



March 2025

# CLOUD COMPUTING

## Private Sector Leading Practices in Acquisition, Cybersecurity, and Workforce Development

# GAO Highlights

Highlights of [GAO-25-106369](#), a report to congressional addressees

## Why GAO Did This Study

Private sector companies spend billions of dollars adopting cloud computing, with the federal government making other substantial investments. Across the private and public sectors, organizations adopt cloud computing solutions to realize a range of potential benefits, such as lowering IT costs. In pursuing these benefits, organizations may also encounter various risks and challenges.

Given the evolving nature of cloud computing, identifying leading practices used by the private sector could provide valuable insights. These insights could help inform federal policymakers and program managers in their efforts to adopt cloud solutions.

This report identifies (1) leading practices in the private sector for adopting cloud solutions and (2) approaches to address challenges in the private sector regarding the adoption of cloud solutions.

GAO reviewed prior work and federal and nonfederal guidance related to cloud computing. GAO then surveyed a nongeneralizable sample of 18 private sector companies identified as leaders in business and technological innovation across multiple industries about their experiences adopting cloud computing solutions. We also asked companies about their approaches for addressing challenges and related technical considerations associated with adopting cloud computing solutions. GAO validated the leading cloud adoption practices by soliciting and incorporating feedback from cloud computing subject matter experts at academic institutions.

For more information, contact Brian Bothwell at (202) 512-6888 or [bothwellb@gao.gov](mailto:bothwellb@gao.gov), or Vijay A. D'Souza at (202) 512-7650 or [dsouzav@gao.gov](mailto:dsouzav@gao.gov).

March 2025

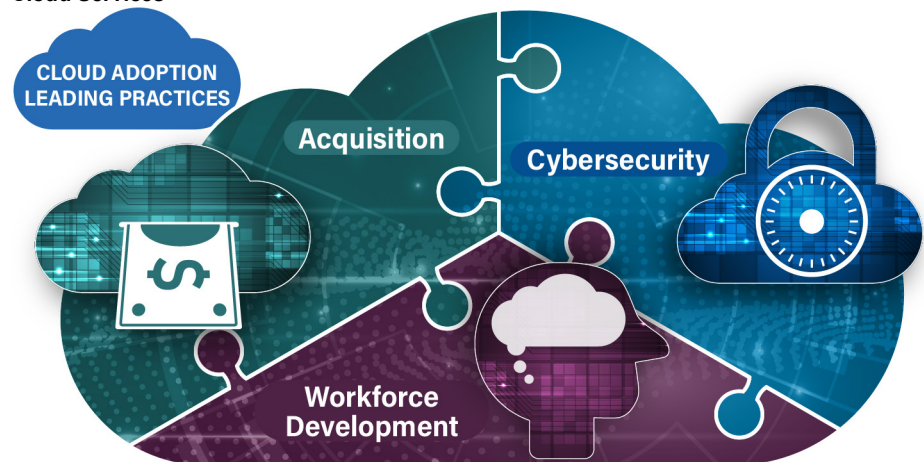
## CLOUD COMPUTING

### Private Sector Leading Practices in Acquisition, Cybersecurity, and Workforce Development

## What GAO Found

Eighteen private sector companies surveyed by GAO reported using the majority of 19 leading practices across three management areas—acquisition, cybersecurity, and workforce development—when adopting and implementing cloud computing solutions. Subject matter experts from academia agreed these are leading practices for cloud adoption, and the majority of companies found them very or extremely important for an effective cloud adoption strategy.

#### Cloud Management Areas Where Companies Reported Using Leading Practices for Adopting Cloud Services



Source: GAO (data and icons); Rabbit\_1990/stock.adobe.com (images). | GAO-25-106369

Examples of leading practices reported by private sector companies included:

- **Acquisition:** Companies reported using 7 leading practices, including defining the business case for the cloud adoption, negotiating clear terms and agreements, and assessing service performance against expectations.
- **Cybersecurity:** Companies reported using 6 leading practices, including implementing incident response procedures, establishing continuous monitoring, and clarifying cloud security responsibilities.
- **Workforce Development:** Companies reported using 6 leading practices, including identifying skill gaps, retaining and recruiting staff, and shifting internal culture.

Companies also identified potential challenges that organizations may encounter when adopting new cloud solutions, including approaches for addressing those challenges and related technical considerations. Companies reported that addressing these technical considerations enhanced flexibility, mitigated risks, and optimized cloud resource utilization. For example, one company reported implementing a multi-cloud strategy early in its migration to a cloud environment, which helped enable flexibility across different providers. However, to realize these benefits, companies reported requiring additional investments, such as in workforce training and cybersecurity tools.

---

# Contents

---

---

Letter		1
	Background	3
	Companies Reported 19 Leading Practices for Adopting Cloud Computing Solutions	10
	Companies Apply Various Methods to Address Cloud Adoption Challenges and Other Technical Considerations	50
	Company Comments	57
Appendix I	Objectives, Scope, and Methodology	59
Appendix II	Survey Questions Administered to Private Sector Companies and Their Responses	65
Appendix III	GAO Contacts and Staff Acknowledgments	77
Appendix IV	Additional Source Information for Images	78
Related GAO Products		79
Tables		
	Table 1: Technical Considerations Related to the Adoption of Cloud Computing Solutions	7
	Table 2: Seven Leading Practices Companies Reported for Acquiring Cloud Solutions	12
	Table 3: Six Leading Practices Companies Reported for Securing Cloud Solutions	26
	Table 4: Six Leading Practices Companies Reported for Developing a Cloud Workforce	40
	Table 5: Potential Challenges Companies Reported for Adopting Cloud Computing Solutions	50
	Table 6: Selected Federal and Nonfederal Cloud Computing Guidance Resources	59

---

---

Table 7: Private Sector Companies that Participated in a 2024 Survey on Cloud Computing Leading Practices	63
---	----

---

Figures

Figure 1: Nineteen Leading Practices that Companies Reported Using for Adopting Cloud Services	11
Figure 2: Security Responsibilities Associated with On-Premises Computing and Each Cloud Service Model	28

---

**Abbreviations**

CEO	chief executive officer
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
FedRAMP	Federal Risk and Authorization Management Program
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IT	information technology
ICAM	Identity, Credential, and Access Management
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PaaS	Platform as a Service
PaC	Policy as Code
Provider	cloud service provider
SaaS	Software as a Service

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 24, 2025

The Honorable Gerald E. Connolly  
Ranking Member  
Committee on Oversight and Government Reform  
House of Representatives

The Honorable Nancy Mace  
Chairwoman  
Subcommittee on Cybersecurity, Information Technology, and  
Government Innovation  
Committee on Oversight and Government Reform  
House of Representatives

The Honorable Jamie Raskin  
House of Representatives

Private sector companies spend billions of dollars adopting<sup>1</sup> cloud computing solutions, with the federal government making other substantial investments.<sup>2</sup> Across the private and public sectors, organizations use cloud computing to realize a range of potential benefits, such as IT cost savings and enhanced scalability. In pursuing these benefits, organizations may also encounter various risks and challenges, such as managing shared cybersecurity responsibilities with the cloud service provider (provider) or maintaining flexibility to change providers as needed.

---

<sup>1</sup>Embracing a new technology generally occurs in two distinct stages: implementation and adoption. While implementation refers to the process of obtaining and activating the new technology, adoption is the process of acceptance and active use of the new technology. For the purposes of this report, adoption will be used to refer to both implementation and adoption stages.

<sup>2</sup>The National Institute of Standards and Technology (NIST) defines cloud computing as “on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” NIST, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145 (September 2011). For the purposes of this report, we use the term “cloud computing solution” to refer to the adoption of one or more cloud resources to meet a particular operational need.

---

Since 2010, major federal agencies have been migrating their data and applications to the cloud.<sup>3</sup> In June 2019, the Office of Management and Budget (OMB) updated its guidance to accelerate agency adoption of cloud solutions.<sup>4</sup> Specifically, OMB’s guidance addressed three key areas—acquisition, cybersecurity, and workforce development—where federal agencies experienced challenges.

Multiple public and private sector organizations have developed cloud guidance, frameworks, and requirements, and applied various practices related to cloud solutions. GAO has found that private sector practices have proven helpful in informing government improvement efforts, such as in IT management and defense acquisitions.<sup>5</sup> Given the evolving nature of cloud computing, identifying leading practices used by the private sector could provide valuable insights.<sup>6</sup> These insights could help inform federal policymakers and program managers in their efforts to adopt cloud solutions.

We prepared this report at the initiative of the Comptroller General. This report identifies (1) leading practices in the private sector for adopting cloud solutions and (2) approaches in the private sector to address challenges regarding the adoption of cloud solutions.

To address these two objectives, we (1) reviewed prior GAO work and federal and nonfederal guidance related to cloud computing to identify potential leading practices in the areas of acquisition, cybersecurity, and

---

<sup>3</sup>In fiscal year 2022, federal agencies obligated about \$7 billion on cloud computing contracts, including approximately \$3 billion by the Department of Defense.

<sup>4</sup>See OMB, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019). OMB refers to these three areas as procurement, security, and workforce. For the purposes of this report, we use acquisition, cybersecurity, and workforce development to refer to these three areas.

<sup>5</sup>See, for example, GAO, *Chief Information Officers: Private Sector Practices Can Inform Government Roles*, [GAO-22-104603](#) (Washington, D.C.: Sept. 15, 2022), *Weapon Systems Annual Assessment: Programs Are Not Consistently Implementing Practices That Can Help Accelerate Acquisitions*, [GAO-23-106059](#) (Washington, D.C.: June 8, 2023), and *Weapon Systems Annual Assessment: DOD Is Not Yet Well-Positioned to Field Systems with Speed*, [GAO-24-106831](#) (Washington, D.C.: June 17, 2024).

<sup>6</sup>GAO defines leading practices as practices for which there is sufficient evidence that the practice is better than some others at achieving the desired outcome, in multiple contexts. The definition of certain leading practices terms used in this report (e.g., business case) may differ across sectors depending on the product being acquired. In addition, discussion of cloud service level agreements or other terms and conditions in the private sector may differ from government contracts and may vary by state laws.

---

workforce development; (2) elicited the participation of 18 private sector leading companies based on rankings in well-recognized lists and awards, among other factors; (3) created, pretested, and administered a survey to those companies and conducted follow-up interviews; and (4) validated the leading cloud adoption practices by soliciting and incorporating feedback from cloud computing subject matter experts at academic institutions. We also asked companies about their approaches for addressing challenges and related technical considerations associated with adopting cloud computing solutions. Appendix I provides detailed information on our objectives, scope, and methodology, including the list of participating companies and academic institutions.

We conducted our work from November 2022 to March 2025 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

---

## Background

Cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned, or made available for immediate use. Purchasing IT services through a cloud service provider can also enable organizations to avoid paying the full cost for the resources that would typically be needed on premises to provide such services. This approach allows organizations to buy computing services more quickly and possibly at a lower cost than building, operating, and maintaining these resources themselves.

---

## Organizations Can Select from Various Cloud Service and Deployment Models

Cloud computing provides solutions for obtaining IT services more efficiently. According to National Institute of Standards and Technology (NIST), cloud computing offers several benefits, including on-demand self-service, resource pooling, rapid elasticity, and measured service.<sup>7</sup> These benefits enable organizations to efficiently scale, control cost, and access shared resources.

---

<sup>7</sup>See NIST, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145 (September 2011).

---

To realize those benefits, organizations can select different cloud solutions, which can comprise one or more cloud services, to support their operations. NIST has identified three primary cloud service models, each of which has unique features and security implications.<sup>8</sup> These include:

- Infrastructure as a Service (IaaS) includes infrastructure for data storage, computing power, and backup and recovery services, among other purposes. The provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment. The organization manages the operating system, programming tools and services, and applications. An organization and its IaaS provider generally share security responsibilities for data, identity and access management, and networking.
- Platform as a Service (PaaS) includes platforms for developing, testing, and deploying applications or information dashboards, among other purposes. The provider delivers and manages the infrastructure and operating system while providing software development kits or other PaaS tools the organization can use to develop applications. An organization and its PaaS provider generally share security responsibilities for data, identity and access management, networking, and applications.
- Software as a Service (SaaS) includes applications for billing, email and office productivity, human resources functions, and document management, among other purposes. The provider delivers one or more applications and all the resources (operating system and programming tools) and underlying infrastructure, which the organization can use on demand. An organization and its SaaS provider generally share security responsibilities for data and identity and access management.

In addition, organizations can choose from a variety of arrangements for obtaining cloud solutions (called cloud deployment models). NIST has identified four cloud deployment models:<sup>9</sup>

---

<sup>8</sup>See NIST, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145 (September 2011) and *NIST Cloud Computing Reference Architecture*, Special Publication 500-292 (September 2011).

<sup>9</sup>See NIST, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145 (September 2011).



- 
- Private cloud. The service is set up specifically for one organization, although there may be multiple customers within that organization and the cloud may exist on or off the organization’s premises.
  - Community cloud. The service is set up for organizations with similar requirements. The cloud may be managed by the organizations or a third party and may exist on or off the organizations’ premises.
  - Public cloud. A service that is available to the general public and is owned and operated by the provider.
  - Hybrid cloud. A service comprising two or more of the three deployment models (private, community, or public) that are bound together by technology that enables data and application portability.

Organizations may also adopt services from more than one provider, resulting in a multi-cloud environment. A multi-cloud strategy includes a range of advantages and potential challenges for organizations. For example, diversifying across multiple cloud platforms can help avoid vendor lock-in and mitigate the effects of potential service outages.<sup>10</sup> However, supporting multiple cloud platforms also increases costs related to maintaining a skilled workforce due to the need for specialized expertise to use each cloud environment effectively.

---

## Operational Frameworks for Effective Cloud Management

Organizations can implement operational frameworks—including FinOps, DevOps, and DevSecOps—to help manage their adoption and use of cloud computing solutions.<sup>11</sup> Each framework addresses specific aspects of cloud management. By implementing these operational frameworks, organizations may streamline cloud operations, control costs, and proactively secure their cloud computing resources.

FinOps is an operational framework that combines finance and IT operations to enable organizations to manage and optimize their cloud spending through better financial accountability and collaboration across teams. By applying FinOps principles, organizations can align their cloud use with financial goals, making it easier to track, control, and predict

---

<sup>10</sup>A 2022 report from the House Judiciary Committee described vendor lock-in as a situation where the costs of switching vendors are sufficiently high that users stay with an incumbent firm rather than switch to a firm whose product or service they would prefer. See U.S. House Committee on the Judiciary; *Investigation Of Competition In Digital Markets*, H. Prt. 117-8, part I, at 31-32 (Washington, D.C.: Government Publishing Office, 2022.)

<sup>11</sup>The term FinOps refers to the combination of finance and IT operations, and DevOps refers to the combination of software development and IT operations. DevSecOps expands on DevOps by incorporating security elements.

---

cloud spending. FinOps encourages teams to actively monitor and adjust cloud usage according to budget limits and performance goals, as a means of improving cost efficiency and resource allocation. This approach helps organizations balance innovation with cost management, ensuring that cloud investments are both efficient and aligned with organizational objectives.

According to the FinOps Foundation's framework, an organization's implementation should be guided by six principles<sup>12</sup>:

- Teams need to collaborate. An organization's finance, IT, product, and operations teams should work closely in real time to optimize acquired cloud services for enhanced efficiency and technological innovation.
- Decisions are driven by business value of cloud. Organizations should use value-based metrics to assess business effects and view cloud computing primarily as a tool for innovation. This includes intentional trade-offs between cost, quality, and speed.
- Everyone takes ownership for their cloud usage. An organization's engineers and product teams should be responsible for managing costs and resource use within their budgets and treat cost as a key efficiency metric from the beginning of the software development cycle.
- FinOps data should be accessible and timely. Organizations should ensure real-time cost data are accessible to all levels of the organization to drive better cloud utilization. Regular monitoring, financial forecasting, benchmarking, and variance analyses can help teams understand cost trends and improve planning.
- A centralized team drives FinOps. A centralized team promotes shared accountability, manages rate and discount optimizations, and enables engineers to focus on optimizing cloud usage instead of financial negotiations.
- Take advantage of the variable cost model of the cloud. Organizations should use the flexibility of a variable cost model to deliver more value

---

<sup>12</sup>Summarized from FinOps Principles by FinOps Foundation, licensed under a Creative Commons Attribution 4.0 International License. The FinOps Foundation is a trade organization that advocates for cloud financial management through promoting best practices, individual training, certification programs, and establishing standards. According to the FinOps Foundation, the organization comprises over 23,000 members representing more than 10,000 private sector companies.

---

through iterative, just-in-time planning and purchasing, while embracing proactive system design and continuous optimization.

DevOps is an operational framework that combines development and IT operations to improve collaboration and accelerate software delivery. By integrating these teams and automating processes, DevOps helps organizations deploy applications faster while reducing errors and downtime. This approach encourages continuous testing and monitoring so teams can quickly identify and fix issues in real time. DevOps principles enable organizations to respond to customer needs more efficiently, supporting innovation and competitive advantage in the cloud.

DevSecOps builds on DevOps by integrating security concerns early in the software development process. DevSecOps promotes close collaboration between development, security, and operations teams, ensuring that security remains a continuous priority without slowing down development. This approach allows teams to identify and address vulnerabilities as they emerge, which can reduce security risks and improve compliance of deployed applications.

---

## Technical Considerations Related to Cloud Computing

Given the various ways cloud solutions can be deployed, organizations need to evaluate a variety of technical considerations and their related potential benefits and challenges. These technical considerations can influence the success of cloud adoption in different ways. To maximize the benefits of cloud computing, organizations should assess how these technical considerations may affect their long-term outcomes. Table 1 identifies and describes some of these technical considerations.

