Guidehouse

guidehouse.com

Cloud Security Management

Keeping Pace with the Cloud Security Threat Landscape

Why should federal agencies focus on security and controls in their cloud environments?

Rapid adoption of cloud computing presents opportunities to revolutionize information technology (IT) operations. One major benefit is the ability to dramatically cut purchasing and the provisioning of hardware, while also reducing computing downtime.[1] As with many technology trends, cloud computing was first adopted broadly in the commercial sector. In recent years, its adoption in the federal sector has grown significantly. Recognizing that not all cloud computing is equal and to help ensure information security is incorporated in solutions, the US government established the Federal Risk and Authorization Management Program (FedRAMP), which promulgated requirements for securing cloud environments used by federal agencies.

Migrating to a FedRAMP cloud environment does not eliminate agencies' responsibility for maintaining information security controls over their cloud environments and the information systems operating within them. As federal agencies migrate to cloud environments, often information security controls are secondary to architecture design, application performance, workforce training, migration planning, computing and storage costs planning, and other concerns for IT management. In addition, it is not always clear what controls are the responsibility of agencies versus cloud services providers, and some security risks and controls may go unaddressed.

Does cloud computing protect federal agencies from cybersecurity threats?

Depending on data security requirements and business requirements, federal organizations may choose between software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) models and private, public, community, and hybrid cloud deployment models.

Using hosted cloud solutions effectively puts the organization's data in the hands of a third party, and responsibility over designing and operating controls varies based on service model. In 2019, the Cloud Security Alliance (CSA) asked 241 cloud security experts to weigh in on 11 salient threats, risks, and vulnerabilities in cloud environments. The results are listed below, ranging from highest to lowest severity:[2]

1. **Data breaches**

2. **Misconfiguration and inadequate change control**

3. **Lack of cloud security architecture and strategy**

4. **Insufficient identity, credential, access, and key management**

5. **Account hijacking**

6. **Insider threat**

7. **Insecure interfaces and application programming interfaces**

8. **Weak control plane**

9. **Metastructure and applistructure failures**

10. **Limited cloud usage visibility**

11. **Abuse and nefarious use of cloud services**

Of the many data breaches making headlines in recent history are highly recognized commercial and US government organizations—Microsoft, Walgreens, Marriott, Amtrak, FireEye, Sony, Target, Equifax, Facebook, the IRS, the US Office of Personnel Management, and the US Marshals Service, to name a few. With constant and evolving cyber threats, organizations must remain ever vigilant in maintaining their data security structures.

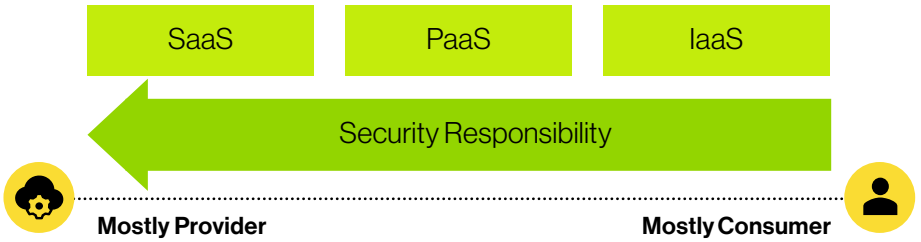
What Should Federal Organizations Expect of Their Cloud Service Providers?

Cloud service providers (CSP) play a critical role in security for federal agencies leveraging their services. Agencies should expect their CSPs to provide detailed service-level agreements or similar documents that clearly lay out each party's responsibilities for security to include the controls that will be operated by the CSP and the controls that fall under responsibility of customer agencies—complementary user entity controls (CUEC). Agencies are responsible for the design and operation of CUECs. Responsibility for cloud security and controls varies depending on the CSP and the features/products, service models, i.e., SaaS, and deployment models, i.e., private cloud.

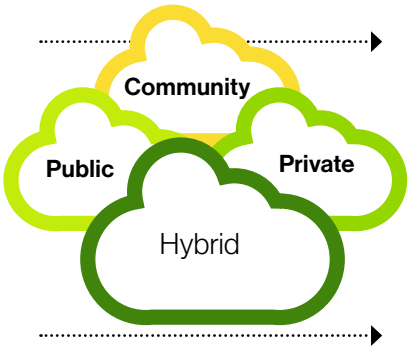
CSPs should also provide agencies with third-party attestation reports, i.e., Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and System and Organization Controls (SOC) 1 reports, over the services they operate on behalf of agencies. SSAE 18 and SOC 1 reports, published by independent external auditors, provide customer agencies insight into the effectiveness of CSPs' design and operation of controls over the operating system, database, and application layers of the information security control environment for which they are responsible.

