

I n f o r m e d C I O

Presented in conjunction with

InformationWeek
Government

Cloud Compliance in Government

Compute clouds in federal government data centers must adhere to a range of requirements aimed at security, privacy and other areas of governance. In this report, the third in a four-part series on government clouds, we assess the key specs that need to be factored into federal cloud architecture.

By J. Nicholas Hoover



T
A
B
L
E
O
F
C
O
N
T
E
N
T
S

- 3 Author's Bio
- 4 Executive Summary
- 5 Research Synopsis
- 6 Cloud Compliance in Government
- 6 What Compliance Issues Are Raised by Cloud Computing?
- 7 Figure 1: Benefits of Private Clouds for Federal Government
- 8 How Do We Stay True to FISMA?
- 8 Does the FISMA Comprehensive Risk Management Framework Apply to Cloud Computing?
- 9 How Do We Manage C&A in the Cloud?
- 10 How Do Multi-Tenancy and Virtualization Complicate Things?
- 11 Figure 2: Sources Influencing Private Cloud Architecture
- 11 What Are the Issues Around Cloud Storage?
- 12 Do Export Control Regulations Apply?
- 13 How Are Things Different for the Department of Defense?
- 14 What About Other Specifications and Regulations?
- 14 Are There Potential Gotchas?



Nick Hoover is a senior editor covering IT strategy and implementation in federal, state and local government for *InformationWeek* and *InformationWeek Government*. Nick joined *InformationWeek* in 2005, writing about networking, voice over IP, government policy, collaboration tools and covering the Microsoft beat. Nick was a graduate student in journalism at American University, where he was a general assignment intern for the *Washington Examiner* and news editor of an online magazine at American. He's a resident of Baltimore and travels to Washington, D.C., regularly to meet with federal agency CIOs and attend industry events.



Compliance can easily become a headache, especially when dealing with new technologies. New paradigms mean new twists on old questions about security, access, privacy and more. Nowhere has the head-scratching on compliance been as heavy as late as in cloud computing. From the Federal Information Security Management Act to the Export Administrative Regulations, compliance in the cloud requires a fresh analysis.

Among the key compliance concerns, FISMA likely looms largest: 80% of *InformationWeek* survey respondents placed assuring security of systems and data among the top three biggest issues their organizations face in moving ahead with cloud computing. Agencies will have to ensure that, among other things, cloud computing deployments meet system authorization requirements and can be continuously monitored. Multi-tenancy, virtualization, transparency by service providers, encryption and identity management all take on new roles in cloud compliance. A new General Services Administration-led process, known as FedRAMP, could soon simplify this process greatly, taking much of the hard work out of agencies' hands.

Records management could also pose new challenges, especially with public clouds. For example, since another agency or third party may be hosting agency data, records retention policies have to be explicitly laid out and followed by that third party, and safeguards have to be put in place to ensure an agency can get its data out when that's required.

There are other compliance implications as well. Export control regulations might require deep analyses of any data agencies allow to be hosted in overseas data centers; the Department of Defense has its own set of compliance requirements; and everything from the Health Insurance Portability and Accountability Act to the Federal Educational Rights and Privacy Act might apply, depending on circumstances.



Research Synopsis

Survey Name: *InformationWeek Analytics/InformationWeek Government Federal Government Cloud Computing Survey*

Survey Date: March 2010

Region: United States

Number of Respondents: 216

Purpose:

To determine and capture interest in the role of private clouds in federal agencies.

Methodology:

InformationWeek Analytics surveyed business technology decision-makers at U.S. federal government agencies. The survey was conducted online, and respondents were recruited via an e-mail invitation containing an embedded link to the survey. The e-mail invitation was sent to qualified *InformationWeek* and *InformationWeek Government* newsletter subscribers.

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

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



Cloud Compliance in Government

Compute clouds in government data centers must comply with a range of requirements designed to support data and system security, privacy, and other important areas of IT governance. In this report, the third in our four-part series on cloud computing in government, we explore the compliance issues that must be considered as federal agencies push ahead with cloud computing strategies.

The Federal Information Security Management Act looms large, with 80% of respondents to a recent *InformationWeek Government* survey pointing to security as one of the three biggest issues their organizations face in moving ahead with cloud computing. Multi-tenancy, virtualization, encryption and identity management are some of the technologies that affect cloud security and compliance. A new General Services Administration-led process, the Federal Risk and Authorization Management Program (FedRAMP), promises to simplify the certification and accreditation process, but it's still in the early stages.