---

**Table 1: Technical Considerations Related to the Adoption of Cloud Computing Solutions**

Technical consideration	Description
Cloud-native design	Cloud-native design refers to developing applications that can run on different cloud service providers' environments without requiring major adjustments, such as by using containerization technology (see below). Cloud-native technologies enable organizations to build and run scalable applications independent of any cloud service provider's proprietary features, resulting in enhanced flexibility to change cloud service providers as needed.
Provider-native design	Provider-native design refers to developing applications tailored to a specific cloud service provider's environment. While provider-native applications can be difficult to move to different cloud environments, such applications benefit from the chosen cloud service provider's built-in tools, such as for enhanced monitoring or scaling of cloud resources.
Containerization	Containerization is a method for packaging and running an application within a virtualized environment called a container. Containers standardize how software applications run, which supports compatibility across multiple cloud service providers' environments despite differences in their configurations.

Technical consideration	Description
Infrastructure as Code (IaC)	IaC is a method for managing and provisioning computing infrastructure through machine-readable configuration files rather than manual setup. It automates the development and maintenance of resources like operating systems and storage, enabling developers to consistently define the state of infrastructure. By using IaC to automate these processes, organizations avoid manual configurations that may be prone to errors.
Cloud integration tools	Cloud integration broadly refers to the process of connecting and coordinating various cloud systems, applications, or services to enhance workflow and interoperability. Cloud integration tools, such as application programming interface management platforms, enable organizations to automate workflows and share data across cloud systems in real time, among other advantages.
Data user fees	Data user fees (ingress and egress) are related to how users transfer and access data in a cloud environment. Data ingress is the process of transferring data into a cloud environment. Data egress occurs when users transfer and access data from a storage location to enable data to be used or processed in some way. While data ingress is often free to users, cloud service providers generally charge data egress fees for transferring data out of storage, including transferring data from one provider to another, such as at the end of a contract.

Source: GAO analysis of private sector company survey data and federal and nonfederal guidance documents on cloud computing. | GAO-25-106369

## Prior GAO Reports on Private Sector Leading Practices and on Agencies' Efforts to Adopt Cloud Solutions

GAO has found that leading practices in the private sector can help inform federal agencies' efforts to enhance their operations, including managing technological innovation.<sup>13</sup> For over 20 years, GAO has made numerous recommendations to federal agencies to implement knowledge-based practices for their major acquisition programs that underpin successful product development within leading companies. Over this time, agency implementation of these practices saved taxpayers tens of billions of dollars.<sup>14</sup> Identifying similar practices that companies rely on when adopting cloud solutions can provide crucial, cutting-edge information to acquisition leaders in government and, in turn, ultimately help frame changes to agencies' acquisition processes. For example, in March 2022, GAO made nine recommendations to three federal agencies to update acquisition policies to fully implement key principles of product

<sup>13</sup>For example, see GAO, *Leading Practices: Iterative Cycles Enable Rapid Delivery of Complex, Innovative Products*, [GAO-23-106222](#) (Washington, D.C.: July 27, 2023) and *Leading Practices: Agency Acquisition Policies Could Better Implement Key Product Development Principles*, [GAO-22-104513](#) (Washington, D.C.: Mar. 10, 2022).

<sup>14</sup>For example, we identified \$136.1 billion in costs avoided after the Department of Defense took positive steps by adopting a framework for applying knowledge-based practices. See GAO, *Performance and Accountability Report: Fiscal Year 2019*, [GAO-20-1SP](#) (Washington, D.C.: Nov. 19, 2019); and *Performance and Accountability Report: Fiscal Year 2017*, [GAO-18-2SP](#) (Washington, D.C.: Nov. 15, 2017).

---

development used by leading companies. All three agencies concurred with our recommendations.<sup>15</sup>

GAO previously found that other factors beyond policies can affect agency outcomes, including structural differences between government and private industry. However, as noted, GAO's prior work also demonstrates that key principles from private industry can be thoughtfully applied to government acquisition efforts to improve outcomes, even with different cultures and incentives. For example, in September 2022, GAO reported that the majority of 71 private sector Chief Information Officer (CIO) survey respondents reported having responsibilities that aligned with those of agency CIOs in 13 of 14 key IT management areas.<sup>16</sup> These areas included strategic planning, investment management, and information security, among others. Responsibilities assigned to the federal CIOs also corresponded to those of private sector CIOs in 10 of the 14 key IT management areas. Similarly, GAO found that federal CIO responsibilities corresponded to those of private sector survey respondents in each of five relevant responsibility areas.

GAO has also previously reported on the federal government's efforts to adopt cloud computing solutions, including challenges that agencies have experienced in their efforts. Specifically, GAO's body of work shows that federal agencies have experienced challenges with acquiring cloud services, ensuring cybersecurity of these services, developing a skilled workforce, and tracking related costs and savings.<sup>17</sup> For example, in April 2016, GAO reported that five of the major agencies we reviewed did not always incorporate key practices for service level agreements in their contracts when acquiring cloud services.<sup>18</sup> As of January 2025, all six recommendations included in that report were closed as implemented.

In addition, in December 2019, GAO reported that four major agencies we selected for a detailed review did not consistently include required information in their cloud system's security plans or identify required information in remedial action plans that were to list cloud service

---

<sup>15</sup>[GAO-22-104513](#).

<sup>16</sup>See GAO, *Chief Information Officers: Private Sector Practices Can Inform Government Roles*, [GAO-22-104603](#) (Washington, D.C.: Sept. 15, 2022).

<sup>17</sup>[GAO-23-106222](#).

<sup>18</sup>See GAO, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, [GAO-16-325](#) (Washington, D.C.: Apr. 7, 2016).

---

deficiencies and how they will be mitigated.<sup>19</sup> Similarly, GAO found that selected federal agencies did not include new cloud-related skills and a skills gap analysis for cloud personnel in a workforce development strategy and did not strategically plan for communicating with employees to prepare them for changes that would occur due to the cloud migration.<sup>20</sup>

In April 2019, GAO also reported that federal agencies experienced challenges in tracking and reporting cloud spending and savings data.<sup>21</sup> For example, federal agencies often used 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.

---

## Companies Reported 19 Leading Practices for Adopting Cloud Computing Solutions

We surveyed 18 private sector companies across various industries about their experiences with adopting cloud computing solutions. These companies, which included companies from the health care, media, manufacturing, information technology, hotels, arts and culture, retail, banking, finance, insurance, telecommunications, investing, and pharmaceuticals industries, reported using up to 19 leading practices. They also rated and described the importance of each leading practice. The leading practices address three areas: acquisition, cybersecurity, and workforce development (see fig. 1).

---

<sup>19</sup>See GAO, *Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed*, [GAO-20-126](#) (Washington, D.C.: Dec. 12, 2019).

<sup>20</sup>For example, see GAO, *Coast Guard: Actions Needed to Enhance IT Program Implementation*, [GAO-22-105092](#) (Washington, D.C.: July 28, 2022); *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization*, [GAO-22-104070](#) (Washington, D.C.: June 29, 2022); and *State Department: Additional Actions Needed to Address IT Workforce Challenges*, [GAO-22-105932](#) (Washington, D.C.: July 12, 2022).

<sup>21</sup>See GAO, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*, [GAO-19-58](#) (Washington, D.C.: Apr. 4, 2019).

**Figure 1: Nineteen Leading Practices that Companies Reported Using for Adopting Cloud Services**



Source: GAO (data and icons); Rabbit\_1990/stock.adobe.com (images). | GAO-25-106369

The following descriptions provide more detail on each of the 19 leading practices for adopting cloud solutions. The descriptions include comments from companies regarding how they applied each practice and why they considered each practice to be important to their overall cloud adoption strategy, as well as comments from subject matter experts in cloud computing from academia.

### Companies Reported Seven Leading Practices for Acquiring Cloud Computing Solutions

Companies reported using seven acquisition leading practices when adopting cloud computing solutions (see app. II for additional information about responses from companies). From defining the business case for a cloud adoption to assessing the adopted cloud solution’s performance, most companies found each of these leading practices to be very or



extremely important to their cloud adoption strategies. Table 2 identifies and describes these practices.

**Table 2: Seven Leading Practices Companies Reported for Acquiring Cloud Solutions**

Leading Practice	Description
Define the business case	Define the current operational environment and critical IT needs before pursuing a cloud computing solution.
Develop reliable cost estimates	Develop and update cost estimates based on reliable market research for cloud computing solutions that can meet critical IT needs.
Ensure mission alignment	Select a cloud service provider whose compliance posture and business practices align with long-term mission needs.
Include key stakeholders	Solicit input from and involve relevant stakeholders throughout the acquisition process.
Negotiate clear terms and agreements	Negotiate clearly defined responsibilities and performance metrics supported by enforcement and remediation plans.
Pilot proposed solutions	Demonstrate the proposed cloud computing solution works as intended in an operational environment as part of the acquisition process.
Assess performance against expectations	Assess the performance of acquired cloud computing solutions to ensure that expectations have been and continue to be met.

Source: GAO analysis of private sector company survey data and federal and nonfederal guidance documents on cloud computing. | GAO-25-106369

Note: We asked 18 leading companies across various industries in the private sector to assess the importance of leading practices in acquisition during the adoption of their company's cloud services. Specifically, we asked: "(a) Has your company applied these practices as part of its cloud computing acquisition strategy? (b) How important were the practices to your company's adoption and implementation of cloud services as a consumer? and (c) What comments do you have on your answers or on the content and wording of our proposed leading practices?" In addition, we asked companies to provide any additional practices they use that were not included in our survey.



An organization's adoption of a cloud computing solution should be supported by a business case that defines the current operational environment and critical IT needs in the context of the larger business strategy. Organizations should consider important factors such as IT



---

spending and resources, existing applications, data, workforce capabilities, regulatory or other requirements, and relevant agreements. These factors should be documented in a way that provides the CIO with an appropriate level of visibility and specificity of these factors to help ensure effective management and oversight of the cloud adoption.

All 18 companies reported applying this practice, and all of them considered it to be very or extremely important. For example, companies highlighted the importance of aligning cloud adoption with strategic goals and IT needs while maintaining flexibility to optimize value and competitiveness. One company stated that clearly identifying critical IT needs helps organizations avoid overspending on unnecessary features and services, enabling them to select a cloud solution that offers the best value and return on investment. However, another company noted that organizations should avoid letting existing infrastructure investments overly influence future cloud adoption decisions, adding that staying flexible and open to different platforms is important for meeting IT needs and staying competitive.

### **Accounting for the Broader Strategic Benefits of Cloud Computing**

Companies reported that migrating to a cloud environment or building on existing cloud infrastructure supports strategic objectives beyond reducing operational costs. For example, one company reported that its cloud adoption strategy was designed to enhance business agility, speed-to-market, resiliency, and security, in addition to cost savings. Another company highlighted that migrating to a cloud environment enhanced its data analysis capabilities and customer services, noting that not all cloud solutions reduce costs. Instead, the company recommended that organizations consider cloud computing's other advantages. For example, one company emphasized the strategic value of co-investment and co-innovation with a cloud service provider, which can augment existing capacity and expertise and relieve some of the burden of technological innovation on the company.

Source: GAO analysis of private sector company survey and interview data. | GAO-25-106369

Regarding its application of the practice, one company reported conducting a workload analysis. Specifically, the company assessed its performance, scalability, and availability requirements, as well as issues related to cybersecurity and data management. According to the company, a workload analysis can help organizations understand their resource requirements and determine which systems are suitable for migration to the cloud. Further, such an analysis can help identify which

---

legacy systems may require modifications or cause performance issues in the cloud environment.

Subject matter experts from four academic institutions agreed that defining the business case is a leading practice for acquiring cloud solutions. For example, one subject matter expert stated that organizations should consider how their IT needs may change over the lifetime of the cloud solution. According to another subject matter expert, it is extremely important to define the business case for acquiring a cloud solution as an organization cannot effectively obtain what it does not know it needs.



An organization's adoption of a cloud computing solution should be informed by cost estimates developed and updated based on reliable market research. Conducting market research includes considering factors such as services, features, and pricing models offered by various cloud service providers. Pricing models vary by cloud service and can include pay-as-you-go, reserved instances, spot instances, and premium support, among others.<sup>22</sup> Completing cost-benefit and comparative performance analyses for multiple cloud solutions using clearly defined

---

<sup>22</sup>Pay-as-you-go, or on-demand pricing, is a pricing model where users are charged based on actual usage of cloud resources, with no upfront commitment or fixed costs. Alternatively, reserved instances require users to commit to using a specific amount of cloud resources for a longer period, such as 1-3 years, at a discounted rate compared to on-demand pricing. Spot instances pertain to cloud resources offered at a significantly reduced price when providers have excess capacity, but which can be interrupted if resources are needed elsewhere. Premium support packages include additional benefits from the provider, such as increased access to technical assistance and faster response times.

---

metrics can reveal each option's associated benefits, risks, and challenges. When assessing whether an option or pricing model fits within an allotted IT budget, organizations should consider any hidden costs of migrating to a cloud environment that may not be reflected in the upfront cost of services.<sup>23</sup> As these hidden costs become known, whether through piloting the proposed cloud solution or other means, organizations should then update their cost estimates to better reflect the true cost of migrating to a cloud environment.

All 18 companies reported applying this practice, and 13 considered it to be very or extremely important to their overall cloud acquisition strategy. For example, companies highlighted the importance of reliable cost estimates and market research for selecting cloud solutions that maximize value and meet organizational needs. One company emphasized that developing reliable cost estimates is important for making informed decisions when selecting cloud solutions. By understanding the financial implications of different options, organizations can choose the cloud solution that offers the best value and meets their critical IT needs without exceeding their allotted budget. Further, the company added that, after conducting market research, organizations can enter negotiations with providers with knowledge that can be leveraged to secure more favorable terms, discounts, or additional services that provide greater value for the investment. Another company noted that conducting market research is also critical to ensure end-users receive cloud solutions that are best-of-breed, rather than just the lowest upfront cost.<sup>24</sup>

Regarding their application of the practice, several companies reported implementing FinOps principles to make more informed decisions about scaling their cloud infrastructure. FinOps enables better visibility into cloud computing costs, allowing organizations to balance performance needs with cost efficiency. For example, one company used FinOps to track key metrics and ensure modernization efforts aligned with business goals, which reduced its time-to-market and improved resiliency (i.e., maintaining high availability and disaster recovery capabilities). Another

---

<sup>23</sup>Examples of hidden cloud migration costs include resources expended on contract negotiations, data egress fees, and workforce factors such as organizational readiness and required training.

<sup>24</sup>Best-of-breed refers to those cloud solutions offered by vendors that are known to be the best at performing a specific task. These solutions are generally favored over cloud platforms that can perform several functions, but which may not perform each function as well as a single solution intended only for the desired capability.

---

company applied FinOps to forecast costs and value delivered, emphasizing availability, resiliency, and efficiency through automation. In one case, the company compared steps required by different cloud applications to perform the same task and assessed their potential effect on employee productivity and pay. By automating key processes, the company reported improving overall efficiency. Another company highlighted how FinOps helped it ensure precise cost estimates and financial accountability and manage cloud operations efficiently to experience cost savings.

While not referencing FinOps directly, other companies reported establishing centralized cloud finance teams or continuous monitoring of cloud expenditures to manage their cloud computing efforts and identify unauthorized or unused systems and services more effectively. One company reported that it forecasts cloud infrastructure cost growth by combining top-down analyses of cloud adoption and consumption rates with bottom-up budgets developed by application teams. According to the company, this dual approach helps ensure accurate financial planning and align cloud spending with long-term business needs. Although cost estimates are critical for determining which cloud solutions meet business needs, companies also consider providers' alignment with long-term industry and business needs (see next practice).

Subject matter experts from four academic institutions agreed that developing reliable cost estimates is a leading practice for acquiring cloud solutions. Subject matter experts also stated that costs for cloud solutions can be difficult to predict or change rapidly as an organization's needs evolve. As a result, one subject matter expert suggested that organizations ensure written agreements include provisions to return hosted data for a reasonable cost if operational experiences differ from expectations. Further, another subject matter expert noted that organizations may benefit from substantially revising their cost estimates for new cloud solutions after completing a 3-month trial period.



An organization’s adoption of a cloud computing solution should include selecting a provider whose compliance posture and business practices align with the organization’s long-term mission needs. Ensuring mission alignment includes reviewing a provider’s end user and legal agreements, privacy policies, security disclosures, and proof of compliance with applicable legal requirements. Additionally, organizations must consider other potential legal implications of selecting cloud service providers, such as the geographic location of a provider’s physical infrastructure. This practice also includes assessing a provider’s capabilities for co-innovation, which can help support a collaborative partnership as mission needs evolve over time.

**Factors to Consider When Ensuring Mission Alignment with a Cloud Service Provider**

One company that viewed ensuring mission alignment as essential identified four factors to consider regarding a provider’s operations:

**Key priorities.** Identify important priorities, including security, sustainability, social responsibility, data privacy, and innovation.

**Provider roadmap.** Review the provider’s roadmap and strategy to ensure alignment with the organization’s priorities.

**Data policies.** Assess the provider’s data privacy and security policies, including compliance with applicable regulations.

**Transparency.** Look for transparency in the provider’s operations and evidence of accountability for any breaches or issues.

Source: GAO analysis of private sector company survey data. | GAO-25-106369

All 18 companies reported applying this practice, and 14 considered it to be very or extremely important. For example, companies highlighted the importance of mission alignment with providers to ensure long-term success, mitigate risks, and support compliance across operations. Companies also emphasized that mission alignment is important for ensuring a sustainable, long-term relationship with the provider rather than simply a transactional relationship. Further, one company added that acquiring cloud solutions from a provider with strong mission alignment can mitigate risks related to service continuity, support regulatory compliance, and foster cost predictability. Two companies noted that this practice is particularly important for organizations with a global footprint, as they must assess a provider’s ability to adhere to and support all current and future legal and privacy compliance requirements in all their geographic areas of operations.