Cloud Services Models

CSPs and customer agencies share the responsibility of securing information systems within a cloud environment based on service model (see image below).



Agencies' expectations of CSPs to manage cloud risks, security, and controls will vary depending on the service model utilized. CSPs take on most of the responsibility for managing cloud risks, security, and controls within a SaaS service model, a moderate amount of responsibility within a PaaS model, and the least amount of responsibility under an IaaS model. The inverse of this is true for agencies. It is critical that all parties are clear on their responsibilities for designing and operating effective security and controls, so all risks are considered and control requirements are addressed.



Agency has greater responsibility for operating cloud security

Cloud Deployment Models

In addition to service models, cloud deployment models (pictured to the left) also must be considered in determining ownership of risks and controls .

CSPs take on most of the responsibility for managing cloud risks, security, and controls within public and community cloud deployment models; and with private deployment models, that responsibility lies largely with customer agencies. However, with hybrid deployment models, that responsibility is shared between CSPs and customer organizations.

What is Guidehouse's approach to cloud security?

Guidehouse offers proven, industry-leading services to assist federal agencies in optimizing their cloud security and controls through strategy-setting, organizational readiness, security and controls assessment, and workforce readiness. Our cloud security and controls services consider more than 300 controls, information security laws and regulations, and leading industry standards and practices. Our cloud security and controls services are tailored to reflect each agency's unique risks, compliance requirements, and business needs.

Cloud Security and Controls Strategy

Guidehouse assists federal agencies in weaving information security and controls into their cloud strategy and operations. Our solutions consider the cloud service and deployment models to be implemented, as well as the information systems to be operated in each cloud environment, the types of data each information system will hold, the organization's information security requirements, and best practices for securing cloud environments. In our experience, agencies that consider security and controls in their cloud strategy and migration plans lay a foundation for sustainable, integrated risk management, and compliance with laws, regulations, and policy. They avoid having to retrofit solutions to meet compliance requirements, and implement manual, resource-intensive mitigating processes and controls.

Cloud Security and Controls Organizational Readiness

Guidehouse assists federal agencies in determining their readiness to operate and maintain security and controls over their cloud environments for effective and efficient risk and compliance management. This includes distinguishing the roles and responsibilities of the CSP and the agency. We make actionable and impactful recommendations to agencies, prioritized based on risk and impact to the organization's cloud security and controls environment.

Our approach in assessing agencies' cloud security and controls organizational readiness considers leading practices, including the following:

1. Establish a governance structure, including policies and procedures over cloud security risk and compliance management
2. Define roles and responsibilities and align the agency's cloud services information security workforce, including identifying any gaps in resources and resources' knowledge, skills, and abilities
3. Prepare the agency's cloud services information security workforce in understanding cloud security risks and compliance requirements and their roles and responsibilities, including designing and operating processes and controls
4. Identify and address the operational, security, and privacy requirements for the agency's cloud services
5. Maximize the use of automated controls to reduce reliance on resource-intensive manual controls.
6. Apply emerging technology to optimize the efficiency of the control environment

Cloud Security and Controls Assessment

Guidehouse assists agencies in verifying the design and operating effectiveness of the security and controls of their cloud environments. We offer scalable assessments that vary in scope based on agencies' preferences and requirements. This includes assessing the full population of security risks and controls designed and operated by an agency or focusing on a subset of controls that are of highest concern to management. Our cloud security and controls assessments consider industry-leading practices in securing cloud environments, the applicable laws, regulations, and policies for each agency, and guidance from the following:

- National Institute of Standards and Technology (NIST), including its Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, and Revision 5, Security and Privacy Controls for Information Systems and Organizations
- NIST's Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- Federal Information Security Modernization Act of 2014 (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)

We conduct pre-cloud migration assessments to validate agencies are designing and implementing controls that meet risk and compliance requirements and optimizing use of automation and emerging technology to avoid manually operated controls, and we also conduct post-cloud migration assessments. We identify control gaps and opportunities to improve security and controls with automated solutions, including emerging technology such as data analytics, robotic process automation (RPA), and machine learning (ML) and artificial intelligence (AI). We document and prioritize our actionable recommendations, so agency management may focus its remediation efforts based on risk and impact. Often, we work closely with agencies' cloud security management teams in crafting roadmaps for implementing remedial actions and integrating continuous monitoring over cloud security and controls and implementation of automated solutions.

95%

The percentage of cloud security failures through 2020 leading analyst firm Gartner projects will be the fault of customers.

– Gartner, 2019

Cloud Security and Controls Workforce Preparedness

Guidehouse helps agencies assess the readiness of their cloud security personnel to perform their roles and responsibilities effectively and efficiently. This includes validating their understanding of what they should expect from their CSPs and how they may advise their customers on their responsibilities, i.e., designing and operating CUECs. We identify gaps in the knowledge, skills, and abilities of the cloud security team and work closely with agency management to set a course to close the gaps. This may include internal agency training, external training available from vendors and professional organizations, and professional certification programs. We also develop custom training to meet agencies' cloud security and controls learning needs.

