

Cloud Security for Federal Agencies

This paper helps federal agency executives evaluate security and privacy features when choosing a cloud service provider (CSP). We explain the FedRAMP delineation of responsibility between the agency and the CSP, and how to assess the risk and value of the CSP's offering. Using a CSP certified through GSA and FedRAMP provides an initial risk assessment of the cloud offering. Knowing what is included in the services and the inherited controls allows agencies to gain the most value for the least risk.

A critical issue, but not a barrier

Cloud computing offers federal agencies a powerful means to reduce costs, deliver more timely services, improve IT risk management and significantly lessen burdens on internal IT resources. While the promised value is compelling, agencies cite security and data privacy concerns as primary reasons for not migrating systems to the cloud. They are concerned about losing control as a result of the multi-tenant nature of cloud computing. They want visibility into cloud availability and potential security incidents, as well as integration with their security programs, to respond to incidents, audit findings and investigations.

To address these concerns, CSPs should provide controls that are as good if not better than an agency's own data center's to protect against unauthorized access and data leakage, and provide a comprehensive level of reporting visibility into their cloud environments.

The General Services Administration (GSA) and Office of Management and Budget (OMB) have focused on security and data privacy as top priorities to facilitate cloud adoption through the Federal Cloud Computing Initiative, GSA's Blanket Purchase Agreement (BPA) for cloud Infrastructure as a Service (IaaS) and the Federal Risk and Authorization Management Program (FedRAMP), the government-wide program providing a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. Prior to FedRAMP, agencies moving to the cloud were individually responsible for undertaking the assessment and authorization (A&A) process and spent resources to maintain the Authority to Operate (ATO).

Using the FedRAMP provisional ATO to manage risk

Under the IaaS BPA and now FedRAMP, GSA offers a common security A&A framework for cloud infrastructure based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, and NIST 800-145, *The NIST Definition of Cloud Computing*. They define the controls CSPs must implement, such as vulnerability scanning; incident monitoring, logging and reporting; and continuous monitoring, access and authentication for certified government cloud computing systems for multi-agency use. FedRAMP vets the Third Party Assessment Organizations (3PAOs) following the same standards for performing conformity assessments to yield more consistent outcomes for comparison.

Under GSA's IaaS BPA, CSPs must obtain an ATO from GSA to support agency systems up to a Federal Information Processing Standard (FIPS) 199 Moderate Risk Impact level. ATOs provide independent risk assessments of CSP security postures. Agencies have begun accepting the GSA ATO for their own risk assessment purposes. They show a strong preference for the FedRAMP provisional ATO, once available, by including it as a requirement for procured CSP services.

"It is not sufficient to consider only the potential value of moving to cloud services. Agencies should make risk-based decisions which carefully consider the readiness of commercial or government providers to fulfill their Federal needs."

**Federal Cloud
Computing Strategy**

An agency can use either the GSA ATO or FedRAMP provisional ATO as the basis for determining whether a CSP's risk is acceptable for their risk tolerance and what additional cost and effort are needed to mitigate within tolerable limits. The agency can continue to use the ATO as long as the CSP maintains its ATO status with GSA or FedRAMP.

Evaluating security and privacy

*The Federal Cloud Computing Strategy*¹ recommends agencies carefully consider their cloud security needs across a number of dimensions, including statutory compliance, data characteristics, privacy and confidentiality, integrity, data controls and access policies, and governance. In addition, NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, identifies nine security and privacy considerations for planning, reviewing, negotiating or initiating a public cloud service outsourcing arrangement. Table 1 compares these considerations with the specific NIST SP 800-53 rev 3 controls a CSP should implement and indicates the artifacts a CSP should provide for review to mitigate and reduce agency concerns.

Table 1: Comparing SP 800-144 Security and Privacy Considerations with Typical CSP Offering for IaaS

Considerations	Description	NIST 800-53 controls addressing the issues	ATO artifacts to review
1. Governance	Control and oversight over policies, procedures and standards for application development, as well as the design, implementation, testing and monitoring of deployed services.	Certification, Authorization, and Security Assessment – continuous monitoring Configuration Management – component inventory Planning – Security-related activity planning Risk Assessment – risk assessment, vulnerability scanning System and Services Acquisitions – lifecycle support, software usage restrictions, developer security testing	Code review Penetration test results System Security Plan (SSP)
2. Compliance	Conformance with an established specification, standard, regulation or law: data location, law and regulation	Planning – SSP description of data location, law and regulation	GSA ATO and FedRAMP ATO in the future SSP
3. Trust	Organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the cloud provider: insider access, data ownership, composite services, visibility, risk management	Access Control – separation of duties Personnel Security – personnel screening	Separation of duties matrix SSP
4. Architecture	The architecture of the software systems used to deliver cloud services comprises hardware and software residing in the cloud: attach surface, virtual network protection, ancillary data, client side protection, server side protection	Planning – SSP description of the architecture System and Communication Protection – boundary protection	SSP
5. Identity and Access Management	Organizational identification and authentication framework: authentication, access control	Identification and authentication – user identification and authentication	Customer touch points SSP
6. Software Isolation	Dynamic flexible delivery of service and isolation of subscriber resources: hypervisor complexity, attach vectors	Planning – SSP description of the architecture Risk Assessment – vulnerability scanning and penetration testing	Security Assessment Report (SAR) SAR