Regarding its application of the practice, one company reported that it assigned its strategic sourcing team to evaluate potential providers for

---

mission alignment. The company used a standardized process that reviewed each potential provider's privacy and security policies and certifications against company requirements. Another company assessed how various providers' technological capabilities aligned with the company's own internal application development and technology adoption strategies. Such assessments can use a heat map to visualize areas of alignment for easy comparison across providers.<sup>25</sup> Organizations may find that some providers are better positioned than others to support specific IT needs. For example, companies interested in serverless applications found some providers better suited to meet these needs, while others were more appropriate for containerized workloads, which can require close consultation and support from the provider.

Subject matter experts from four academic institutions agreed that ensuring mission alignment is a leading practice for acquiring cloud solutions. One subject matter expert added that, while the major cloud service providers are similar across most metrics, organizations should be aware that some providers deprioritize quality of service when using third-party data of competitors. Further, some providers may offer unrealistically low pricing options because the provider has implemented other ways of monetizing or mining the data organizations store in their cloud environment. When assessing the potential lifespan of a relationship with a particular provider, another subject matter expert said it is important for organizations to also consider whether the provider's other customers use the same cloud solutions; if so, those solutions are less likely to be discontinued and may be offered at a lower cost.

---

<sup>25</sup>A heat map is a visual tool that helps organizations compare cloud service providers by highlighting strengths and weaknesses across key criteria such as cost, performance, and compliance, enabling informed decision-making.





An organization’s adoption of a cloud computing solution should include soliciting input from and involving relevant stakeholders throughout the acquisition process. Organizations that include key stakeholders for specific aspects of the cloud acquisition process—such as an attorney to review service level agreements and participate in negotiations—can help ensure accountability for cloud acquisition decisions.<sup>26</sup> By conducting a thorough stakeholder analysis and clearly communicating the cloud adoption strategy with relevant stakeholders, organizations can improve decision-making and foster greater support for migrating to a cloud environment. Involving stakeholders, including stakeholders who represent differing and varying perspectives, helps ensure that everyone’s perspectives and needs are considered, from defining the business case to subsequently evaluating whether an acquired cloud solution meets the organization’s needs. In addition, CIOs can better meet organizational priorities by taking user satisfaction and feedback into account when developing and executing a cloud modernization strategy.

All 18 companies reported applying this practice, and 14 considered it to be very or extremely important. For example, companies highlighted the importance of including stakeholders in the acquisition process to help ensure better decision-making and stronger organizational support for the

<sup>26</sup>The cloud migration should be led by the appropriate leadership and properly defined, funded, and reviewed. According to OMB, the cloud service budget development process should include representation from the Chief Financial Officer, Chief Administrative Officer, and CIO in the planning, programming, and budgeting stages. The CIO should approve the IT components of any plans through a process defined by senior leadership that balances IT investments with other uses of IT funding. See OMB, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

---

cloud adoption. Companies also emphasized that including and soliciting input from a wide range of relevant stakeholders is important for fostering more inclusive, well-rounded, and successful cloud adoption outcomes. One company added that cloud acquisition teams benefit from being transparent and collaborative, including partnerships across departments and with senior management. The company further stated this approach can empower organizations to effectively identify critical workloads and select providers that can meet requirements relevant to each department.

### **Building Consensus for a Cloud Migration**

One company described how its Chief Executive Officer's (CEO) leadership and vision successfully built consensus around migrating to a new cloud service provider. The company's initial bottom-up cloud migration effort began before cloud computing was fully integrated into its larger business strategy. Recognizing the strategic benefits of cloud adoption, the CEO led an effort that identified gaps in its first provider's data analytics capabilities and shifted the focus from cost savings to enhancing data analysis, improving service quality, and maintaining a competitive edge. The company said this top-down approach fostered collaboration across departments and helped gain stakeholder buy-in for adopting cloud solutions from a new provider. After evaluating multiple providers, the company selected one that met its needs. According to the company, the CEO's emphasis on co-innovation with the provider was also critical since the company could not have independently developed the advanced data analysis tools included in the cloud solution.

Source: GAO analysis of private sector company survey data. | GAO-25-106369

Regarding their application of the practice, companies reported that it is critical to establish a cross-functional cloud adoption team with representation from management and departments responsible for compliance, finance, legal, programming, and IT. One company reported that it provides multiple opportunities for relevant stakeholders to share feedback on the proposed cloud solution to ensure financial, programmatic, legal, and operational alignment prior to completing the acquisition process. Another company stated that involving IT stakeholders—including network professionals, security professionals, and system administrators—early in the acquisition process can help identify specific IT needs and preferences and inform the selection criteria for a provider.



---

Subject matter experts from three of four academic institutions agreed that including key stakeholders is a leading practice for acquiring cloud solutions. For example, one subject matter expert stated that this practice can help define the business case for the cloud adoption and reveal metrics that are important for certain applications but may get overlooked—particularly with respect to cybersecurity, service availability, or data management. Another subject matter expert specified that, while organizations should not need to include feedback from their own customers in the decision process for adopting a new cloud solution, it is important to shield customers from potential negative externalities. They added that customers may be considered stakeholders and help inform an organization’s cloud acquisition strategy if the potential solutions are designed to improve the customer’s experience or offer a new functionality.



Organizations should negotiate clearly defined responsibilities and performance metrics with the provider and establish enforcement or remediation plans. Cloud service level agreements define the level of service and performance expected from a provider, how that performance will be measured, enforcement mechanisms to ensure the specified performance levels are achieved, and remediation plans and exit strategies in the event of underperformance or the need to terminate service. These agreements are distinct from, but can be incorporated within, vendor contracts that include the general terms and conditions, rights, and responsibilities of both the provider and consumer. In addition, cloud service level agreements often point out exclusions, or factors for which the provider cannot be held accountable, that may cause unacceptable performance. It is important to note what these exclusions are and to have a process in place for escalating exclusions and other

---

potential exceptions for review by relevant stakeholders. Negotiating specific terms and agreements can be difficult when working with major cloud service providers, which largely have standardized agreements. However, negotiating teams should understand their organization's mandatory terms and conditions and enter negotiations prepared to walk away from unfavorable agreements.

All 18 companies reported that they apply this practice, and 17 considered it to be very or extremely important. For example, companies highlighted the importance of defining expectations and responsibilities in service level agreements to ensure reliable cloud adoption outcomes. Companies also reported that negotiating clear service level agreements is important for helping to ensure that acquired cloud solutions meet expectations and that agreements include clear steps to follow if the cloud solution does not meet agreed upon standards of performance, security, and reliability. One company added that clarifying roles and responsibilities also enables a smoother, more reliable partnership with the provider and helps avoid potential misunderstandings or disputes. Further, another company emphasized that this practice is particularly important since the shared responsibility model used with cloud service providers is a significant change from traditional on-premises data centers managed by a central IT infrastructure team.

#### GAO Key Practices for Cloud Computing Service Level Agreements

In April 2016, GAO reported a list of 10 practices that were key for federal agencies to incorporate into a contract to help ensure cloud services are performed effectively, efficiently, and securely. Those practices addressed four management areas:

**Roles and responsibilities.** Specify roles and responsibilities of all parties and define key terms.

**Performance measures.** Define clear metrics for performance, availability, monitoring, and continuity of operations, and describe related exception periods.

**Security.** Specify security requirements and reporting procedures.

**Consequences.** Specify a range of enforceable consequences for noncompliance with aspects of the service level agreement.

Source: GAO summary of key practices reported in [GAO-16-325](#). | [GAO-25-106369](#)

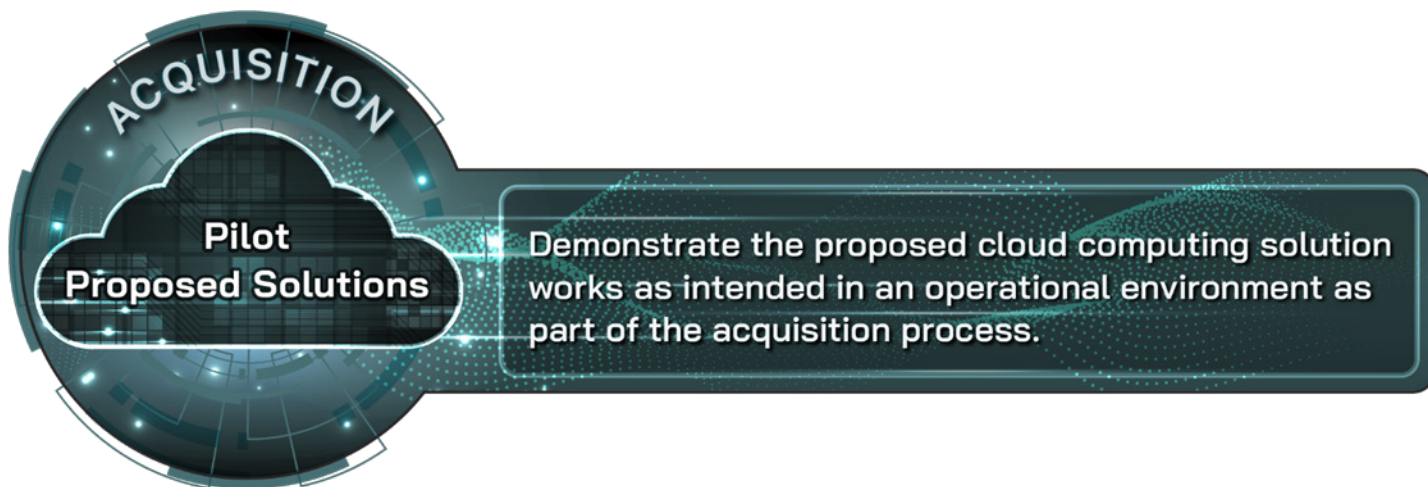
Regarding its application of the practice, one company reported that limiting the use of nonnegotiable terms and conditions when acquiring a new cloud solution helps ensure that contracts are fair, focused on essential needs, and flexible enough to accommodate changes. Another company stated that it includes required contract terms and conditions in requests for proposals from providers to help ensure providers are fully aware of the company's requirements early in the acquisition process. Further, one company noted that the quality of a provider's standardized terms and conditions can be a good indicator of the quality of its back-office operations, which can significantly affect the long-term success of both the provider and its customers.

One company reported multiple instances of declining potential agreements that it determined were unacceptable, despite favorable cost estimates. While it developed this practice when cloud computing was not yet as widespread and many providers refused to negotiate terms, the company has perceived an ongoing shift in industry practices around negotiations as more companies begin refusing nonnegotiable cloud service terms and agreements. The company added that an organization's relative size and effect on a provider's annual revenue can

---

also provide leverage in negotiations, both initially and during contract renewal periods. According to the company, although switching providers can be costly and time consuming, organizations that plan for this contingency can enhance their negotiating position during contract renewal periods.

Subject matter experts from four academic institutions agreed that negotiating clear terms and agreements is a leading practice for acquiring cloud solutions. For example, one subject matter expert stated that, while it can be difficult to quantify some metrics, such as scalability and quality of service, it is important to clarify these metrics in the service level agreement to the extent possible. According to another subject matter expert, effective service level agreements generally include a customer behavioral expectation, or clause that articulates how much workload an organization plans to place on a particular cloud service, including whether the workload may be unbalanced or prone to surging. An agreement that does not stipulate a customer behavioral expectation may indicate that the provider plans to charge a rate that accounts for the worst possible behavior a customer could produce. If an organization expects to have a more balanced workload, then such an agreement may impose unnecessary costs.



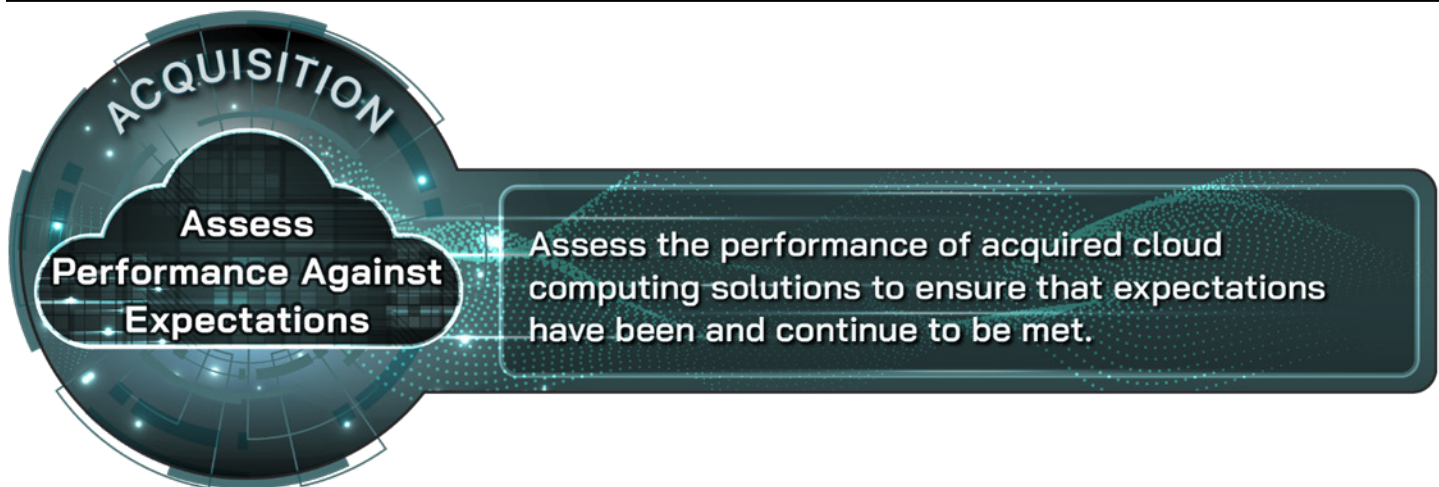
Organizations should demonstrate that the proposed cloud solution works as intended in an operational environment as part of the acquisition process. Piloting or otherwise testing a prototype of a cloud computing solution against clear and appropriate metrics before fully migrating to a cloud environment is critical to validate that the solution will work as intended in an organization's operational environment. Demonstrating the cloud solution's effectiveness and compatibility up front can save time,

---

reduce costs, and prevent issues that may otherwise go unnoticed until the organization's workflows became dependent on the cloud solution. Moreover, this practice can help narrow down multiple cloud solutions based on feedback from end users and other stakeholders.

Seventeen of 18 companies reported applying this practice, and 15 considered it to be very or extremely important. For example, companies highlighted the importance of piloting proposed cloud solutions to evaluate their performance before committing to the cloud adoption. One company reported that piloting proposed cloud solutions is important even in cases where all the major cloud service providers have options that have been proven to work as intended. The company stated that, in these cases, demonstrating each option's performance in an operational environment is an effective way of determining which provider's cloud solution best meets IT needs. Further, one company reported that some providers offer free sandboxing or proof of concept capabilities for users to use and test proposed cloud solutions before making the decision to migrate to the cloud environment. Regarding its application of the practice, another company reported that it created its own sandbox environment that closely resembled its operational environment to test new cloud solutions.

Subject matter experts from four academic institutions agreed that piloting proposed solutions is a leading practice for acquiring cloud solutions. For example, one subject matter expert noted that the pilot phase of the acquisition process provides an opportunity to test for failures and evaluate a cloud solution's performance under spikes in workload or changes to application characteristics and hardware platform configurations. In addition, another subject matter expert reported that it is important to allow a cloud solution to operate for a long enough period to collect sufficient data to inform and update cost estimates. According to one subject matter expert, such a trial period helps organizations to move from application-level monitoring to acceptance testing and validating whether all aspects of the service level agreement are meeting expectations.



An organization’s adoption of cloud computing solutions should include assessing the performance of newly acquired solutions over time to ensure they are meeting expectations. This practice includes periodic reviews paired with continuous monitoring of performance metrics to ensure all contractual obligations are consistently being met and risks are managed effectively. Such assessments can also provide a way to develop performance benchmarks during and after the pilot phase and derive lessons learned about the acquisition process.

Seventeen of 18 companies reported applying this practice, and 16 considered it to be very or extremely important. For example, companies highlighted the importance of assessing the performance of acquired cloud solutions to ensure they meet IT needs and deliver intended benefits. One company reported that assessing the performance of newly acquired cloud solutions is important for confirming the solution is effective and allows for timely adjustments or changes if needed. Further, companies added that this practice helps ensure providers not only deliver solutions that functionally work, but also that those solutions consistently meet the company’s critical IT needs. Ultimately, companies stated that periodic evaluations of monitored performance metrics can help inform management about whether the organization is consistently realizing the intended benefits of the new cloud solution.

Regarding their application of the practice, companies reported that they document performance metrics and facilitate periodic reviews of those metrics with internal stakeholders and their cloud service providers to help ensure consistent performance and accountability for newly acquired cloud solutions. One company noted how it implemented monitoring tools and dashboards to continuously track the performance of its cloud

solutions. The company further stated that these monitoring tools and dashboards enable organizations to regularly track key metrics in real time for early identification of performance issues.

Subject matter experts from four academic institutions agreed that assessing performance against expectations is a leading practice for acquiring cloud solutions. For example, one subject matter expert stated that this practice helps to ensure that service level agreements remain applicable and appropriate as the technologies underpinning a provider's offerings evolve. Another subject matter expert reiterated that, while periodic reviews are important, organizations should also ensure performance metrics are continuously monitored.

### Companies Reported Six Leading Practices for Securing Cloud Computing Solutions

Companies reported using six leading cybersecurity practices when adopting cloud computing solutions (see app. II for additional information about responses from companies). From defining cloud security responsibilities to documenting incident response procedures, most companies also considered these leading practices to be very or extremely important. Table 3 identifies and describes these practices.