Our training for agencies is role-based and developed to reflect the needs of each customer. Topics may include cloud security risks, compliance requirements, leading industry practices for securing cloud environments, designing and operating controls, and applying automation in operating security processes and controls, including using emerging technology.

Methods to upskill the agency workforce on cloud security include building security awareness, training on cloud security basics and literacy, and promoting professional development that includes acquiring relevant licenses and certifications. Guidehouse has a breadth of security and controls professionals capable of training the agency workforce responsible for implementing and operating secure cloud environments.

Why Guidehouse

Guidehouse is an innovative consulting organization with more than 20 years of serving as a trusted advisor to federal organizations. We employ more than 8,000 professionals, of which 2,000 are dedicated to supporting our public sector clients. Our cloud security and controls services are rooted in our long and successful history supporting our federal clients in IT audit and audit readiness, cloud strategy and implementation, and organizational change management.

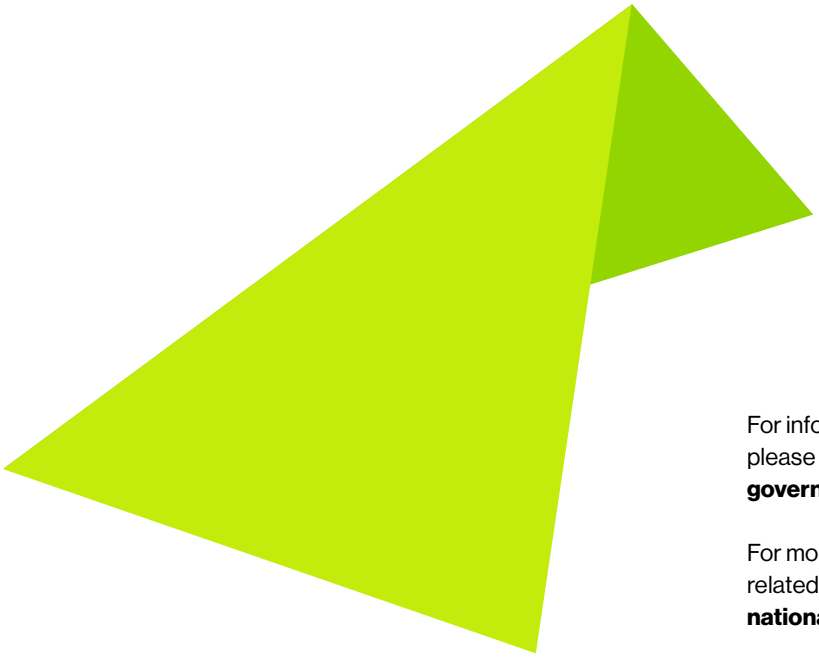
We assist federal agencies in preparing for and/or verifying their ability to rely on their cloud security and controls; preparing for external audits, such as FISMA; preparing for and/or conducting assessment of internal controls in connection with authorization and accreditation (A&A) programs and with their Office of Management and Budget's Appendix A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, compliance programs. We also support service organizations' preparedness to deliver and sustain cloud services that meet federal information security requirements.

The table below presents some talent metrics relevant to our professionals' experience in information security.

Relevant Guidehouse Professionals' Certifications/Areas of Expertise	
IT/Information Security Credentials	**Counts**
Internal Control/Audit/Risk Professionals	800+
Information Technology Professionals	250+
Professionals with IT Security/Controls certifications, i.e., Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM)	115+
Practitioners with Agile Certifications, i.e., Certified Scrum Master (CSM), Scaled Agile Framework (SAFe)	200+
FISMA, SOC, and Financial Statement Audits over 20 years	150+
A-123 Assessments over 15 years	115+

1. Security Guidance: For Critical Areas of Focus in Cloud Computing v4.0, https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.
2. CSA-Cloud-Computing-Top-Threats 2019, August 6, 2019, https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/.

Guidehouse



For information on contract vehicles held by Guidehouse, please visit our website at **https://guidehouse.com/government-contract-vehicles.**

For more information on our professional services related to cloud security and controls, please contact **nationalsecurity@guidehouse.com.**

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology/analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets and agenda-setting issues driving national and global economies. For more information, please visit: **www.guidehouse.com**.

Email: nationalsecurity@guidehouse.com / **Web:** guidehouse.com / @guidehouse linkedin.com/company/guidehouse

© 2021 Guidehouse Inc. All rights reserved. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. GH-130 WP Cloud Security Management