



**System and Organization Controls (SOC) 3  
Report on Management's Assertion Related to its  
Data Analysis and Visualization Software System  
Relevant to Security  
For the Period  
May 1, 2021 to April 30, 2022  
Together with  
Independent Service Auditors' Report**



## **Table of Contents**

I. Independent Service Auditors' Report	3
II. Assertion of Sigma Management	6
III. Description of Sigma's Data Analysis and Visualization Software System	8



## I. Independent Service Auditors' Report

## **Independent Service Auditors' Report**

To the Management of Sigma Computing, Inc. (Sigma)

### **Scope**

We have examined Sigma's accompanying assertion titled "Assertion of Sigma Management" (assertion) that the controls within Sigma's Data Analysis and Visualization Software System (system) were effective throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Sigma's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (trust services criteria)*.

### **Service Organization's Responsibilities**

Sigma is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Sigma's service commitments and system requirements were achieved. Sigma has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Sigma is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

### **Service Auditors' Responsibilities**

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve Sigma’s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Sigma’s service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

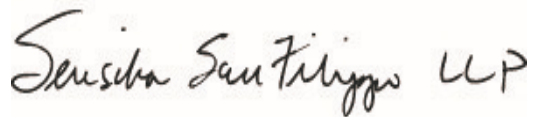
### **Inherent Limitations**

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### **Opinion**

In our opinion, management’s assertion that the controls within Sigma’s Data Analysis and Visualization Software System were effective throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Sigma’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

A handwritten signature in cursive script that reads "Susana San Filipe LLP".

San Jose, California  
June 9, 2022



## II. Assertion of Sigma Management



## Assertion of Sigma Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Sigma Computing, Inc. (d.b.a. Sigma) Data Analysis and Visualization Software System (system) throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Sigma's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Sigma's Description of the System," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Sigma's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Sigma's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 1, 2021 to April 30, 2022, to provide reasonable assurance that Sigma's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Sigma Management  
June 9, 2022



### III. Description of Sigma's Data Analysis and Visualization Software System





## **Description of Sigma's Data Analysis and Visualization Software System**

This report describes the control structure of Sigma Computing, Inc.'s (Sigma or Company) Data Analysis and Visualization Software System (the Service) for the period ending April 30, 2022. This description summarizes the services provided by Sigma, details the controls that have been implemented, and contains a description of the Service. However, it does not encompass every aspect of Sigma services and procedures, rather, the description enables customers to understand the Service.

### **Company Background**

Sigma is the only analytics solution built entirely for the cloud data warehouse. Sigma leverages the performance, concurrency, and simplicity of the cloud needed to analyze all of an organization's data in one location. Sigma's technology combines the power of data warehousing, the flexibility of SQL and the elasticity of the cloud at a fraction of the cost of traditional business intelligence solutions.

Founded in 2014, Sigma is privately held and headquartered in San Francisco. Sigma is backed by leading venture capital investors including Sutter Hill Ventures and Altimeter Capital.

Find out more at [sigmacomputing.com](https://sigmacomputing.com)

### **Overview of the Service**

Sigma provides a spreadsheet-like interface to serve as the front-end access point for your data warehouse, enabling business experts to ask their toughest questions without help from the data team. No coding, no proprietary languages or backend GUIs - all Sigma consumers are treated as first-class citizens, with all of Sigma's modeling and data prep capabilities.

Sigma provides broad support for analytics - 99% of SQL queries, JSON-parsing, data prep, charting, dash boarding - and all without moving or storing any data outside your data warehouse (Secure by design).

Sigma is different from a traditional business intelligence solution because of its architecture. Sigma has introduced a patent-pending methodology to translate spreadsheet functions into query code, built for the cloud to revolutionize data analysis.

### **The Principal Service Commitments and System Requirements**

The Company makes service commitments to its customers and has established system requirements as part of the Service. Some of these commitments are principal to the performance of the Service and relate to applicable trust services criteria. The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Service to provide reasonable assurance that the service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in the Problem Resolution Standards and other customer agreements such as the Sigma Master Software License and Service



agreement and the Sigma Privacy Statement, as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- **Security:** The Company has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, and other relevant security controls.

