Compliance and Regulations

Compliance and Regulations

In 28 Minutes

- Google Cloud Platform is compliant with several important certifications/regulations/standards:
  - **ISO/IEC 27001** (security controls that can help manage information risks)
  - **ISO/IEC 27017** (information security controls applicable to the provision and use of cloud services)
  - **ISO/IEC 27018** (critical components of cloud privacy - personally identifiable information (PII))
  - **ISO/IEC 27701** (global privacy standard)
  - **PCI DSS** - Payment Card Industry (PCI) Data Security Standards (DSS)
  - **SOC 1** (Auditing standard - How well does the vendor keep their books?)
  - **SOC 2** (Assessment of service provider controls - Security, Availability, Processing Integrity, Confidentiality, Privacy)

Google Cloud

Compliance and Regulations - 2

In 28 Minutes

- Google Cloud Platform is compliant with several important certifications/regulations/standards:
  - **COPPA**: Children's Online Privacy Protection Act of 1998
    - Special requirements on websites created for children under the age of 13
  - **HIPAA**: Health Insurance Portability and Accountability Act of 1996
    - Data privacy and security requirements for organizations handling protected health information (PHI)
  - **General Data Protection Regulation (GDPR)**: Strengthens personal data protection in Europe
- **Customers are responsible** for ensuring that their applications are **compliant with certifications/regulations/standards**

Google Cloud

HIPAA

- **HIPAA Compliance is a shared responsibility**:
  - GCP supports HIPAA compliance
  - BUT customers are responsible for evaluating HIPAA compliance
- Execute a **Google Cloud Business Associate Agreement (BAA)**
  - You can request a BAA directly from your account manager
    - HIPAA BAA covers GCP's entire infrastructure (across all regions)
      - Multi-regional service redundancy including usage of Preemptible VMs
    - Do not use Google Cloud Products not covered by BAA
- **Recommended Best Practices**:
  - Follow IAM best practices
  - Consider enabling Object Versioning on Cloud Storage buckets
  - Recommended: Export audit logs to Cloud Storage (archival) and BigQuery (analytics)
  - Disable request caching of PHI in Cloud CDN
- Reference: ***https://cloud.google.com/security/compliance/hipaa/***

PCI Data Security Standards (DSS)

In 28 Minutes

- **Payment Card Industry DSS: Enhance card-holder security**
- **Best Practices and Recommendations**:
  - Create a new Google Cloud account for your payment processing environment
    - Isolate from other environments
  - Restrict access to payment processing environment
    - Follow "principle of least privilege"
  - Control inbound and outbound traffic
    - Creating firewall rules to allow ONLY following inbound traffic
      - HTTPS requests from customers
      - Responses from third-party payment processor
      - Office network - for auditing and management
    - Only allow outbound traffic (HTTPS) to third-party payment processor
      - Compute Engine and GKE are recommended compute services (App Engine, Cloud Functions do NOT support egress firewall rules)
  - Create an HTTPS load balancer with signed SSL certificate
  - Create hardened secure Linux image with the minimum software needed to run

Google Cloud

PCI DSS - Other Recommendations

In 28 Minutes

- **Best Practices and Recommendations:**
  - **Automated most of the processes:**
    - Deploy using Cloud Deployment Manager
    - Configuration management using Chef, Puppet, Ansible, or Salt
    - Build an automated recovery plan
  - **Implement Forseti Security:** open-source tools to improve security of GCP environments:
    - Inventory: Compare your Google Cloud resources (inventory) over time
    - Scanner: Compare role-based access policies over time
    - Enforcer: Compare firewall rules with a specified state
    - Explain: Provides visibility into your IAM policies
  - **Enable** VPC Flow Logs, Access Transparency Logs, Firewall Rules Logging and Configure Monitoring Alerts
    - Stream audit logs to Cloud Storage and use bucket locks to make logs immutable
    - Streaming audit logs to BigQuery for analysis
  - **Using Cloud Data Loss Prevention** to sanitize data:
    - Grant apps access to PCI data only after it has been sanitized with Cloud Data Loss Prevention