government: *You clearly have many ideas about federal IT, but you're leaving your job. Do you think you can be a force for good from the outside?*

Vivek Kundra: I intend to be. I'm passionate about public service, and I care about these issues. Federal IT is not immune to the laws of physics, and the most fundamental law of physics is entropy—everything moves toward disorder unless you are constantly investing energy in maintaining order. How do we fight entropy? To me, the answer has to do with the way the government works with people outside government, because government cannot do everything itself. Today, however, the US government does a horrible job of engaging outside experts. This is going to be a long-term challenge: how do we make sure that in 20 years we're engaging the private sector, nongovernmental organizations, the universities, state and local governments, and even other countries that are doing amazing things?

McKinsey on Government: *Of all those external communities, which do you think is the most underleveraged or undervalued today?*

Vivek Kundra: I would say the private sector—particularly start-ups. There are small companies out there that may not have the funding to sit down with top government officials, but they're creating the future. How do you give them a point of entry? As part of the IT reform effort, I purposely spent a lot of time in Silicon Valley; I met with a lot of companies from Houston, Austin, and the technology corridors of Boston and New York City; and we've brought in start-ups to pitch to the Federal CIO Council. It's been amazing. CIOs' eyes open up, and they say things like, "I didn't know this technology existed—this is exactly the problem I'm trying to solve!" Suddenly they're fundamentally rethinking how they run their IT departments. They're realizing they don't have to spend hundreds of millions—they can have access to the latest thinking and cutting-edge technology for a fraction of the cost.

McKinsey on Government: *You're well aware that talent is a big issue in government. How optimistic are you that if you bring in these new ideas from the outside, there will be people on the inside who will be open to and capable of understanding and implementing them?*

Vivek Kundra: The great news is that we now have the government's first-ever technology fellows program. We're partnering with leading universities, and it's structural, so these are not just one-off fellowships. Right now we've got fellows working on IT projects at the National Archives and Records Administration and at the Patent and Trademark Office. It's going to be even more exciting going forward, because the federal government is attacking the most transformative set of issues—counterterrorism, intelligence, cybersecurity—and fellows will have the opportunity to work on these issues.

McKinsey on Government: *The US government is about to make what could be severe budget cuts. Do you think these cuts will speed change or stop change?*

Vivek Kundra: If budgets are cut significantly, of course there's going to be an impact on IT departments' ability to get things done, at least in the short term. But I believe it's also an opportunity for the secretaries and deputy secretaries to double down on technology so that they can do more with less. And it will be interesting to see how the private sector responds: the smartest companies are going to look at this opportunity and say, "How do we create value on day one?" Imagine a world with zero-dollar contracts, where vendors get paid for actually delivering something rather than for the promise of delivering something. That could potentially be one of the biggest transformations in government contracting and technology acquisition.

McKinsey on Government: *Thank you, Vivek. You've been very generous with your time, so just one more question: any final reflections on your tenure as US CIO?*

Vivek Kundra: When I look back at the last two-and-a-half years, I can't help but think about coming to the United States for the first time—it was 1985 and I was 11 years old, and I couldn't speak a word of English. I remember I went up to these four kids who looked like my friends back in Tanzania, and I started speaking to them in Swahili, and they looked at me like, "Who is this guy?" So I started speaking louder in Swahili, and the next thing you know they're beating me up because they thought I was making fun of them. I learned English by watching the TV show *Three's Company*.

Imagine a world with zero-dollar contracts, where vendors get paid for actually delivering something rather than for the promise of delivering something

I look back at that time and then I fast-forward to my life now, and I feel I've been very fortunate. I've served at every level of government—from Arlington County to the state of Virginia to the city of Washington, DC, and now the United States of America. I've been able to give a little bit back to this country that gave me so much. When I look at this job specifically, I'm humbled that I had the opportunity to work for an amazing president, a president who *gets* technology—it made my job a lot easier. The president actually deeply believes in this; it's not a minor issue for him. I have nothing but great stories from this experience. As I move on, my biggest fear is that I'll never have another job as exciting as this one.

Nancy Killefer is a director in McKinsey's Washington, DC, office. **Kreg Nichols** is a principal in the Atlanta office.
Copyright © 2011 McKinsey & Company. All rights reserved.

Capturing value through IT consolidation and shared services

Agencies should look beyond data-center consolidation for opportunities to streamline IT assets. By pursuing a range of initiatives, agencies can boost effectiveness while cutting IT costs by up to 20 percent—without reducing head count.

Ankur Ghia

Many public-sector chief information officers (CIOs) intuitively know that they could be getting significantly more bang for their IT buck. They are aware that their organizations own underutilized IT assets: servers with extra capacity, dozens of data centers that are expensive to operate and maintain, and redundant and subscale IT shops. In most cases, government agencies accumulated these assets over decades; as government expanded, agencies built more IT infrastructure, but as technology evolved, agencies did not consistently "clean house" and streamline their asset base.

In general, government CIOs recognize the untapped savings in IT consolidation and, ultimately, in adopting a shared-services model for IT. But even in countries where policy makers have mandated such efforts—the United States, for instance, where the government has called for the closure of 800 of its 2,000-plus data centers by 2015—many agencies are unsure how best to proceed, given that their experience has been in adding capacity to meet individual program needs rather than reducing IT assets. And those agencies that have already embarked on consolidation programs seldom look beyond data centers, thus missing out on other opportunities to reduce IT costs while boosting effectiveness.

Data-center consolidation is only one way of capturing value. In fact, in our recent work with several civilian and defense agencies, we have

uncovered opportunities to reduce overall IT spend by as much as 20 percent through various consolidation and shared-services initiatives. Furthermore, agencies can capture the benefits of many of these initiatives without reducing head count or launching a disruptive reorganization. In this article, we identify the main levers for capturing value from IT consolidation, and we summarize the organizational and process-related factors that have helped agencies successfully implement an IT consolidation program or, in some cases, an IT shared-services model.

Where the opportunities lie

Opportunities for IT consolidation—whether in IT infrastructure, end-user support, application development and maintenance (ADM), or management and administration—abound in public-sector organizations. A typical agency can take advantage of 20 to 30 consolidation opportunities, each of which falls into one of the following categories: better utilizing capacity, pooling IT staff, sharing best practices, consolidating procurement, and managing demand through central governance. Some of these initiatives can be implemented fairly quickly, while others require dedicated, longer-term efforts to restructure the way IT services are delivered.

Utilizing spare capacity to eliminate waste.

Even an agency with only a single data center is likely to own servers with average utilization below 5 percent and server racks with spare capacity. In our experience, most public-sector servers within data centers are only about 20 to 30 percent utilized on average per day, compared with 70 to 80 percent in best-practice companies. A European government, in outlining a number of options for IT consolidation, found that consolidating servers and data centers would yield annual savings of 20 to 30 percent on a baseline of more than €500 million.

Some agencies have begun to consolidate their data centers using a two-tier approach: they have started to "virtualize" their server environment—thus reducing the number of physical servers they own—and have then consolidated the remaining physical servers into fewer data centers. (For a case example, see "A city consolidates its data centers," p. 24.)

Data centers represent clear, short-term opportunities to capture value by better using existing resources and forgoing future IT purchases. But agencies should not stop at data centers; they can similarly rationalize and consolidate other technology assets—call centers, for instance, as well as IT networks and domains.

Pooling IT staff to capture scale advantages.

Particularly in an IT environment that consists of small, subscale IT shops maintained by individual offices and bureaus, pooling IT support staff can be a significant lever. Because most IT shops are staffed to handle peak workloads, employees are underutilized during most of the year. Pooling typically results in faster and better service. It can also reduce dependency on contract labor, as specialized skills are more likely to be found in a larger, pooled support organization than in a subscale IT shop.

One public-sector agency had traditionally operated its data center with a "box owning" mentality—that is, systems administrators were dedicated to particular applications regardless of how much or how little work those applications needed. As a result, administrators dedicated to highly demanding systems were often overloaded, while those in charge of less demanding systems were busy only

once every two weeks. Pooling these systems administrators allowed the agency to normalize the workload and free up 30 to 40 percent labor capacity for additional work. Pooling requires thoughtful preparation, collaboration with employees, constant and transparent communication, and recognition of the unique skill sets of the employees being pooled.

Sharing best practices across organizational silos. An additional benefit of pooling is that it lends itself to the sharing of knowledge and best practices across organizations, which can drastically improve service quality and efficiency. For example, in assessing several agencies within the same government department, we found a tenfold variation in the productivity of call-center agents. Site visits and interviews with agency staff revealed that the variation derived in part from some agencies' use of special remote-resolution tools (for example, remote takeover of user PCs) and call-center-agent scripts (such as a basic checklist of items to cover during a call) that allowed agents to take more calls, resolve issues faster, and prevent incidents from recurring. When all agents in the department began adopting those practices, some of which required little or no IT investment, the agents who had previously been low performers improved their productivity.

Agencies can use a range of tools to gather and disseminate best practices. Some agencies use a central online knowledge repository to collect knowledge assets and ensure that they are available across the organization. Others have implemented peer-to-peer structures for disseminating lessons learned in the work environment—for example, brown-bag lunches for knowledge sharing or "shadow" programs in which employees learn by observing other employees as they perform their day-to-day tasks.

Using common pricing practices and consolidating procurement. We have observed sizable differences in the prices that governments pay for hardware and software. In the United States, despite detailed contracting and procurement schedules and guidelines laid out by the General Services Administration, one agency might pay twice as much as another agency for similar computers and mobile devices. Pricing of services is even more difficult to standardize; not surprisingly, wide variation exists in that area as well.

These pricing variations exist for several reasons. One is that subscale agencies tend to benefit from fewer discounts than do larger agencies with greater buying power. Also, agencies in a single department may be using different vendors for the same or similar commodity IT purchases, thus limiting the department's buying power. Another reason for price disparities is that some agencies operate on a staggered buying schedule—they negotiate prices for piecemeal purchases rather than large multiyear contracts. Finally, there is little product standardization in the federal government, and customized orders are always more expensive.

Centralized procurement would address many of these issues. Agencies that centralize procurement plan and schedule periodic spending (such as PC upgrades) in advance, buy products in bulk, and distribute them to users in a timely manner. They evaluate and, where possible, aggregate unplanned purchases and procure them through a competitive process. At such agencies, most planned and unplanned purchases are

standardized and often available through an IT product/service catalog developed by the central IT function. Undoubtedly, some agencies will occasionally need to make specialized IT purchases (an agency might require satellite phones, for example), but these will be the exception rather than the rule. Agencies should define standardized processes and escalation mechanisms for exceptions as well.

Managing demand through central governance. Demand management is one of the most important levers for capturing IT consolidation savings. A central governance body can eliminate unnecessary IT expenditures or aggregate similar IT purchases into a standardized product or service. Although many agencies have groups (often called investment-review boards or change-control boards) that are meant to serve such a purpose, challenges remain. Such groups are often decentralized, which means they have no cross-agency visibility; their power may be limited, in that they serve a tracking function but have little decision-making authority; or their scope may be quite narrow (for example, they may oversee only certain small pockets of IT). In best-in-class companies, a strong central governance body owns the IT product/service catalog, manages IT requirements and demand, and coordinates procurement activities. Often, this central body also has budget authority over IT spending and maintains continuous engagement with internal customers.

A European government recently moved toward best practice by appointing a national CIO charged with developing a strategic view on IT for the national government and aligning ministry CIOs on key IT standards and objectives. Although ministry CIOs do not report directly to the new national CIO, he has the authority to review and influence the ministries' IT road maps and large projects. He is also in charge of nationally deployed transformation programs, including data-center consolidation and the creation of a single IT network for all government ministries.

Establishing a central IT governance structure is a long-term effort that requires full engagement from stakeholders and senior leaders both within the IT function and across government; a detailed understanding of each agency's IT requirements is also necessary. The first step in establishing such a structure is a thorough analysis of user needs, followed by more tactical steps such as the development of IT product/service catalogs, the design of charge-back mechanisms, and the creation of an end-state governance map that clearly defines roles and responsibilities.

Success factors in implementation

The exhibit shows how an agency might prioritize its consolidation initiatives, taking into account each initiative's savings potential and implementation timeline. In our work with public-sector institutions worldwide, we have found that IT consolidation is not easy—but it is achievable. Success often depends on adhering to four core principles.

Adopt a customer-service mind-set. Every user of IT services, regardless of which unit or organization he or she belongs to, should be viewed as an equal customer. Often, a department creates an IT shared service simply by merging smaller IT functions into the largest agency's IT organization. In these cases, leadership must ensure that the needs and requirements of all agencies are understood and

Exhibit

Initiatives can be prioritized based on timing and potential savings.

ILLUSTRATIVE

Utilizing spare capacity

- **a** Consolidate data-center hardware
- **b** Improve hardware utilization
- **c** Improve utilization of data-center square footage
- **d** Consolidate and rationalize networks and domains
- **e** Consolidate call centers

Pooling IT staff

- **f** Pool, streamline, and improve the skills of data-center staff
- **g** Increase call-center productivity by pooling staff
- **h** Pool end-user support and improve coverage

Sharing best practices

- **i** Use online tools and effective IVR[1] to reduce call volumes
- **j** Move tickets upstream from on-site support to call centers
- **k** Use scripts and other tools to improve resolution rate
- **l** Use lean techniques to improve operational efficiencies

Using common pricing and procurement

- **m** Move data centers to lowest-cost locations
- **n** Move to best pricing for desktops and laptops
- **o** Standardize contractor rates
- **p** Reduce contractor overhead and support spending

Managing demand through central governance

- **q** Reduce number of devices per employee
- **r** Improve license procurement and management
- **s** Increase device life span
- **t** Manage demand and rationalize scope of programs
- **u** Streamline overhead and support roles

[1]Interactive voice response.

that standard service-level agreements are in place to measure the quality of IT delivery. When a European government recently undertook a consolidation effort, it made sure to select the new central IT organization's leaders from among several agencies—including the smaller agencies—so that smaller agencies would not feel as though they were victims of a hostile takeover. The leaders of the central organization took pains to assure all agencies that their needs would be heard.