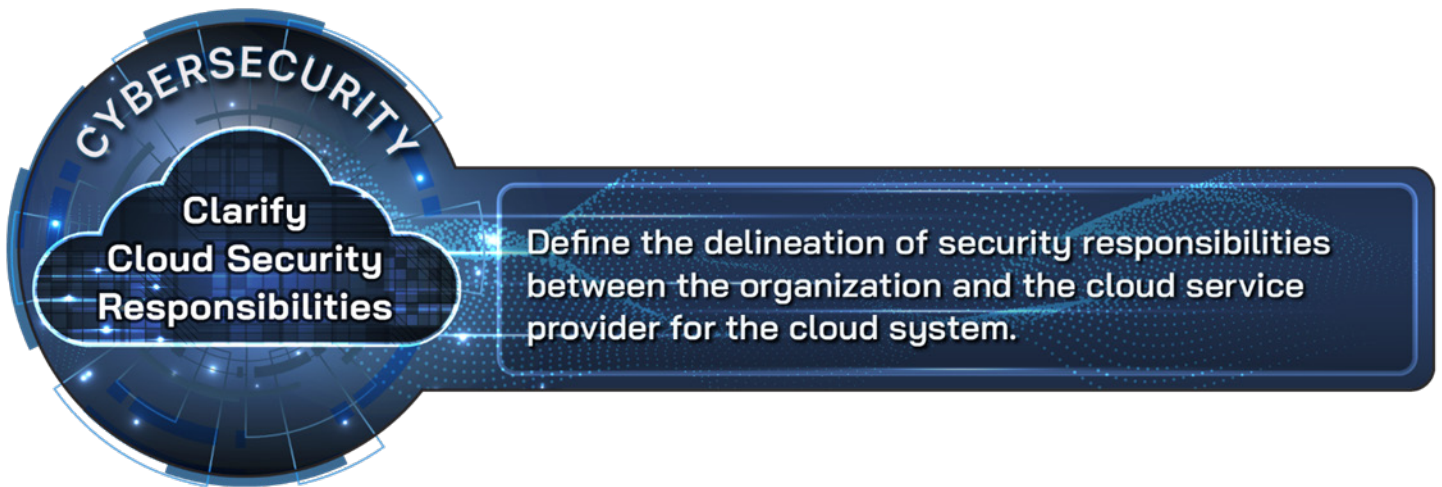
**Table 3: Six Leading Practices Companies Reported for Securing Cloud Solutions**

Leading Practice	Description
Clarify cloud security responsibilities	Define the delineation of security responsibilities between the organization and the cloud service provider for the cloud system.
Develop identity and access procedures	Develop and implement the identity, credential, and access management policies and procedures for the cloud system.
Establish continuous monitoring	Develop and implement a plan for continuously monitoring the cloud system.
Define security metrics	Define security metrics in a service level agreement with the cloud service provider.
Standardize risk and authorization processes	Use a standardized risk and authorization process when conducting risk assessments, security authorizations, and granting an authority to operate for the cloud system.
Plan incident response procedures	Develop and implement procedures for responding to and recovering from security and privacy incidents for the cloud system.

Source: GAO prior work and analysis of survey data on private sector cloud computing leading practices. | GAO-25-106369

Note: We asked 18 leading companies across various industries in the private sector to assess the importance of leading practices in cybersecurity during the adoption of their company's cloud services. Specifically, we asked: "(a) Has your company applied these practices as part of its cloud computing cybersecurity strategy? (b) How important were the practices to your company's adoption and implementation of cloud services as a consumer? and (c) What comments do you have on your answers or on the content and wording of our proposed leading practices?" In addition, we asked companies to provide any additional practices they use that were not included in our survey.





Organizations should ensure the different aspects of security responsibilities for the cloud model the organization adopts are well defined and clearly understood. Depending on the cloud service model, the organization and the provider can each be responsible for different aspects of security and may also share other responsibilities.<sup>27</sup> Well defined security roles and functions help organizations to ensure that each responsibility is fully addressed in documentation and implemented by each entity. Organizations must understand this delineation of responsibilities to confirm that appropriate mechanisms and tools are in place to manage the different aspects of cloud security that fall under each entity's scope of responsibility.<sup>28</sup>

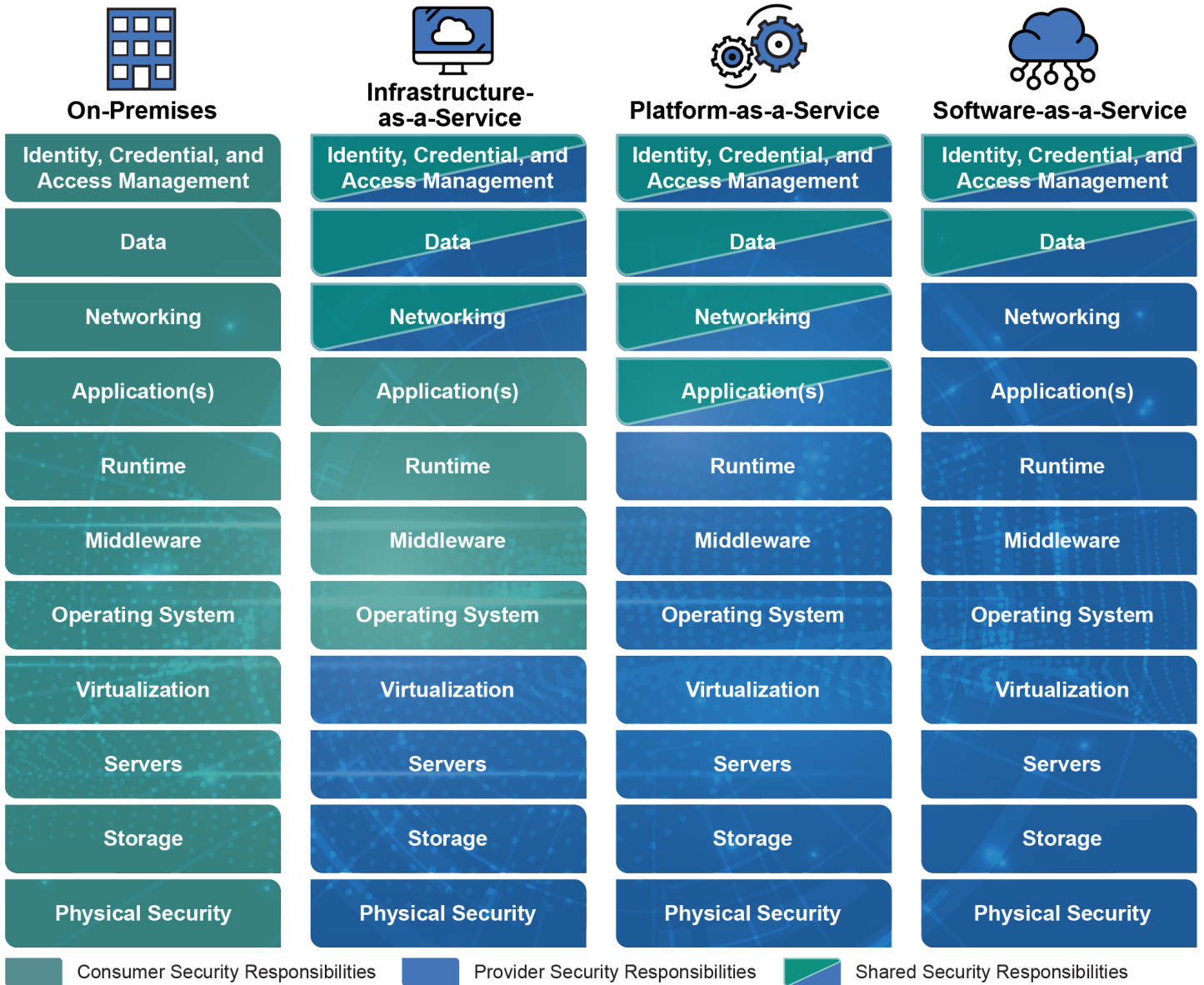
The Cybersecurity and Infrastructure Security Agency (CISA) identifies 11 security requirement areas that an organization should consider when assessing the delineation of security responsibilities for the cloud system between the provider, itself, or both.<sup>29</sup> These security responsibilities include identity credential and access management, data, networking, and applications. Figure 2 describes the security responsibilities under on-premises computing and each of the three cloud service models.

<sup>27</sup>In cloud computing there are shared responsibilities, including security responsibilities that differ based on the type of cloud model (i.e., SaaS, PaaS, IaaS) and deployment type (i.e., public cloud, private cloud, hybrid cloud, and multi-cloud).

<sup>28</sup>NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-144 (Gaithersburg, MD: December 2011).

<sup>29</sup>CISA, United States Digital Service, and Federal Risk and Authorization Management Program, *Cloud Security Technical Reference Architecture*, Version 2.0 (Washington, D.C.: June 2022). CISA is an agency within the Department of Homeland Security.

**Figure 2: Security Responsibilities Associated with On-Premises Computing and Each Cloud Service Model**



Source: Cybersecurity and Infrastructure Security Agency (CISA), United States Digital Service, and Federal Risk and Authorization Management Program (data); 32 pixels/rabbit\_1990/stock.adobe.com (icons and images). | GAO-25-106369

For example, according to one company, when adopting services under the IaaS model, the provider is responsible for the underlying



---

infrastructure, such as servers and physical security that support cloud services. The company's responsibilities under this model include securing access to the data and applications it stores within the cloud system and managing security down to the operating system level.

Sixteen of the 18 companies reported applying this practice and considered it to be very or extremely important. For example, companies indicated an important aspect of this practice is that the company adopting the cloud model must fully understand the delineation of security responsibilities within the shared responsibility model. These companies also noted that it is the company's responsibility to ensure it understands the division of security responsibilities between itself and the provider. For example, one company reported that it initially held a misconception that security for the cloud was mostly the responsibility of the provider. However, the company learned during its adoption of cloud solutions that the provider may require the company to be responsible for some aspects of cloud security. Further, while one company indicated that it relied on the provider to define the delineation of responsibilities for both parties, the company nonetheless emphasized the need to ensure it fully understood the security responsibilities delineated by the provider.

### **Enhancing Partnerships with Providers**

Forming partnership arrangements beyond vendor-customer relationships or interactions with account sales managers at providers is beneficial for cloud security. For one company, forming partnership arrangements with the cloud security subject matter experts at the cloud service provider has been positive. For example, the company indicated that building partnerships with cloud security subject matter experts has helped the company to ensure that the incident response teams know how to contact the provider and whom to contact in the event of a cybersecurity breach, which is essential given the shared responsibility nature of cloud. This company noted that this is beyond the relationship with the vendor.

Source: GAO analysis of private sector company survey data. | GAO-25-106369

Regarding approaches to applying the practice of delineating security roles and functions, some companies identified how and where they documented and communicated security responsibilities. For example, one company reported that this practice includes identifying these responsibilities during the acquisition process and describing them in the cloud service contract. Another company reported identifying and

---

describing these responsibilities through postings to online sites accessible by the parties to the cloud services contract.

Other companies indicated that they relied on cloud service providers to define the security responsibilities of the company and the provider. Companies noted that it is standard practice for the providers to delineate security responsibilities based on the service model, and that these are predetermined security responsibilities built into their cloud service product. According to one company, attempting to deviate from this approach would be inefficient. For example, this company reported that the provider outlines security responsibilities, and the organization has limited influence over what aspects of security the provider will cover within its service. Similarly, another company stated that providers have already defined security responsibilities within their shared responsibility model for their cloud services. In applying this practice, the same company stated that the necessary work for the consumer is to ensure that its organization understands the shared responsibility model.

Subject matter experts from four academic institutions agreed that clarifying provider security responsibilities is a leading practice for cloud security. They also provided additional comments about applying this practice. For example, one subject matter expert indicated that the use of a cloud solution imposes a shared security obligation and the organization adopting the cloud solution must learn to manage and work effectively with this new obligation. Another subject matter expert reported that it is particularly important to understand the delineation of security responsibilities when using multiple providers that offer different security guarantees for different portions of the service (e.g., some offer encryption in hardware, while others offer encryption within the application code). In addition, one subject matter expert stated that it is also important to define user-level responsibilities.



Organizations adopting cloud solutions should ensure the Identity, Credential, and Access Management (ICAM) policies and procedures are developed and implemented.<sup>30</sup> Clearly documenting ICAM policies and procedures helps an organization ensure effective adoption and that it provides the right individual access to the right resource, at the right time, and for the right reason. Applying this practice requires that the documentation include identity and authentication procedures for the cloud system. For example, the use of phishing-resistant multifactor authentication for its users of the cloud system should be included in the documentation. In addition, the documentation should incorporate access control policy and procedures that outline how to (1) identify the authorized users of the system, group and role membership, and access authorizations; (2) identify, document, and define system access authorizations to support separation of duties; and (3) employ least privilege for specific duties and systems.<sup>31</sup>

Seventeen of the 18 companies reported applying this practice and considered it to be very or extremely important. Additionally, companies provided a variety of perspectives on this practice. For example, one company stated this practice is extremely important because of the significant role that identity and access plays in cloud security. This company added that this is particularly important because cloud systems

<sup>30</sup>Credentials are used to verify the identity of users, authenticate them, and grant access to storage systems and tools. Different forms of credentials exist, including physical keys, tokens and cards, passwords, digital private keys, session cookies, and digital certificates on websites, among others.

<sup>31</sup>The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more.

---

often do not have the extra layer of security associated with traditional data centers that offered on-site direct network protections. Another company stated that identity and access authorizations are two of the most important foundational capabilities for cloud adoption to maintain a secure environment, particularly if the organization intends to support hybrid architectures such as public and private cloud models, and more than one provider.<sup>32</sup> Similarly, another company noted that identity practices, particularly for privileged services and credentials, are an important control for cloud environments.

Companies also provided details of approaches they took to apply this practice. For example, one company cited the importance of documenting how to, among other things, register and authenticate first-time users; manage password resets or account lockouts; and grant or revoke access permission. Another company noted that the company uses an Identity-Aware Proxy, which can be a helpful tool to implement security procedures.<sup>33</sup> According to the company, the Identity-Aware Proxy ensures that all access to the cloud is from known accredited sources when the company enables any service within its cloud offerings.<sup>34</sup>

Subject matter experts from four academic institutions agreed that documenting security procedures is a leading practice for cloud security. However, one subject matter expert warned that documenting ICAM procedures might not cover certain security vulnerabilities.<sup>35</sup> For example, while only authorized users have access to an organization's cloud-based application, other users could also access the platform if the cloud is multi-tenant.<sup>36</sup> In a multi-tenant cloud environment, multiple users and organizations share the same resources and storage. While there are

---

<sup>32</sup>Hybrid architecture is the cloud infrastructure that is a composition of two or more deployment models (i.e., Private, Community, or Public). In this instance, multiple deployment models are connected through a standardized or proprietary technology offered by the cloud provider to maintain compatibility of data and applications.

<sup>33</sup>Identity-Aware Proxy is a cloud security service that provides secure access to users based on authentication and authorization.

<sup>34</sup>Cloud offerings consist of, for example, components and services available in the cloud instead of on premise.

<sup>35</sup>A vulnerability is defined as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

<sup>36</sup>Multi-tenancy is defined as the allocation of physical or virtual resources such that multiple cloud tenants and their computations and data are isolated from and inaccessible to one another.

---

security boundaries in place to keep each tenant’s data separated, incomplete or unclear ICAM documentation can result in vulnerabilities or misconfiguration of access controls that can potentially affect all tenants.



Organizations adopting cloud solutions should develop and implement a plan for continuously monitoring their cloud systems. Continuous monitoring helps the organization (i.e., the consumer) to ensure that it has ongoing awareness of its cloud security and privacy posture to support its organizational risk management decisions. Applying this practice includes developing and implementing a plan for continuously monitoring the security controls that are the organization’s responsibility. In addition, this practice includes performing periodic (e.g., monthly) reviews of continuous monitoring reports (e.g., security control assessments) from the provider. Further, this practice also includes documenting how an organization plans to use vulnerability management procedures and tools to monitor the cloud infrastructure and collect and review audit logs.

Sixteen of the 18 companies reported applying this practice and considered it to be very or extremely important. Additionally, companies provided perspectives on the approaches and mechanisms they used to implement continuous monitoring of their cloud system. For example, three companies reported one common approach—using automated solutions that are readily available for continuous monitoring of the cloud. For example, one company indicated that it implemented cloud native built-in monitoring tools and third-party solutions for monitoring, including centralized logging solutions to aggregate logs. This company noted that its security team regularly reviews report logs for anomalies or security incidents. Another company stated the level of automation in providers’ offerings enables a mix of preventative, detective, and remediative

---

controls for cloud security posture monitoring.<sup>37</sup> Additionally, one company indicated that it used Cloud Security Posture Management and is progressing to a cloud-native application protection platform to manage the continuous monitoring of its cloud system.<sup>38</sup>

In addition to using readily available automated solutions, companies provided a range of approaches on how to implement this practice. For example, one company emphasized the importance of prioritizing continuous monitoring practices based on risk. According to the company, this approach will help ensure that organizations address the most critical vulnerabilities and issues in a timely and appropriate manner. Another company indicated that using Policy as Code (PaC) to help enforce the required configuration is critical both at build time (deployment) and during run time (in production).<sup>39</sup> While one company indicated it did not apply this control to all its cloud applications, it did continuously monitor the cloud applications that the company considered sensitive. This company indicated that it performed continuous monitoring in these instances and incremental monitoring for less sensitive cloud applications.

Subject matter experts from four academic institutions agreed that establishing continuous monitoring is a leading practice for cloud security. They also provided additional comments about this practice's importance and use. For example, one subject matter expert stated that establishing continuous monitoring is often overlooked. Another indicated that, in applying this practice, root cause analysis and diagnostics systems can help quickly identify and isolate sources of security vulnerabilities as they occur.

---

<sup>37</sup>*Preventative controls* such as security and risk assessments provide continuous monitoring and visibility into identities and their permission sets with an automated risk-based context. *Detective controls* such as continuous monitoring and alerting provide insight into system and resource data for continuous reporting and alerts based on metrics or suspicious activity. *Remediative controls* provide automatic remediation of misconfigurations from both users and automated deployments in a cloud environment.

<sup>38</sup>Cloud Security Posture Management means a continuous process of monitoring a cloud environment by identifying, alerting on, and mitigating cloud vulnerabilities; reducing risk; and improving cloud security. The Cloud-Native Application Protection Platform goes beyond monitoring and managing cloud infrastructure configurations. It integrates multiple security capabilities into a unified platform that includes other security functions, such as Cloud Security Posture Management.