## Components of the Platform Used to Provide Services

### *Infrastructure*

All services used in the production environment are hosted in Google Cloud (GCP) and Amazon Web Services (AWS). The Service includes the following infrastructure elements:

Service Used	Service Category	Services Provided
Google Cloud Load Balancing	Network	Distribute load balanced compute resources in single or multiple regions, to meet high availability requirements.
Cloud IAM	Access	Allows access control and visibility for centrally managing cloud resources.
Google Kubernetes Engine (GKE)	Kubernetes	The Company uses this managed, production-ready environment for deploying containerized applications.
Cloud Key Management Service (KMS)	Key Management	The Company uses the cloud-hosted key management service to manage cryptographic keys as part of the cloud services.
BigQuery	Data Warehouse	The Company leverages the server less data warehouse that scales storage and computing power needs.
Cloud SQL	SQL	The Company uses the managed database service to set up, maintain, manage, and administer the relational database.
Cloud Pub/Sub	Event and Messaging Service	The Company uses the scalable foundation for stream analytics and event-driven computing systems.



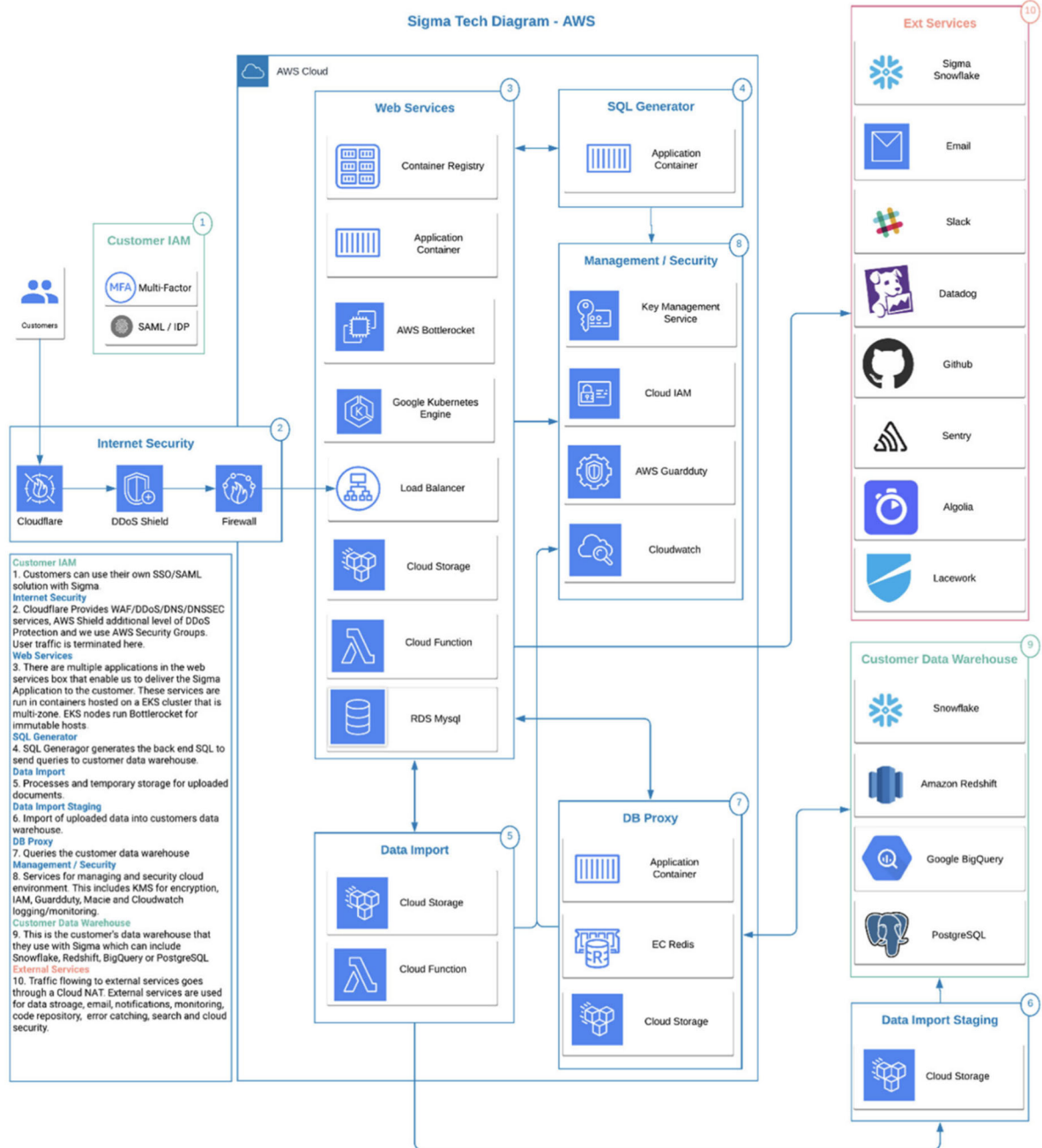
Service Used	Service Category	Services Provided
Cloud Composer	Orchestration	The Company uses workflow orchestration service to author, schedule, and monitor pipelines that span across clouds.
Cloud Storage	Storage	The Company uses object storage for internal usage.
Google Container Registry (GCR)	Storage	The Company uses the registry to store, manage, and secure your Docker container images.