Create a road map and pilot each opportunity. IT consolidation is often a multiyear journey. Many constraints—contract structures, lease agreements, and management focus, to name just a few—can limit the speed of implementation. Successful agencies thus create a portfolio of both short- and long-term initiatives that spans multiple years. They pilot each initiative to validate opportunities and refine the action plan, and only then do they design a detailed blueprint for rollout. For example, during an operational-improvement pilot in a public agency, the agency's leaders realized that a component of the action plan they had previously designed was unworkable in a real-world scenario: the plan called for the relocation of a small number of employees whose labor contracts stipulated that they remain at their current location. The agency leaders collaborated with frontline IT staff to modify the design: instead of relocating the employees, they set up virtual work environments for those employees. After only a few weeks of testing and refining, agency leaders and staff were able to roll out the new operating model.

Foster 'champions' within the agencies. Cultural challenges are often the most difficult to overcome. Employees can be set in their ways, believing that their environment is unique and that consolidation could disrupt the agency's mission. To combat this mind-set, leaders should engage key stakeholders within each agency early in the process and enlist their help to drive the initiatives. Having stakeholders lead initiatives can help ensure implementation and adoption. One agency currently undergoing a large-scale IT transformation has created a steering committee with eight members from across the organization. Most of these members do not have an IT background but sit in functions (such as human resources, communications, and finance) that will play critical roles in moving the transformation effort forward.

Work collaboratively with unions. Labor unions are sometimes neglected during IT consolidation efforts. If leaders foresee any impact on the workforce, the union should be involved early and often. Sharing the goals of the effort and maintaining a partnership with the union (for example, by having a union representative on the steering committee) can go a long way to avoid lengthy bargaining or negotiations later in the journey. In a recent data-center-productivity effort for a civilian agency, the agency's leaders worked closely with the union to implement a new operating model within weeks of developing a design. Agency leaders nurtured the relationship by regularly communicating with union leaders and ensuring that their feedback was incorporated in the final plan.

• • •

Consolidating IT functions and establishing shared services is a long-term commitment: a marathon, not a sprint. Quick wins are important to gain momentum and to capture some short-term savings, but lasting change takes a dedicated, sustained effort within and across government organizations.

Ankur Ghia is an associate principal in McKinsey's Washington, DC, office.
Copyright © 2011 McKinsey & Company. All rights reserved.

A city consolidates its data centers

The experience of one US city provides lessons on how public-sector organizations can design and execute a data-center consolidation.

James Kaplan, Rishi Roy, and Ryan Taylor

Even prior to the recent economic downturn, a trend toward data-center consolidation was becoming evident among large government entities. In their quest for cost-savings opportunities, the state governments of Texas, Oregon, Michigan, and California—as well as many federal agencies—have in the past few years embarked on efforts to consolidate their data centers.

A large US city—looking to stretch its IT budget, increase efficiency, and improve the quality of its services—is in the second year of a five-year initiative to consolidate more than 50 data-center facilities into only 2 locations. Technology change programs of this scale are inherently complicated in the public sector, but the city's experience so far provides lessons on how public-sector organizations can overcome the challenges that can hinder data-center consolidation.

The starting point

To get a clear picture of its IT landscape, the city commissioned a review of the IT environments of each of its agencies. Among other findings, the review revealed that the city owned several thousand servers—many of which had aged well beyond the typical four- to six-year refresh cycle—scattered across more than 50 data centers and data closets. Assets

Kate Miller

were underutilized, with servers often dedicated to single applications. Due to their age and subscale capacity, many of the data-center facilities were unreliable and inefficient. Support services were highly fragmented across city agencies and inconsistent in quality; many agencies lacked even technical service-desk functionality.

This situation was partially a result of the city's project-by-project funding and budgeting processes. Most agencies built their own data centers, bought their own servers, and hired their own IT staff, with no transparency into other city agencies' IT assets. What's more, the city had paid high prices for IT infrastructure: project-based purchases meant that the city realized little purchasing leverage.

The city administration, which had intuited a significant opportunity to improve IT effectiveness and efficiency, now had a supporting fact base and a compelling case for change.

The future-state model

The city decided to adopt a shared-services model for IT. City agencies would transfer most of their IT assets and IT infrastructure staff, as well as a portion of their budgets, to the city government's central IT function. The city would provide a highly standardized set of infrastructure services, hosted in two modern data centers designed to meet industry standards for reliability and security.

Before starting the physical migration, the city developed its facilities strategy (including site-selection criteria and technical design), created a catalog of standard services that would be available to city agencies at specified costs, and defined the target technical architecture. The central IT function's support of IT services would be modeled on ITIL,[1] a widely accepted best-practice framework for IT services management.

The city established a program-management office (PMO) to drive implementation. The PMO oversaw the assessment of each agency's infrastructure footprint (assets, labor, and spending), as well as the creation of detailed migration plans and a financial model. In addition, the PMO created a performance dashboard to give each agency full transparency into the city's IT infrastructure, services, and service-level agreements both before and after the transition. The PMO continues to coordinate the efforts of all parties involved and to monitor program risks and issues.

The lessons

City officials knew that consolidation would not be easy. And the public-sector setting presents a number of unique challenges for designing and executing a data-center consolidation, including the following:

Developing an accurate baseline of infrastructure spend. As noted, this city government was typical of public-sector organizations in that its IT spending was decentralized across dozens of groups. In addition, due to complex funding models, most infrastructure investments were embedded in project budgets, with little to no itemization of the IT components. To create an IT spending baseline, the city had to ask each agency to come up with a zero-based estimate of what it spent, relying primarily on a physical-asset count and a review of recent purchase orders for unit-cost estimates.

[1] Information Technology Infrastructure Library.

To ensure transparency into IT spending, the city's budget office established new governance processes that require all IT infrastructure-related funding to be approved by the central organization.

Capturing value from the consolidation. In the private sector, companies can capture short-term labor savings by improving efficiency and reducing head count. Such actions are not always feasible in the public sector. Furthermore, public-sector funds are allocated on an agency-by-agency basis, and some agencies are loath to give even part of their budgets to a central organization. These two challenges make it more difficult for public-sector organizations to capture value from consolidation. The city addressed the first challenge by framing the consolidation program with respect to long-term cost avoidance: there would be no layoffs, but neither would there be any new hires. Instead, agencies would have to rely on their existing IT staff to meet their growing IT needs. As for the second challenge, the mayor and the budget office issued a top-down mandate requiring agencies to transfer the appropriate funding to the central organization. To make the transfers as smooth and uncontroversial as possible, the city charged each agency an amount that covered only the cost of the resources the agency used (for example, an agency using five servers would transfer funds equal to the cost of those five servers).

Creating a credible central organization. Many agencies did not, at first, trust the central IT organization to provide infrastructure services with the required reliability and responsiveness. In fact, some larger agencies had IT operations that were at least as efficient and innovative as the central group; those agencies were wary of ceding control of their IT infrastructure and assets, and IT employees at those agencies were hesitant about joining the central organization. The central IT function took a number of steps to build credibility: it recruited top IT talent from the private sector, created a cross-agency governance council that included influential people in the agency CIO community, and courted one of the city's largest and best-run agencies to support the consolidation and participate in a high-profile pilot. That agency's leaders publicly championed the program and jointly developed solutions with the central IT organization.

Managing a wide range of stakeholders. In a public-sector IT consolidation program, decision makers are necessarily accountable to many stakeholders—including elected officials, labor unions, local companies, and city residents. Unless properly managed, any one of these stakeholder groups can hinder progress. To ensure stakeholder alignment, public-sector organizations should carefully document and communicate the rationale for all major decisions. In this case, for example, political

To ensure stakeholder alignment, public-sector organizations should carefully document and communicate the rationale for all major decisions

considerations might have resulted in a suboptimal choice for one of the planned data centers. The jurisdiction's project team thus invested substantial time laying out a robust set of decision criteria (for example, resiliency and disaster-recovery implications) and articulating how each option performed relative to these criteria. This rigorous documentation was essential to helping all stakeholders agree on the way forward.

Among the data-center consolidation program's expected benefits are run-rate cost savings of more than 15 percent, attributable in large part to improved asset utilization, increased energy efficiency, lower vendor rates, and higher labor productivity. In the first year, the program saved $5 million, and in five years, savings are projected to reach $40 million. In addition, city agencies will benefit from better and more consistent services, as well as access to a greater breadth of IT capabilities. The city has already had visible successes—for example, the transition of several prominent agencies and the offering of new IT services (such as disaster-recovery services, which were previously inaccessible to small agencies).

• • •

Although these early wins should help garner continued support, city leadership will need to demonstrate a high level of commitment to maintain the program's momentum. The city must address a number of cultural and behavioral challenges—among them, the lack of incentive among the front line to improve performance, individual agencies' reluctance to relinquish control, and constraints stemming from civil-service rules and union contracts. Formal mechanisms for engaging and motivating the front line will be particularly important if implementation is to succeed; the frontline staff, after all, will have to execute—and live with—the changes. Addressing these challenges will enable the city to realize the full value of its data-center consolidation program.

James Kaplan is a principal in McKinsey's Business Technology Office, where **Rishi Roy** is a consultant and **Ryan Taylor** is an associate principal. Copyright © 2011 McKinsey & Company. All rights reserved.

Seven imperatives for success in IT megaprojects

To implement public-sector IT megaprojects successfully, leaders must pay close attention to process, people, and governance. We discuss seven imperatives that, although not technically difficult, require dramatic changes in mind-sets and ways of working.

Kreg Nichols, Shantnu Sharma, and Richard Spires

Rapid advancements in information technology have benefited governments around the world, enabling them to provide new services and become more efficient. But as IT programs become larger and more complex, they also bring considerable and rising risk. In a recent study, McKinsey and Oxford University showed that one in six IT change initiatives overruns its budget by 200 percent and takes about 70 percent longer to implement than originally planned.[1]

While many IT program failures in the private sector remain largely hidden from view, public-sector failures can receive national or worldwide attention. In an effort to understand what causes such failures and what brings success, we interviewed more than 50 IT and procurement leaders in both the public and private sector and analyzed a variety of IT programs across the performance spectrum. We summarize our findings in this article.

Why programs fail

Government IT programs run into trouble for some of the same reasons that private-sector IT programs do. Other challenges—a complex budget process, for instance—are unique to the public sector. We found that the primary contributors to failure in large IT government programs are the following:

[1] Alexander Budzier and Bent Flyvbjerg, "Why your IT project may be riskier than you think," *Harvard Business Review*, September 2011.

Multiyear time frames. Government agencies typically execute large-scale IT programs in multiyear cycles—an approach that artificially increases the complexity of programs and leads to higher failure rates. Sometimes cycles are unnecessarily long because the team seeks to build everything—including infrastructure—from scratch instead of reusing existing infrastructure. The problem can worsen when teams try to prevent failure by assiduously following a traditional approach, even in the face of continued missed deadlines and customer disappointments. To complicate matters, the pace of technological change continues to accelerate. Ever-shorter product life cycles combine with higher-than-needed program complexity to further increase program risk and the probability of failure. Once these multiyear IT programs are finally in place, they end up delivering functionality on outdated technology that often does not meet true business needs.

A very broad requirements scope. Best-practice IT program management calls for limiting the requirements-gathering cycle to a defined, upfront phase during which program leaders prioritize high-level requirements and decide what the program can deliver based on timelines, resources, and business needs. In the public sector, however, the IT funding process calls for very specific requirements up front instead of later in the program life cycle. Furthermore, program leaders often accommodate the requests of the greatest number of stakeholders. The many additional requirements and interfaces increase complexity exponentially, resulting in significant delays and cost overruns. Due to weak governance, new requirements are added even during program execution—increasing complexity and causing further delay.

Complex budgeting and funding processes. Large-scale public IT programs suffer from protracted funding cycles, budget uncertainties, and other challenges not often found in the private sector. With regard to funding approval, IT leaders must often articulate program budget requests and technology needs years in advance—an upfront time lag that contributes to technology obsolescence. Also, teams often compensate for inefficiencies in the budget process by front-loading their budget requests. When a program manager is projecting budgets five to seven years out, the budget requests are almost always inaccurate. Once the program has the money, other issues arise. Funds are typically appropriated only for a given fiscal year. Teams have limited ability to move portions of current-year funding to the next year or to reallocate money among programs in the same portfolio—even when changes in the technology landscape or in business needs require a reallocation.

Limited IT acquisition skills. Nearly all IT programs require procurement of hardware, software, services, or a combination of these. Agencies therefore need a firm understanding of acquisition best practices, federal acquisition rules, and IT. Federal contracting officers are invariably experts in the first two but often lack IT expertise, thus creating a communications mismatch—there is no easy way to translate a program's technical requirements into the procurement team's non-IT language. This mismatch extends the program timeline and, at worst, results in suboptimal acquisition, as the procurement team is typically not engaged early enough to be able to use creative contract vehicles (such as prototypes or requests for information) to help meet program needs. It also creates an opportunity for vendors to exploit

Many large IT programs run into difficulty because stakeholders are not fully aligned on the desired outcomes or the approaches to meet those outcomes

the contracting team's lack of IT expertise to their advantage. In cases in which acquisition personnel do have IT expertise, they are not required to dedicate their time exclusively to IT acquisition. The resulting multitasking on IT and non-IT acquisition can delay program timelines.

