Learn more about controls for workloads and services

So far, you've learned that mapping controls to frameworks is an important part of the cloud security analyst's role. The process of identifying, implementing, and mapping controls is an essential part of risk management and compliance because it documents the evidence and rationale behind the chosen controls, and helps identify any potential gaps. In this reading, you'll learn more about using controls at the workload level and service level for Google Cloud.

Workload level

You can use control frameworks like NIST CSF or NIST SP 500-53 to check for and map controls at a workload level. Workload includes a business function, like purchasing or business intelligence. For example, a web application firewall (WAF) for protection of web facing assets might be a suggested or required control in a framework. The security team should check the specific workload to ensure that there is a WAF in use, and that it's properly configured to filter inbound traffic. If the workload is not internet facing, then the security team should note that. If the workload is not internet facing, then the WAF control in the framework is not needed, and will not be present in the implemented services.

In a workload view, there is a set of services and a flow of data through a system to achieve an outcome. Workloads are considered during the design and architecture stages, and control architecture and service selection is driven by organizational needs. For example, data collection, like what data will be collected from whom, how it will be handled, how users and services will be authenticated and authorized to do specific tasks, and what encryption is needed on the flows and data stores, informs what architecture and selection of services should be used. Google Cloud has a broad architectural guide that can be found here.

Workloads are the technical solution to a business need or objective, and services support and enable these workloads. Organizations can have many workloads composed of services and code that link these services. For example, an organization might have an internal procurement site. Internal procurement is the process of acquiring goods and services inside an organization instead of buying from outside suppliers. In this scenario, the workload is procurement, and is made up of services. These services could include serving a web page from a kubernetes cluster, creating code behind the page that handles input, validating input, and writing the input into a database. If the workload is business intelligence, the services might include GKE, CloudSQL, and IAM. The services that support a workload must be implemented securely and be in alignment with the desired security posture.

Service level

There is guidance for securing and hardening each service. As a cloud security professional, it's important to be familiar with the guidance to secure or harden services that support your workload. Common services include:

- **Access control for cloud storage**: The ability to restrict access to information stored on the cloud
- **Customer managed encryption keys (CMEK)**: Encryption keys that are managed using Cloud Key Management Service (KMS), and enable the user to have greater control over the keys used to encrypt data at rest within supported Google Cloud services
- **Google Kubernetes Engine (GKE):** A managed Kubernetes service that you can use to deploy and operate containerized applications at scale using Google's infrastructure
- **MySQL:** An open sourced data management service
- **CloudSQL:** A fully-managed database service that helps you set up, maintain, manage, and administer your relational databases on Google Cloud Platform
- **BigQuery:** A fully managed enterprise data warehouse that helps organizations manage and analyze data

Key takeaways

To review, workloads are the technical solution to an organizational need or objective, and services support and enable these workloads. Workloads and services are determined by organizational needs. Frameworks can help security teams determine the controls that need to be in place for workloads. Controls also need to be in place to secure or harden services that support workloads. Using up to date guidance on securing and hardening services is essential to help maintain your desired security posture, while also helping meet your organizational needs.

Resources for more information

Review these Google Cloud resources for more information about the services detailed in this reading:

- The Overview of access control guide describes how to secure access control for cloud storage.
- The Customer-managed encryption keys document provides guidance on securing CMEKs.
- You can find guidance on securing and hardening GKE on the Harden your cluster's security page.
- Use the Hardening a MySQL instance page to find guidance on securing and hardening MySQL.
- Refer to Improving CLoud SQL for SQL Server for guidance on securing CloudSQL.

- The Introduction to data governance document describes the concept of data governance, and what controls you might need to secure BigQuery resources.