“The overarching issue with cloud computing is not really about any particular technology but instead about the federal government being able to meet security requirements in a complete, coherent and consistent fashion and express them in context with the environment,” says Ron Ross, senior computer scientist with the National Institute of Standards and Technology and head of NIST's FISMA implementation project.

Records management could pose new challenges, especially in public clouds. Since another agency or third party may be hosting an agency's data, records retention policies have to be explicitly laid out and followed by that third party, and safeguards must be put in place to ensure the agency can get its data out of the service provider's cloud when required.

In addition, export control regulations limit the hosting of data in overseas data centers, the Department of Defense has its own set of compliance requirements, and everything from the Health Insurance Portability and Accountability Act to the Federal Educational Rights and Privacy Act can apply in some the circumstances.

The following analysis is intended to help government IT pros develop a cloud computing strategy that meets the many government requirements that come into play.

What compliance issues are raised by cloud computing? Name the compliance requirements that apply to government IT systems, and most apply to cloud computing, too. “In general, compliance is not any different in the cloud,” says Katie Lewin, director of the



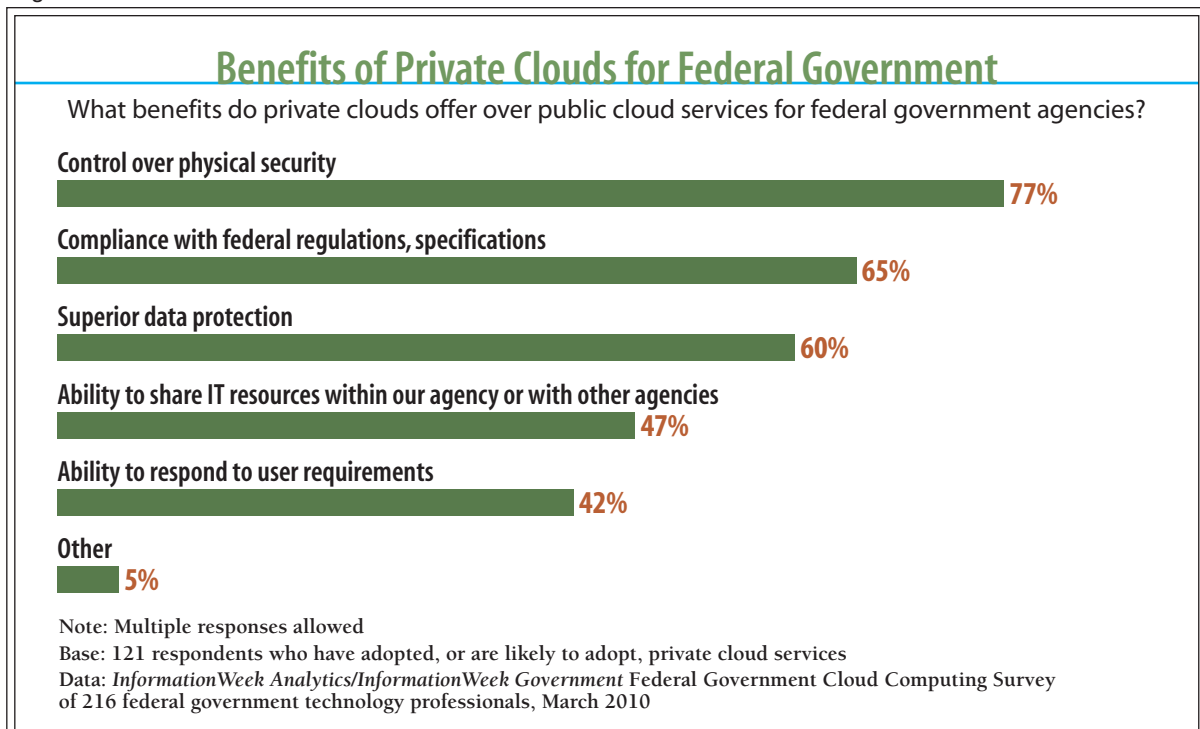
General Services Administration’s cloud computing program. “Agencies are still going to have to consider the same statutes and regulations. And, as applicable, they’ll still have to be complied with.”