¹ www.cio.gov/documents/federal-cloud-computing-strategy.pdf

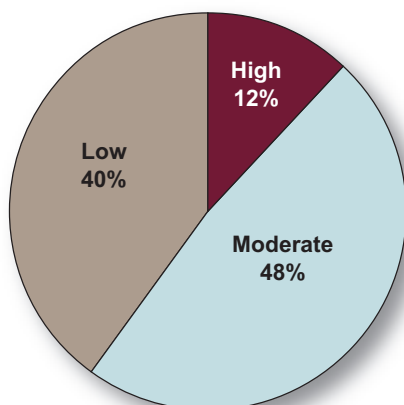
Considerations	Description	NIST 800-53 controls addressing the issues	ATO artifacts to review
7. Data Protection	Organizations moving sensitive and regulated data into the cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure: data isolation, data sanitization	Media Protection – sanitation and disposal Planning – SSP description of the architecture	SSP
8. Availability	The extent to which an organization's full set of computational resources is accessible and usable: temporary outages, prolonged and permanent outages, denial of service, value concentration	Contingency Planning (CP) and results of CP testing System and Communications Protection	CP and CP test results
9. Incident Response	Organized method for dealing with the consequences of an attack against the security of a computer system	Incident Response and Auditing	Incident Response Plan SSP

Realizing greater security for a majority of federal systems

By using GSA's IaaS BPA for cloud solutions, federal agencies can meet OMB's "Cloud First" policy and readily comply with the Federal Information Security Management Act's (FISMA's) comprehensive framework for securing a large majority of agency IT systems. The basis for determining the level of risk impact is FIPS 199. Figure 1 shows 88% of categorized federal systems are classified as FIPS Low or Moderate Risk Impact. Agencies may find federally certified IaaS services, from security to service levels, are as good as or better than their own infrastructure.

- **40% of categorized systems are classified as Low Risk Impact.** Examples include public-facing websites with non-sensitive data as well as applications such as inventory systems. Systems with public data that is subject to transparency requirements have been among the first to leverage the cloud. For example, the Recovery Accountability and Transparency Board deployed Recovery.gov in the cloud. The Department of Homeland Security (DHS) has also leveraged the cloud for public information. When considering the public cloud for such systems, agencies should ensure CSPs meet both federal security requirements and the NIST definition of cloud computing.
- **48% of categorized systems are classified as Moderate Risk Impact.** These include systems supporting operations and those processing sensitive data such as personally identifiable information (PII), Confidential Business Information (CBI) and personal health information. Federal financial systems that process budget and procurement information, purchase card numbers, banking information for payments, or Social Security Numbers.

Figure 1: FIPS Risk Impact of Categorized Federal Systems



Source: Fiscal Year 2009 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002

Agency vs. CSP responsibilities

An ATO letter from GSA for IaaS CSPs or FedRAMP outlines the different responsibilities between CSPs and agencies for applying appropriate controls under three conditions:

1. Controls implemented by the CSP for the authorization boundary for a given deployment type
2. Agency touch points implemented by the CSP – shared controls between the CSP and agency for specific types of interactions with the CSP's services
3. Agency responsibility for applying controls to applications and data using the CSP services.

The distinctions emphasize different security boundaries and the respective responsibilities to applying controls to each boundary as a way to better to assess risk when using a CSP's services.