<sup>39</sup>PaC enables organizations to monitor, remediate, and automatically enforce policies.



Organizations adopting cloud solutions should ensure security metrics are well-defined in a service level agreement with the cloud service provider. Defining security metrics enables an organization to better assess the security of its cloud solutions. Applying this practice includes ensuring that the organization's service level agreement with the provider defines (1) performance metrics; (2) how the performance would be measured; and (3) enforcement mechanisms to help ensure the specified performance levels are achieved.

Eleven of the 18 companies reported applying this practice and, of these, 10 considered it to be very or extremely important and one considered it to be moderately important. Additionally, companies provided a variety of comments about this practice. For example, companies indicated that service level agreements typically focus on metrics like availability and uptime rather than security. Companies also indicated that they managed internal company metrics for the cloud consumer's portion of the shared responsibility model. One company added that organizations should also ensure that the provider holds security certifications based on broadly accepted information security control frameworks designed for cloud services. Additionally, companies noted it is beneficial to include contractual provisions to ensure that the acquiring company has the right to audit cloud service provider security data and that the provider is responsible for liabilities that may arise. Others pointed out that security metrics are often not part of service level agreements in practice, but that metrics should be required. For example, agreements should include



---

metrics that track patch intervals,<sup>40</sup> vulnerability scanning, penetration testing, or metrics tailored to different cloud service offerings.<sup>41</sup>

Subject matter experts from four academic institutions agreed that defining security metrics is a leading practice for cloud security. However, two subject matter experts indicated that doing so can be difficult. For example, one stated that it is often infeasible to define security using a specific set of metrics. Further, this subject matter expert cautioned that cybersecurity should be viewed holistically, and that metrics can encourage a narrow definition that introduces limitations.



Organizations adopting cloud computing solutions should use a standardized process when conducting risk assessments, security authorizations, and authorizing operational deployment for their cloud system. Using a standardized approach helps organizations to ensure that the organization's security authorization requirements are met. Additionally, organizations may follow accepted industry cybersecurity frameworks, such as those developed by NIST or the Federal Risk and

---

<sup>40</sup>According to NIST, a patch is an update to an operating system, application, or other software issued specifically to correct problems with the software. See NIST, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, Special Publication 800-40r4 (April 2022).

<sup>41</sup>According to NIST, vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an entity's security policy. Penetration testing can help to exploit vulnerabilities, such as misconfigurations and kernel flaws, including but not limited to misconfigured security settings or security flaws in the kernel code that enforces the overall security model for a system. See NIST, *Technical Guide to Information Security Testing and Assessment*, Special Publication 800-115 (September 2008).



---

Authorization Management Program (FedRAMP).<sup>42</sup> These accepted industry frameworks provide standardized requirements that an organization may follow in performing risk assessments and evaluating authorization processes. Applying this practice includes ensuring that the cloud service provider is contractually obligated to meet and maintain the requirements of the standardized approach selected by the organization.

Seventeen of the 18 companies reported applying this practice and considered it to be very or extremely important. Additionally, companies provided a variety of perspectives on the practice and described implementation approaches. For example, one company indicated that following a standardized process is crucial when conducting risk assessments, cloud security authorizations, and granting an authority to operate in a cloud environment. Another company stated that it is important to scale risk assessment and mitigation efforts based on the perceived and actual risk of the service provided.

Companies also tailored their approaches. For example, some companies stated that they used standardized benchmarks, such as those established by NIST, in evaluating cloud services and determining configuration standards. However, others combined internal policies with added benchmarks from recognized frameworks. According to one company, it employs multiple processes and controls for conducting risk assessments and security authorizations. These processes and controls include (1) performing a detailed security review of the cloud service provider and obtaining appropriate legal agreements; (2) implementing an enablement process that involves justifying the need for the service, ensuring the service is in scope for relevant contractual agreements, and documenting security practices and configurations for the service; (3) applying PaC controls to ensure the service is on an approved list before deployment; (4) employing a cloud intake process to ensure development teams have not introduced undue risk; and (5) auditing to evaluate critical systems after implementation.

Companies also indicated that standardized processes can be developed internally as opposed to relying on externally developed standardized processes or frameworks. For example, one company stated it employed

---

<sup>42</sup>FedRAMP is a federal program established to provide a standard approach to assessing and authorizing cloud computing services, and products that results in a joint authorization of cloud providers with respect to a common security risk model. The joint authorization issued can be reused and leveraged across the federal government in cloud computing deployments for which the security risk model applies.

---

a standard process with specific checkpoints for applications being migrated to a cloud environment. This company stated that each new or modified application must pass key reviews, such as a cloud architecture review, at the design, build, test, and validation phases. Although it employed multiple governance processes and controls, another company said it did not include a process to grant authority to operate in the cloud. While granting authority to operate is not a requirement for this company, it has stated that it considers periodic re-reviews of cloud applications to serve this purpose.

Subject matter experts from four academic institutions agreed that having a standardized risk and authorization security process is a leading practice for cloud security. However, one subject matter expert cautioned that cybersecurity standards are not universally agreed upon, adding that each organization's security posture has many facets that represent many kinds of risks.



An organization should develop and implement procedures for responding to and recovering from security and privacy incidents. These procedures help organizations ensure they can quickly address and recover from security incidents and that information resources are protected. Without fully documenting procedures, organizations could be delayed in responding to and recovering from security or privacy incidents for their cloud systems. Furthermore, organizations may not be able to ensure that recovery activities are effective.

Fifteen of the 18 companies reported applying this practice and, of these, 14 considered it to be very or extremely important and one considered it to be moderately important. Additionally, companies provided varying

---

perspectives on how they applied this practice. For example, companies stated that because shared responsibilities may not always be fully understood by all parties, documenting response processes and establishing communication channels helps ensure all parties are clear on their responsibilities. One company stated that it conducted recovery and response “tabletop exercises” to ensure procedures are documented, understood, and vetted through simulated exercises. These exercises include the company’s board of directors and executives, as well as legal and cybersecurity business unit leadership teams. The company stated that the purpose of these exercises is to assess common threats specific to its industry and how the company will respond, communicate internally and externally, and perform gap analyses for continuous improvement. Additionally, this company stated that it used a process called “responsible reporting,” which allows users of its system to identify, without penalty or threat of retribution based on their interactions with their system and solutions, any potential vulnerabilities.<sup>43</sup> Another company stated that it created a comprehensive incident response plan that outlines the roles, responsibilities, and communication channels to be used during incidents. A third company agreed that cloud security recovery protocols should be part of an incident response plan and noted that cloud services usually have redundancy that can be procured to add resilience to incident response procedures.

Implementing automated systems and establishing threat detection and vulnerability assessment teams helps with securing cloud solutions. For example, one company that implemented an automated incident response system said it helps proactively block cyber threats and maintain a secure cloud environment. Additionally, one company indicated it had established a sub-group within its information security department to develop threat detection triggers that provide malicious activity alerts, define response playbooks, and provide training on how to respond. Ensuring security logs are enabled is one of the early steps the company performs when onboarding a new cloud service provider. The company has also established a vulnerability assurance team that scans

---

<sup>43</sup>According to NIST, a tabletop exercise is a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. See NIST, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, Special Publication 800-84 (September 2006).

for vulnerabilities. These teams handle its cloud solutions and on-premises threats.

Subject matter experts from four academic institutions agreed that planning for security incident response procedures is a leading practice for cloud security. One subject matter expert stated that planning for these procedures is very important given that immediate response is critical in security incidents. This subject matter expert added that root cause analysis can help with diagnosing which part of the cloud system is affected so that part of the cloud system can be isolated.

### Companies Reported Six Leading Practices for Developing a Cloud Workforce

Companies reported using six workforce development leading practices when adopting cloud solutions (see app. II for additional information about responses from companies). From before cloud computing migration begins to ensuring that the workforce can provide sufficient support once cloud computing is adopted, most companies found each of these leading practices to be very or extremely important to their cloud adoption strategies. Table 4 identifies and describes these practices.

**Table 4: Six Leading Practices Companies Reported for Developing a Cloud Workforce**

Leading Practice	Description
Identify skill gaps	Identify workforce skill gaps resulting from the adoption of cloud computing solutions.
Retain and recruit	Evaluate retention and recruiting strategies to address skill gaps resulting from the adoption of cloud computing solutions.
Provide resources	Ensure appropriate resources to operate systems in a cloud environment are available to the workforce.
Communicate consistently	Ensure the workforce has dedicated opportunities to communicate with leadership before, during, and after migrating to a cloud environment.
Outsource selectively	Outsource selectively when internal workforce is limited, to maximize cloud utilization and security.
Shift culture	Ensure that internal controls and culture are in line with adopting cloud computing solutions.

Source: GAO analysis of survey data on private sector cloud computing leading practices. | GAO-25-106369

Note: We asked 18 leading companies across various industries in the private sector to assess the importance of leading practices in workforce development during the adoption of their company's cloud services. Specifically, we asked: "(a) Has your company applied these practices as part of its cloud computing workforce development strategy? (b) How important were the practices to your company's adoption and implementation of cloud services as a consumer? and (c) What comments do you have on your answers or on the content and wording of our proposed leading practices?" In addition, companies were asked to provide any additional practices they use that were not included in the survey.



Organizations should identify relevant skill gaps in their workforce resulting from their adoption of cloud computing solutions. This includes identifying the skills required to manage the complexities of a cloud migration as well as how to support the cloud solution once fully deployed. An organization’s current workforce may lack the skills or knowledge required to facilitate a cloud migration or to maintain the solution once migrated. A skills gap analysis can help identify any technical or nontechnical skill gaps and enables management to determine which deficiencies represent a critical need.

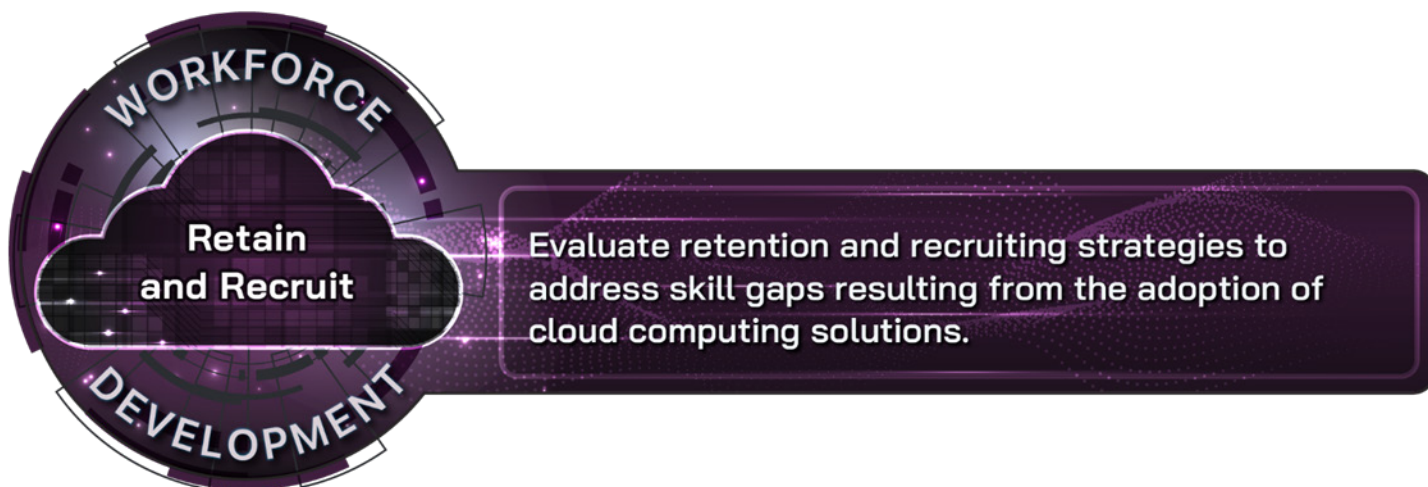
Sixteen of 18 companies reported applying this practice, and 15 considered it to be very or extremely important to their overall cloud workforce development strategy. For example, companies indicated that effective cloud adoption relies on identifying a workforce’s skill gaps. One company indicated that identifying skill gaps allows organizations to provide targeted training and support to their workforce, which improves productivity and efficiency. According to the company, success depends in part on a workforce’s ability to understand, manage, and effectively use adopted cloud solutions. Regarding its application of the practice, a company noted the importance of having a dedicated function for cloud talent focused on skill assessments and connecting employees with internal and external learning content. Another company described implementing a multifaceted approach, which included reorientating existing talent toward new skill requirements, retention efforts, and establishing external partnerships for recruiting to maximize their workforce’s potential in a cloud environment.

Other companies warned about the negative effect of not performing a skills gap analysis before adopting a cloud solution. Specifically, one

---

company cautioned that people are often forgotten when migrating to a cloud environment, and another company noted that performing an analysis earlier during the cloud adoption process could have been helpful. For example, one company stated that it had run into several issues with teams not being knowledgeable enough to support their cloud solutions, which negatively impacted the company later.

Subject matter experts from four academic institutions agreed that identifying skill gaps is a leading practice for developing a cloud workforce. They also generally shared similar insights on its application and importance. For example, one subject matter expert indicated that, unlike organizations lifting and shifting applications to an externally managed cloud environment where all their procedures remain the same, organizations that intend to start building cloud-based applications will need to identify skill gaps and upskill staff to be effective.



Organizations adopting cloud computing solutions should evaluate their retention and recruiting strategies to identify and address skill gaps. Investing in the right people—specifically, by retaining current employees and recruiting new employees—is critical to successfully adopting cloud computing solutions. Once developed, workforce retention and recruiting strategies should be evaluated and updated to help ensure that an organization has the right people with the right skills needed to be successful operating in a cloud environment.

Sixteen of 18 companies reported applying this practice, and 13 considered it to be very or extremely important to their overall cloud workforce development strategy. One company noted that part of evaluating an organization’s recruitment and retention strategy includes



---

collecting feedback from employees. For example, collecting this feedback helped the company ensure issues, concerns, and questions were addressed both professionally and personally, which increased employee retention rates. The company added that understanding the skills required to be successful at all levels of cloud engineering and development ensures better outcomes when hiring the talent necessary to achieve success.

To help recruit talent, one company reported assessing its compensation levels against the market and updating its compensation package to address identified gaps. However, another company noted that, while investments in talent are critical, hiring staff with needed skills may not always be an option depending on the customization of the cloud solution. To help retain and improve existing talent, one company said it ensures every relevant employee has a career plan that includes time reserved for training in new technologies.

Subject matter experts from four academic institutions agreed that retaining and recruiting is a leading practice for developing a cloud workforce. The subject matter experts also generally shared similar insights on its application and importance. For example, one subject matter expert reiterated the usefulness of identifying clear career development pathways, including future work roles and leadership development.



Organizations adopting cloud computing solutions should ensure staff operating cloud computing solutions are empowered with the resources they need to be effective in the cloud environment. These resources include training, time, and tools such as self-service platforms. By



---

providing these resources, organizations can equip their staff to keep pace with technological innovation and help drive cloud adoption.

Fifteen of 18 companies reported applying this practice, and 15 considered it to be very or extremely important to their overall cloud workforce development strategy. For example, companies reported that workforce success in adopting cloud solutions depends on access to appropriate resources, comprehensive training, and opportunities for continuous learning and innovation. One company noted that neither the workforce nor the company can be successful without appropriate resources in place to do the job. Another company noted the importance of ensuring a strong emphasis on education and training, so the workforce is better positioned for innovation, regardless of the specific cloud solution. In commenting on the practice, one company highlighted the importance of budgeting time for employees to learn and grow by establishing “invest in yourself” days, during which employees are free to prioritize their own learning over other business objectives or deliverables. Further, multiple companies stated that self-service platforms that incorporate automation, abstract more technical aspects of cloud computing away from end users, and standardize product offerings assist in the workforce’s ability to implement cloud solutions.

Regarding how they applied the practice, companies reported providing a wide variety of training opportunities, both internally and externally, with some companies partnering directly with cloud service providers for training. Training suggestions also included online self-paced courses, in addition to cloud bootcamps where teams have a dedicated place to learn and practice skills while being supported by trainers. Multiple companies specifically recognized the importance of providing training environments, such as sandboxes, for trainees to practice hands-on and with real-world scenarios. Two companies also stressed the timing of training provided, warning that if newly learned skills were not used relatively quickly, knowledge and skillsets tended to fade.

Two companies highlighted the importance of onboarding new technical staff and providing consistent training or refresher courses for current staff because cloud computing develops at a much faster pace than traditional infrastructure. One company specified that these efforts should include regular collaboration between providers, leadership, and staff to identify training needs and upcoming technologies that may be used in future cloud initiatives. The company added that failing to have a proper training methodology places the company at risk of falling behind on cloud computing technology. Another company stated that training within

---

the organization should begin before formally committing to the implementation of cloud solutions, while another company noted training should go beyond technical skills and include other considerations such as cost optimization.

Subject matter experts from three of four academic institutions agreed that providing workforce development resources is a leading practice for developing a cloud workforce. For example, one subject matter expert reiterated the importance of training related to cost optimization, since the billing structure of cloud computing can lead to delayed realization of surprisingly high costs. Another subject matter expert reiterated the importance of providing training before migrating to a cloud environment.



Organizations adopting cloud computing solutions should ensure that their workforce has dedicated opportunities to communicate with leadership before, during, and after migrating to a cloud environment. This practice includes developing a communication plan that helps ensure an organization's workforce has opportunities to provide feedback throughout the cloud migration process. Communicating consistently can help employees understand the changes that occur when adopting cloud computing solutions. For example, organizations can ease workforce concerns by clearly articulating how the current workforce will align once cloud adoption is complete. Organizations may obtain useful feedback from staff impacted by a new cloud solution that can enhance the organization's cloud migration. Consistent communication should continue after the organization adopts each cloud service to help ensure that employees continue to have opportunities to raise concerns and provide feedback.