Likewise, the questions government IT pros need to ask as their agencies move into the cloud will often be the same as those related to on-premises systems, says Tim Grance, program manager for cyber and network security at the NIST.

If and when agencies consider cloud services offered from outside their own data centers (as opposed to services made available from their own private clouds), that means seeking information from cloud service providers on issues that would normally be baked into their in-house systems, such as FISMA-related security controls and records management policies.

One of the things that government IT pros like about the private cloud model is that it’s easier for them to comply with federal regulations. In a survey of 216 government IT pros by *InformationWeek Government*, 65% of respondents indicated that compliance with federal

Figure 1





regulations and specifications was one of the benefits that private clouds offer over public cloud services. In fact, compliance was second only to control over physical security among the benefits.

When agencies move existing applications to public cloud services, some of the compliance requirements may already pass muster. For example, when the Recovery and Transparency Board moved the Recovery.gov site to Amazon's Elastic Compute Cloud, it simply moved an existing, government-approved system into the cloud. "We started with a physical environment, so we knew what the baseline configurations were for everything and had already done a certification and accreditation package," says Rob Groat, CTO for Smartronix, the lead contractor on Recovery.gov. That up-front work, says Groat, made the compliance effort associated with the EC2 move much easier.

How do we stay true to FISMA? Security is government agencies' No. 1 concern in the cloud, so it's little surprise that FISMA represents the biggest compliance issue that government IT pros face. In fact, 80% of respondents to our survey placed security as one of the top three issues in moving ahead with cloud computing, though only 19% say their organization has completed a review of cloud computing's security implications.

Such reviews aren't simple. FISMA comprises 18 control families and more than 120 individual controls that need to be assessed in determining whether a system is secure. Controls range from those that deal with the personnel accessing systems (i.e., the trustworthiness of a service provider's system administrators) to contingency planning (i.e., what's the back-up plan if a provider goes out of business).

Cybersecurity in government is being closely monitored by the public and Congress. "There's no negotiating on FISMA," says Robert Ames, deputy CTO for IBM's federal business. "It's not something you can't have and continue to do business with government. FISMA is the biggest hurdle to the cloud that is discussed most freely and most broadly."

Does the FISMA comprehensive risk management framework apply to cloud computing?

Yes, NIST's risk management framework, a six-step risk management concept, is key to FISMA compliance, and can help place FISMA within the cloud construct. The first step in the framework, categorization, requires agencies to ask what information is being sent to the cloud or cloud provider, and classify it as low, moderate or high risk depending on how secure it needs to be.



Second, agencies must select security controls. Normally, agencies would build these controls themselves, but with a cloud operated by a third party, the user of the cloud would need to ensure those controls make it into the contract language. Vendors then take the third step of implementing the controls. It's up to the user to ask vendors to prove that they've been implemented or at least detail how they've been implemented.

Next, someone must confirm that the controls are properly and effectively in place. Here, an independent assessment is likely to be more trustworthy than an assessment done by the government or the service provider, NIST's Ross says. Fifth, agencies must authorize the system to operate based on the assessment. In general, this will be something that agencies will be able to do on their own or through the emerging FedRAMP process.

Finally, continuous monitoring needs to take place now that the systems are authorized and operating. This can be a challenge if it isn't your cloud. "All these service providers understand security, too, and want to do the right thing," Ross says. "But you need to say, here's the info we need back and here's the frequency we need to see the information." There's still a learning curve for vendors in terms of what information they should be giving to their government customers and how often, Ross says.

How do we manage C&A in the cloud? For now, agencies will have to continue managing existing certification and accreditation processes for cloud computing. Once official, FedRAMP will be a government-wide risk management program that should significantly decrease the amount of FISMA compliance work agencies must do to get up and running on cloud services by allowing them to leverage previous authorizations and eventually by providing ongoing risk assessments and continuous monitoring.

FedRAMP is still in development. Microsoft and Google are putting their services through the process as part of the pilot program, while GSA and NIST, which helped build the process, are evangelizing it.

FedRAMP takes advantage of the fact that NIST Special Publication 800-37 defines three approaches to IT authorizations, one of which is leveraged authorization. Where one agency has already authorized a system and another wants to use the same system, it can do so, as long as it works to manage risks unique to itself. "This can save a huge amount of money for taxpayers," says Ross.