Figure 2. Agency vs. CSP Control Responsibilities

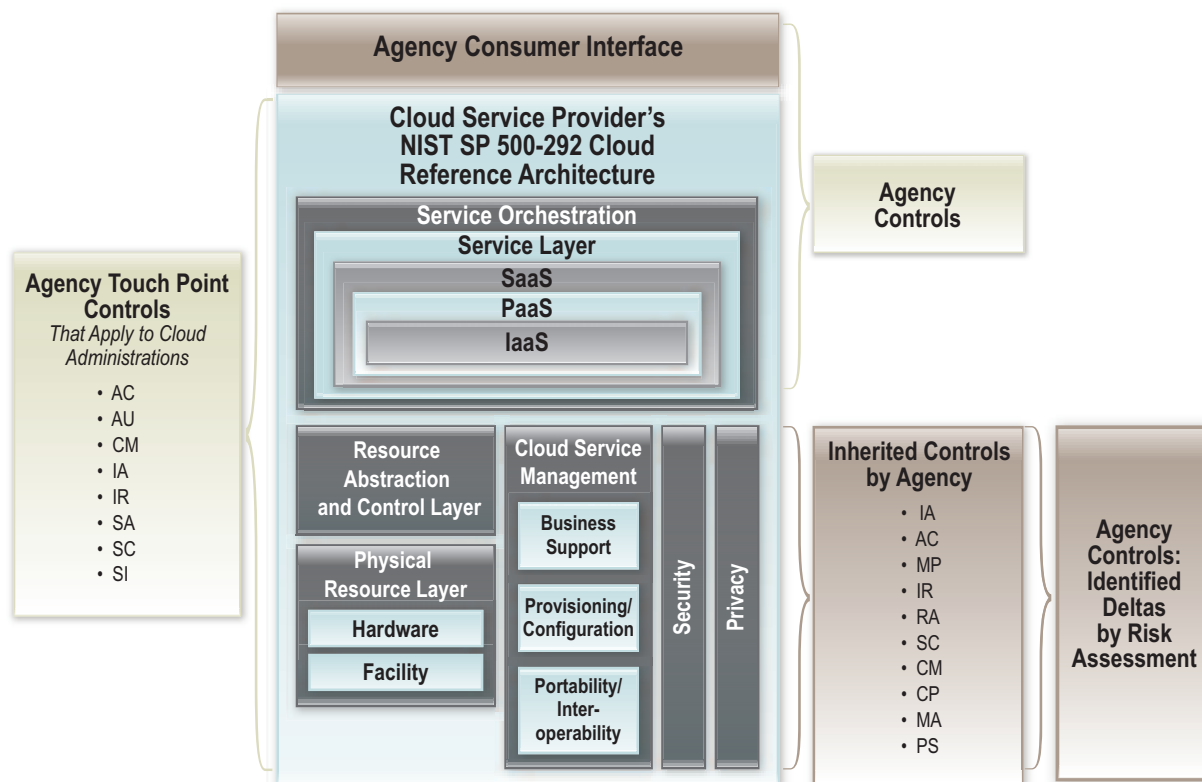


Figure 2 shows how control responsibility varies by the boundary between the CSP's authorization boundary and an agency's authorization boundary in the service layer. Identifying responsibility gaps allows agencies to decide what additional security controls, performance reporting or other standards of compliance are needed, and whether to address those internally or through their CSP.

Example controls include:

- Governance, Risk and Compliance (GRC) – security event and incident management, system operational risk management, OS-related security, patching and vulnerability scanning and configuration management
- Data risk management – strong authentication, identity management and data loss prevention
- Infrastructure protection management – Intrusion protection services, endpoint protection, log management services, firewalls management and system antivirus software configuration.

"FedRAMP establishes a standardized approach to security assessment, authorization and continuous monitoring. It will save cost, time, money and staff associated with doing this work."

Steven Van Roekel
Federal Chief Information Officer

What's in the boundary?

CSPs establish the authorization boundary and should represent the functional elements within the NIST cloud reference architecture SP-500-292. The boundary varies depending on the CSP's cloud deployment model and the services an agency procures. Within the boundary, the CSP decides how it implements controls and documents them in an SSP, mapping implementation with functional elements for each deployment model. Missing or ill-defined control implementations may indicate the CSP does not fully provide all operating characteristics of a true cloud or has defined a narrow boundary. It is important to consider what the boundary contains and the implementation of NIST SP 800-53 rev 3 controls. A narrow boundary shifts the relative risk between the CSP and agency, placing cost and burden on the agency and diminishing the value of the cloud service. See NIST 800-144 for more details.

Inherited controls

The agency inherits controls from the CSP boundary. Most are at the physical resource layer and include the Physical and Environmental (PE) and Media Protection (MP) controls from NIST 800-53 rev 3. They may also include some Provisioning, Configuration, Portability and Interoperability elements within the Cloud Service Management element, and security services such as continuous security monitoring and identity and access management from the Security element. A thorough review of the SSP can determine the extent an agency inherits the CSP's controls.

Evaluating for risk

FedRAMP provides a provisional ATO that an agency can use to evaluate the relative risk of a CSP and issue its own ATO. An SSP and security assessment report (SAR) provide the basis for a risk assessment to determine control deltas between two relative boundaries. Any agency considering a CSP should request to review these documents.

The first boundary is the CSP. The risk assessment looks at how the CSP implements NIST 800-53 rev 3 security controls within its authorization boundary compared to an agency's implementation of the same controls for either a general support system or major application it would have in its own data center.