Primary Software		
Software	System Components	Purpose
Datadog	Infrastructure Monitoring	Monitoring and metrics on servers and services.
Container-Optimized OS from Google	Operating System	Linux distribution operating system.
GitHub	Code Repository	Restricted repository for source code development
Sentry	Communication	Alerting
CloudFlare	Monitoring	CDN, WAF and DNS
GuardRails.io	Monitoring	Static Code Analysis
Lacework	Monitoring	Cloud, Security and Compliance
Snowflake	Data Storage	Cloud-based data warehouse

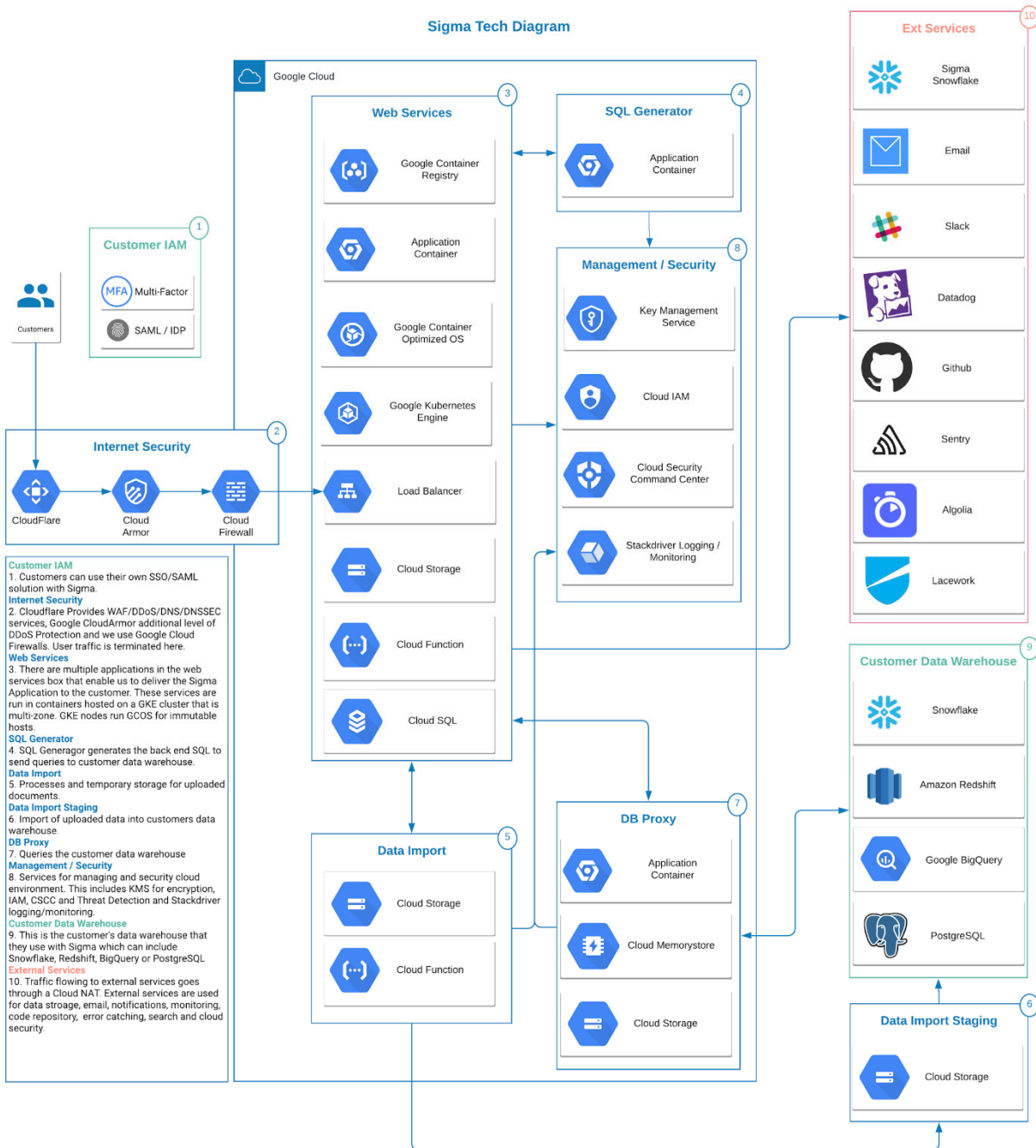
#### Sigma Service

The Sigma service employs a multi-layered security architecture that employs isolation to protect customer data and access to that data. Sigma's architecture physically separates but logically integrates storage and compute. Sigma's multi-cluster, shared data architecture consists of the independent components represented in the diagram below.