Lack of expertise in program management. Successful execution of large-scale IT programs is contingent upon the assignment of an experienced and qualified program manager. However, there is a shortage of qualified program-management personnel in government. Often, an individual is asked to take on the role of program manager based on capabilities shown in another role, such as mission operations. While such capabilities are valuable, those individuals lack the critical cross-domain expertise—a broad understanding of IT, procurement, and the mission or business function—to deliver a complex IT program. Furthermore, since there is no formal federal career path for IT program managers, time spent in program management may not result in career advancement, giving talented individuals little incentive to pursue program-management roles. Exacerbating the situation is the rapidly evolving IT landscape; each arm of the federal government tries to identify technology trends and emerging best practices on its own. As a result, there is significant variance across the government and among program managers as to what constitutes a best practice and at what pace it should be implemented. Vendors sometimes use this disconnect to their advantage in contracting.

Weak governance. Every government IT program has a broad set of stakeholders, including agency leaders, business-process owners, and the IT, acquisition, finance, security, and legal functions. Many large IT programs run into difficulty because stakeholders are not fully aligned on the desired outcomes or the approaches to meet those outcomes. Furthermore, there is typically no well-defined set of accountabilities and decision rights, and no disciplined approach for gathering and considering stakeholder input and thinking through the implications. Program managers sometimes receive conflicting direction from multiple oversight organizations; stakeholders sometimes make decisions outside the program that nonetheless can have a material impact on the program's execution.

Best practices

We found broad consensus among IT leaders on best practices for large-scale IT programs. Leaders readily admit that many of the practices are not technically difficult to implement but require dramatic changes in employees' mindsets and ways of working. Each of the following imperatives addresses one or more of the pitfalls discussed above. These imperatives fall into three broad categories: the first two are process oriented, the next two focus on people, and the final three deal with governance.

Leverage incremental or agile development

To show business value—and in light of ever-shortening technology life cycles—IT programs must deliver functionality within months instead of with a "big bang" at the end of a multiyear development cycle. Best-practice organizations schedule releases in shorter but well-defined time frames—at least every 6 to 12 months. Each release meets a set of high-level requirements that are later refined based on constant feedback from end users and other stakeholders. There is a hard time limit (say, 3 months) for the creation of detailed specifications, after which new requirements are pushed out into future releases. The staff moves seamlessly from one release to the next: the requirements team, for instance, starts gathering requirements for the upcoming release while the developers work on the current release. A significant benefit of this approach is that the requirements team can obtain detailed feedback from people who are using the system in a production environment. Such feedback can aid both in improving the usability of the system's existing functionality and in providing requirements and design guidelines for the creation of new functionality. This type of approach is what allowed the US Department of Health and Human Services to launch HealthCare.gov, a widely praised consumer-facing Web site, in 90 days.

Incremental development reduces the overall workload but increases the required effort for certain functions and changes the type of work for others. Program managers, for example, must manage multiple pieces and the dependencies among them. Procurement staff must provide flexible contract vehicles that allow for changes as the requirements for new releases are defined. They must let no more than a few months pass between receiving funding and awarding contracts. And these contracts must specify well-thought-out business objectives, a vision of the future-state IT architecture, guiding principles for agile design and development, and a sourcing plan for the initial phase.

Granted, there may be programs for which architectural limitations and legacy considerations rule out incremental development as an option—but parts of the approach (for example, locking down a release and setting hard deadlines for accepting new requirements) could still be useful for injecting discipline into the process.

Separate application development from infrastructure

Another best practice for large-scale IT programs is to separate application development from the underlying IT infrastructure. To simplify operations, achieve efficiencies, and promote the reuse of existing services, leading IT organizations are driving infrastructure standardization, mandating that new IT programs build mission or business functionality on well-defined and separately provided infrastructure where possible.

The implications for schedule and costs are considerable. It is an opportunity not only to make the most of investments by using IT infrastructure across all applications but also to improve end-to-end project timing, since applications can be hosted on the existing infrastructure footprint instead of on a new infrastructure that would have to be built from scratch. Another advantage is better capacity management, since infrastructure is built for aggregate demand levels.

Build program-management capabilities

Managing IT releases every 6 to 12 months requires a cadre of strong program managers supported by competent project managers. To attract and retain the best program managers, government agencies must develop a career track for these professionals and allow them to move easily within the agency and across government institutions. Agencies should, for instance, take full advantage of the Intergovernmental Personnel Act Mobility Program, which allows federal government employees to rotate through state and local governments, colleges and universities, federally funded research centers, and other eligible organizations.

Some agencies already recognize the importance of program-management talent. The Department of Veterans Affairs (VA) and the Department of Defense (DOD) both offer robust training in project- and program-management disciplines, along with on-the-job rotational assignments and mentorship programs for less experienced program managers.

Best-practice organizations support program managers with state-of-the-art tools and knowledge-management systems. Some agencies have created online portals, specifically for program managers, that serve as knowledge repositories (for best practices, process descriptions, templates, and tools) and personnel directories (for example, to help program managers identify and contact others with relevant experience). Both the Internal Revenue Service and the Department of Homeland Security have established formal centers of excellence to harvest best practices and offer expertise in areas as diverse as systems engineering, requirements management, IT security, and accessibility.

Have specialists do all IT procurement

Best-practice organizations hire and train IT acquisition specialists. In the government, this may require the creation of a distinct occupational series specific to IT acquisition, as well as pay and career-advancement paths competitive with those in the private sector. Another best practice is providing cross-functional training and on-the-job experience for IT acquisition specialists—for example, by embedding them in program teams, thus helping them gain the knowledge necessary to better translate business and technical requirements into effective procurement.

To attract and retain the best program managers, agencies must develop a career track for these professionals

Of course, not all agencies have the scale to warrant a separate IT procurement group. Smaller agencies—as well as larger agencies seeking an alternative to in-house IT procurement—can still have access to specialists through shared-service organizations. For example, both the Bureau of the Public Debt and the VA have specialized groups that charge fees for IT acquisition services.

Some agencies have had success in attracting and retaining talent by casting a wider net, building up IT procurement staff in geographic areas with considerable talent pools but less competition among employers. Instead of hiring in the Washington, DC, area, for instance, some agencies have hired in New Jersey, Texas, Florida, or college towns in other states.

Best-practice organizations also strengthen the IT acquisition capabilities of non-acquisition staff. Some use classroom training, encouraging managers—whether they work in IT acquisition or in other areas—to take IT courses such as those offered at the General Services Administration's Federal Acquisition Institute or the DOD's Acquisition University.

Establish an integrated program team

To help align stakeholders and ensure success from the start of a large IT program, leading companies establish multidisciplinary integrated program teams (IPTs) consisting of business-process owners, IT managers, technical personnel, acquisition personnel, and finance personnel, as well as representatives from the HR and legal functions as needed. Key members of the IPT—including, importantly, the program manager—are dedicated to the program and collocated during its most critical stages, and they remain in place throughout the design, development, and implementation phases of a program's life cycle.

IPTs are highly beneficial to government agencies as well. Senior agency executives should approve the composition of the IPT and reinforce its accountability. For critical or very large programs, it may make sense to get the deputy secretary or the senior-most governance body of the department to approve the IPT's composition.

IPT members should be held accountable for meeting the goals of their functional units as well as of the overall program. Contract officers, for example, may tend to focus on preventing protests and lawsuits, which could lead them to make overly conservative decisions that slow down a program's progress. IPTs should therefore develop performance metrics—for the program as well as for individuals—that strike the right balance of speed, effectiveness, and compliance.

Exhibit

Program- and portfolio-level governance roles should be clearly delineated.

Responsibilities of the governance boards

Function	Program level These governance boards provide guidance, decision making, and oversight of one or more programs	Portfolio and enterprise level These governance boards manage investment decisions, strategy, and operations of a collection of related programs
Define strategy	• Align under portfolio guidance • Approve key program-planning documents	• Determine needs, priorities, strategies, and initiatives
Evaluate investments	• Monitor program costs/benefits • Ensure the program has the right leadership and expertise • Tailor life-cycle governance	• Authorize and oversee portfolio • Designate program governance and stakeholder participation
Make decisions	• Make decisions on milestone transitions and significant changes to scope	• Make critical program decisions that escalate from program governance
Monitor performance	• Monitor overall program health • Escalate issues outside cost/schedule variance thresholds	• Set portfolio metrics and targets • Monitor and report continuously • Integrate with planning and budgeting processes
Manage risks	• Monitor program risks and support risk mitigation • Escalate issues above risk tolerance	• Establish risk-management framework and criteria

Clarify decision rights and accountability for investments

To better align a program's stakeholders, agencies should establish distinct program-level and portfolio-level governance (exhibit). The program-level governance board should comprise executives from stakeholder organizations—including the business owner, IT, procurement, and finance—thus promoting a partnership model and ensuring that no single organization dominates.

Teams should apply best practices of program-manager engagement to ensure effective execution of programs and projects. There should be a single reporting chain, with clear escalation mechanisms, from the program manager to the program-level governance board and then to the portfolio-level governance board. The program manager should also have frequent meetings with agency executives—such as the chief information officer (CIO) or the business owner—to report progress, raise red flags, and engage in collaborative problem solving. Leaders should keep in mind that such meetings will be effective only if the agency establishes cultural norms that encourage transparency. For example, if the program manager delivers bad news, agency leaders should avoid shooting the messenger.

The program manager should be held accountable for establishing the overall program objective and aligning the goals of each stakeholder group. To ensure business, IT, and all other stakeholders share responsibility, the program governance board should sign off on each initiative and milestone review. In most IT programs, achieving alignment should not be a one-time event that occurs at the beginning of a program; rather, it should be an ongoing process throughout the program's life cycle.

Increase external outreach to ensure up-to-date organizational knowledge

To navigate the ever-changing IT market, a government needs mechanisms for collecting and disseminating technology knowledge and trends, and for allowing personnel to engage with colleagues and draw on external expertise from the private sector and academia. Currently, the Federal CIO Council is establishing a best-practices collaboration portal, both to serve as a repository of best-practice examples and artifacts and to bring IT practitioners together to exchange ideas and lessons learned, as well as to provide help to programs independent of agency boundaries. Examples of potential approaches to engage external expertise include fellowship opportunities for private-sector experts, regular "office hours" led by CIOs from the private sector, coaching programs that link private-sector CIOs to government executives, and regular "industry days" on timely IT topics.

• • •

Each of the best practices we have described is useful on its own, and each requires a significant investment of time, effort, and management capital. Organizations should pilot these practices within a few business units and then create an enterprise-wide rollout plan. Many agencies, however, become complacent after they have implemented only a subset of the imperatives or partially implemented all of them. Such agencies do not achieve all of the impact these practices can offer and fail to maximize the return on their investment dollars. Only by acting on all seven imperatives can agencies assure success in managing large-scale IT programs.

Kreg Nichols is a principal in McKinsey's Atlanta office, and **Shantnu Sharma** is a consultant in the Boston office. **Richard Spires** is CIO of the US Department of Homeland Security and vice chairman of the Federal CIO Council.

Transforming IT:
A German success story

A once-underperforming IT function has become one of Europe's leading public-sector IT providers—due in large part to the leadership of Klaus Vitt, chief information officer of the German Federal Employment Agency. In this interview, Vitt reflects on the challenges of IT transformation and how to do it right.

Sebastian Muschter and Katrin Suder

Effecting change in large organizations is notoriously difficult—particularly in the public sector, where entrenched employees, complex procedures, and disparate stakeholder agendas constrain ambitious change efforts. But the challenges are surmountable, as shown by recent transformations in certain agencies. The German Federal Employment Agency (Bundesagentur für Arbeit, or BA), for one, is on a multiyear journey to transform its IT function, and its efforts have already yielded dramatic improvements in performance, flexibility, and reliability. Benchmarking of European public-sector IT organizations shows that the 90,000-employee BA—Germany's largest government agency—is best practice in a variety of performance metrics, including cost per user and IT infrastructure integrity.

The BA's IT transformation began in 2006, when Klaus Vitt, an IT executive with almost 30 years of private-sector experience, joined the agency as chief information officer (CIO). Vitt came to the BA from Deutsche Telekom, where he served in a variety of IT leadership positions from 1996 to 2006. Prior to that, he spent 14 years at the media company Bertelsmann. In an annual ranking of the country's best CIOs in both the private and public sectors, German magazine *CIO* has twice named Vitt among its top 10.

Recently, Vitt spoke to McKinsey's Sebastian Muschter and Katrin Suder in Nuremberg.

McKinsey on Government: *What was the BA's IT department like when you took over?*

Klaus Vitt: When I came on board, the situation at the BA was worse than I had anticipated. Some of the technologies it was using were so outdated, especially the legacy applications in human resources and finance, that only a handful of soon-to-retire employees were still able to make changes to the code. I remember one situation where we had a problem with the payroll system and we had to think about how we could pay salaries in cash that month.

Klaus Vitt

Some major projects were facing serious difficulties, and urgent action was needed to get them back on track. There was no strategic framework, let alone a five-year plan, for how the IT landscape was supposed to evolve. No system of objectives was in place that could help determine whether investments were truly moving the IT landscape forward. There was a lack of effective management structures, and there were no clear lines of communication. As a result, employees had a critical view of IT, with departments complaining in particular about the lack of transparency and resources. In short, there was plenty to do. The first thing we did was develop an IT strategy for the next five years and broadly communicate it to our employees and the general public.

McKinsey on Government: *That strategy called for major changes in several areas, including IT infrastructure, applications, and large-project management. We would like to better understand the changes in those three areas. Let's start with IT infrastructure: what has happened there?*

Klaus Vitt: The BA originally had a decentralized structure; IT was decentralized as well. We sought to bring the scattered elements of IT together. We started by centralizing the databases and applications. Today, we're working on the final step, which is consolidating the BA's 178 data centers into 11. We're setting up our operations and infrastructure like an IT factory—with no operator on site, but with standardized processes, products, and production. All processes are organized according to the ITIL framework,[1] and we've identified indicators that allow us to compare actual and target performance for each process every month.