The second boundary is the agency's application or data within the context of a deployment type. That risk assessment looks at how the agency implements its security controls, based on NIST 800-53 rev 3, within the boundary that includes the services provided by the CSP and any inherited controls from the CSP.

Evaluating cloud security benefits

Knowing the services included in a CSP offering and assessing the risk based on a review of a GSA or FedRAMP provisional ATO allows an agency to better appreciate the benefits inherent to cloud computing, from automated security management to redundancy and improved disaster recovery.

For federally certified cloud infrastructure, additional benefits to agencies include:

- Background check by the federal government of CSP personnel with significant security responsibility
- Continuous monitoring, backup and restoration of data
- Guarantee that data centers are located on U.S. soil
- Clearly delineated data ownership and protection approaches stating that agencies own their data and spelling out mutually agreed processes for Freedom of Information Act or other data requests
- Clear scope of security models and environments pre-tested by the government to meet FISMA Moderate Risk Impact requirements and provide continuous monitoring (agencies with higher security requirements can work with certified CSPs to design and deploy systems that meet more stringent specifications)
- Transparency into security features included in a cloud bid, and additional services available or desired by the agency to meet its specific needs
- Ability to solve many security challenges more effectively using the significant investments made by CSPs to deliver superior controls and enterprise-class production environments that are federally certified
- Faster authorization through reuse of existing security authorizations and separate authorization by the agency for agency- and application-specific requirements
- Savings in time and money by using existing security authorizations, eliminating the need to visit data centers and pursue and justify separate authorizations. OMB estimates agencies could save between 30-40 percent compared to what they are paying now.
- More time and resources to focus on continuous monitoring and risk mitigation of systems remaining in the agencies' data centers.

"Ensuring data and systems security is one of the biggest and most important challenges for federal agencies moving to the cloud. FedRAMP's uniform set of security authorizations can eliminate the need for each agency to conduct duplicative, time-consuming, costly security reviews."

David McClure
GSA's Associate Administrator for
Citizen Services and Innovative Technologies

Next steps

CGI offers a disciplined transition process to get you to the cloud with confidence. To learn how to find greater security in the cloud for your agency, or to talk to a CGI cloud expert about your specific situation, contact your CGI Federal program manager or visit us at www.cgi.com/federalcloud.

Why CGI

As one of the 12 awardees under the BPA for IaaS, CGI was the first to receive a full ATO that can be leveraged by agencies, and the first to have federal customers, such as DHS, to go live with critical national websites in our cloud. (Two DHS sites were deployed to the cloud in just weeks.) We also have been an active participant in FedRAMP discussions, including as chair of TechAmerica's public sector task group providing industry input into FedRAMP. GSA has indicated that the IaaS BPA will be the first to go through FedRAMP. CGI is well positioned to be first to comply.

Our ATO means we have been thoroughly tested as to how well we implement NIST 800-53 rev 3 security controls and perform continuous monitoring. We have also passed stringent National Agency Checks with Investigations according to HSPD-12 criteria. CGI's multi-agency ATO offers a greater likelihood of agency acceptance.

CGI's cloud offerings compel the development of well-managed cloud initiatives because processes, governance, security and compliance are all embedded in our offering. Since we own all aspects of our cloud, we were able to build security and privacy into the fabric of the operation and provide the level of security transparency demanded by government clients.

In addition, as a full-service cloud and security partner, we provide a host of services to assess and strengthen agency security strategies, including security governance and engineering, cybersecurity and managed security services. Our certified, accredited and cleared professionals follow proven best practices such as ITIL and SANS.

Finally, CGI brings 35 years of experience in managing infrastructure, security and business and IT services for complex organizations. We:

- Are trusted by more than 180 CIOs to manage their IT infrastructure
- Provide infrastructure support for 50+ federal agencies
- Operate a significant cybersecurity practice
- Follow rigorous service management and governance processes proven against demanding requirements
- Can blend cloud with traditional hosting, transfer of customer data in-house and access to robust common services
- Deliver entire applications to meet critical needs faster than agency data centers could deliver just the infrastructure. For example, in just six weeks, we built and deployed:
 - FederalReporting.gov in a virtualized hosting environment to handle Recovery Act funding recipient reporting
 - A national cloud-based portal to support a major health reform initiative which includes data from more than 3,000 commercial and public sector organizations.

About CGI

A global leader in IT, business process and professional services, CGI partners with federal agencies to provide end-to-end solutions for defense, civilian and intelligence missions. For 35 years, we have delivered quality services to help clients achieve results at every stage of the program, product, and business lifecycle. We deliver end-to-end solutions in application and technology management, systems integration and consulting, business process management and services, advanced engineering and technology services, and operational support services. Our proven capabilities in high-demand areas include cloud, cybersecurity, biometrics, citizen services, data exchange, health IT and energy/environment. CGI has 31,000 employees in 125 offices worldwide.