GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Snapshot

Cloud Computing: Federal Agencies Face Four Challenges

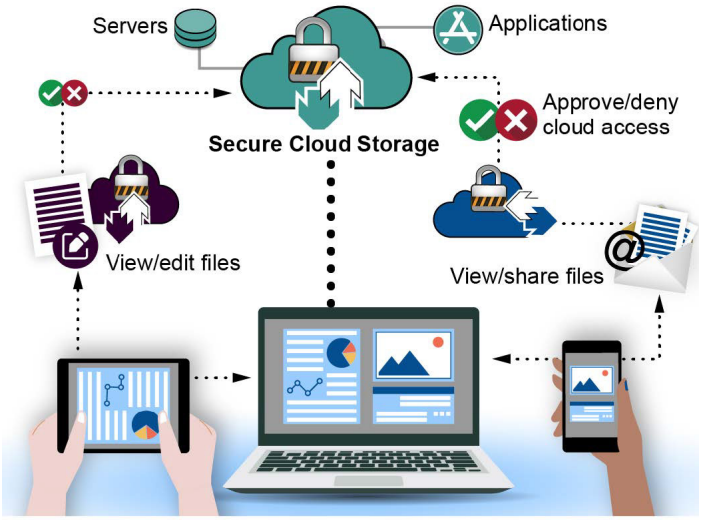
GAO-22-106195 · September 2022

As the federal government transitions to cloud computing, agencies face challenges in four areas: ensuring cybersecurity, procuring cloud services, maintaining a skilled workforce, and tracking costs and savings. Our work in these areas—and the implementation of our recommendations—can help agencies overcome these challenges.

The Big Picture

Federal agencies plan to spend billions of dollars each year to support their IT and cybersecurity efforts, including transitioning IT resources to secure, cost-effective commercial cloud services. Federal agencies can use cloud computing to access IT resources—such as servers that store digital files—through the Internet faster and for less money than it would take to own and maintain such resources.

Illustration of a cloud computing environment



Source: GAO; images: ST.art/stock.adobe.com. | GAO-22-106195

What GAO's Work Shows

Our body of work highlights four main challenges related to the federal government's adoption of cloud services and our recommendations for improvement. Federal agencies have not fully implemented all of the recommendations.

1. Ensuring Cybersecurity

In 2011, the Office of Management and Budget (OMB) established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach for selecting and authorizing the use of cloud services that meet federal security requirements.

In December 2019, we reported that, while all 24 major federal agencies were participating in FedRAMP, many of these agencies continued to use cloud services that were not authorized through the program. In addition, the four major agencies we selected for a detailed review did not always:

- include required information in their cloud system's security plans;
- summarize security control test results in security assessment reports; and
- identify required information in remedial action plans that are to list cloud service deficiencies and how they will be mitigated.

We found that one cause of these weaknesses was that FedRAMP's requirements and guidance on implementing these control activities were not always clear and the program's process for monitoring the status of security controls over cloud services was limited.

➢ **We recommended** that OMB hold agencies accountable for authorizing cloud services through FedRAMP. We made an additional 24 recommendations to federal agencies related to improving the implementation of the FedRAMP program, including clarifying guidance on program requirements and responsibilities.

2. Procuring Cloud Services

An important part of procuring cloud services is incorporating a service level agreement into the

contract. These agreements define the level of service and performance that the agency expects the contractor to meet. In April 2016, we reported that five of the major agencies that we selected for review did not always incorporate key practices for these agreements in their cloud service contracts. For example, the agencies did not always specify:

- what constitutes a security breach and the responsibilities for notifying the agency;
- how data and networks will be managed; and
- the range of enforceable consequences for non-compliance with the agreement.

This was primarily due to the lack of guidance that fully addressed the key practices.

➢ **We recommended** that four of the agencies develop guidance that fully incorporates the key practices and that the fifth agency update its guidance to include all of the key practices.

3. Maintaining a Skilled Workforce

Having skilled IT personnel is key to supporting the federal government's cloud adoption efforts.

Illustration of a cloud computing workforce

Source: apinan/stock.adobe.com. | GAO-22-106195

Nonetheless, we reported cloud-related workforce challenges at three federal agencies.

- The Coast Guard did not include new cloud-related skills and a skills gap analysis for cloud personnel in its workforce development strategy.
- The Department of Defense (DOD) did not strategically plan for communicating with employees to prepare them for changes that would occur due to the move to cloud services.
- The Department of State's strategic plan did not include performance measures, targets, or goals to monitor progress towards clarifying job responsibilities and requirements needed to support the cloud environment.

➢ **We recommended** that the Coast Guard, DOD, and the Department of State take actions by updating their strategic plans to address the workforce issues related to cloud computing.

4. Tracking Costs and Savings

Federal policies and guidance have stressed the importance of reducing acquisition and operating costs by purchasing cloud services through the adoption of cloud computing. However, in April 2019, we reported that federal agencies experienced challenges in tracking and reporting cloud spending and savings data. For example, federal agencies were often using inconsistent data to calculate cloud spending and were not clear about the costs they were required to track. In addition, agencies had difficulty in systematically tracking savings data and expressed that OMB guidance did not require them to explicitly report savings from cloud implementations. We reported that, as a result, it is likely that agency-reported cloud spending and savings figures are inaccurate.

➢ **We recommended** that OMB require agencies to explicitly report cloud savings, and that agencies establish a repeatable mechanism to track cloud savings and avoidances.

More from GAO's IT Portfolio

Cybersecurity

Information Technology

Information Management

About GAO:

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. This document is based on GAO audit products. This work of the United States may include copyrighted material, details at https://www.gao.gov/copyright.

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.

U.S. Government Accountability Office, 441 G Street NW, Washington, DC

Contact Us

For more information about this Snapshot, contact: Jennifer R. Franks, Director, Information Technology & Cybersecurity, (404) 679-1831

Chuck Young, Managing Director, Public Affairs, (202) 512-4800

A. Nicole Clowers, Managing Director, Congressional Relations, (202) 512-7114

Contributors: Chris Businsky, Donna Epler, Nicole Jarvis (assistant director), and Di'Mond Spencer (analyst-in-charge)

Source (cover photo): Gorodenkoff/stock.adobe.com