HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

September 6, 2019

Google
11th Ave
Sunnyvale, CA 94089

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® CSF Assurance Program, the following platform of the Organization ("Scope") meets the HITRUST CSF® v9.2 certification criteria:

Google: Apigee Management Platform (Apigee Edge)

The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time,
- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs),
- No data security breach reportable to a federal or state agency by law or regulation has occurred,
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria, and
- Timely completion of the interim assessment as defined in the HITRUST CSF Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations within the industry, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For those HITRUST CSF control requirements that are not currently being met, the Organization must have a CAP that outlines its plans for meeting such requirements.

HITRUST performs a quality assurance review consistent with the HITRUST CSF Assurance Program requirements to ensure that the scores are consistent with the testing performed by the Authorized External Assessor. In addition to the full report that follows, users of the report can refer to the document Leveraging HITRUST CSF Assessment Reports: A Guide for New Users for questions on interpreting the results contained herein or contact HITRUST customer support at support@hitrustalliance.net. A full copy of the HITRUST CSF Certification Report has also

been issued to the organization listed above; if interested in obtaining a copy of the full report, you will need to contact the organization directly. Users of this report are also assumed to be familiar with and understand the services provided by the Organization listed above, and what specific services are being used by the user organization.

Additional information on the HITRUST CSF Certification program can be found at the HITRUST website at https://hitrustalliance.net.

HITRUST

Assessment Context

Prepared for	Google 11th Ave Sunnyvale, CA 94089
Contact	Denis Canuel Program Manager deniscanuel@google.com
Date of Report	September 6, 2019
Period of Assessment	June 3, 2019 – August 23, 2019
Period of HITRUST QA	September, 2019
Assessment Option	HITRUST CSF Security Assessment
Procedures Performed by Assessor	On-site 3rd party testing included: • Interviews • Review of documents • Review and testing of technical settings
Company Background	Apigee is an API management platform
Number of Employees	300
Geographic Scope of Operations Considered for the Assessment	Off-shore (outside U.S.)
Organizational Risk Factors	
Number of Records that are currently held:	Less than 10 Million Records
Systematic Risk Factors	
Does the system(s) store, process, or transmit PHI?	Yes
Is the system(s) accessible from the Internet?	Yes
Is the system(s) accessible by a Third Party?	No
Does the system(s) transmit or receive data with a third party/business partner?	Yes
Is the system(s) accessible from a public location?	No
Are Mobile devices used in the environment?	Yes
Number of interfaces to other systems:	Fewer than 25
Number of users of the system(s):	Fewer than 500
Number of transactions per day:	Greater than 85,000
Regulatory Risk Factors	
None selected	

Scope of Systems in the Assessment

Organization and Industry Segment Overview

Google LLC (“Google” or “the Company”) provides the Apigee API Management Platform (“Apigee”) that enables enterprises to secure, manage, scale, and analyze their digital businesses. The core API management product includes developer services, monitoring and reporting services, and a mediation and intelligence engine. Together these services provide an enterprise with the foundation to leverage existing systems, shared databases, security frameworks, management infrastructure, and operational tools. Apigee also includes bot detection and prevention capabilities, which enable the blocking or throttling of bad bot traffic based on analysis of billions of API calls using machine intelligence.

Apigee is a self-service API management product that enables businesses to securely expose their digital assets through APIs for developers and partners who are building applications. The platform enables enterprises to measure the success of their digital initiatives with end-to-end analytics.

Service(s) / Product(s) Provided

There are three services that comprise the Apigee API Management platform also known as Apigee Edge:

- Developer Ecosystems
- Monitoring and Reporting
- Mediation and Intelligence Engine

DEVELOPER ECOSYSTEMS

A developer portal is deployed by an enterprise to provide a community for developers with the resources necessary to learn about the enterprise’s APIs, become a registered developer, and collaborate with peers and with the enterprise. Tools such as blogs, frequently asked questions (FAQs), and forums allow developers to interact with one another to present solutions. Modeling and developer management provides streamlined developer registration with a manual or automatic registration process.

Developer keys can be approved automatically or manually for a given API product. Interactive API documentation and modeling through Apigee’s SmartDocs feature supports the design and documentation of new APIs as well as learning, testing, and evaluation of existing APIs. In addition, terms of service (TOS) and acceptance for APIs can be managed.

MONITORING AND REPORTING

This API analytics solution helps customers make better business decisions through an understanding of customer behavior and interactions, using real-time data from their APIs and from the edge of their business.

- Business metrics help provide organizations with a complete picture of their customers, including how those customers use their services with partner APIs, social networks, and other products.

- Operational analytics monitors the health and performance of production APIs, enabling enterprises to plan for traffic spikes, identify slow and error-prone APIs, find root causes, and understand traffic anomalies.
- Application performance monitoring measures mobile application usage and performance of applications on different platforms, carriers, and devices.
- Customers can segment their audience by top developers and apps, understand usage by API method to know where to invest, create custom reports on business-level information, and see long term usage trends.

MEDIATION AND INTELLIGENCE ENGINE

API management enables the transformation of existing back-end services to APIs with over 40 policies designed for “configure rather than code” deployment. A unified security model is provided throughout the platform; it provides secure portal access and can support other pre-existing security programs by using pluggable authentication. Apigee enables developers with API programmability, which allows for the extension of the mediation and intelligence engine capabilities with support for Java, JavaScript, Node.js, and Python.

This report includes the Apigee API Management Platform as described above. The accompanying description includes only policies, procedures, and control activities at Google and does not include policies, procedures, and control activities at any subservice organizations (see below for further discussion of subservice organizations).

Primary System(s)

The Apigee API Management platform:

- Apigee API Manager (Apigee Edge) (Bi-hosted at Google GCP and at AWS)
- Infrastructure Support

Google utilizes the following to manage the Apigee Edge system:

- Jump Server
- Puppet Master
- Monitoring
- Zookeeper
- Cassandra
- Collection Service
- Cloud Storage
- Preprocessing
- Spark
- Redshift
- Postgres
- Message Processor
- Router

Service(s) Outsourced

Apigee Edge is a cloud-based product that utilizes cloud services from Cloud Service Providers: Amazon Web Services (AWS) and Google’s Cloud Platform (GCP).

Scope Overview

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
Apigee Edge	• Jump Server • Puppet Master • Monitoring • Zookeeper • Cassandra • Collection Service • Cloud Storage • Preprocessing • Spark • Redshift • Postgres • Message Processor • Router	Developer Ecosystems	X			
		Monitoring and Reporting	X			
		Mediation and Intelligence Engine	X			

Scope Description

The scope for this certification is the Apigee Management platform (Apigee Edge) which includes the Developer Ecosystems, Monitoring and Reporting, and Mediation and Intelligence Engine services. These services are hosted in two environments: Google GCP and AWS. Apigee is supported by numerous internal Google-developed applications and cloud-based hosting services. Covered information resides only at the cloud storage locations which is implemented by Apigee customers and is never stored locally on Google devices.