---

Fifteen of 18 companies reported applying this practice, and 11 considered it to be very or extremely important to their overall cloud workforce development strategy. For example, one company noted that this practice helps address the expected resistance and denial phases of adopting cloud computing solutions. Another company noted that its engineering and product teams have regular meetings in which product teams can communicate what is working, what is not working, how a strategy may need to shift, and what needs to be done to make improvements. The company added that understanding expectations prior to moving to the cloud helps ensure there are opportunities to communicate and agree upon the validity of those expectations.

Regarding how it applied the practice, one company noted that its cloud program management includes an IT communications team that regularly connects with senior management, IT leadership, and staff via multiple communication channels. Another company keeps its workforce informed about progress, challenges, and milestones and formed a “cloud success team” to help answer cloud migration questions.

### **Clear Communication Helps Organizations Embrace Change**

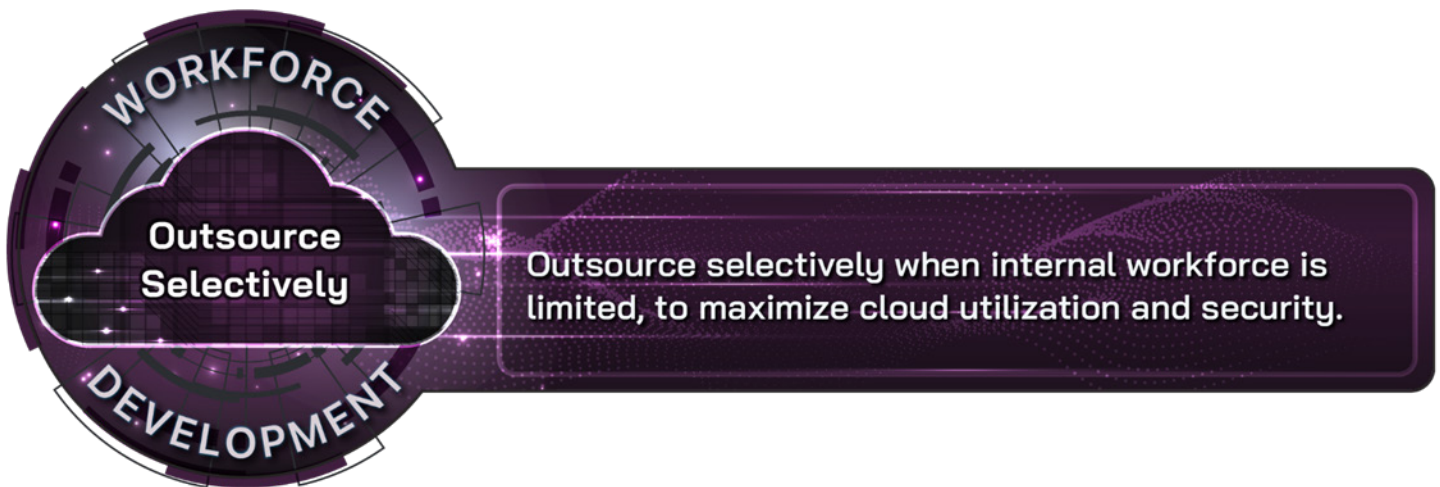
One company emphasized that coming to a mutual understanding around the cloud migration, both from the perspective of company-to-vendor and company-to-workforce, was crucial to its successful adoption of cloud solutions. The company partially attributes its ability to come to a mutual understanding by communicating clearly in common language and avoiding overly complex industry terms. In doing so, it was able to effectively articulate its needs and challenges during negotiations with providers, limiting the potential of dispersed follow-on efforts, which can cause increased complexities for the workforce. Additionally, the company acknowledged that communicating clearly with the workforce about the migration was crucial for the workforce to understand and embrace the change. Multiple companies agreed that having a mutual understanding and agreement of internal stakeholders aided in their successful adoption of cloud solutions.

Source: GAO analysis of private sector company interview statements and survey data. | GAO-25-106369

Subject matter experts from four academic institutions agreed that consistent communication between the workforce and leadership is a leading practice for developing a cloud workforce. For example, two subject matter experts reiterated the importance of workforce

---

communication for understanding requirements and expectations regarding new cloud solutions.



Organizations should selectively outsource to supplement their internal workforces and maximize cloud utilization and security. Outsourced staff can be used to fill identified skill gaps, either as the solution to those gaps or as a temporary measure while individuals with relevant skills are recruited. Organizations should also consider what functions can be outsourced without risking the loss of institutional knowledge.

Fifteen of 18 companies reported applying this practice, and 10 considered it to be very or extremely important to their overall cloud workforce development strategy. For example, one company stated this practice helps to ensure the effect of skill shortages in the talent pool are strategically addressed to augment its internal workforce. This company added that outsourcing its staff accelerated its cloud adoption efforts by supplementing its existing workforce with the requisite technical skills. Another company noted it leverages cloud service provider support staff to confirm the company is adhering to best practices. Further, another company stated that getting direct support from providers helps resolve issues faster and build the right cloud environment architecture.

Regarding how they applied the practice, companies noted risks associated with outsourced staff. For example, one company cautioned that outsourced staff may not be upfront about their skills. Companies also highlighted the risk of not having a proper knowledge transfer plan in place when a contract ends or when a contractor leaves. Another company added that it was cautious about over-relying on outsourced

---

staff, as skillsets are harder to retain, and it prefers to build capabilities in-house.

One company reported relying heavily on outsourced staff, but that it strategically identifies where the outsourced staff might be needed to mitigate the effect of knowledge leaving the company at the end of the contract period. The company added that it periodically reviews staffing needs, portfolio planning, and financial assessments to ensure workload expectations meet staffing plans and capacity. Further, a formal handoff from outsourced staff or the involvement of an internal employee during the effort ensures the company retains the necessary knowledge. The company added that outsourced staff are generally used when its internal workforce is at capacity, and the additional work efforts are for a limited time and scope.

Subject matter experts from three of four academic institutions agreed that outsourcing selectively is a leading practice for developing a cloud workforce. For example, one subject matter expert reiterated the risk of assuming outsourced staff have the needed skills and experience. Another subject matter expert reiterated the need for a plan when outsourced work ends.



Organizations adopting cloud computing solutions should ensure their internal controls and culture are in line with migrating to a cloud environment. Factors to consider include the functions and capabilities of existing staff, existing business processes, and internal frameworks and guidelines. Understanding the interdependencies and strengths of the operational environment before adopting cloud computing helps the organization innovate and more effectively use resources budgeted for

---

the cloud migration. This understanding can reveal which functions, processes, or procedures should be reshaped to help the organization maximize the use and effectiveness of the new cloud environment.

Sixteen of 18 companies reported applying this practice, and 15 considered it to be very or extremely important to their overall cloud workforce development strategy. For example, companies noted the importance of having a change management strategy for workforce development and warned against carrying over what the organization did on-premises to the cloud. One approach identified was to have teams with access to cloud solutions review expectations for operating within the cloud environment at regular intervals, as some expectations might be new when compared to on-premises computing. For example, one company reminds its staff of shared responsibilities and that they should not assume everything will operate more effectively simply because a solution is cloud-based.

One company considered controls, compliance, and risk as important pillars for its business culture. The company reported making significant investments to adapt control objectives and procedures to be effective in a cloud environment and remain compliant with existing practices and obligations. Another company stated that it is critical to ensure that the controls and operational instructions that were initially used for on-premises solutions can be adapted for cloud computing without reducing their effectiveness. Further, new operating practices and tools to manage those practices need to be clearly defined, understood, and optimized for desired productivity.

Another company highlighted the importance of cultural readiness when adopting cloud solutions, adding that it created a program office to ensure appropriate upskilling as well as frequent communications regarding modern engineering practices. In addition, realizing the value of cloud solutions requires shifting from existing on-premises operations, making workforce development essential to transition staff to newer, cloud-focused roles. Internal policy development may also be needed since policy can dictate workforce roles. However, if narrow in scope, policy can limit an organization's workforce from taking advantage of cloud computing solutions that improve automation, operations, and security. According to the company, proper internal policy development can be key to allowing current staff to skill-up to strategic cloud roles.

Subject matter experts from four academic institutions agreed that shifting culture is a leading practice for developing a cloud workforce. For

example, one subject matter expert indicated that it is important to clarify the objectives, timeline, and challenges of the transition with staff and provide tailored training prior to migrating to a cloud environment. Further, it can be helpful for organizations to proactively invest in tools that facilitate the migration, such as monitoring and diagnostics systems frameworks, that can reduce the burden of the migration on affected staff.

## Companies Apply Various Methods to Address Cloud Adoption Challenges and Other Technical Considerations

Companies identified potential challenges, such as mitigating vendor lock-in, that may arise when adopting cloud computing solutions. To address these challenges, companies reported applying a broad range of methods and approaches in the areas of acquisition, cybersecurity, and workforce development. In addition, due to the various ways cloud solutions can be deployed, companies also identified technical considerations that can affect the long-term success of an organization’s cloud initiatives. These technical considerations can lead to additional challenges if organizations do not proactively consider their potential implications.

## Companies Addressed Challenges in Acquisition, Cybersecurity, and Workforce Development when Adopting Cloud Computing Solutions

Companies identified potential challenges related to cloud adoption and various approaches or methods for addressing those challenges. While some challenges were specific to one management area, such as acquisition or cybersecurity, others cut across management areas (see table 5). In addressing these challenges, companies helped ensure the success of their cloud adoption efforts.

**Table 5: Potential Challenges Companies Reported for Adopting Cloud Computing Solutions**

	Acquisition	Cybersecurity	Workforce Development
Mitigating vendor lock-in	✓		
Coordinating cloud acquisitions at large organizations	✓		
Controlling and estimating costs	✓		✓
Onboarding complex processes and legacy systems	✓	✓	
Balancing security and transparency		✓	
Ensuring access management		✓	
Addressing inadequate governance			✓
Overcoming skill shortages			✓

Source: GAO analysis of private sector company survey data. | GAO-25-106369



---

Note: We asked 18 leading companies across various industries in the private sector to identify challenges that organizations may need to address when adopting cloud services. For example, we asked: "What, if any, acquisition challenges (e.g., barriers, concerns, or operational hurdles) has your company experienced in adopting or implementing cloud services as a consumer? And what specific actions has your company taken to address or mitigate them?" We asked a similar pair of questions for cybersecurity and workforce development.

## Mitigating Vendor Lock-In

Two companies reported experiencing challenges with mitigating vendor lock-in (i.e., maintaining the flexibility to switch providers when needed) when acquiring cloud solutions. The potential for vendor lock-in varies by provider and cloud service, with some services limiting options more than others by making it more difficult or expensive to move data or applications to other platforms. Organizations seek to minimize the potential of vendor lock-in, where possible, to maintain control and avoid higher costs or limited capabilities from their cloud solutions in the future.

To mitigate vendor lock-in, one company reported adopting a multi-cloud strategy early in its migration to a cloud environment, which helped enable flexibility across different providers. The company also incorporated containerization technology to disassociate its applications from specific cloud platforms. Further, another company highlighted the importance of cloud environment interoperability, data portability, and application compatibility for organizations seeking to avoid vendor lock-in and artificially increased costs.

## Coordinating Cloud Acquisitions at Large Organizations

Two companies with multiple business units reported experiencing challenges with coordinating their cloud solution acquisitions across their enterprise. Further, it can be challenging for a large organization to establish an account with a cloud service provider that adheres to internal standards and includes appropriate contract governance. For example, one company described how one vendor attempted to sell the same cloud solutions to multiple business units within the company.

To better coordinate its cloud adoption efforts, the company created a centralized cloud acquisition team to strategically manage all contracts and prevent the company from committing to multiple contracts for the same services. In addition to facilitating better internal coordination, the company noted that this approach may result in cost savings due to the discounted price of consolidating smaller contracts. Another company also reported centrally managing contract governance for its cloud services to help ensure accurate billing and credit distribution. This approach included establishing a dedicated team to ensure new accounts adhere to standards using automation.

---

---

## Controlling and Estimating Costs

Six companies reported experiencing challenges with effectively controlling and estimating the current and projected costs of their acquired cloud solutions. Additionally, unexpectedly high costs may arise from having an inexperienced workforce. Cloud pricing models can be complex, with costs that vary based on size, expected consumption, and contractual negotiations, making it difficult to forecast spending in the long term. Further, one subject matter expert noted that services are typically billed in delayed cycles, such as weekly or monthly, making usage costs less visible to users. One company identified that inefficiencies can also occur when organizations do not fully utilize acquired cloud solutions, such as in cases where they have purchased excess licenses or seats. Without careful planning, organizations adopting cloud solutions may face unexpected expenses or cost overruns.

To address these challenges, companies used several proactive approaches. To help control costs, one company reported providing a centralized cloud financial support team with full access to accounting and bookkeeping details for all the business units that use its acquired cloud solutions. Another company reported that market research was critical in ensuring fair pricing, adding that it can take several rounds of negotiation before an agreement is signed. Similarly, one company reported being able to develop an enterprise-wide budgeting strategy and cost estimation tools after conducting market research. These developments helped the company to align its cloud technology investments with critical IT needs to meet strategic business objectives in a more cost-conscious way.

Companies also conducted cost optimization training to educate their workforce, with one company highlighting that cost management and workforce development are critical to the long-term success of cloud adoption efforts. To further control cloud spending, several companies restricted self-service cloud dashboards to only preapproved offerings, with one noting that strategically limiting potential cloud solutions is necessary to ensure consistency across an enterprise. One company also reported implementing a license management system and distributing a monthly usage and spending report to increase awareness of wasted cloud resources.

## Onboarding Complex Processes and Legacy Systems

Five companies reported experiencing challenges with onboarding complex processes or integrating existing workflows and legacy systems to a cloud environment. For example, an organization may discover that its legacy systems are incompatible with modern cloud platforms, requiring significant adjustments or upgrades. Several companies

---

reported related challenges, such as documenting application dependencies, strategically shutting off legacy systems, and maintaining an accurate IT inventory record. Further, one company noted that new service launches are generally not considered enterprise-ready and integrating them could pose cybersecurity challenges.

To address challenges associated with onboarding complex processes, companies reported establishing a systematic program to migrate all on-premises applications and data to the cloud environment, including building automation tools and templates to simplify the process. Further, one company reported documenting its application dependencies by conducting application analyses and mapping based on their current operational environment. The company then documented its results in a configuration management database. To maintain an accurate inventory of IT infrastructure, the company also reported performing a monthly reconciliation with the provider to ensure the accuracy of its records during and after the initial migration to the cloud environment. To mitigate cybersecurity risks, one company prioritized working with its cloud service provider to address consistency across a set of key enterprise cybersecurity principles for new services.

## Balancing Security and Transparency

Two companies reported experiencing challenges with balancing the security of their cloud computing solutions with transparency into provider practices. According to one company, cybersecurity and risk assessments have become more difficult as cloud services grow in complexity with more dependencies. Further, another company reported that gaining visibility into a provider's real-time cybersecurity posture and addressing concentration risk from consolidating infrastructure on specific providers were significant challenges.

To address these challenges, companies used several proactive approaches. For example, one company reported investing in cybersecurity and risk threat modeling capabilities and threat modeling solutions specific to its industry. Another company reported seeking more visibility into its provider's security posture by taking steps to review the provider's vulnerability detection and patching process to understand its risk exposure. The company also evaluated risks that arose from consolidating its infrastructure with a specific provider for a specific service in a specific region. The company noted that the risk is greater when its third-party affiliates are using the same provider and services in the same region. Further, one company commented that it is important to evaluate the transparency of a cloud service provider's security practices

---

against the organization's needs (e.g., data residency and sovereignty) when securing cloud solutions.

### Ensuring Access Management

Two companies reported experiencing challenges with managing access to secure cloud solutions. For example, one company noted it is challenging to assign user privileges in a way that balances security and productivity while maintaining appropriate segregation of duties. Another company noted challenges associated with intellectual property. Specifically, the company indicated that beyond basic privacy concerns are concerns involving cloud services that may access, operate, and manage the company's intellectual property.

To address these challenges, one company indicated it implemented a rigid process involving the CIO and chief information security officer teams. These teams perform a deeper analysis of the products and expect the provider to offer additional details on the practices they follow to secure their services. Another company reported taking several actions to address this challenge, including (1) assigning access privileges at the relevant level within the resource hierarchy to limit the risk exposure from a compromised account; (2) enforcing multifactor authentication for all cloud platform access; (3) implementing a privilege elevation model with a privileged identity management tool that requests justification or routes to a manager for approval before additional access rights are granted for a short period of time; (4) reviewing code changes so that one developer or engineer does not push changes to production without oversight; and (5) maintaining a separation of duties for cloud network privileges that impact multiple subscriptions.

### Addressing Inadequate Governance

Two companies reported experiencing challenges with outdated policies and procedures originally established for on-premises computing. For example, one company said the lack of policies and procedures developed for cloud computing can lead to a lack of consistency in the early stages of cloud adoption, which increases complexities for the workforce. Another company described its first attempt to migrate to a cloud environment as chaotic and inefficient due to a lack of proper governance.

To address this challenge, one company created policies and procedures based on prior experience with cloud computing solutions and leveraged provider resources, such as cloud adoption frameworks, so it did not have to develop practices during the adoption effort. Before another company's major initiative to migrate to a cloud environment, it established a rigorous

---

governance model, which the company stated was crucial for scaling operations and aligning with industry standards.

## Overcoming Skill Shortages

Six companies reported experiencing challenges due to a lack of available talent, both internal and external, when adopting cloud computing solutions. For example, one company, which preferred to minimize its usage of outsourced staff, acknowledged difficulties with upskilling and reskilling their internal workforce. The company questioned the validity of cloud service provider certifications and stressed the importance of training the right employees, at the right time, with the right training. Further, overly trained and certified employees or employees trained too far in advance of the cloud migration become more marketable to other organizations and difficult to retain. Multiple companies also acknowledged the difficulty of recruiting, due to the lack of a qualified external talent pool.

