




*Mason Evans*

# Leveraging Assured Workloads for Public Sector Clients

August 1, 2023



In today's digital age, United States government agencies are leveraging cloud computing to streamline operations, enhance citizen services, and improve data security. Due to security and compliance requirements regarding where government data is stored and how it is accessed, some cloud providers have developed specific government clouds that exist in isolated environments, including physically separate data centers. While these government clouds may satisfy security and compliance requirements, they [offer different services and capabilities on commercial compared to public clouds](#). Google Cloud takes a unified infrastructure approach by offering one public cloud, tailored to meet government compliance requirements through the use of Assured Workloads, removing the need to maintain separate environments for government and commercial customers.

Deloitte's cyber practice—with our extensive domain and industry experience and collaboration with Google Cloud—can utilize [Assured Workloads](#) to help organizations establish and maintain a secure and compliant environment on the public cloud.

**Deloitte can work with an organization to leverage Assured Workloads to help them:**



## Adhere to Compliance and Regulatory Requirements

Public sector organizations are entrusted with safeguarding highly sensitive data, ranging from citizen records to national security information. Assured Workloads offers a secure and compliant cloud environment by integrating a set of controls aligned to various industry standards and frameworks including Federal Risk and Authorization Management Program (FedRAMP), Defense Federal Acquisition Regulation Supplement (DFARS), Criminal Justice Information Services (CJIS), and Department of Defense Impact Level 5 (DoD IL5) compliance programs, among others. Deloitte can help organizations understand which data protection regulations, privacy laws, and industry-specific mandates are applicable to their workloads to assess if they are compliant within the Assured Workloads environment.



## Implement a Secure Cloud Architecture

Assured Workloads places emphasis on transparency and control, empowering public sector organizations to have a granular view and control over their cloud environment.

To help comply with data residency requirements, Google Cloud provides an organization the ability to control the regions where data at rest is stored based on the compliance program for a particular workload. While Google Cloud applies encryption at rest and in transit by default, an organization can gain more control over how data is encrypted using the Cloud Key Management Service to generate, use, rotate, and destroy encryption keys according to the compliance program selected and individual policies.

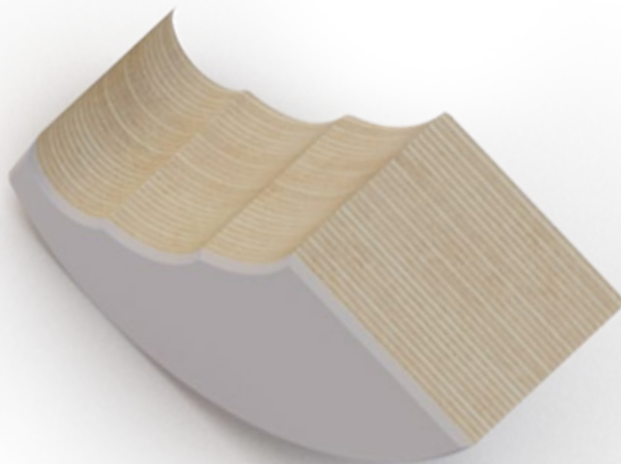
Deloitte can work closely with organizations to provide guidance on secure cloud architecture design, cloud security assessments, and the implementation of security controls to help them maintain confidentiality, integrity, and availability of data within the Assured Workloads environment. This includes recommendations on security settings, access controls, and appropriate encryption services tailored to an organization's specific needs or attributes (e.g., physical location or citizenship).



---

## Monitor and Mitigate Cyber Threats

[Assured Workloads monitoring](#) scans an organization's environment in real time and provides alerts whenever organizational policy changes violate the defined compliance posture. The monitoring dashboard shows which policy is being violated and provides guidance on how to resolve the finding. In addition to the monitoring capability, Deloitte can help organizations proactively identify and manage cyber threats within the Assured Workloads environment through threat hunting, vulnerability management, and the implementation of advanced security analytics capabilities so that organizations can proactively address vulnerabilities, promptly respond to incidents, and maintain a secure and compliant cloud environment.



# The Bottom Line

Assured Workloads provides public sector organizations with the infrastructure needed to support the security, compliance, and efficiency of their critical workloads on a public cloud. As a trusted professional services organization, Deloitte brings deep industry knowledge, technical experience, and a commitment to excellence in implementing and managing Assured Workloads for public sector clients. By working with Deloitte, organizations can unlock the potential of assured workloads and confidently navigate the ever-evolving cybersecurity landscape, enabling organizations to focus on their core mission of delivering public value while ensuring data integrity and privacy.

---

**For latest news and to learn more about the Deloitte and Google Cloud alliance in our Government and Public Services practice, please [visit our website](#).**



**Mason Evans**

*Managing Director*

Deloitte & Touche LLP

masevans@deloitte.com

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.