

Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing

GAO-10-513 May 27, 2010

[Highlights Page](#) (PDF) [Full Report](#) (PDF, 53 pages) [Accessible Text](#)
[Recommendations](#) (HTML)

Summary

Cloud computing, an emerging form of computing where users have access to scalable, on-demand capabilities that are provided through Internet-based technologies, has the potential to provide information technology services more quickly and at a lower cost, but also to introduce information security risks. Accordingly, GAO was asked to (1) identify the models of cloud computing, (2) identify the information security implications of using cloud computing services in the federal government, and (3) assess federal guidance and efforts to address information security when using cloud computing. To do so, GAO reviewed relevant publications, white papers, and other documentation from federal agencies and industry groups; conducted interviews with representatives from these organizations; and surveyed 24 major federal agencies.

Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. They include a private cloud, operated solely for an organization; a community cloud, shared by several organizations; and a public cloud, available to any paying customer. Cloud computing can both increase and decrease the security of information systems in federal agencies. Potential information security benefits include those related to the use of virtualization, such as faster deployment of patches, and from economies of scale, such as potentially reduced costs for disaster recovery. Risks include dependence on the security practices and assurances of a vendor, dependency on the vendor, and concerns related to sharing of computing resources. However, these risks may vary based on the cloud deployment model. Private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation. Federal agencies have begun efforts to address information security issues for cloud computing, but key guidance is lacking and efforts remain incomplete. Although individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance. For example, only nine agencies reported having approved and documented policies and procedures for

writing comprehensive agreements with vendors when using cloud computing. Agencies have also identified challenges in implementing existing federal information security guidance and the need to streamline and automate the process of implementing this guidance. These concerns include having a process to assess vendor compliance with government information security requirements and the division of information security responsibilities between the customer and vendor. Furthermore, while several governmentwide cloud computing security initiatives are under way by organizations such as the Office of Management and Budget (OMB) and the General Services Administration (GSA), little has been completed as a result of these efforts. For example, OMB has not yet finished a cloud computing strategy. GSA has begun a procurement for cloud computing services, but has faced challenges in completing the procurement due in part to information security concerns. In addition, while the Department of Commerce's National Institute of Standards and Technology has begun efforts to address cloud computing information security, it has not yet issued cloud-specific security guidance. Until specific guidance and processes are developed to guide agencies in planning for and establishing information security for cloud computing, they may not have effective information security controls in place for cloud computing programs.

Recommendations

Our recommendations from this work are listed below with a Contact for more information. Status will change from "In process" to "Open," "Closed - implemented," or "Closed - not implemented" based on our follow up work.

Director: Gregory C. Wilshusen

Team: Government Accountability Office: Information Technology

Phone: (202) 512-6244

Recommendations for Executive Action

Recommendation: To assist federal agencies in identifying uses for cloud computing and information security measures to use in implementing cloud computing, the Director of OMB should establish milestones for completing a strategy for implementing the federal cloud computing initiative.

Agency Affected: Executive Office of the President: Office of Management and Budget

Status: In process

Comments: When we confirm what actions the agency has taken in response to this recommendation, we will provide updated information.

Recommendation: To assist federal agencies in identifying uses for cloud computing and information security measures to use in implementing cloud computing, the Director of OMB should ensure the strategy addresses the information security challenges associated with cloud computing, such as needed agency-specific guidance, the appropriate use of attestation standards for control assessments of cloud computing service providers, division of information security responsibilities between customer and provider, the shared assessment and authorization process, and the possibility for precertification of cloud computing service providers.

Agency Affected: Executive Office of the President: Office of Management and Budget

Status: In process

Comments: When we confirm what actions the agency has taken in response to this recommendation, we will provide updated information.

Recommendation: To assist federal agencies in identifying uses for cloud computing and information security measures to use in implementing cloud computing, the Director of OMB should direct the Chief Information Officer (CIO) Council Cloud Computing Executive Steering Committee to develop a plan, including milestones, for completing a governmentwide security assessment and authorization process for cloud services.

Agency Affected: Executive Office of the President: Office of Management and Budget

Status: In process

Comments: When we confirm what actions the agency has taken in response to this recommendation, we will provide updated information.

Recommendation: To assist federal agencies in selecting and acquiring precertified cloud computing products and services, the Administrator of GSA, as part of the procurement for infrastructure as a service cloud computing technologies, should ensure that full consideration is given to the information security challenges of cloud computing, including a need for a shared assessment and authorization process.

Agency Affected: General Services Administration

Status: In process

Comments: When we confirm what actions the agency has taken in response to this recommendation, we will provide updated information.

Recommendation: To assist federal agencies in implementing appropriate information security controls when using cloud computing, the Secretary of Commerce should direct the Administrator of National Institute of Standards and Technology (NIST) to issue cloud computing information security guidance to federal agencies to more fully address key cloud computing domain areas that are lacking in SP 800-53, such as virtualization, data center operations, and portability and interoperability, and include a process for defining roles and responsibilities of cloud computing service providers and customers.

Agency Affected: Department of Commerce

Status: In process

Comments: When we confirm what actions the agency has taken in response to this recommendation, we will provide updated information.