Another important consideration as we were thinking about IT infrastructure was energy efficiency. The BA has been interested in "green IT" since before there was even a name for it. Rising energy costs have always been a concern for us; after all, we have 170,000 networked PCs and the corresponding IT infrastructure. At one point, we calculated that the energy costs for running a server over five years are practically equal to the purchase price of a new one.

McKinsey on Government: *Indeed, a few months ago, the BA received the federal government's Green IT Flagship Project Award for 2010. What are some of the things you're doing on that front?*

Klaus Vitt: We've developed a comprehensive green IT strategy, as part of which we set an ambitious target of reducing energy use in IT by 40 percent by 2013—a reduction of about 53,000 megawatt hours. We now require information on

[1] The Information Technology Infrastructure Library (ITIL) is a set of widely adopted best practices in IT service management.

energy consumption in our requests for bids. And we're not just taking these steps because of an obligation at the federal level, but because it really pays off for us. We achieve enormous cost savings for the BA—we're talking about millions of euros each year for electricity alone.

McKinsey on Government: *The second area we'd like you to talk about is the application landscape, where your goal is to set up a service-oriented architecture (SOA). Why is this new direction necessary?*

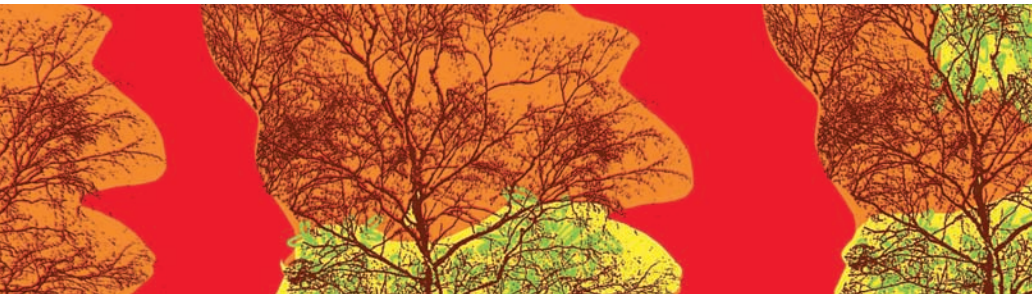
Klaus Vitt: SOA can deliver role-based user interfaces—interfaces that show employees only the IT functions they actually use. This is in stark contrast to how users work with our systems today: an employee in one of our call centers must know how to operate 14 different IT applications to cover all possible customer requests. In the end, he uses just 20 percent of these applications for his area of work, but he still must be familiar with all their functionality to find and select the right 20 percent. Because we employ a large share of temporary employees in our call centers, training them on these applications entails a considerable investment.

We took a close look at SOA and saw that role-based user interfaces that span multiple applications could significantly lower both effort and expense. Call-center employees would see only the IT functions they need for their day-to-day work, in the order in which they need them.

McKinsey on Government: *Implementing SOA is a complex undertaking. What challenges are you facing?*

Klaus Vitt: The biggest challenge is not the technology, but rather breaking down existing IT applications into different kinds of services—that is, understanding which components of applications can be standardized and which cannot—and we have a limited number of people with the skills to do this work. In addition, we must maintain more than one interface per application; we need to keep the existing user interfaces because there are expert users outside the call centers who use only a few applications but use them extensively. Finally, managers in business and IT have to get used to the idea that they no longer have free rein over the look and feel and functionality of their applications.

Implementing a transformation thus requires a step-by-step approach and the intensive support of management on both the IT and business sides. We're building prototypes to help users get accustomed to the new systems, and we're conducting pilots. All in all, we expect implementation to take two to three years.



McKinsey on Government: *A third focus of the BA's IT transformation effort is better management of large projects. What changes have taken place in this regard?*

Klaus Vitt: First we analyzed why problems occurred. One key factor was that the scope of the projects kept increasing over time. Of course, there were good reasons for expanding the projects, but there was no structured process to immediately clarify the impact of the additional requirements on the schedule and costs. To address this issue, we developed a centralized project-management function, provided training to managers and employees, and established guidelines for planning and carrying out projects. In addition, we built up a pool of three top project managers—one we hired externally, and the others we moved from internal roles—for our large projects.

Another thing: we laid out responsibilities clearly. Every project now has a steering committee with well-defined rights and responsibilities. However, this committee provides only overarching management and control. A project manager who meets project milestones and stays within the scope and budget is free to make decisions as he or she sees fit; the steering committee gets involved only if these boundaries are crossed.

We also initiated a cultural shift in IT. The BA is a fairly democratic institution in which decisions are mostly made in committees. This culture creates a lot of buy-in, but it was frequently three steps forward, two steps back—discussions that were concluded months ago were reopened, suddenly everybody was in doubt again about the right direction, and implementation stalled. This, I realized quickly, had to stop if the IT organization were ever to move forward in a lasting way. The IT management team had a team-building workshop during which we had to construct, as quickly as possible, a wooden shelf from prefabricated pieces that only fit together a certain way. The first time, it took us more than 10 minutes to figure out the right sequence. The second time, we learned that agreeing on a plan should be the first step and that diligent execution should follow. We did it in less than two minutes. I still apply this lesson today: we discuss first, make a decision, and then the discussion is over and it's all about implementation.

McKinsey on Government: *You introduced many changes at the BA over a relatively short period of time. What concrete steps did you take to get employees on board with these changes?*

Klaus Vitt: We stressed open communication from the very beginning. We laid out our transformation program in roundtable discussions, making sure employees knew about the coming changes early and in detail. Many also wanted to know how we made upper-level decisions. We therefore communicated how a topic comes up for consideration by the IT leadership and what kind of decision-making process we follow. We repeated these roundtables for a good three years. Today, each of our employees understands the BA's IT strategy, the reasons for it, and its implications for his or her area.

Every employee also knows our IT targets. We introduced a system of objectives broken down into concrete annual plans, with monthly tracking of relevant targets. We develop the targets bottom up from the teams rather than top down: we created an IT leadership circle that sets focus areas for the year, but each unit defines its targets on its own. We then consolidate the individual team targets and align on overarching targets for the group. This approach not

only makes it easier for different groups to work together but also builds strong employee identification with and commitment to the targets.

We can develop a target system like this in just three months. The IT leadership circle—me, five of my direct reports, and a couple of other functional heads—selects the focus areas in October, and the consolidation process is completed by December. In January, every employee knows the current year's targets.

McKinsey on Government: *You've talked about some of the success factors for a large-scale IT transformation: a comprehensive strategy, clear management structures, and a transparent system of targets. Are there any others?*

Klaus Vitt: Active risk management is also central to success. No project manager enjoys thinking about risks and their consequences, but the fact is, in every area there are risks that could keep a project from meeting its goals. The key is to raise awareness of this simple truth in our day-to-day business. Every project manager now has to file a monthly risk report.

Rigorous performance management is just as important. We currently have 40 projects running in parallel. To be able to reliably track their progress, we introduced a traffic-light system. It offers a monthly portfolio view that shows whether each project is in the green, yellow, or red zone. If a signal switches to yellow or red, we can quickly respond. For our particularly large and important projects, we also now have external reviewers check that we have not missed any hidden issues.

McKinsey on Government: *Do you find it harder to carry out a transformation with public-sector employees than with employees in private enterprise?*

Klaus Vitt: Like private-sector employees, the BA's employees are highly motivated, team-oriented, and knowledgeable in their fields. However, because salary structures in the public sector are quite different from those in the private market, we have difficulty attracting and retaining experienced IT specialists. We compensate for this through our informal apprenticeship program whereby we equip new hires over the course of three to five years to take on management or specialist tasks. We currently have 120 apprentices working for us.

McKinsey on Government: *Aside from salary structures, what have you found to be the biggest differences between the public and private sectors when it comes to implementing change processes?*

Klaus Vitt: The differences in technical requirements are minimal. The BA's IT department is comparable to that of a large insurance company, for example. But two differences from a for-profit company do play a significant role in IT transformations: the first has to do with how we award contracts, and the second involves the political decision-making process.

Public agencies are required to observe strict rules when awarding contracts. I found this hard to get used to. For large projects, the process from the initial description of the needed services to the final award of the contract can

take up to 18 months. Only then can the actual work begin, and it takes another two years or so. Large projects can thus easily require three to four years—a time frame that places many demands on planning.

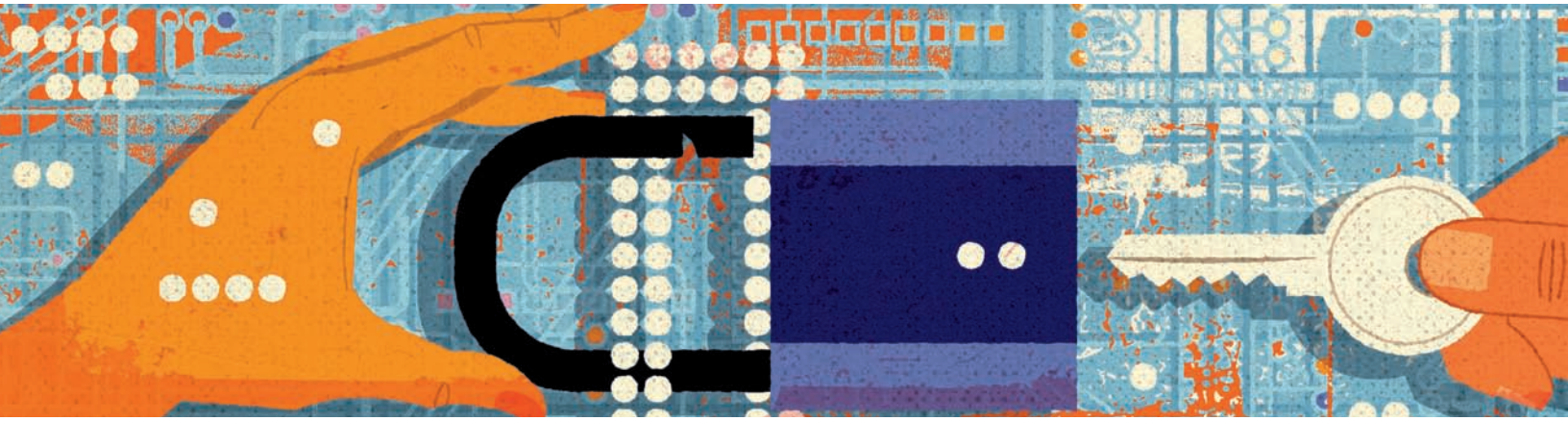
The political decision-making process also sets the public sector apart. IT is central to implementing a number of political initiatives: approving new benefits, offering new processes, or tracking new statistics. We need a certain amount of lead time to make the changes and conduct the required testing. But because reaching policy decisions often takes longer than planned—and the start dates for programs are not postponed—the time to make the necessary IT changes gets cut. One vivid example of such a situation was the introduction of the benefits program for the long-term unemployed. The BA had to set up a completely new benefits process within a very short period of time. The fact that the implementation window kept getting smaller and smaller was the reason for many of the subsequent problems. We learned from this experience, and since then, we have earned the credibility to tell policy makers how much lead time we need.

McKinsey on Government: *Let's look ahead: what projects will the BA's IT organization tackle next?*

Klaus Vitt: The next challenges will involve keeping our current projects—such as the introduction of our document-management system and our new enterprise-resource-planning system—on schedule. Also, we've developed a 2015 IT strategy, and successfully implementing that strategy will of course constitute a further milestone. Moving IT in the direction of SOA is central to this effort. Another important topic that will increasingly occupy the BA is the switch to e-government—making online transactions user-friendly enough that clients can take care of as many things as possible themselves. Doing so isn't really a big technical challenge, but again, we first need the legal basis that allows us to offer such functions on the Internet.

As you see, we still have plenty on the agenda. The vision has remained the same for years: we want to be the highest-performing IT provider in the public sector in Germany.

Sebastian Muschter is a principal in McKinsey's Frankfurt office. **Katrin Suder** is a director in the Berlin office.
Copyright © 2011 McKinsey & Company. All rights reserved.



Can you hack it?
Managing the cybersecurity challenge

To secure cyberspace, technology alone is not enough. Strong management plays an equally important role.

John Dowdy, Joseph Hubback, Dennis Layton, and James Solyom

Cyberspace, according to the US government, is "the interdependent network of information technology infrastructures," including "the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[1] Governments and corporations worldwide are beginning to recognize the fact that securing cyberspace—protecting its confidentiality, integrity, and availability—is of paramount importance.

In its 2009 cyberspace policy review, the Obama administration asserted that "threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies."[2]

Europe has similar concerns: the United Kingdom's National Security Strategy, for example, cites "hostile attacks upon UK cyberspace by other states and large-scale cyber crime" as a Tier 1 threat.[3]

Yet governments today have a poor understanding of the cybersecurity landscape and the scale of the challenge. One reason for this lack of clarity is that the term "cyberattack" is often used to describe everything from low-probability catastrophic events (such as devastating attacks on infrastructure) to higher-frequency threats (such as cyberespionage and intellectual-property theft). In addition, there is a dearth of reliable data on the economic cost of attacks on government. Most top-down estimates of the scale of the issue

[1] National Security Presidential Directive 54 and Homeland Security Presidential Directive 23, as per *Cyberspace policy review*, p. 1.
[2] Ibid.
[3] *A strong Britain in an age of uncertainty: The national security strategy*, UK government, October 2010.

are based primarily on questionable assumptions that yield implausible figures[4] and thus do not offer a sound basis for decisions about policy or government interventions.