## AWS Technical Diagram



## GCP Technical Diagram



## Software

Sigma leverages industry standard third-party software tools to support the Service. There are four key categories of software tools used: 1) system configuration and provisioning software, 2) source code management software, and 3) monitoring software and 4) security software for static code analysis.



The Engineering team uses system configuration and provisioning software to deploy a secure and consistent configuration across different systems using a standard image for host servers. The host servers are only permitted to communicate with authenticated connections by authorized Company personnel.

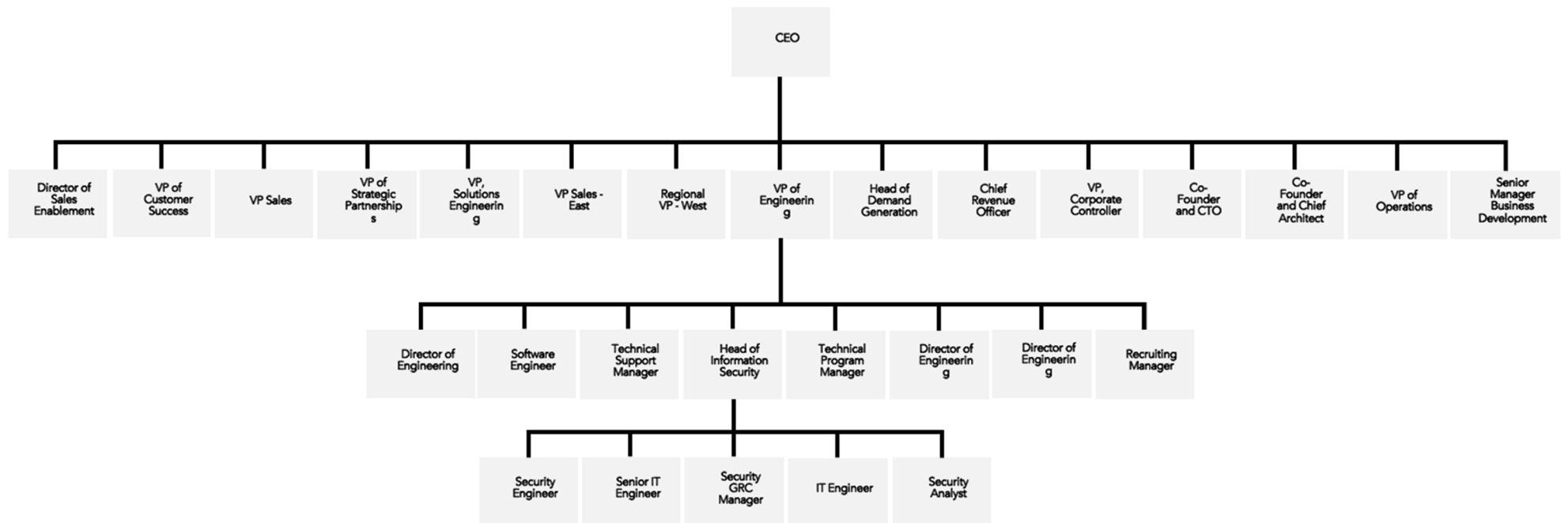
Sigma uses and restricts access to the source code. Repositories are stored in the cloud and code is version controlled. The Software (product) development process incorporates peer reviews as a mandatory step to strengthen the development and quality processes.