Among the roadblocks to leveraged authorization have been agencies' vastly different security requirements. In short, different agencies want and need different controls. "One agency's FISMA-moderate is different from some other agency's FISMA-moderate, so you could end up in this never-ending cycle to be stamped with approval," says IBM's Ames. Such inconsistencies break the cloud computing model, characterized by economies of scale and efficiency.

Civilian, defense and intelligence agencies have all been engaged in the creation of FedRAMP, giving it a wide base of support. Even if an agency doesn't want to entrust its entire certification to FedRAMP, it can leverage FedRAMP for part of the process. In other words, FedRAMP can do some of the job, and the agency can answer additional questions on its own.

FedRAMP can be used for public cloud services or private clouds. With private clouds, multiple agencies might get together to work on compliance early in the development process to define the controls they want employed.

How do multi-tenancy and virtualization complicate things? A common question around cloud computing is whether multi-tenancy—an architectural approach where multiple users, departments or customers share the same server—can be FISMA-compliant, since FISMA addresses access control. "We're not only concerned with how folks should have access to the cloud," says Ross. "When we're in the cloud, you still need to have separation of data."

The answer is, yes, it is possible for a multi-tenant server to be made FISMA-compliant through use of robust virtual partitions. "You just have to ask more serious questions as the data goes from low to moderate to high security impact," Ross says. "It's about how difficult it would be to subvert the mechanisms that separate users. As the data becomes more sensitive, the requirements in term of multi-tenancy are going to become more stringent."

The issue is that hypervisors replace physical space between servers and firewalls with logical separation. "In a virtual or multi-tenant environment, you may have to incorporate compensating controls," says Smartronix' Groat. "The biggest challenge is understanding the boundaries and defining the boundaries and the controls around that."

Government IT pros should check whether the hypervisor manufacturer allows third-party code in its hypervisor, what its software assurance practices are and what controls can be built around the hypervisor to deny cross-boundary attacks. Note that some private clouds, though