In this article, we propose a cybersecurity taxonomy to help government leaders understand the landscape, and a "value at risk" framework that government leaders can use to prioritize and focus on the most serious threats. It is our firm belief that cybersecurity is first and foremost a management problem, not simply a technical problem, and therefore our taxonomy and framework take a senior-management perspective. We also outline four principles for a best-practice management response to cyberthreats. Adhering to these principles will enable government to act as an effective protector of valuable assets.

Understanding the landscape and the value at risk

We have developed a six-part taxonomy of the cybersecurity problem (Exhibit 1). The logic behind our taxonomy is that an attack will occur if an attacker has both the capability and the incentive to strike at vulnerabilities in a target's assets. Today, attackers' capabilities and incentives are increasing—the former due to technological developments and the latter due to the fact that more data and assets are now accessible online.[5] The relative lack of traceability means that attackers continue to feel little threat of retribution. Meanwhile, targets' vulnerabilities are decreasing, but at a slower pace than the increase in attackers' capabilities, which suggests that attacks will continue to increase in frequency and impact.

The taxonomy is helpful for understanding the cybersecurity landscape, but to identify and plan for the most serious threats, government leaders must be able to quantify the impact of attacks. What, for example, was the cost of the alleged loss of data relating to the F-35 Joint Strike Fighter? What was the cost to the US government of the release of its data by Wikileaks? There is a lack of data, from private enterprise or government, to help answer these questions. Various estimates put the direct cost of a cyberattack on a large company at between $1.6 million and $7.2 million.[6] At the extreme, the reported attacks on the F-35 program could compromise the US government's estimated $323 billion development cost.[7]

Extrapolating such estimates into economy-wide figures is problematic. How many attacks of this magnitude occur, and with what regularity? In a 2011 survey, more than 80 percent of critical-infrastructure providers reported being the victim of large-scale cyberattacks or infiltrations.[8] And many incidents that are detected go unreported, in part because reporting requirements vary by jurisdiction but also because there are clear disincentives—especially for corporations—to report breaches.

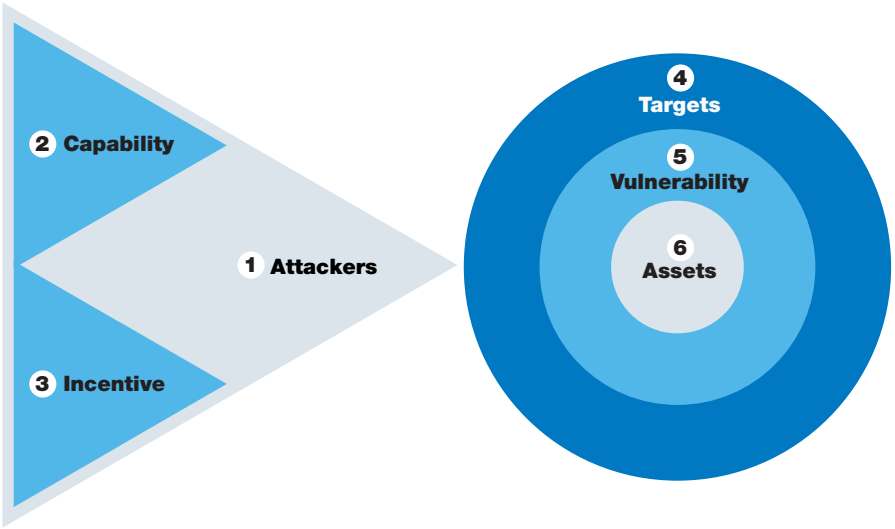
We have used our taxonomy to create a relative value-at-risk analysis that offers government leaders insights into the likelihood and impact of

[4] See "Sex, lies and cyber-crime surveys," Dinei Florêncio and Cormac Herley, Microsoft Research, June 2011.
[5] For more on the impact of ever-increasing amounts of data, see *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, May 2011.
[6] Ponemon Institute 2009 Annual Study: "Cost of a data breach"; *Symantec Internet Security Threat Report 2010*, PricewaterhouseCoopers Information Security Breaches survey, 2010.
[7] US General Accounting Office, "Testimony before the Subcommittees on Air and Land Forces and Seapower and Expeditionary Forces, Committee on Armed Services, U.S. House of Representatives," GAO-10-478T, March 24,2010.
[8] McAfee and Center for Strategic and International Studies (CSIS), "In the dark: Crucial industries confront cyberattacks," 2011.

To identify and plan for the most serious threats, government leaders must be able to quantify the impact of attacks

Exhibit 1

The taxonomy of cybersecurity helps government leaders understand the landscape.



1 Four groups of attackers[1]
a. Governments
b. Enterprises
c. Cybercriminals
d. Cyberterrorists or "hacktivists"

2 Capability
The ability to steal, hijack, impair, or damage

3 Incentive
The motive to attack

4 Four types of target entity
a. Public sector
b. Private enterprise
c. Individuals
d. Critical national infrastructure (CNI)

5 Vulnerability
Can be technical (eg, lack of a firewall) or human (eg, employees being tricked by phishing e-mails)

6 Assets
a. Data (such as IP[2], customer records, or classified national secrets)
b. Systems, which vary in criticality from low (eg, informational Web sites) to high (eg, nuclear monitoring systems)

[1]Members of multiple groups can work together in a single attack, in either a coordinated or an uncoordinated way.
[2]Intellectual property.

attacks for each combination of attacker and target (Exhibit 2). We see value at risk as a combination of three elements: the attacker's capability, the asset's vulnerability, and the relative financial and nonfinancial costs of the attack. Our estimates of relative costs—which take into account financial value but also factors such as national security and the protection of civil liberties—were informed by available data, our experience working in both the public and private sectors, and extensive interviews with leaders and IT specialists worldwide.

As the exhibit shows, the highest value at risk applies to enterprise-held intellectual property (IP). IP is both extremely valuable and

Exhibit 2

A value-at-risk analysis offers insights into where the most serious threats are.

Estimation of value at risk relative to existing protection: Low, Medium, High

An attack could be consistent with the attacker's incentives: ●

		Targets and assets								
Attackers	**Incentives**	**Public sector**			**Private enterprise**			**CNI**[2]	**Individuals**	
		Classified information	Sensitive information	Systems	IP[1]	Non-IP data	Systems	Systems	Personal information	Systems
Government	Strategic advantage	Medium ●	●	Medium ●	High ●	Medium ●	Medium ●	Medium ● War	Medium ●	●
Private enterprise	Financial gain	●	●		High ●	Medium ●		●	●	
Cyber-criminals	Financial gain	●	●	●	Medium ●	Medium ●	●	●	●	●
Cyber-terrorists, hacktivists	Protest, fun, terror	●	●	●	Medium ●	Medium ●	●	●		●

[1]Intellectual property.
[2]Critical national infrastructure (eg, power station).

vulnerable. It is easily stolen from electronic systems, often without the theft even being noticed. We estimate the value of the S&P 500's IP to be between $600 billion and $1.2 trillion.[9] Governments have a critical interest in ensuring the protection of IP due to its importance to both economic growth and the government's own defense investments (for example, IP held by defense suppliers).

Medium value-at-risk attacks should be a second-level priority. In the private sector, these are primarily attacks on non-IP assets, such as customer data. Another medium value-at-risk concern: the threat from foreign governments to critical national infrastructure (CNI). Here, the very high relative costs are dispersed across a wide range of assets, locations, and sectors, thus reducing the risk of a catastrophic attack. Furthermore, given that the primary threat to CNI is from other governments, an attack on CNI systems could be construed as an act of war—and is therefore less likely, as there are implicit retaliatory threats already in place.

Another group of medium value-at-risk assets consists of government systems and classified data. For example, we estimate the UK public

[9]Based on discounted value of research-and-development expenditures and corroborated by the value of intellectual-property-relevant intangible assets on S&P 500 balance sheets.

sector's maximum loss from cyber-enabled fraud to be $5.2 billion.[10] Although significant, this figure is small in comparison with the value at stake for private-sector IP losses. Furthermore, most governments already invest heavily in reducing the vulnerability of internal data, thus reducing the risk of attack.

A management challenge

Responding to the threat of cyberattacks requires more than simply increasing spending on technical defense mechanisms such as firewalls and antivirus software. It requires senior-management attention and a broad range of both technical and nontechnical capabilities.

There are four principles that underlie a best-practice management response to the cybersecurity threat. They apply equally at any level of government; the assurance questions for each principle enable all managers to test the effectiveness of their response.

Define and prioritize risks

"Do we have a clear understanding of our portfolio of network-enabled assets and their respective value at risk? Do we have sufficiently robust best practices and expertise in-house to adequately protect them?"

To manage a cybersecurity program effectively, leaders must clearly define what they are protecting and prioritize the threats they face. We suggest a three-step process to define and prioritize risks.

The first step is to conduct an organization-wide asset audit. Leaders must identify the assets—normally, the data and systems—that could be at risk from a cyberattack. The audit should encompass the entire spectrum of network-enabled assets, including those that may not traditionally be seen as at risk (such as systems that are not online but that may be connected to the outside world through USB ports). The audit should also consider assets held by other organizations, especially suppliers. The alleged compromise of the F-35 plans, for example, followed intrusions into the systems of two or three contractors rather than the systems belonging to the Department of Defense (DOD).[11]

The second step is to conduct a risk assessment to gauge the impact and likelihood of attacks on each asset. The organization should estimate both financial and reputational impact using a relative scale (such as a simple low/medium/high). A distributed denial-of-service (DDOS) attack on the Treasury Department's Web site, for instance, may rank low for financial impact and medium for reputational impact. Then, for each asset, the organization should estimate the likelihood of a successful attack, again using a relative scale—taking into account the attacker's incentive, the attacker's capability, and the target's vulnerability. For example, a DDOS attack on the Treasury Web site may be rated high for attacker incentive and capability and medium for vulnerability.

The third step is to categorize assets according to value at risk. Often two categories will suffice: lower value-at-risk assets (such as informational Web sites), which existing best practice should cover, and higher value-at-risk assets (such as vital systems), which require additional measures. Some of these measures—more advanced security and vulnerability management, for example—may involve building deep internal expertise or contracting for external assistance.

[10] McKinsey analysis based on *National Fraud Authority Report*, 2010, Her Majesty's Revenue and Customs data.
[11] "Computer spies breach fighter-jet project," *The Wall Street Journal*, April 21, 2009.

Assign responsibility for cyberthreat mitigation

"Who are the named and empowered individuals responsible for our highest-priority network-enabled assets? Who is responsible for setting and executing our cybersecurity strategy? What is the process for linking those individuals so that we have a consistent and coordinated approach that does not undermine the efficiency of our operations?"

Cybersecurity is a cross-functional issue. Organization-wide responsibility for policy should rest with a board member of the department or agency. Below board level, organizations should clearly define responsibility for cybersecurity so that they can take a comprehensive series of actions to mitigate threats.

Leaders should assign responsibility for cybersecurity in three areas. Ownership of each area may be delegated to the relevant department (for instance, the human-resources director could be accountable for people policies). The three areas are as follows:

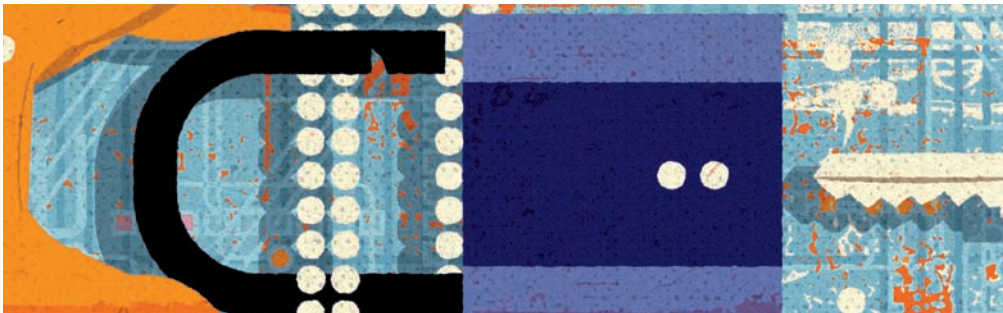
Technology. Technology must be used to maximum advantage to counter cyberattacks. The organization must have the level of technical capabilities required and should prioritize technical spending in the areas of highest risk. Basic security best practices should be embedded within the architecture (for example, limiting administrator rights or conducting simulations of cyberattacks to test resilience).

Process and procedure. Procedures must be established to limit and mitigate the impact of attacks. Responsibility in this area includes ensuring that information about attacks is available to leaders within the business (for example, predictive threat analysis based on aggregating and analyzing e-mail headers) and that data assets are suitably categorized (for example, working with business owners to determine appropriate encryption levels).

People. Personnel policies must be in place to minimize risk. This includes providing training to support the policy and regularly testing compliance.

Supplementing the organization-wide policies, leaders should assign high-risk assets to individuals to ensure that cybersecurity threats are seen as a business risk rather than simply an IT problem—for example, protection of health records may be the responsibility of an operations manager. The risk owner, however, should not be the same person who has business responsibility for an asset, so as to avoid conflicting incentives or priorities: an owner of classified data, for example, may want to improve functionality by combining data sets—at the expense of security.[12]

[12] For some threats, additionally assigning responsibility by threat vector may be appropriate—giving (often technical) teams or individuals the responsibility of tackling a particular threat (for example, distributed denial-of-service attacks across all Web sites operated by a government department).



Manage the performance of those responsible

"What is the basis for managing the performance of those responsible for the protection of our network-enabled assets? How are we performing against those assessments?"