Monitoring software provides Sigma personnel with views for tracking performance and effectiveness of the systems used to support the Service. Alerts are configured to notify the Engineering team when components of the Service operate outside acceptable thresholds. Alerts related to security incidents are triaged, addressed, and remediated in a timely manner to meet business commitments.

### *People*

The organizational structure at the Company starts with the executive management team and is supported by key department managers and team members to ensure that duties are segregated across the organization.

**See Diagram Next Page:**





The teams and roles that support the Service are:

1. Engineering – creation and deployment of the Sigma service
2. Product – prioritization and project management
3. Design – UX design
4. Analytics – insights around how customers are using the service, and how Sigma can improve its product
5. Customer Success/Support – onsite and remote support for customers of Sigma

Sigma's organizational structure is defined by key areas of authority, responsibility and the appropriate lines of reporting of personnel. Management maintains separation of duties within the organization through defined roles and responsibilities, as well as through physical and logical security controls.

- Executive Management: provides oversight and strategic planning of operations
- CRO (Chief Revenue Officer): responsible for Sigma's sales strategy and execution, including Sigma's direct sales team, sales operations, customer success, and implementation partners
- VP of Engineering: owns reporting and data processes, also responsible for the Product & Infrastructure Engineering.
- VP of Design: owns the visual interaction layer of Sigma
- VP of Marketing: owns Sigma's outbound communication to press, analysts, prospects, and customers
- VP of Operations: owns finance, G&A, and legal
- Head of Information Security: responsible for developing enterprise-wide security programs, incident management, security awareness, monitoring, and implementation of the privacy and compliance program.

### *Policies and Procedures*

Sigma documents its overall security approach in its security and continuity policies and standards.

- Employee Handbook
  - Standards of Conduct
- Information Security
  - Risk





- Network and Firewall
- Physical Access
- Access Management
- Change Management
- Business Continuity and Disaster Recovery Plan

### *Data*

Since Sigma is a custodianship of client data, data security and protection are a core aspect of the business. Data and analytics used and generated by Sigma clients could be either publicly available or proprietary. Both data types and their respective analyses generated by the Service are secure and protected on the production database.

### **Applicable Trust Services Criteria and the Related Controls**

The Company's internal control environment is affected by the entity's Board, management and other personnel designed to enable the achievement of objectives related to effectiveness and efficiency of operations, and compliance with applicable laws and regulations. The following section is a description of the five components of internal control for Sigma. These components are (1) control environment; (2) risk assessment; (3) information and communication systems; (4) monitoring and testing; and (5) control activities.

The Service controls established by Sigma and discussed in Section III have been parenthetically referenced to the comprehensive list of Trust Services Criteria (TSC) and related controls detailed and tested in Section IV of this report.