To address this challenge, one company reported partnering with universities and industry associations as well as considering applicants with more diverse backgrounds and experiences. While another company and one subject matter expert warned that outsourcing staff may not be possible depending on the cloud computing solution, a company addressed this challenge by only outsourcing staff for more routine cloud operations. As a result, the company's internal workforce can dedicate more of their time to the more advanced aspects of their cloud computing solutions.

---

## Companies Identified Multi-Cloud and Cloud-Native Design as Key Technical Considerations when Adopting Cloud Solutions

In addition to the specific approaches to address challenges discussed above, 10 companies described how multi-cloud or cloud-native design affected their decision-making. These considerations were reported to enhance flexibility, mitigate risks, and optimize resource utilization, while requiring additional investments in workforce training and cybersecurity tools. These technical considerations can lead to additional challenges if organizations do not proactively consider their potential implications.

## Multi-Cloud Strategy

Companies identified adopting a multi-cloud strategy as affecting their cloud acquisition, cybersecurity, and workforce development decisions. While one company noted that there was little technical distinction among U.S. cloud service providers, others indicated that navigating multi-cloud environments affected their cloud acquisition strategies. For example, one company stated that differentiation among providers is more apparent for more sophisticated cloud offerings and technologies, such as those that incorporate artificial intelligence. The company cautioned that due to these differences among certain providers, portability and interoperability

---

can be difficult to achieve. Further, other companies reported having to avoid vendor lock-in and restrictive licensing models as they considered different providers. However, one company added that adopting a multi-cloud approach can optimize costs by incorporating the best service models from each provider based on the provider's ability to scale resources and cost-effectively meet other business needs.

One company noted that operating in a multi-cloud environment adds complexity to cybersecurity decisions. The company indicated that when pursuing services from multiple providers it is better to invest in provider-agnostic security tools rather than relying on native security tools offered by each provider. According to the company, a provider-agnostic approach can mean an organization has to learn, manage, and maintain multiple security solutions per cloud service provider. However, the alternative can leave organizations with suboptimal coverage, such as from a single provider attempting to offer multi-cloud coverage capabilities.

Further, several companies using a multi-cloud strategy described how their workforce required additional training and supporting materials to adapt to the differences between providers, which in turn required more effort and funding. As a result, companies reported prioritizing training programs that help ensure their workforce is proficient across multiple cloud platforms. For example, one company highlighted its use of vendor-neutral training, such as cloud architecture principles, security best practices, and DevOps methodologies, due to the need to work across diverse cloud platforms. This training helped the company also ensure flexibility and adaptability in a multi-cloud environment. Another company added that this approach mitigates dependency risks and enhances flexibility in choosing the most suitable cloud services for various business needs.

## Cloud-Native Design

Companies also identified cloud-native (i.e., provider-agnostic) design, including the use of containerization technology, as affecting their cloud acquisition and cybersecurity decisions. For example, one company noted that provider-native applications can make it difficult to decouple company assets from cloud service providers. As a result, the company reported intentionally incorporating cloud-native design to support its long-term technology and business strategy.

According to one company, integrating containerization training into its workforce development initiatives helped teams efficiently deploy and manage containerized applications. This company reported also using



---

cloud integration tools to streamline data and applications across cloud platforms and on-premises environments, while emphasizing training on these tools to help ensure seamless interoperability and data flow. According to the company, these efforts enabled its workforce to better adapt to evolving technical landscapes and optimize cloud utilization. Further, another company noted that integration with other cloud services, including those from other providers, is important. According to the company, this can be achieved through configuration settings or application programming interfaces.

One company added that shifting to self-service onboarding of new services via containerization technology with built-in security requirements and serverless infrastructure helped accelerate development and data analytics without compromising security or existing policies. While containerization makes multi-cloud use easier due to containers being more portable, the company stated that containerization can cause organizations to lose some benefits. These include some provider managed services offered under the PaaS and SaaS deployment models.

Another company stated that it creates agnostic controls based on risk assessments and considered this process important. This process involves identifying and applying technical controls to mitigate risks across different providers, as each provider handles identity and access management and network separation differently. This company stated that it prioritizes protecting its data and information by ensuring compliance with requirements across various cloud environments. A third company also indicated that it ensured that its monitoring solutions and controls were not bound to a specific provider.

---

## Company Comments

We provided relevant portions of a draft of this report to participating companies for review and comment. Companies provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

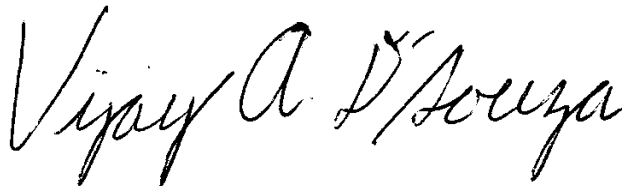
If you or your staff have any questions about this report, please contact Brian Bothwell at (202) 512-6888 or [BothwellB@gao.gov](mailto:BothwellB@gao.gov) or Vijay A. D'Souza at (202) 512-7650 or [DSouzaV@gao.gov](mailto:DSouzaV@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on

---

the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.



Brian Bothwell  
Director  
Science, Technology Assessment, and Analytics



Vijay A. D'Souza  
Director  
Information Technology and Cybersecurity

# Appendix I: Objectives, Scope, and Methodology

Our objectives were to identify (1) leading practices in the private sector for adopting cloud solutions and (2) approaches in the private sector to address challenges regarding the adoption of cloud solutions.

To address these two objectives, we (1) reviewed prior GAO work and federal and nonfederal guidance related to cloud computing to identify potential leading practices in the areas of acquisition, cybersecurity, and workforce development; (2) elicited the participation of 18 private sector leading companies based on rankings in well-recognized lists and awards, among other factors; (3) created, pretested, and administered a survey to those companies and conducted follow-up interviews; and (4) validated the leading cloud adoption practices by soliciting and incorporating feedback from cloud computing subject matter experts at academic institutions. We also asked companies about their approaches for addressing challenges and related technical considerations associated with adopting cloud computing solutions. The following provides details on each of these four steps, as well as how their results were used to complete each of our two objectives.

## Step 1: Review federal and non-federal guidance and prior GAO work related to cloud computing

To identify a comprehensive list of leading practices for adopting and implementing cloud computing services, we first analyzed relevant federal and nonfederal guidance resources targeted at helping federal agencies and other organizations migrate to a cloud environment. Table 5 includes a selection of these resources. In addition, we reviewed prior GAO reports related to cloud computing initiatives in the federal government,<sup>1</sup> and performed a search of other related literature, including studies, journals, research papers, and news articles.

**Table 6: Selected Federal and Nonfederal Cloud Computing Guidance Resources**

Organization	Guidance	Published date
CDG	Best Practice Guide for Cloud and as-a-Service Procurements	2023
CSA	Security Guidance for Critical Areas of Focus in Cloud Computing (v4.0)	July 2017

<sup>1</sup>For example, we reviewed the following four reports: GAO, *Chief Information Officers: Private Sector Practices Can Inform Government Roles*, [GAO-22-104603](#) (Washington, D.C.: Sept. 15, 2022); *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization*, [GAO-22-104070](#) (Washington, D.C.: July 28, 2022); *Cloud Computing: DOD Needs to Improve Tracking of Data User Fees*, [GAO-23-106247](#) (Washington, D.C.: Sept. 12, 2023); and *Cloud Security: Selected Agencies Need to Fully Implement Key Practices*, [GAO-23-105482](#) (Washington, D.C.: May 18, 2023).

**Appendix I: Objectives, Scope, and Methodology**

<b>Organization</b>	<b>Guidance</b>	<b>Published date</b>
CISA	Cloud Security Technical Reference Architecture (v2.0)	June 2022
GSA	Best Business Practices for USG Cloud Adoption	December 2016
	Cloud Adoption Center of Excellence Playbook	September 2020
	Federal Cloud Strategy Guide: Agency Best Practices for Cloud Migration (v1.1)	February 2021
NIST	Special Publication 500-291, Version 2: NIST Cloud Computing Standards Roadmap	July 2013
	Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing	December 2011
NSA	Mitigating Cloud Vulnerabilities	January 2020
OMB	Federal Cloud Computing Strategy	June 2019
	Circular No. A-130: Managing Information as a Strategic Resource	July 2016
PCI SSC	Cloud Computing Guidelines (v3.0)	April 2018

CDG = Center for Digital Government

CISA = Cybersecurity and Infrastructure Agency

CSA = Cloud Security Alliance

GSA = General Services Administration

NIST = National Institute of Standards and Technology

NSA = National Security Agency

OMB = Office of Management and Budget

PCI = Payment card industry

SSC = Security Standards Council

USG = United States Government

Source: GAO analysis of federal and nonfederal cloud computing guidance. | GAO-25-106369

Based on our review of this information, we identified three cloud management areas—acquisition, cybersecurity, and workforce development—and 21 potential leading practices regarding the effective adoption and implementation of cloud computing solutions that may be applicable to the private sector.

**Step 2: Select private sector companies to include in the survey**

To better ensure that we surveyed private sector companies with valuable experiences regarding the adoption of cloud computing solutions, we took steps to choose private sector companies that have demonstrated excellence in technological innovation and effective business practices. We collected data from Leadership Connect’s “Top 1,000 Companies,” “Company CIO & CISO,” and “Top Companies – Government Affairs” databases. Based on information contained in these databases, we identified a set of 100 companies by considering each company’s number of employees, annual revenue, domestic location, and primary industries

and excluded those companies that were missing relevant information. We also identified 34 companies that had been recognized in multiple award lists for technological innovation and business practices. These lists were the Boston Consulting Group's Most Innovative Companies, Business Intelligence Group's Innovation Awards, the Fast Company Top 50 Most Innovative Companies, the Massachusetts Institute of Technology's Technology Review's 50 Smartest Companies, Thomson Reuters' Top 100 Global Technology Leaders, and PWC's Global Innovation 1000 study.

From this selected set of companies, we applied professional judgement to select an initial nongeneralizable sample of 25 companies spanning multiple industries. Over the course of the survey period described in step 3 below, we incrementally expanded the list of companies we selected from this initial set of companies to 101 to increase our survey participation. In soliciting their participation, we attempted to identify the representative or representatives at each company most knowledgeable about its approach to effectively adopting and implementing cloud services as a consumer, such as a company's Chief Information Officer (CIO).

Because the selection of the companies for this study was a nongeneralizable sample, the results are not intended to represent all private sector companies. To this end, the companies we selected are not representative of all private sector companies, and the individuals we surveyed are not representative of all individuals in the private sector. In addition, the practical difficulties of conducting any survey may introduce non-sampling errors. For example, errors can be introduced into the results due to differences in how a particular question is interpreted, the sources of information available to respondents, or the types of people who do not respond to a question. We included steps in both the data collection and data analysis stages to minimize such non-sampling errors. In addition, we reviewed the U.S. System for Award Management to identify if companies had exclusions and removed companies with active exclusions as of April 2024 from our sample.<sup>2</sup>

---

<sup>2</sup>The System for Award Management is the official U.S. government website for publishing and managing federal contracting opportunities. An exclusion identifies an entity excluded from receiving federal contracts, certain subcontracts, and certain types of federal financial and nonfinancial assistance and benefits.

---

Step 3: Create, pretest,  
and administer the survey  
to companies

We developed questions for the survey based on the list of proposed leading practices for adopting and implementing cloud computing solutions. To solicit feedback on those practices and identify any practices not included in our proposed list, we included questions related to each of the three management areas critical to migrating to a cloud environment. Specifically, the survey asked companies about their use of each practice, each practice's importance to the relevant management area within their company's overall cloud adoption strategy, and any comments they may have about each practice. We also included two open-ended questions soliciting general feedback on the full list of proposed leading practices in each management area, as well as any practices they use that were not included in our survey.

With regard to approaches for addressing challenges companies have experienced when adopting cloud computing solutions, we included three open-ended questions soliciting their experiences applying leading practices in all three management areas. Specifically, we asked companies about challenges and related actions taken to address those challenges they have navigated when adopting cloud solutions and other technical considerations. In addition, we prompted companies to share examples where their company successfully adopted cloud services by asking about positive outcomes from their application of practices in each management area.

In December 2023, we conducted a survey pretest with a private sector company to help further refine our questions, develop new questions, and clarify any ambiguous questions. We then revised the survey, as necessary, to reduce the likelihood of overall and item non-response, as well as any reporting errors on our questions.

To further improve the content and format of the survey, we consulted with external subject matter experts on cloud computing in the private sector and reviewed the format of a previous GAO survey on CIO responsibilities. An internal survey specialist helped design the survey and another internal survey specialist independently reviewed the survey's content for methodological appropriateness. To ensure relevancy to private sector companies when we surveyed them, as described above, we analyzed practices intended for both private sector companies and federal agencies and modified the language to be more applicable to private sector companies. For example, we removed references to the Federal Risk and Authorization Management Program



(FedRAMP) from GAO’s previously reported cybersecurity key practices included in our survey.<sup>3</sup>

From February to June 2024, we administered the web survey to the individuals that companies identified as most knowledgeable about their cloud computing adoption and implementation efforts at 23 private sector companies that had agreed to participate. To improve the response rate, we sent email reminders and followed up with phone calls. We ended survey collection on June 17, 2024. Of 23 surveys sent, we obtained responses from 18 companies, for a nearly 78 percent response rate. Table 6 provides the full list of 18 companies whose representatives submitted responses to our survey.

**Table 7: Private Sector Companies that Participated in a 2024 Survey on Cloud Computing Leading Practices**

Company	Industry
Alphabet, Inc.	Media, Information Technology (IT)
Best Buy Co., Inc.	IT, Retail
Broadcom Inc.	IT
Capital One Financial Corporation	Banking, Finance
Eli Lilly and Company	Pharmaceuticals, Manufacturing
HCA Healthcare, Inc.	Health Care
HP, Inc.	Manufacturing, IT
Intel Corporation	Manufacturing, IT
Johnson & Johnson	Health Care, Pharmaceuticals, Manufacturing
JPMorgan Chase & Co.	Banking, Finance, Investing
McKesson Corporation	Health Care, Distribution, IT
Microsoft Corporation	IT
Molina Healthcare, Inc.	Health Care
Nationwide Mutual Insurance Company	Insurance
StoneX Group, Inc.	Finance
The Traveler’s Companies, Inc.	Finance, Insurance
The Walt Disney Company	Arts & Culture, Media, Hotels
Verizon Communications, Inc.	Telecommunications

Source: GAO summary of companies identified by GAO analysis of Leadership Connect data and company information. | GAO-25-106369

<sup>3</sup>GAO, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices*, GAO-23-105482 (Washington, D.C.: May 18, 2023).

We conducted follow-up interviews with selected companies based on the feedback they provided in the survey, among other factors. For example, we interviewed companies with varying experience adopting cloud computing solutions or to collect supporting documentation regarding specific leading practices. In addition, we asked clarifying questions as necessary to better understand the meaning of unclear responses.

The final survey sent to participants and a summary of their responses are replicated in appendix II. Our survey specialist electronically extracted data from the survey responses. We examined the survey results and performed computer analyses to identify missing data, inconsistencies, and other indications of error, and corrected any that we found. For example, GAO staff and an independent GAO analyst performed quantitative data analyses and a review of open-ended responses and checked the data for accuracy.

---

**Step 4: Validate leading practices with cloud computing subject matter experts from academia**

To further validate our leading practices and obtain additional narrative and supporting context for our reporting objectives, we identified subject matter experts in cloud computing from four academic institutions, including those highly ranked in computer science according to U.S. News and World Report. Participating academic institutions included Cornell University, the Massachusetts Institute of Technology, and the Universities of Maryland and Washington. We shared our list of cloud computing leading practices developed using information from the survey distributed to private sector companies and related follow-up interviews with subject matter experts from these institutions to ensure our leading practices reflected the latest knowledge in their field. We then further analyzed the survey responses we received to determine their consistency with results from our coordination with subject matter experts in cloud computing from academia.

We conducted our work from November 2022 to March 2025 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

---

# Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses

---

We administered a web-based survey to 23 private sector companies identified as leaders in business and technological innovation. We administered the survey to refine a list of potential leading practices derived from federal and nonfederal guidance documents and identify additional leading practices missing from those guidance documents, if any, that selected companies employ to help ensure the successful adoption and implementation of cloud services at their organization. The survey also solicited examples of successes and potential or realized challenges those practitioners had experienced using the identified leading practices, including related actions taken to address any realized challenges.

The following sections list the survey questions that we administered and the aggregated results from the responses under each question. Practitioners from 18 leading companies responded to the survey. Narrative answers to open ended text questions are not included below for brevity and to limit the possibility of identification of individual companies.

---

## Survey on Private Sector Cloud Computing Leading Practices

The U.S. Government Accountability Office (GAO), an independent nonpartisan agency of Congress, is identifying leading practices used by private sector companies to effectively adopt and implement cloud computing in their organizations, with a focus on their applicability and potential to improve the federal government's transition to cloud computing.

This survey covers (1) leading practices used by private sector companies in adopting and implementing cloud services as a consumer, particularly in acquisition, cybersecurity, and workforce development, and (2) successes and challenges encountered in application of these practices.

Your company is among the 25 leading private sector companies that we selected from across different sectors such as commerce, communications, and financial services to participate in our survey. Your company's input will be vital in applying proven private sector leading practices to the public sector.

To complete this survey, we are asking that the representative(s) at your company most knowledgeable about the company's approach to effectively adopting and implementing cloud services **respond to the questions below from a cloud consumer perspective.** We define a

cloud consumer as a person or organization that maintains a business relationship with, and uses a service from, a cloud provider.

This survey is focused on the perspectives of cloud consumers. Please ensure that a company's cloud service provider or components within your company that provide cloud services are not involved with responding to any questions contained in the survey.

GAO plans to report survey results in the aggregate. In its public report, GAO will not include individually identifiable data from this survey unless we receive written consent from the relevant company. By participating in the survey, your company will be included in the public list of survey participants that will be published in the final report. For general information about our information security and privacy practices, visit <https://www.gao.gov/surveys>.