Key performance indicators (KPIs) for the individuals responsible for cybersecurity should include metrics mirroring the three areas for threat mitigation, as follows:

Technological KPIs. These KPIs point to the number and type of electronic touchpoints, both internal and external, and highlight the quality of management of these connections. An example of such a KPI is the number of days that elapse between Microsoft issuing a critical software update and the entire organization installing it.

Process and procedural KPIs. These KPIs can include data-policy indicators that measure the success of data segmentation and risk-assessment activities (for example, the proportion of data that are suitably encrypted) and operational-policy indicators that measure the implementation success of policy (for example, the number of attempted security-policy breaches within a certain period).

People KPIs. People KPIs measure the success rate of training, employee conformity to security guidelines, or employee knowledge and use of best-practice e-mail behavior. They may be assessed through spot tests.

To support these KPIs, organizations should put in place a performance-management review system and a set of incentives and consequences. Organizations should also ensure accurate flow of information on the frequency and type of attacks, as well as on compliance with management practices.

Develop a cyberattack contingency plan

"What is our plan if we experience a significant security breach? How will we communicate internally and externally?"

Governments must have a robust response plan in the event of a successful cyberattack. A best-practice plan includes three phases: crisis management, recovery, and postmortem.

The first phase is immediate crisis management, or how the organization should respond when it detects an attack. This should feature two elements: a communications response and a system response, both of which should be proportionate to the impact of the attack.

The communications response, typically owned by the head of public relations, should aim to give stakeholders the information they need to know. This is particularly important for governments, given the likelihood of media and public interest. Key stakeholders will vary depending on the area of government attacked and should be identified in advance. For example, if there is an attack on a system for sharing patient information among hospitals, the stakeholders may include hospital staff, nonhospital doctors, patients, data-protection authorities, and other organizations using similar systems. Immediately following a DDOS attack on its Web site, the United Kingdom's Serious Organised Crime Agency (SOCA) promptly issued a media statement describing the extent of the attack and informing the public that it had taken its Web site offline.[13] Some news reports characterized the attack itself as embarrassing for SOCA, but its communications response was best practice.

The system response, the main goal of which is to terminate or ring-fence the breach, is normally owned by the head of IT. Again, the response

[13] "Soca website taken down after LulzSec 'DDoS attack,'" BBC News, June 20, 2011.

should be commensurate with the impact of the attack. For example, an agency should not necessarily sever its IT communication links for a relatively low-level DDOS attack—but it may want to cut off access in the event of a significant intrusion or hijack of its systems. Organizations should codify and practice these measures beforehand, not develop them on the fly. Once an organization contains the breach, it should initiate backup systems (such as a mirror Web site). A crucial part of the system response should be to inform IT departments in other government organizations of the nature of the attack so that they can upgrade their protection. For example, detection of a targeted phishing attack on the DOD should trigger a warning to all other US government departments.

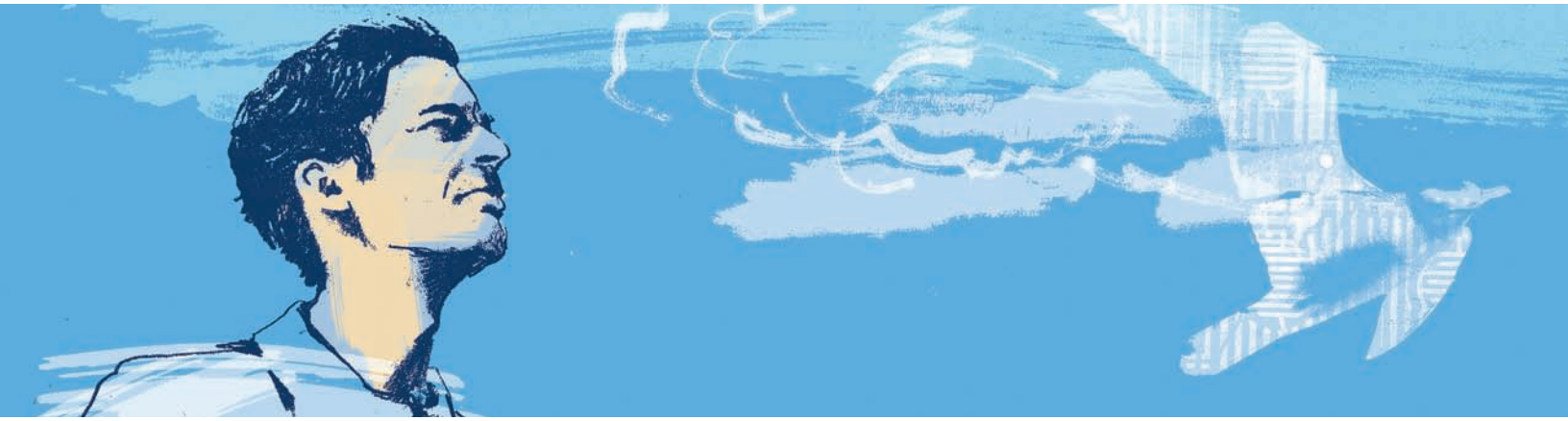
The second phase is recovery, which is predominantly a technical response that builds on the immediate system response in the previous phase. The purpose is to repair damaged systems and data, fix the vulnerability that led to the attack, and bring systems back online. An ineffective recovery response leaves the target exposed to more attacks, which can lead to further embarrassment and cost.

The third phase is the postmortem, normally enacted by the corporate risk owner. The purpose of the postmortem is self-evaluation: to flush out the causes of the attack and prevent a similar one from recurring, to investigate attackers and their motives and explore opportunities for restitution, and to evaluate the success of the response plan. The response plan should include a board-level report that details the agreed-on actions to be taken, with clear time frames and owners for each. A successful postmortem may include supporting a criminal investigation.

• • •

Cybersecurity is a growing and ever-changing challenge. Government responses and policies regarding cybersecurity should not be static but instead should be continually adapted and refreshed as new knowledge becomes available. While existing efforts to share knowledge among organizations (such as the forums hosted by the US Office of Cybersecurity and Communications) are laudable, there is still too little knowledge sharing when it comes to cybersecurity, resulting in organizations not being as well prepared for attacks as they could be. A greater level of collaboration is particularly important among leading targets such as governments, advanced industries, and financial institutions. Within the public sector, sharing should happen at many levels—not only shared information and shared storytelling but shared action as well—reflecting the interconnectedness of government departments.

John Dowdy is the global leader of McKinsey's Aerospace and Defense practice. He is a director in the London office, where **Joseph Hubback** and **James Solyom** are consultants and **Dennis Layton** is a principal. The authors wish to thank Tucker Bailey, Assaf Egozi, Scott Gebicke, James Kaplan, Edward Lock, Chris Rezek, Giacomo Sonnino, and Allen Weinberg for their contributions to this article. Copyright © 2011 McKinsey & Company. All rights reserved.



Getting ahead in the cloud

The transition to cloud computing will be especially challenging for governments, given their myriad IT systems and their security, budgetary, and organizational constraints. We look at four critical actions they must take.

Kreg Nichols and Kara Sprague

Cloud computing—a computing model in which users purchase IT resources as a service, allowing them to take a pay-as-you-go approach—has deservedly garnered a lot of attention recently in both the private and public sector. Often referred to as simply "the cloud," cloud computing in many respects resembles a utility that supplies water or electric power: with the cloud, users can access IT resources at any time and from multiple locations, track their usage levels, and scale up their IT capacity as needed without large upfront investments in software or hardware. By enabling this flexibility, cloud computing improves IT efficiency—potential savings amount to 20 to 30 percent across the entire IT budget (including facilities, telecommunications, infrastructure, software, labor, and external services)—and makes IT organizations more agile. In the public sector, cloud computing will allow agencies to invest freed-up resources in mission-critical activities and become more responsive to new laws and regulations and to citizens' evolving needs.

Governments around the world have recognized the potential for cloud computing to transform the way they invest in, deploy, and access IT resources. The US federal government's "Cloud First" policy mandates that all federal agencies migrate at least three IT services to the cloud by mid-2012. The federal cloud-computing strategy, which the White House issued earlier this year, elaborates on this imperative and estimates that $20 billion—one-quarter of the

Kate Miller

US federal government's total IT spending—could potentially be reallocated to cloud-computing solutions.[1] In Europe, the vice president of the European Commission, who is also the European commissioner for digital agenda, declared that the region must become not just "cloud friendly" but "cloud active." Asia's public sector is also broadly embracing cloud computing. India's government, for example, plans to issue a cloud policy by 2012 and is seeking to deploy cloud technologies to deliver e-government services.

With the strategic imperative in place, government agencies must choose which parts of their IT environment, both legacy and new spending, to migrate to the cloud and, in each case, determine the appropriate cloud service and deployment model. (For descriptions of these options, see "Cloud basics," p. 53.) At the same time, they must create more flexible budgetary processes and funding models to support cloud-related investments and adopt new mind-sets and capabilities to realize the full benefits of cloud computing.

Based on our experience guiding clients through cloud-computing transformations and our understanding of the public sector's particular challenges, we see four critical actions that public-sector chief information officers (CIOs) must take in developing and implementing a cloud-computing strategy.

Choosing a service model

When confronting an extensive legacy IT environment, many CIOs find themselves asking, "Where do I start?" when considering what to migrate to the cloud and which service model to use. There is no single answer—the optimal service model depends on the specific requirements of each "workload" within an organization's IT environment. A workload is an integrated set of demands on IT, generally fulfilled through one or more applications. Human-resources management and financial management are two examples of workloads.

Rather than reviewing each of the potentially thousands of applications in its portfolio in detail, an organization should group applications into 30 to 50 workloads. For example, collaboration and messaging is a workload that encompasses the entire set of functionality relating to e-mail, calendaring, instant messaging, and shared workspaces. As a rule of thumb, each workload should be broad enough that a commercially available software package can deliver the required functionality. If the workload is defined too broadly, however, it will not be useful as the basis for the analyses described below.

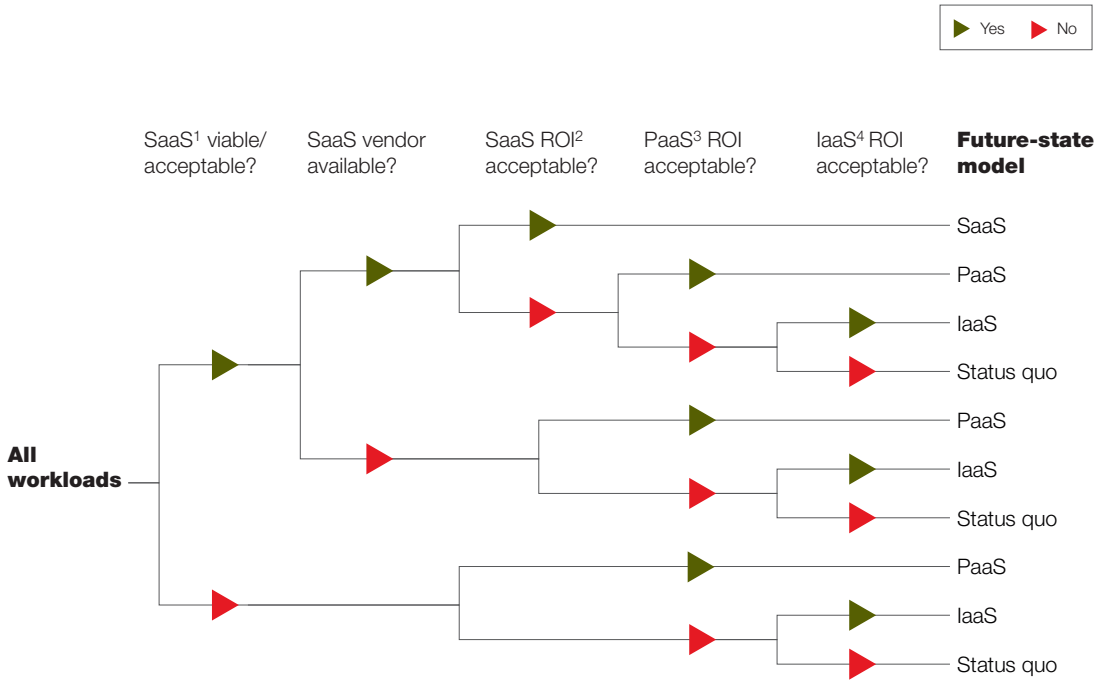
Once the agency has grouped its applications into workloads, the next step is to evaluate the performance and health of the current solution for each workload—that is, the degree to which the solution meets current and future needs. For example, does the solution work reliably on a daily basis? How easy and affordable is it to make changes to accommodate new requirements? Can the solution be rapidly scaled up to address unforeseen spikes in demand? Is end-user satisfaction with the solution high or low? The workloads that score low on this performance-and-health assessment are prime candidates for cloud migration.

For each workload it wants to migrate, the agency must then determine the optimal cloud service model: infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). Exhibit 1 illustrates a framework that can be used to make this decision. The structure of

[1] Vivek Kundra, *Federal cloud computing strategy*, Washington, DC, February 8, 2011.

Exhibit 1

A decision framework allows organizations to choose the optimal 'as a service' model.



[1]Software as a service.
[2]Return on investment.
[3]Platform as a service.
[4]Infrastructure as a service.

the decision tree will depend on an organization's priorities. For example, an organization that prioritizes speed of deployment and flexibility over the ability to customize solutions would look first to a SaaS model. The decision tree depicted in Exhibit 1 indicates a preference for SaaS adoption where possible. The organization first determines whether SaaS is a viable solution (for some public-sector workloads, for example, the security risks of placing data outside a firewall may simply be too high). If the answer is yes, the organization determines whether a SaaS vendor is available, and, if so, evaluates the economics of the SaaS model. For workloads that cannot be migrated to SaaS, the organization considers PaaS and IaaS. For some workloads, the best answer may turn out to be the status quo rather than migration to any cloud service model.

