ROAR Third-Party Vendor Assessment Report

Vendor: Google Cloud Platform (GCP) and Firestore
Assessor: Adam Richie-Halford

Overview

Google Cloud Platform (GCP), including its Firebase services, is a widely-used cloud infrastructure provider known for its robust security practices. This assessment evaluates GCP and Firebase's compliance with recognized industry standards and certifications. It verifies that GCP and Firebase are suitable third-party vendors to store and process ROAR data.

Certifications and Compliance

- **SOC 2 Type II**: GCP and Firestore are certified under SOC 2 Type II, which demonstrates adherence to strict security controls across the following Trust Service Criteria: security, availability, processing integrity, confidentiality, and privacy. The SOC 2 report confirms that GCP's internal controls are effectively designed and operate to protect customer data from unauthorized access and data breaches. The audit includes regular testing of security processes, access management, incident response, and data encryption practices.
- **ISO 27001**: GCP complies with the ISO 27001 standard, an internationally recognized framework for managing information security. This certification ensures that GCP has implemented a comprehensive Information Security Management System (ISMS), which includes risk management, data protection measures, and systematic security controls. The ISO 27001 certification also covers ongoing monitoring and continual improvement processes to address emerging threats.

GCP's SOC 2 Type II reports or ISO 27001 certificates can be obtained from the GCP Compliance Reports Manager. I have verified that the SOC 2 Type II report and the ISO 27001 certifications are both current and available.

Security Practices

- **Data Encryption**: GCP employs AES-256 encryption for data at rest and HTTPS/TLS encryption for data in transit. Firestore, as part of GCP, inherits these encryption practices, guaranteeing that all stored data is protected against unauthorized access.

- **Access Management**: GCP uses role-based access control (RBAC) and multi-factor authentication (MFA) for privileged access. This minimizes the risk of unauthorized data exposure by ensuring that access is granted only to verified users with a legitimate need.
- **Incident Response**: The platform follows a structured incident response plan, which includes real-time monitoring, automated alerts, and predefined procedures for detecting, investigating, and mitigating security incidents. SOC 2 and FedRAMP audits have confirmed the effectiveness of GCP's incident response capabilities.

Conclusion

Google Cloud Platform and Firestore meet the security requirements for handling high-risk data, including compliance with SOC 2 Type II, ISO 27001. These certifications, combined with GCP's robust security practices, validate its suitability for storing and processing ROAR information.