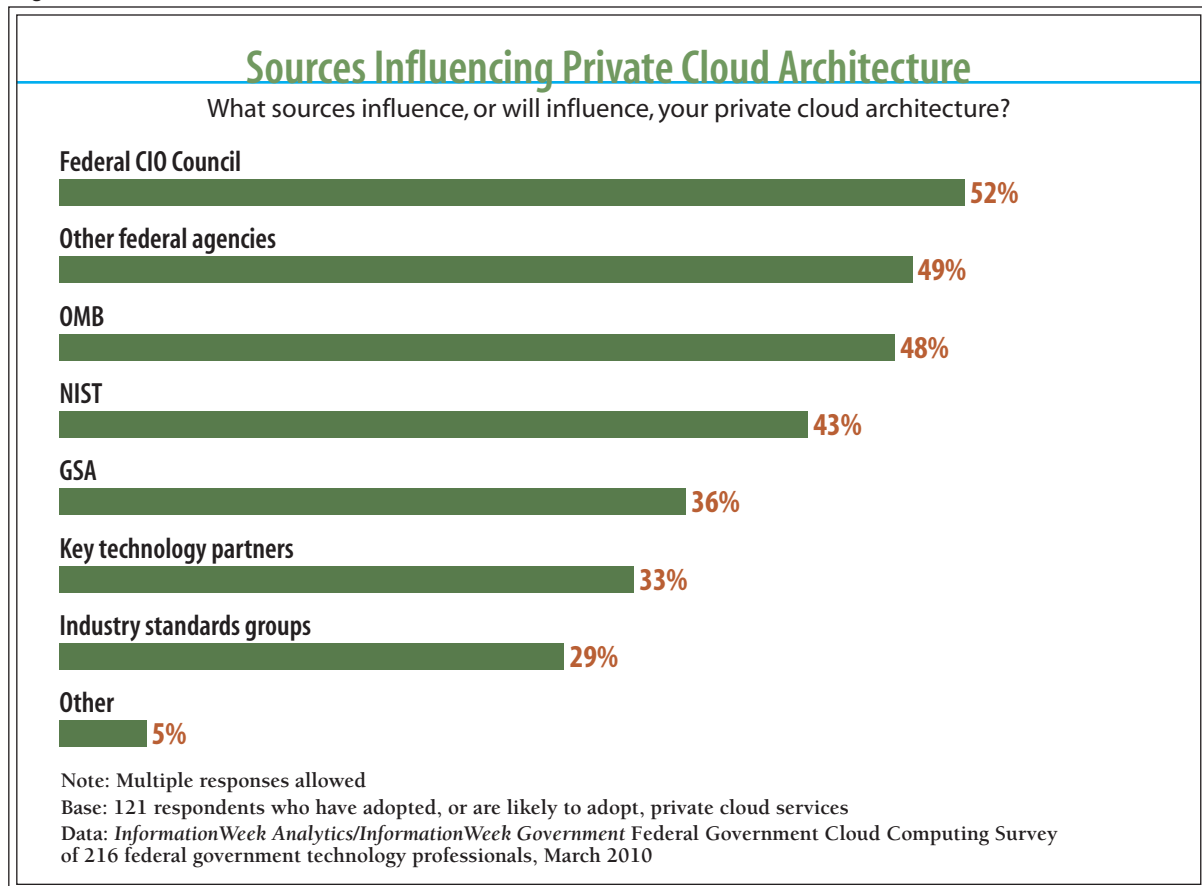


virtualized, don't use multi-tenancy. Some public cloud providers, like Microsoft, offer dedicated tenant versions of their services to ameliorate concerns.

When it comes to architectural decisions that influence how private clouds are built, government IT pros tend to look to policy makers within federal government, such as the Federal CIO Council, and other government agencies, for guidance rather than industry sources, according to our survey.

What are the issues around cloud storage? As with other IT systems, private and public clouds, because they handle government data, must comply with federal records management regulations, including title 44 of the U.S. Code and parts of title 36 of the Code of Federal Regulations.

Figure 2





In general, records management for cloud computing is just like records management for other IT systems. Agencies must define what will be a record by determining what constitutes an important business asset to the agency. And records can't be destroyed without permission from the National Archives and Records Administration, often until a specified period has passed, though more rarely records may be permanent.

However, records management in the cloud poses new challenges, as another agency or third-party service provider may host the data. For example, where there is a multi-agency private cloud, such as the Department of the Interior's National Business Center, one agency may have physical custody of the records via ownership of the servers, but another owns the data.

If that's the case, says Arian Ravanbakhsh, electronic records policy specialist for the National Archives and Records Administration, the questions that need to be asked include: Who's responsible for ensuring record-keeping? How are records disposed? And, can data be easily retrieved? The discussion should include details about what records need to be created and maintained and how the parties will do so, he says.

In terms of data deletion, an agency must know if there's one or multiple copies of the data, and whether the cloud provider (commercial or another government agency) can implement data retention and deletion as required.

Then there's the matter of data retrieval. Say your agency contracts with a cloud provider to store some data that's part of a laboratory experiment. Can you get that data out when the experiment ends or if you want to switch cloud service providers? "A lack of portability standards may result in difficulty removing records for record-keeping requirements or complicate the transition to another environment," warns a NARA FAQ on records management in the cloud.

Prescriptive guidance for meeting regulatory requirements isn't in place yet. NARA issued a basic records management FAQ on cloud computing, and plans to issue a bulletin in August that will address key issues in greater detail. It has also issued guidance on how to manage records in multi-agency environments.

Do export control regulations apply? Public cloud providers may have data centers overseas. That can raise concerns about whether an agency is complying with export control regulations.

There are laws that determine what kind of data can be stored or sent overseas. Under the



Export Administrative Regulations (EAR) and the International Trafficking in Arms Regulations (ITAR), certain “controlled technical data” can’t be sent to foreign nations. Violations carry penalties of up to \$1 million.

Controlled technical data is basically the how-to information for manufacturing, developing, producing and using a controlled product. There are many controlled items, from tanks to electronics. For example, under ITAR, there’s a munitions list of controlled items, and within that list are categories for, say, vessels of war.

Government IT pros need to keep a line of communication open with compliance officers who might deal with export controls. There’s often a disconnect between the two, and determining just what’s controlled data is typically a work-intensive process, says Eric McClafferty, a partner with law firm Kelley Drye & Warren LLP. “If you’re not looking behind the door at what different services do, your data could be stored God knows where offshore,” he says. “If that’s the case, there’s a possibility that there are going to be a lot of export violations.”