Selecting the right deployment model

Once an agency has chosen a service model, it must determine the appropriate deployment model (public, private, hybrid, or community) for each workload. The selection of the deployment model is typically based on requirements relating

Cloud basics

The US National Institute of Standards and Technology provides the following definitions for cloud service and deployment models:

Service models

Infrastructure as a service (IaaS) provides users with processing, storage, networks, and other computing infrastructure resources. The user does not manage or control the infrastructure but has control over operating systems, applications, and programming frameworks.

Platform as a service (PaaS) enables users to deploy applications developed using specified programming languages or frameworks and tools onto a cloud infrastructure. The user does not manage or control the underlying infrastructure but has control over deployed applications.

Software as a service (SaaS) enables users to access applications running on a cloud infrastructure from various end-user devices (generally through a Web browser). The user does not manage or control the underlying cloud infrastructure or individual application capabilities other than a limited number of user-specific application settings.

Deployment models

Private clouds are operated solely for one organization. They may be managed by the organization itself or by a third party, and they may be located on or off the user's premises.

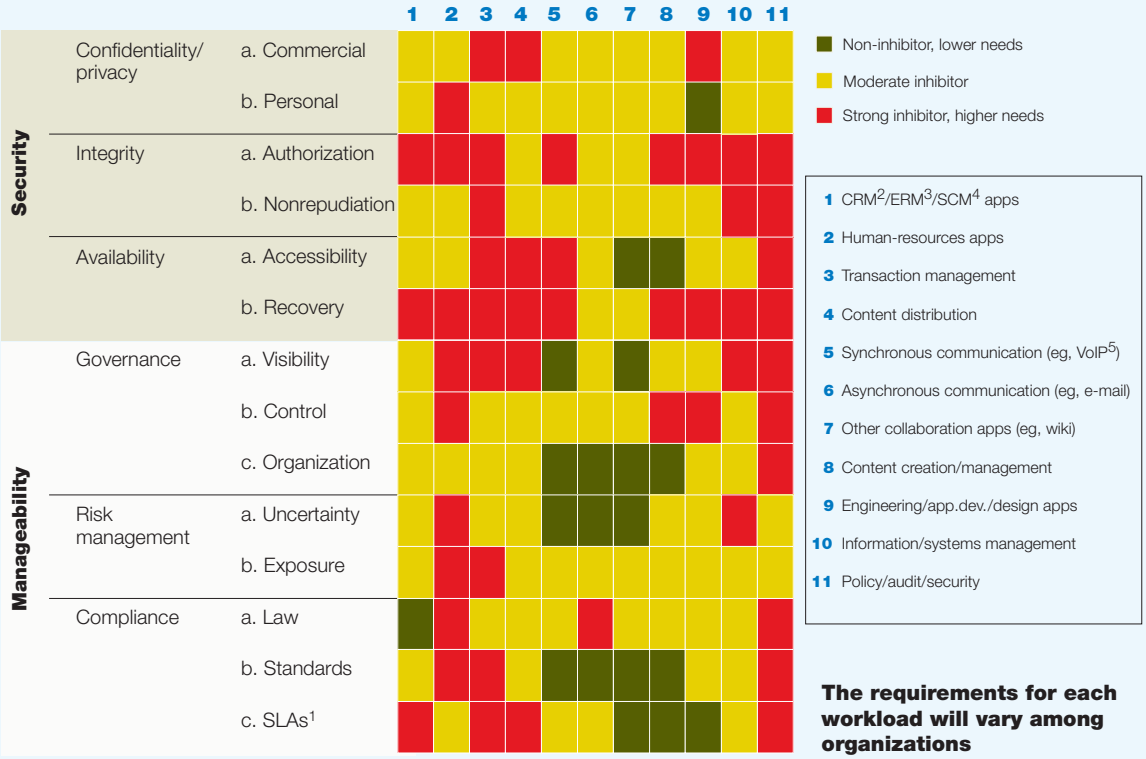
Public clouds are open to the general public or a large industry group and are owned and managed by a cloud service provider. These are located off the user's premises.

Hybrid clouds combine two or more clouds (private or public) that remain unique entities but are bound together by technology that enables data and application portability.

Community clouds feature infrastructure that is shared by several organizations and supports a specific community of users. They may be managed by the user organizations or a third party, and they may be located on or off the user's premises.

Exhibit 2

Organizations can use a heat map to assess the security and manageability of workloads . . .

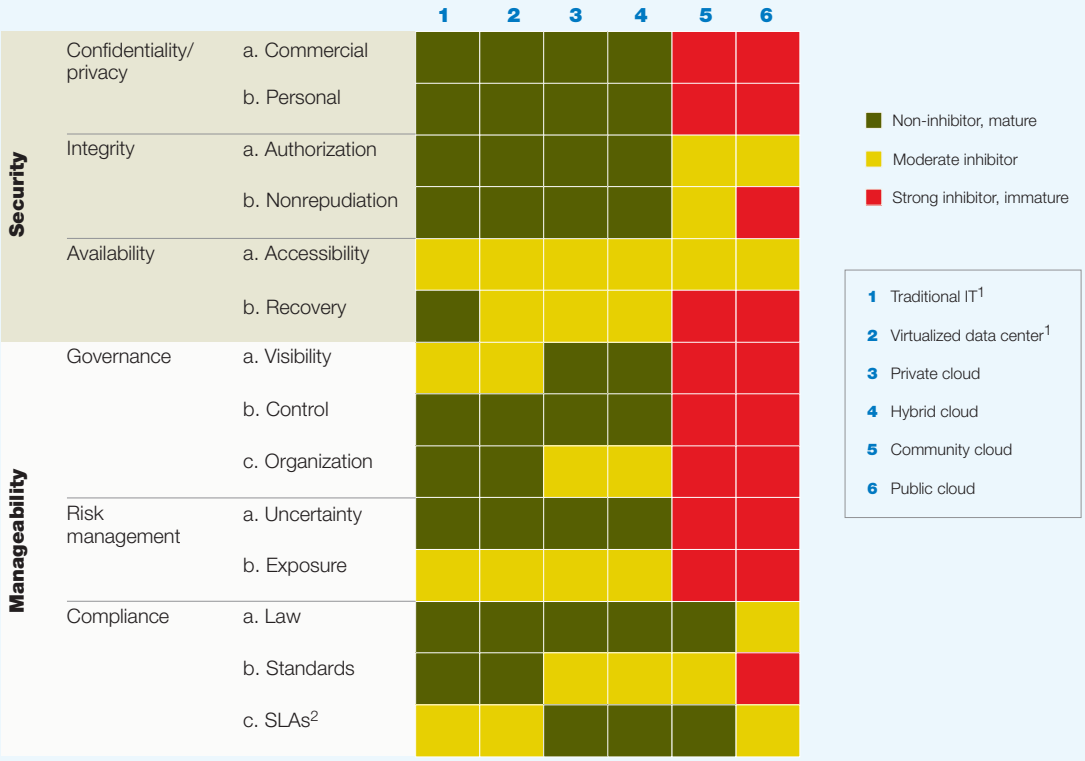


[1]Service-level agreements.
[2]Customer-relationship management.
[3]Enterprise risk management.
[4]Supply-chain management.
[5]Voice over Internet Protocol.

to IT security (confidentiality/privacy, integrity, and availability) and manageability (governance, risk management, and compliance).

We have found that concerns relating to IT security and manageability are the primary inhibitors to cloud adoption—even in the face of strategic imperatives mandating the adoption of cloud solutions. Public-sector CIOs should shift the discussion away from blanket generalizations about the unacceptability of cloud solutions to a careful examination of the relevant security and manageability issues. To facilitate this discussion, and in collaboration with key stakeholders (including the Cloud Security Alliance, a broad coalition that promotes best practices in cloud security), we have developed a framework for a comprehensive assessment of the IT security and manageability issues that organizations are likely to encounter (Exhibit 2).

. . . as well as the security and manageability of deployment models.



[1]Could be either on- or off-premises, captive, or outsourced.
[2]Service-level agreements.

Each of the two heat maps in Exhibit 2 lists 14 elements of security and manageability on the vertical axis. Agencies should use the first heat map to record their workload-specific requirements for each of the 14 elements, considering the nature of the information managed by the workload, the roles or individuals with access to the workload, and the infrastructure requirements for running the workload. On the illustrative heat map shown here, the agency's concerns are mostly about authorization (for example, the verification required for users to modify or delete content), recovery (including capabilities for archiving and restoring data), and visibility (for example, monitoring and reporting capabilities). The second heat map evaluates the maturity of the solutions for each of the 14 elements offered by traditional IT, a virtualized data center,[2] and the four cloud deployment models. This evaluation shows that

[2]A virtualized data center is, like the cloud, a virtual infrastructure environment—but it does not offer the full suite of cloud-computing capabilities (such as real-time provisioning or advanced metering for charge-backs).

the agency's best choice would be a private or hybrid cloud, since these deployment models offer the most mature solutions for addressing the agency's most critical concerns.

We expect many public-sector agencies will initially choose a private or community cloud managed by a shared-service agency (such as the US federal government's General Services Administration). Indeed, in many cases, a private cloud will be more secure and manageable than existing public-sector IT systems because organizations can build security and manageability features into the overall architecture from the start, rather than having to add features to a legacy system. Public clouds may become a viable option for the public sector if they mature in their ability to address the security and manageability issues listed above.

Gaining flexibility in budgeting and funding

Public-sector organizations must make choices about their cloud-computing strategy in the face of rigid budgeting and funding cycles. Decision makers must typically secure funding years in advance, limiting their ability to redirect funding as technology advances or needs change. In cases in which funding is dedicated to individual projects rather than agencies or departments, it is difficult to invest in new IT platforms or architectures for which the business case is based on reducing the costs of future projects. What's more, individual agencies may not be able to afford the level of investment required to migrate to the cloud.

In its cloud-implementation plan, each organization must find creative ways to address existing budgeting and funding limitations. For instance, the funding request for a large IT deployment could include the cost of implementing a private cloud, as well as the costs of smaller projects that would take advantage of the new private cloud. Agencies may also consider working with IT vendors and service providers on financing options that would reduce the up-front capital needed to bootstrap public-sector cloud migrations.

The transition to cloud computing will require broad consensus within the government and tight collaboration among CIOs, finance leaders (chief financial officers, chief purchasing officers, and the central budgeting organization), and IT vendors. Public-sector CIOs can start the dialogue by developing a perspective on what the future-state IT model would be for their respective workloads if they faced no budgetary constraints. This future-state model can then form the basis for discussions between the finance and IT vendor communities regarding which workloads to migrate to the cloud and how to fund the migration. CIOs should seize the opportunity to take a fresh look at their vendor relationships. As their agencies transition to cloud computing, CIOs can explore relationships with new vendors staking a claim in the market, as well as pursue new arrangements with established vendors experimenting with ways to support cloud models.

Central budget authorities should take on the responsibility of coordinating and orchestrating the migration, aggregating requirements and demand from their constituent agencies, and interfacing with IT vendors to drive the development of solutions. These central budgeting organizations should spearhead a process to allocate appropriate funding to cross-agency IT efficiency programs. A more sustainable long-term solution will entail adopting a new service-based funding model for IT: rather than owning IT assets, agencies would share cloud services on

a usage-based charge-back model. For smaller agencies in particular, this model would obviate the need to build new data centers.

Adopting new mind-sets and capabilities

In the technical transition from traditional IT to the cloud, IT staff will no longer have to procure the required hardware and software and then install, configure, and test the operating system and applications; instead, they will simply select the optimal configurations from a service catalog. The use of a service catalog—one of the most critical best practices for cloud technologies—transforms IT provisioning from a lengthy requirements-gathering discussion between IT and business users to a fast, menu-driven selection of the systems configuration most suited to the business requirements. Thus, IT organizations' current emphasis on technical skills such as software configuration or IT systems management will no longer be aligned with their needs. Instead, public-sector IT organizations must develop skills and capabilities in contract management, performance management, and continuous improvement.

The migration to the cloud will necessitate not just new skills but also a new way of managing and deploying IT staff and new core processes for IT operations. The traditional model for provisioning and accessing IT focuses on ownership of IT assets and uses input metrics (for example, the number of servers) to measure and manage performance. Cloud computing, in contrast, focuses on the utilization of IT services and relies on output metrics (such as service levels). Shifting mind-sets and behaviors from an emphasis on asset ownership to an emphasis on service utilization will not be trivial, and it will require a programmatic approach that includes training, incentives, and role modeling.

Another best practice in cloud computing is demand management through detailed reporting and charge-backs. These mechanisms are not only a means to improve funding—they also transform the role of IT by focusing business users on identifying which IT resources they truly require over time. No longer is IT merely the keeper of infrastructure and applications; it becomes a steward of business resources and fiscal responsibility.

• • •

By migrating to the cloud, public-sector organizations will be able to free up IT spend for reinvestment in mission-enabling activities or national objectives such as deficit reduction. With more agile systems and faster deployment times, they will be better at supporting key government operations and providing services to citizens. However, just as the benefits are great, so too are the challenges that must be addressed to achieve them. An investment today in the tools, capabilities, and processes required to surmount the obstacles to cloud migration is likely to yield a significant return in the long term.

Kreg Nichols is a principal in McKinsey's Atlanta office. **Kara Sprague** is an associate principal in the San Francisco office. Copyright © 2011 McKinsey & Company. All rights reserved.

Better all the time: Continuous improvement in IT

By reorganizing its IT function and applying lean IT principles, the Netherlands' largest public-sector agency has drastically improved its performance and reputation. The agency's leaders talk about what they've done—and what still remains to be done—in their pursuit of IT excellence.