### Control Environment

The control environment is the foundation for all areas of the Company. Sigma management emphasizes the importance of controls and ethical behavior throughout the Company; thereby, setting the tone for management and the discipline of employee actions. Management's philosophy and operating style contributes to the underlying strength of the control environment. This philosophy influences how Sigma business activities work, how decisions are made, and how risks are addressed. Sigma's company culture emphasizes the importance of Security throughout the organization. The Security team includes senior members of Engineering and Product, as well as both founders (the CEO and CTO), providing the highest level of visibility and accountability for Security policies and controls.

The control environment that underpins the Sigma organizational environment starts with the executive team and is demonstrated daily by functional managers and other leaders. Responsibility for information



security resides with the designated Security Officer, with duties delegated to the Engineering team. Senior Management has established and communicated an organizational structure that defines the reporting structure in support of the Service.

The Board of Directors (the Board), composed of 7 members including founders and investors, provides guidance and ensures business and internal control objectives are met. The Board charter includes details of the Board's oversight and review of management, as well as its commitment to integrity and ethical values through the Code of Conduct reviewed annually by the Board. The Executive team meets with the Board quarterly to report on how the business meets its business and security objectives. Management approves all Company policies at least annually. Management has assigned the responsibilities of updating and managing these security policies and standards to the senior members of the Security Team.

Senior management refines its hiring strategy as business needs evolve. Current job descriptions exist that describe primary job functions and responsibilities. The Sigma Human Resources (HR) department has a process for screening new hires based on job responsibilities as well as academic and professional requirements. Job responsibilities are documented in job descriptions, which are created by HR and the hiring manager. HR runs background checks through a third-party provider, obtains references and verification checks for prospective employees. New hires are required to sign several agreements including Confidentiality and Proprietary Information and Inventions Agreement. Contractors sign a Non-Disclosure Agreement (NDA). Policies and procedures are documented and communicated to employees at the time of hire. Sigma new hires are required to review relevant compliance practices per the Employee Handbook, and are then required to read, accept, and digitally sign.

Sigma practices a security awareness program to manage risks that encompass general security for employees and contractors working with the Service. New personnel must complete training within their first week of hire and annually thereafter.

Formal performance reviews are conducted annually to evaluate the employees' work and aid in the employees' continuous improvement process.

## **Risk Management**

Risk is managed as part of ongoing operations. The Sigma Security Committee follows a standard risk management framework to identify, assess, mitigate, report, and monitor risks. Sigma uses risk assessments to identify, quantify, and prioritize risks against criteria for risk acceptance and objectives within the organization. The results of the risk assessments are used to determine the appropriate management action and priorities for managing information security and operational risks, driving the implementation of selected controls to protect against these risks. The Sigma Security Committee includes the CEO, both founders, senior members of the Engineering organization (which includes senior members of the Security team), and senior members of the Product organization. This committee meets on at least a monthly basis to review risk assessments and security policies, to review new emerging threats, and to discuss any project that has a security or privacy impact. Sigma management defines the appropriate



threat reduction strategies for the organization, which may result in the creation or modification of security controls.

## **Monitoring**

Monitoring is critical to understanding the effectiveness of controls, whether they are operating as intended, and whether they should be updated to reflect changes in processes. Monitoring is intended to identify and remediate areas of risk. Management is responsible for monitoring the quality and effectiveness of internal control as part of their regular activities. Through ongoing assessments, management maintains clear oversight and responsibility for directing and controlling operations, while communicating and monitoring control activities and procedures for overall effectiveness. This process is accomplished through ongoing activities, separate evaluations, or a combination of the two.

Automated monitoring systems, using a combination of multiple tools, including CloudTrail (for AWS) and Cloud Audit logs (for GCP), internal tools, third-party and open-source tools, continuously check and monitor all systems. Wherever possible, metrics are gathered and trended over time, providing visibility into the infrastructure. Sigma leverages AWS and GCP services for monitoring the production instances and alerting the Engineering team. The Engineering team deploys a threat detection system to check for system anomalies and reviews alerts from the threat detection system. Identified issues are tracked through resolution.

Sigma performs the following control activities to ensure production infrastructure is appropriately managed and monitored.

- Maintaining production instances' security groups and network ACLs for restricting inbound/outbound access to the database.
- Penetration and scanning tests are performed at least annually by an independent third-party provider with critical and high-risk findings reviewed and mitigated.