While EAR and ITAR can both be tricky and carry fines, the key is to work with vendors to ensure your data doesn’t get stored in an off-shore data center. Most cloud service providers—Amazon, Microsoft and Google among them—will ensure your data stays in the continental U.S. upon request. That’s a much simpler task than trying to pour through all your data and determine what’s export-controlled and what isn’t.

How are things different for the Department of Defense? The Department of Defense has additional security requirements. Systems must be certified under the DoD Information Assurance Certification and Accreditation Process, or DIACAP, and classified or top-secret systems carry their own requirements.

DoD cloud services and applications must interoperate with the DoD’s Common Access Card authentication processes. Contractors working on DoD clouds must comply with requirements of the DoD’s Information Assurance Workforce Improvement Program. Configurations need to meet DoD security guidelines under the Security Technical Implementation Guides. And DoD, even more than other agencies, has to be careful to comply with export control guidelines.

With the aid of Booz Allen Hamilton, the Defense Information Systems Agency has worked to streamline the security accreditation process for applications running within its Rapid Access



Computing Environment, or RACE, a private cloud. DISA leverages the use of standardized system configurations and enables users to inherit security controls directly from the underlying and pre-existing architecture, eliminating the need for duplicative certification efforts. It also uses the DoD's Enterprise Mission Assurance Support Service (eMass), a certification workflow automation tool, and now even has an internally developed cloud certification service called CertificationForge.

What about other specifications and regulations? One compliance regime certain cloud deployments may be subject to is the Health Insurance Portability and Accountability Act (HIPAA), which requires, among other things, agencies to ensure the privacy of patient data. This will become key for agencies like the Department of Veterans Affairs and the Department of Health and Human Services as they begin to use cloud computing.

Other possibly applicable requirements include Section 508 compliance for accessibility and compliance with the Federal Educational Rights and Privacy Act to ensure the privacy of student education records.

Though other certifications and compliance specifications like SOX, ISO 270001 or SAS 70 aren't necessarily for the government, vendors will tell you that their products and services meet the standards for SAS 70 or ISO 270001. Those certifications can be helpful, but only to a point. For example, some aren't as prescriptive as FISMA. "SAS 70 can be about anything," says NIST's Grance. "The more important question is, 'What did the auditors ask?'"

That said, there's value in assessing the full scope of compliance frameworks and leveraging commonality where possible. Microsoft has mapped across the different security requirements, noting that many of the controls for Sarbanes-Oxley and HIPAA are the same as controls found in FISMA.

Are there potential gotchas? The first isn't obvious: transparency. Unlike computer systems in an agency's data center, which can be inspected directly, private or public clouds run by third parties will require some degree of openness on the part of the service provider as a way of validating their controls.

Microsoft, for example, provides data center tours, explains its security processes, and discloses how and when security audits are conducted. It also plans to share its 500 pages of informa-



tion on FISMA compliance for its Business Productivity Online Suite with federal customers. Similarly, Smartronix says Amazon provided it with necessary information as it migrated Recovery.gov to the cloud. However, not all service providers are equally accommodating; the CTO of one federal agency told me that he's been turned down for data center tours by cloud service providers because they didn't have the staff to conduct them.

Encryption is another potential issue. Federal agencies are increasingly using encryption to meet the requirements of Federal Information Processing Standard Publication (FIPS) 140-2, but that poses a challenge in the cloud, says Microsoft Federal's chief security officer Bill Billings. "I can verify my servers are using FIPS-compliant software, but I can't tell if the client is FIPS-compliant," Billings says. "In a cloud environment, I can only manage the server side, but I can't manage the client side."

The concept of Network Access Protection, which blocks non-compliant clients from accessing servers until their security gaps are remediated, hasn't yet extended to the public cloud environment.

Another challenge in the cloud is identity and access management. "You don't want to have all different kinds of identity management schemes in the cloud," says NIST's Grance. "However, customers also want federation of identity with their own systems."

Those two goals—economy of scale and consistency and integration with in-house systems—are potentially at odds. It's an issue that remains to be fully solved. In one sign of progress, Microsoft is working to integrate the federated identity services available through its Azure platform-as-a-service into its other cloud offerings.