Robert Carsouw, Wopke Hoekstra, and Joris Hulst

After some high-profile IT failures that resulted in not only negative media attention and a loss of public trust but also significant unplanned costs, the Tax and Customs Administration of the Netherlands knew it was time for radical action. The country's largest government service provider, employing more than 30,000 people, began an IT transformation effort in 2009 that involved a complete reorganization of the IT function as well as the application of lean IT principles. In the years since, the agency has turned around the performance of the IT function. It has restored public trust and improved service quality while reducing costs.

The leaders overseeing the agency's IT transformation are Director-General Peter Veld and Chief Information Officer (CIO) Wim Sijstermans. Veld, who joined the tax authority in 2009, has three decades of public service under his belt. He was most recently director-general of the Dutch Immigration and Naturalization Department. Sijstermans has held his current post since 2008, bringing with him extensive experience as a senior IT executive in both the public and private sector, including several years at Royal Dutch Shell and Sony.

In June 2011, Veld and Sijstermans spoke with McKinsey's Robert Carsouw, Wopke Hoekstra, and Joris Hulst in Amsterdam.

***McKinsey on Government*:** *Let's start with a broad question for you, Peter: given that the*

Dutch tax authority has a wider range of responsibilities than many of its counterparts in other countries, how do you view the role of IT?

Peter Veld: As you said, our agency covers many areas of responsibility. Unlike most other tax authorities, the Dutch tax authority is not only responsible for collecting taxes—we're also in charge of customs, and we administer benefits for certain groups of citizens (child-care benefits, for example). So we are a huge information factory. We process enormous amounts of information. IT is therefore a critical enabler for us, particularly since we are providing more and more of our services electronically. This year, for example, 95 percent of the tax returns we received from individual taxpayers were submitted digitally. Without IT, we cannot possibly achieve the level of efficiency and effectiveness we want.

IT is also important in helping us realize the Dutch national government's collective goal of cutting costs. Our intention is to reduce the tax authority's overall costs by one-sixth by 2015, which is actually quite a substantial reduction for an agency like ours. Fortunately, we see ways in which we can cut IT costs by 30 percent. We can reinvest part of that savings into innovations that will help us cut costs in other areas.

McKinsey on Government: *Your agency is now in the middle of a broad IT transformation. Wim, you were brought in to oversee that transformation. Tell us what it was like when you started.*

Wim Sijstermans: It was fairly obvious at the time that the tax authority's IT performance was subpar on all levels. Projects routinely overran their schedules and budgets. One of the triggers for the transformation—perhaps the last straw—was when, in 2008, the tax authority lost approximately 700,000 citizens' tax returns. It had to tell those taxpayers, "Sorry, but we've misplaced your tax returns. You have to submit them all over again." The state secretary of finance at the time felt compelled to intervene and created a senior-level role to be accountable for IT. The CIO role was created in 2008.

McKinsey on Government: *You were the first CIO that the tax authority ever had. What were your immediate priorities?*

Wim Sijstermans: The first thing I wanted to do—working closely with the director-general and management team at the time—was understand the situation. How did we get here? And we came to three main conclusions. First, the tax authority wasn't lagging behind in terms of technology; in fact, it depended too much on the latest technology to come up with innovative solutions, when what it really needed to do was get the basics right within the organization. Its priorities were not set appropriately. Our second important conclusion was that the IT department was far too complex and lacked IT knowledge. We had far too few managers with sufficient knowledge of IT. We needed not only to build IT capabilities but also to see a fundamental change in attitude and behavior—so we needed to address both the "hard" and "soft" sides. A third observation was that our IT costs were not transparent and we were more expensive than other tax authorities. Incidentally, more expensive does not necessarily mean too expensive. There were good reasons for our higher costs—as Peter pointed out, we provide services that other tax authorities do not provide.

Peter Veld

Wim Sijstermans

McKinsey on Government: *So you identified certain organizational problems. What were the most serious problems concerning the technology itself?*

Wim Sijstermans: The most important technological problem concerned the continuity of the data center. We were good at correcting regular malfunctions, but if we had experienced an act of God or something really serious, we would have had a major problem. One of our recent successes is that we have demonstrably guaranteed our business continuity; even if there is some extreme event, our data are secure and we will be able to continue our operations.

McKinsey on Government: *You're now three years into the IT transformation. Aside from ensuring business continuity, what are some of the biggest changes you've made?*

Wim Sijstermans: One major change is that we've split the IT organization into three parts: IT demand management, IT supply management, and IT strategy. We've made IT demand management a distinct organization, embedded within the different business areas, because it's extremely important to keep it as close to the business as possible. For example, customs IT demand management is literally across the hall from the customs administration; people from both departments routinely drop by one another's offices. We believe IT demand management should be very closely linked to the source of the demand.

And within IT supply management, we've separated infrastructure from application development and maintenance (ADM) because they are very different businesses that require different management structures and organizational models. Infrastructure is truly supply oriented; it's a branch where we'll see more and more consolidation within the government. ADM, on the other hand, is much more demand oriented in the sense that each business has different needs and will make different requests.

Peter Veld: There are two other important changes we've made in IT. One is that we're cutting up projects into smaller pieces. Traditionally, the tax authority would do a big IT project all at once. During the course of the project, complexity would increase, as would budgets, interdependencies, and stakeholders. It's simply too complicated to design and think through a huge multiyear project in one go. Now it's become standard for us to take a phased approach: we finish a small piece and make sure it's what we want before we work on another piece. That way, we don't waste money.

The other important change is that we've come a long way in applying lean IT principles. We've seen marked improvements in attitudes and behaviors among the IT staff.

McKinsey on Government: *Tell us more about what you're doing in lean IT. Our experience has shown us that a lean IT effort can be perceived as a euphemism for cost cutting. To what extent is that true in your organization?*

Peter Veld: There is certainly the risk that lean IT may be perceived as just a way to cut costs and dispose of people, but that is truly not our mentality. For us, lean is here to stay; it will not go away. It is our new way of working. For employees to see it that way, leaders must demonstrate with their actions that lean is about doing a better job for citizens. One of the most significant strengths of lean IT, in fact, is its focus on the client. It forces us to always ask

ourselves, "What's the point of what we're doing? Who will it benefit?"

Wim Sijstermans: For me, lean IT provided the missing link between management and employees, and it put our clients at the center of our work. When we started our transformation efforts, much of the process was driven from the top. It was very much top-down. With lean, there is a direct link between the manager and the employee. Lean IT helps us bring the energy back to the professionals on the shop floor; it helps us create innovation, because the real ideas originate from the shop floor.

McKinsey on Government: *How have employees on the shop floor responded to lean IT?*

Peter Veld: Frankly, a few still have no confidence in it whatsoever. There are managers who were relatively remote from the shop floor who now have to address their staff daily—and for some of them it's quite upsetting. You can send e-mails from a far-off region of the country, but if you have to actually face the troops, it's a different story. And then there are people who initially say, "I already have so much work to do, and now I have to do this, too." I have heard managers say, "This is quite difficult because we have to work on it every day. It's like a straitjacket. It just goes on and on; it's not a matter of a week's hard work and then you're done." Lean IT is very demanding, and it means a change in attitude and behavior for many.

I must admit that initially I was skeptical that IT professionals—developers and technical whizzes—would ever embrace lean IT; I thought they might find the methods too childish. But more and more, employees are seeing the fruits of their efforts and the positive effects of lean IT. They are realizing that lean IT increases customer satisfaction and allows them to share best practices and solve problems more quickly. They see that those who take initiative are rewarded. At the same time, though, they see that performance is now transparent—there's nowhere to hide, and some people find that frightening, even threatening.

I actually think the intensive work methods of lean IT will appeal to the employees of the future. I think the younger generations want varied work, and they want to be challenged to meet targets and demonstrate their capabilities. Lean IT will make work more attractive to them.

McKinsey on Government: *These are major changes: a restructured IT organization, a phased approach to IT project management, and lean IT. How do you know these changes are working?*

Peter Veld: We're already spending less; we've cut costs by about 15 percent. We make far fewer errors. We have better control over projects and more transparency. The public has noticed all this as well—people tell us that they sense things are going much better at the tax authority. Other agencies approach us and say, "We know you're doing well because we haven't read anything negative in the newspapers." Newspapers don't carry positive reports, only negative ones—so not being in the newspapers is the best you can do.

McKinsey on Government: *Congratulations on these successes. Is there any part of the IT transformation effort that you feel hasn't been successful?*

Wim Sijstermans: We wanted to get our portfolio management on track much sooner, but we found that we just didn't have the insights—the metrics, the standards, the data—to be able to estimate how long a project would take or how

much it would cost. We didn't have the historical information we needed to help us make accurate predictions and build sound business cases. We also lacked a certain degree of professionalism. We didn't have enough managers with IT knowledge. So, portfolio management has been a rather difficult and often disappointing process.

But we've taken meaningful steps. In the past two years, we've doubled the number of managers with IT knowledge. When I first started working here, the month of April would come along and we would still be discussing that calendar year's portfolio because we just couldn't reach consensus—whereas now we have insight into the next six quarters. We're making good progress, but we've still got quite a bit of work to do.

McKinsey on Government: *Aside from continuing to work on portfolio management, what are your ambitions for the next year or two?*

Wim Sijstermans: We have three priorities. The first is to further strengthen the foundation—this includes better coordination of supply and demand, and continued investment in our people. We need to attract new talent; we need to build skills and, just as important, we need to retain the people who are good at what they do. We can't hire 3,000 new people; we need some of our longest-tenured employees to keep doing what they've always done very well. We want to honor those people.

Our second priority is acceleration. If we want to reduce our operational costs quickly, we need to speed up the process of providing products and services to our colleagues and to citizens. We believe acceleration will require us to work in multidisciplinary teams more often—we need to continue to bring business and IT together.

The third priority is innovation. There is no continuity without innovation. One of our biggest initiatives in this area is digitization—we want to provide more of our services online and replace the paper communications we send to citizens with digital communications. Specifically, we want to develop a personal Web domain name for every individual taxpayer, and we believe we can do this within a few years. We already provide this service for the business community. Providing more digital services for private citizens will make it much easier for taxpayers to deal with the tax authority.

McKinsey on Government: *Digitization will clearly benefit citizens. How will it benefit the tax authority?*

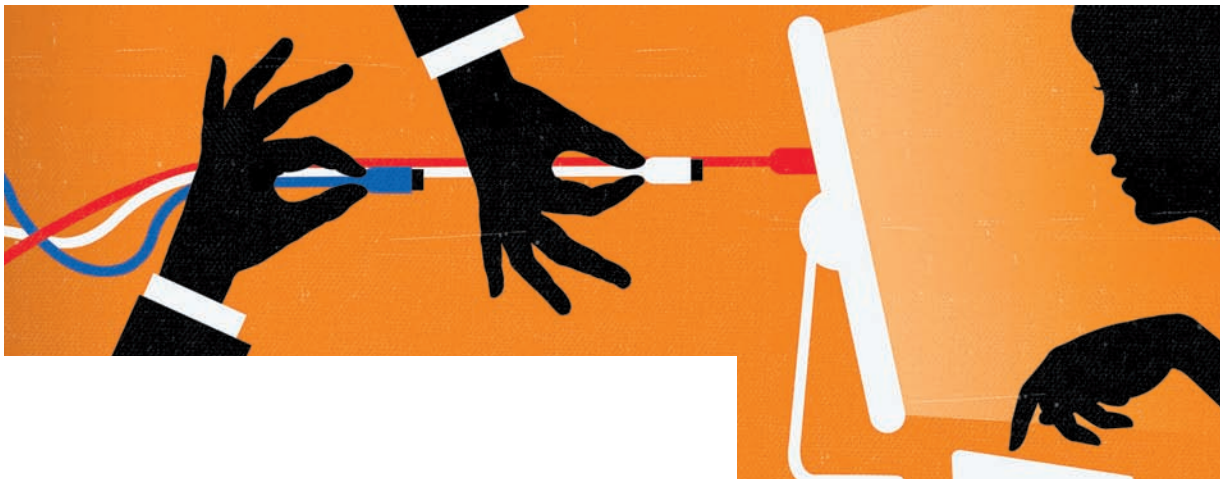
Peter Veld: It will allow us to do our work faster and more efficiently. Right now, even though 95 percent of citizens' tax returns are submitted digitally, our provisional assessments are 100 percent paper based, which costs a lot of money. We have to buy the paper, the envelopes, the postage—it's a huge business case in its own right—but aside from the direct costs, there are indirect costs to both the tax authority and the taxpayer. The fact is, paper assessments lead to more questions, which means more telephone calls, more complaints, and more objections lodged.

McKinsey on Government: *As you tackle the priorities you've just outlined—strengthening the foundation, accelerating the provision of products and services, and innovating—*

are there any lessons you've learned in your IT transformation journey that you can apply going forward?

Peter Veld: One thing that has made a real difference to us is outside input. We opened up our organization and let in a lot more outside influences, thus giving our employees many more opportunities to learn. And we found that, regularly, someone would say, "You think the problem is *x*, but actually you should be looking at *y*."

Wim Sijstermans: Some employees at the Dutch tax authority have been there for many years, so it's helped us to have people from the outside world say to us, "You can also do it this way." That said, our people are our greatest asset. I have the privilege to work with professionals who are dedicated to their work and to the tax agency. We need to leverage their knowledge and capabilities, and to enhance their knowledge where needed. By working closely together and always putting the customer at the center, we can create a great future for our agency and add a lot of value for our citizens and businesses in the Netherlands.



Robert Carsouw is a principal in McKinsey's Amsterdam office, where **Wopke Hoekstra** is an associate principal and **Joris Hulst** is a consultant. Copyright © 2011 McKinsey & Company. All rights reserved.