## **Information and Communications**

Sigma has implemented several methods of communication, both internally and externally, to ensure personnel, partners, customers, and vendors understand their roles and responsibilities, and to communicate any relevant changes in a timely manner.

Internal policies and service documentation are available to communicate responsibilities to Sigma personnel and external system users. Procedural documents are made available internally via Sigma's documentation and are updated based on changing responsibilities.

Communication with Customers, Partners, and Vendors is managed through a variety of channels, including Sigma's Customer Support portal (Intercom) for those topics that affect all customers, or email for those topics that are specific to a particular Customer, Vendor or Partner.



## **Control Activities**

### **Security Organization**

Sigma has a cross-functional Security Team responsible for establishing and maintaining the organization's security policies and procedures across both corporate resources as well as the AWS and GCP infrastructures. This team is also responsible for leading security architectural designs, performing audits and compliance activities, and administering security devices and security applications in the Sigma environment. Sigma leverages the SANS Institute CIS Critical Security Controls as part of its overall security program.

### **Access Management**

Access to networks and systems required to operate and manage Sigma is limited to authorized personnel and processes. Access lists for all Sigma services are reviewed quarterly and updated, when necessary, to reflect current roles and responsibilities. All changes including role changes, department changes and separations are recorded with a ticket for documentation and tracking purposes.

### **Logical Security**

Sigma has implemented adequate controls to manage access to Sigma Services as well as the systems involved in the maintenance and operation of the Sigma Service.

#### GCP Console

Sigma leverages GCP Security Groups as well as the GCP IAM infrastructure to manage access to systems involved in the maintenance and operation of the Sigma Service.

- GCP Security Groups are set up to isolate the production environment from other networks (such as Development branches, Staging, etc.).
- GCP IAM infrastructure is leveraged to control access to resources.
- Admin access to the GCP Console is restricted to a limited number of Sigma Engineers based on their role. Strong passwords are enforced through GCP Security Policies.
- Multifactor authentication is required for GCP Console access.

#### AWS Console

Sigma leverages AWS Accounts, AWS Security Groups, and AWS Identity Access Management (IAM) infrastructure to manage access to systems involved in the maintenance and operation of Sigma.



- Separate AWS accounts are set up to isolate the production environment from other networks (such as Development branches, Staging, etc.).
- AWS IAM infrastructure is leveraged to control access to resources.
- Admin access to the AWS console is restricted to a limited number of Sigma Engineers based on their role.
- Strong passwords are enforced, and multifactor authentication is required for AWS Console access.

### Network Security

All deployed code and configuration changes are reviewed by at least 2 members of the engineering team. Such changes are automatically scanned for known vulnerabilities as part of the review process. The source repositories are continuously checked as well by GitHub. Our cloud service providers notify us of vulnerabilities in our infrastructure software which affects us.

Usage telemetry from our services is collected into our internal data warehouse (Snowflake) and summarized into reports and dashboards used by the engineering team. Selected events are published to our Slack channels, including deployment configuration changes, user sign-ups, and user errors. These channels are monitored by the engineering team.

Penetration tests by an independent third-party expert are conducted at least annually. All issues are documented and assessed based on Sigma-defined risk criteria (see above).

- High and Medium vulnerabilities are documented in GitHub and tracked to closure
- High vulnerabilities are dealt with by the Security Team

The Sigma Security Committee determines and supervises appropriate remediation action.

### **Physical Security**

The Sigma Service is hosted by Google Cloud Platform (GCP) and Amazon Web Services (AWS) in US Regions. Physical access to these data centers requires a legitimate business need and is only granted to authorized data center personnel. All visitors are required to present identification and are escorted by authorized staff. Access is revoked as soon as an employee or contractor no longer requires access.

Sigma leverages GCP and AWS's data center redundancy to ensure continued availability of its services. Redundancy is integrated into the design of not only each individual data center, but also within each region of data centers, where data centers have been built in clusters within global regions.



Sigma also benefits from GCP and AWS's industry-leading fire detection and suppression, power, and climate and temperature controls, all of which are closely monitored and maintained by the data centers. Corporate offices require visitor sign-in and employee escort.