In the following sections, we will ask you to assess the importance of leading practices in acquisition, cybersecurity, and workforce development during the adoption and implementation of cloud computing services at your company. We want to know about your company's experience as a **consumer** of cloud computing services, not as a provider.

We compiled a list of **proposed cloud computing leading practices** from our review of both federal and nonfederal policies and guidance. Your responses will help us understand the approaches employed by private sector companies to achieve successful cloud service adoption and implementation in their organizations and enhance our list of proposed leading practices.

### **Acquisition**

1. Please review our proposed list of leading **acquisition** practices below, and answer the following questions:
  - a) Has your company applied these practices as part of its cloud computing acquisition strategy?

**Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses**

**Number of Responses**

	Yes	No	Don't know	No answer
Defining the current operational environment and critical IT needs before pursuing a cloud service solution.	18	0	0	0
Developing and updating cost estimates based on reliable market research for several cloud service options that can meet critical IT needs.	18	0	0	0
Confirming that the chosen cloud service provider's business practices align with long-term mission needs.	18	0	0	0
Soliciting input from relevant stakeholders (e.g., IT and contracting teams and program management) throughout the acquisition process.	18	0	0	0
Ensuring that service provider responsibilities and performance metrics are well defined, and enforcement or remediation plans are established.	18	0	0	0
Evaluating the performance of acquired cloud services to ensure that critical IT needs have been met.	17	1	0	0
Demonstrating the proposed cloud service works as intended in an operational environment as part of the acquisition process.	17	1	0	0
Limiting the use of nonnegotiable contract terms and conditions to those that meet mission and legal requirements.	16	1	1	0

b) How important were the practices to your company's adoption and implementation of cloud services, as a consumer?

**Number of Responses**

	Extremely	Very	Moderately	Slightly	Not at all	Don't know	No answer
Defining the current operational environment and critical IT needs before pursuing a cloud service solution.	12	6	0	0	0	0	0
Ensuring that service provider responsibilities and performance metrics are well defined, and enforcement or remediation plans are established.	9	8	1	0	0	0	0

**Appendix II: Survey Questions Administered to  
Private Sector Companies and Their  
Responses**

	<b>Extremely</b>	<b>Very Moderately</b>	<b>Slightly</b>	<b>Not at all</b>	<b>Don't know</b>	<b>No answer</b>
Evaluating the performance of acquired cloud services to ensure that critical IT needs have been met.	10	6	1	1	0	0
Demonstrating the proposed cloud service works as intended in an operational environment as part of the acquisition process.	11	4	1	2	0	0
Soliciting input from relevant stakeholders (e.g., IT and contracting teams and program management) throughout the acquisition process.	10	4	4	0	0	0
Developing and updating cost estimates based on reliable market research for several cloud service options that can meet critical IT needs.	10	3	3	2	0	0
Confirming that the chosen cloud service provider's business practices align with long-term mission needs.	7	7	3	1	0	0
Limiting the use of nonnegotiable contract terms and conditions to those that meet mission and legal requirements.	8	4	4	0	1	1

c) What comments do you have on your answers or on the content or wording of our proposed leading practices?

<b>Number of Responses</b>	
	<b>13</b>
Soliciting input from relevant stakeholders (e.g., IT and contracting teams and program management) throughout the acquisition process.	13
Demonstrating the proposed cloud service works as intended in an operational environment as part of the acquisition process.	13
Evaluating the performance of acquired cloud services to ensure that critical IT needs have been met.	12
Developing and updating cost estimates based on reliable market research for several cloud service options that can meet critical IT needs.	12
Ensuring that service provider responsibilities and performance metrics are well defined, and enforcement or remediation plans are established.	12
Confirming that the chosen cloud service provider's business practices align with long-term mission needs.	12
Limiting the use of nonnegotiable contract terms and conditions to those that meet mission and legal requirements.	12

**Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses**

Defining the current operational environment and critical IT needs before pursuing a cloud service solution.	<b>10</b>
--	-----------

2. What, if any, feedback do you have to enhance the full list of proposed **acquisition** practices, such as any potential limitations or specific aspects of the practices we may need to take into consideration?

**Number of Responses**

Companies that provided written response to the question.	<b>18</b>
Companies that did not provide a written response to the question.	<b>0</b>

3. What other important **acquisition** practices not listed above has your company employed as a consumer of cloud services?

**Number of Responses**

Companies that provided written response to the question.	<b>18</b>
Companies that did not provide a written response to the question.	<b>0</b>

4. How have any of the **acquisition** practices you have used contributed to positive outcomes for your company? Please share specific examples, if applicable.

**Number of Responses**

Companies that provided written response to the question.	<b>15</b>
Companies that did not provide a written response to the question.	<b>3</b>

5. How, if at all, have any cloud computing technical considerations (e.g., multi-cloud environments, containerization, or integration tools) affected your company's approach to its **acquisition** practices? Please describe these effects and share specific examples, if applicable.

**Number of Responses**

Companies that provided written response to the question.	<b>15</b>
Companies that did not provide a written response to the question.	<b>3</b>



**Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses**

6. What, if any, **acquisition challenges** (e.g., barriers, concerns, or operational hurdles) has your company experienced in adopting or implementing cloud services as a consumer? And what specific **actions** has your company taken to address or mitigate them?

<b>Number of Responses</b>	
Companies that provided written response to the question.	<b>15</b>
Companies that did not provide a written response to the question.	<b>3</b>

**Cybersecurity**

7. Please review our proposed list of leading **cybersecurity** practices below, and answer the following questions:

a) Has your company applied these practices as part of its cloud computing cybersecurity strategy?

<b>Number of Responses</b>				
	<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>No answer</b>
Documenting the identity, credential, and access management policies and procedures for the cloud system.	<b>17</b>	<b>0</b>	<b>0</b>	<b>1</b>
Using a standardized risk and authorization process when conducting risk assessments, security authorizations, and granting an authority to operate in the cloud environment.	<b>17</b>	<b>0</b>	<b>0</b>	<b>1</b>
Defining the delineation of security responsibilities between your company and the cloud service provider for the cloud system.	<b>16</b>	<b>1</b>	<b>0</b>	<b>1</b>
Developing and implementing a plan for continuously monitoring the cloud system.	<b>16</b>	<b>1</b>	<b>0</b>	<b>1</b>
Documenting procedures for responding to and recovering from security and privacy incidents for the cloud system.	<b>15</b>	<b>2</b>	<b>0</b>	<b>1</b>
Defining security metrics in a service level agreement with the cloud service provider.	<b>11</b>	<b>5</b>	<b>1</b>	<b>1</b>

**Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses**

b) How important were the practices to your company's adoption and implementation of cloud services, as a consumer?

**Number of Responses**

	<b>Extremely</b>	<b>Very Moderately</b>	<b>Slightly</b>	<b>Not at all</b>	<b>Don't know</b>	<b>No answer</b>
Documenting the identity, credential, and access management policies and procedures for the cloud system.	15	2	0	0	0	1
Developing and implementing a plan for continuously monitoring the cloud system.	13	4	0	0	0	1
Using a standardized risk and authorization process when conducting risk assessments, security authorizations, and granting an authority to operate in the cloud environment.	13	4	0	0	0	1
Documenting procedures for responding to and recovering from security and privacy incidents for the cloud system.	13	1	3	0	0	1
Defining the delineation of security responsibilities between your company and the cloud service provider for the cloud system.	12	4	0	0	1	1
Defining security metrics in a service level agreement with the cloud service provider.	8	2	2	3	0	2

c) What comments do you have on your answers or on the content or wording of our proposed leading practices?

**Number of Responses**

Defining the delineation of security responsibilities between your company and the cloud service provider for the cloud system.	<b>10</b>
Developing and implementing a plan for continuously monitoring the cloud system.	<b>10</b>
Defining security metrics in a service level agreement with the cloud service provider.	<b>9</b>
Using a standardized risk and authorization process when conducting risk assessments, security authorizations, and granting an authority to operate in the cloud environment.	<b>9</b>
Documenting procedures for responding to and recovering from security and privacy incidents for the cloud system.	<b>9</b>

**Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses**

Documenting the identity, credential, and access management policies and procedures for the cloud system.	<b>8</b>
---	----------

8. What, if any, feedback do you have to enhance the full list of proposed **cybersecurity** practices, such as any potential limitations or specific aspects of the practices we may need to take into consideration?

**Number of Responses**

Companies that provided written response to the question.	<b>13</b>
Companies that did not provide a written response to the question.	<b>5</b>

9. What other important **cybersecurity** practices not listed above has your company employed as a consumer of cloud services?

**Number of Responses**

Companies that provided written response to the question.	<b>13</b>
Companies that did not provide a written response to the question.	<b>5</b>

10. How have any of the **cybersecurity** practices you have used contributed to positive outcomes for your company? Please share specific examples, if applicable.

**Number of Responses**

Companies that provided written response to the question.	<b>11</b>
Companies that did not provide a written response to the question.	<b>7</b>

11. How, if at all, have any cloud computing technical considerations (e.g., multi-cloud environments, containerization, or integration tools) affected your company's approach to its **cybersecurity** practices? Please describe these effects and share specific examples, if applicable.

**Number of Responses**

Companies that provided written response to the question.	<b>12</b>
Companies that did not provide a written response to the question.	<b>6</b>

**Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses**

12. What, if any, **cybersecurity challenges** (e.g., barriers, concerns, or operational hurdles) has your company experienced in adopting or implementing cloud services, as a consumer? And what specific actions has your company taken to address or mitigate them?

<b>Number of Responses</b>	
Companies that provided written response to the question.	<b>9</b>
Companies that did not provide a written response to the question.	<b>9</b>

**Workforce Development**

13. Please review our proposed list of leading **workforce development** practices below, and answer the following questions:

- a) Has your company applied these practices as part of its cloud computing workforce development strategy?

<b>Number of Responses</b>				
	<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>No answer</b>
Identifying workforce skill gaps resulting from a transition to cloud-based solutions.	<b>16</b>	<b>1</b>	<b>0</b>	<b>1</b>
Evaluating retention and hiring to address skill gaps.	<b>16</b>	<b>1</b>	<b>0</b>	<b>1</b>
Ensuring that internal controls and culture are in line with transitioning to the cloud.	<b>16</b>	<b>1</b>	<b>0</b>	<b>1</b>
Ensuring appropriate resources (e.g., training) to operate systems in a cloud environment are available to the workforce.	<b>15</b>	<b>2</b>	<b>0</b>	<b>1</b>
Ensuring stakeholders and users have dedicated opportunities to communicate before, during, and after transition to the cloud.	<b>15</b>	<b>2</b>	<b>0</b>	<b>1</b>
Using contract support (e.g., cloud service provider offerings) when in-house technical workforce is limited, to maximize cloud utilization and security.	<b>15</b>	<b>2</b>	<b>0</b>	<b>1</b>
Understanding the risks and contractual limitations when contracting work.	<b>14</b>	<b>2</b>	<b>1</b>	<b>1</b>

- b) How important were the practices to your company's adoption and implementation of cloud services, as a consumer?

**Appendix II: Survey Questions Administered to Private Sector Companies and Their Responses**

**Number of Responses**

	<b>Extremely</b>	<b>Very</b>	<b>Moderately</b>	<b>Slightly</b>	<b>Not at all</b>	<b>Don't know</b>	<b>No answer</b>
Ensuring that internal controls and culture are in line with transitioning to the cloud.	8	7	2	0	0	0	1
Ensuring appropriate resources (e.g., training) to operate systems in a cloud environment are available to the workforce.	10	5	1	0	0	1	1
Identifying workforce skill gaps resulting from a transition to cloud-based solutions.	9	6	0	1	0	0	2
Evaluating retention and hiring to address skill gaps.	7	6	2	1	0	0	2
Ensuring stakeholders and users have dedicated opportunities to communicate before, during, and after transition to the cloud.	6	5	4	1	0	1	1
Understanding the risks and contractual limitations when contracting work.	8	4	2	0	0	2	2
Using contract support (e.g., cloud service provider offerings) when in-house technical workforce is limited, to maximize cloud utilization and security.	5	5	3	2	1	0	2

c) What comments do you have on your answers or on the content or wording of our proposed leading practices?

**Number of Responses**

Identifying workforce skill gaps resulting from a transition to cloud-based solutions.	<b>11</b>
Ensuring appropriate resources (e.g., training) to operate systems in a cloud environment are available to the workforce.	<b>10</b>
Using contract support (e.g., cloud service provider offerings) when in-house technical workforce is limited, to maximize cloud utilization and security.	<b>10</b>
Ensuring that internal controls and culture are in line with transitioning to the cloud.	<b>9</b>
Evaluating retention and hiring to address skill gaps.	<b>8</b>
Understanding the risks and contractual limitations when contracting work.	<b>8</b>
Ensuring stakeholders and users have dedicated opportunities to communicate before, during, and after transition to the cloud.	<b>7</b>

---

**Appendix II: Survey Questions Administered to  
Private Sector Companies and Their  
Responses**

---

14. What, if any, feedback do you have on ways to enhance the full list of proposed **workforce development** practices, such as any potential limitations or specific aspects of the practices we may need to take into consideration?

---

**Number of Responses**

Companies that provided written response to the question.	<b>14</b>
Companies that did not provide a written response to the question.	<b>4</b>

---

15. What other important **workforce development** practices not listed above has your company employed as a consumer of cloud services?

---

**Number of Responses**

Companies that provided written response to the question.	<b>14</b>
Companies that did not provide a written response to the question.	<b>4</b>

---

16. How have any of the **workforce development** practices you have used contributed to positive outcomes for your company? Please share specific examples, if applicable.

---

**Number of Responses**

Companies that provided written response to the question.	<b>14</b>
Companies that did not provide a written response to the question.	<b>4</b>

---

17. How, if at all, have any cloud computing technical considerations (e.g., multi-cloud environments, containerization, or integration tools) affected your company's approach to its **workforce development** practices? Please describe these effects and share specific examples, if applicable.

---

**Number of Responses**

Companies that provided written response to the question.	<b>13</b>
Companies that did not provide a written response to the question.	<b>5</b>

---

18. What, if any, **workforce development challenges** (e.g., barriers, concerns, or operational hurdles) has your company experienced in

---

**Appendix II: Survey Questions Administered to  
Private Sector Companies and Their  
Responses**

---

adopting or implementing cloud services as a consumer? And what specific actions has your company taken to address or mitigate them?

---

**Number of Responses**

Companies that provided written response to the question.	<b>13</b>
Companies that did not provide a written response to the question.	<b>5</b>

---

**Administrative Questions**

19. The GAO team may follow up with the primary survey respondent to discuss responses provided to this survey. Please provide contact information for the company representative primarily responsible for completing this survey.

- a) Name:
- b) Position/Title:
- c) Company:
- d) Email:
- e) Phone:

***Thank you for participating in our survey.***

***On the next page you can review a summary of your responses. You will be able to back up if you need to make any changes.***



---

# Appendix III: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Brian Bothwell, (202) 512-6888, [BothwellB@gao.gov](mailto:BothwellB@gao.gov)

Vijay A. D'Souza, (202) 512-7650, [DSouzaV@gao.gov](mailto:DSouzaV@gao.gov)

---

## Staff Acknowledgments

In addition to the contacts named above, John Ortiz (Assistant Director), Michael Holland (Assistant Director), Ian Reed (Analyst in Charge), Paul Bauer, Gilberto Cotto, Yvette Gutierrez, Carl Ramirez, Joe Rando, Hamsini Sivalenka, Andrew Stavisky, Ashley Stewart, Umesh Thakkar, and Andrew Weiss made key contributions to this report.

---

# Appendix IV: Additional Source Information for Images

---

This appendix contains credit, copyright, and other source information for images in this product when that information was not listed adjacent to the image.

Page 12: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 14: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 17: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 19: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 21: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 23: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 25: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 27: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 31: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 33: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 35: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 36: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 38: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 41: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 42: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 43: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 45: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 47: GAO (data); Rabbit\_1990/stock.adobe.com (images).

Page 48: GAO (data); Rabbit\_1990/stock.adobe.com (images).

---

# Related GAO Products

---

*Cloud Computing: Selected Agencies Need to Implement Updated Guidance for Managing Restrictive Licenses.* [GAO-25-107114](#). Washington, D.C.: November 13, 2024.

*Leading Practices: Iterative Cycles Enable Rapid Delivery of Complex, Innovative Products.* [GAO-23-106222](#). Washington, D.C.: July 27, 2023.

*Cloud Computing: Federal Agencies Face Four Challenges.* [GAO-22-106195](#). Washington, D.C.: September 28, 2022.

*Chief Information Officers: Private Sector Practices Can Inform Government Roles.* [GAO-22-104603](#). Washington, D.C.: September 15, 2022.

*Coast Guard: Actions Needed to Enhance IT Program Implementation.* [GAO-22-105092](#). Washington, D.C.: July 28, 2022.

*State Department: Additional Actions Needed to Address IT Workforce Challenges.* [GAO-22-105932](#). Washington, D.C.: July 12, 2022.

*Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization.* [GAO-22-104070](#). Washington, D.C.: June 29, 2022.

*Leading Practices: Agency Acquisition Policies Could Better Implement Key Product Development Principles.* [GAO-22-104513](#). Washington, D.C.: March 10, 2022.

*Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed.* [GAO-20-126](#). Washington, D.C.: December 12, 2019.

*Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked.* [GAO-19-58](#). Washington, D.C.: April 4, 2019.

*Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance.* [GAO-16-325](#). Washington, D.C.: April 7, 2016.

---

---

## GAO's Mission

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. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [X](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at <https://www.gao.gov>.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

---

## Congressional Relations

A. Nicole Clowers, Managing Director, [ClowersA@gao.gov](mailto:ClowersA@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Sarah Kaczmarek, Managing Director, [KaczmarekS@gao.gov](mailto:KaczmarekS@gao.gov), (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

---

## Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.