## **Availability**

### High Reliability Infrastructure

Sigma has chosen AWS and GCP as its strategic supplier of data center services. AWS and GCP undergo an annual SOC 2 audit by a nationally recognized CPA firm, whose report Sigma relies upon as allowed for under AICPA SOC 2 guidance. Their data centers have many high reliability features, including redundant electrical power, uninterruptible power systems (UPS), and multiple telecommunications connections.

## **Change Management**

Changes to the Sigma Service follow the applicable published deployment process, which must include:

- All deployed code and configuration changes are reviewed by at least two members of the engineering team. Such changes are reviewed to ensure they meet Sigma objectives. The source repositories are continuously checked and maintained by GitHub.
- Sigma uses multiple staging environments to develop and test changes to production environments.
- Reviews are conducted by a separate engineer.

## **Risk Mitigation**

Sigma has developed a written business continuity plan with procedures to follow to limit potential business disruptions.

Sigma management reviews the annual SOC report for its hosted data centers to confirm that outsourced controls are appropriately designed and operating effectively.

Sigma has a formal partner document which establishes specific requirements for its partner engagements.

## **Description of Complementary User Entity Controls**

The Service is designed with the assumption that certain controls will be implemented by user organizations. Such controls are called complementary user entity controls. It is not feasible for all the criteria related to the Service to be solely achieved by internal control procedures. Accordingly, user-



entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Sigma.

The following complementary user entity controls assumed in the design of Sigma's controls are suitably designed and operating effectively to meet certain applicable trust services criteria, as specified.

As these items represent only a part of the control considerations that might be pertinent at the user organizations' locations, user organizations' management and their auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

CUECs	
User entities are responsible for:	Applicable Trust Services Criteria
Complying with their contractual obligations and their confidentiality with Sigma.	CC2.1, 2.3, 7.4
Deleting Sigma user accounts for employees who are no longer with the organization	CC6.2, 6.3
Customer shall not (a) rent, lease, or otherwise permit third Parties to use the Software, Equipment, or Services, except for Authorized Users; (b) circumvent or disable any security or other technological features or measures of the Software, Equipment or Services; (c) use the Software, Equipment or Services for any illegal purpose; or (d) reverse engineer, modify, reproduce, or disassemble the Software.	CC9.2
Establishing and managing their user access and any corresponding authentication requirements (passwords, multi-factor use) to use the Service.	CC6.1, 6.2, 6.3
Maintaining appropriate database user-level permissions for the database account or Single Sign On (SSO) method used to create a Database Connection in Sigma. If the customer's database contains sensitive information such as PII, it is the customer's responsibility to ensure the proper permissions are applied.	CC6.1, 6.2, 6.3
Immediately notifying Sigma if any known or suspected incidents or security related breaches happen within their account, or if any user access accounts have been compromised.	CC2.3, 7.3, 7.4
Accepting and following the terms and agreements for using the Service.	CC7.4

### Description of Complementary Subservice Organization Controls (CSOC)

Sigma uses subservice organizations, GCP and AWS, to provide hosting and infrastructure services. This description does not include the control objectives and actual controls provided to the Company by GCP and AWS. Protection of GCP and AWS client data and environments is supported by its stated intention to provide compliance validation for Organization Controls (SOC) 1 and SOC 2. GCP and AWS's service



organization controls are independently audited to determine if they achieved the service commitments and requirements based on their applicable trust services criteria.

Sigma reviews the available SOC reports for its subservice organization annually to evaluate the subservice organizations controls, any identified exceptions, and the complementary user-entity controls to determine their impact to the Service.

In the design of the Service's controls, management expects the following types of controls to be suitably designed and operating effectively at the subservice organizations to meet certain applicable trust services criteria. These controls are Complementary Subservice Organization Controls (CSOCs):

Google Cloud (GCP) and Amazon Web Services (AWS)	
Applicable Trust Services Criteria	The Types of Controls Expected at the Subservice Organization
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	Physical assets are destroyed when no longer required.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.