VIRTUALITICS®

Virtualitics Inc.

Report on Controls at a Service Organization Relevant to Security, Availability, Confidentiality, and Privacy

SOC 3®

For the Period January 1, 2024 to September 30, 2024

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

BARR ADVISORY

Independent Service Auditor's Report

To the Management of Virtualitics Inc. ("Virtualitics"):

Scope

We have examined Virtualitics's accompanying description of its Virtualitics AI Platform, titled "Virtualitics's Description of Its Virtualitics AI Platform," throughout the period January 1, 2024 to September 30, 2024 (description), based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2024 to September 30, 2024, to provide reasonable assurance that Virtualitics's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, availability, and privacy (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).

Virtualitics uses subservice organizations to provide data center infrastructure and hosting services. The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Virtualitics, to achieve Virtualitics's service commitments and system requirements based on the applicable trust services criteria. The description presents Virtualitics's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Virtualitics's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Virtualitics, to achieve Virtualitics's service commitments and system requirements based on the applicable trust services criteria. The description presents Virtualitics's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Virtualitics's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Virtualitics 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 Virtualitics's service commitments and system requirements were achieved. Virtualitics has provided the accompanying assertion titled "Assertion of Virtualitics Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Virtualitics is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and,
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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, in all material respects,

a. The description presents the Virtualitics AI Platform that was designed and implemented throughout the period January 1, 2024 to September 30, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period January 1, 2024 to September 30, 2024, to provide reasonable assurance that Virtualitics's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Virtualitics's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period January 1, 2024 to September 30, 2024, to provide reasonable assurance that Virtualitics's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organizations controls and complementary user entity controls assumed in the design of Virtualitics's controls operated effectively throughout that period.

BARR Advisory, P.A.

Fairway, KS

November 15, 2024

Assertion of Virtualitics Management

We have prepared the accompanying description titled "Virtualitics's Description of Its Virtualitics AI Platform" throughout the period January 1, 2024 to September 30, 2024 (description), based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria) (description criteria). The description is intended to provide users with information about the Virtualitics AI Platform that may be useful when assessing the risks arising from interactions with Virtualitics's system, particularly information about system controls that Virtualitics has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, availability, and privacy (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).

Virtualitics uses subservice organizations to provide data center hosting and infrastructure services. The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Virtualitics, to achieve Virtualitics's service commitments and system requirements based on the applicable trust services criteria. The description presents Virtualitics's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Virtualitics's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Virtualitics, to achieve Virtualitics's service commitments and system requirements based on the applicable trust services criteria. The description presents Virtualitics's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Virtualitics's controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents the Virtualitics AI Platform that was designed and implemented throughout the period January 1, 2024 to September 30, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period January 1, 2024 to September 30, 2024, to provide reasonable assurance that Virtualitics's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Virtualitics's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period January 1, 2024 to September 30, 2024, to provide reasonable assurance that Virtualitics's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organizations controls and complementary user entity controls assumed in the design of Virtualitics's controls operated effectively throughout that period.

Virtualitics Inc.

November 15, 2024

Virtualitics's Description of the Boundaries of Its Virtualitics AI Platform

Description of Services Provided

Founded in 2016, Virtualitics (the "company") provides AI-driven data analytics and a visualization software ecosystem that assists users in finding insights from complex, multi-source data.

Virtualitics's core product, the Virtualitics AI Platform, is a Software as a Service (SaaS) solution that:

- Has the ability to handle multi-source data within the system;
- Merges data from multiple sources while leveraging machine learning techniques to predict future outcomes, based on historical data;
- Produces renders of the data using technology for 3D visualization; and,
- Guides the user to find the visualizations that yield insights from complex data, using AI.

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures.

Infrastructure

The cloud components of the system are hosted in Amazon Web Services (AWS) and Amazon Web Service GovCloud in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. Further, Virtualitics utilizes a hybrid model for production infrastructure as depicted in the network diagram and Primary Infrastructure and Software table below. The network topology includes segmented VPCs and access control lists (ACLs). User requests to Virtualitics's web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to Virtualitics web and application servers is available through a virtual private network (VPN) connection. The hardware components that make up the aforementioned system include servers hosted, managed, and protected by AWS. Production servers at AWS maintain failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high availability data centers with multiple availability zones.

Further, the Synology NAS file server and FortiGate, the underlying firewall for perimeter protection, are hosted within the Virtualitics office located in Pasadena, California.

Software

Virtualitics is responsible for managing the development and operation of the Virtualitics AI Platform including infrastructure components such as servers, databases, and storage systems unless otherwise specified in the Complementary Subservice Organizations Controls table.

People

Virtualitics has a staff organized in the following functional areas:

- **Board of Directors:** Responsible for overseeing the management and direction of a company. This includes setting the overall strategic direction of the company, overseeing the establishment and implementation of policies and procedures, and monitoring the performance of the company's executive management team and overall oversight of the information security program.
- **Executive Management:** Consisting of the chief executive officer (CEO), chief technology officer (CTO), chief information security officer (CISO), chief revenue officer (CRO), chief financial officer (CFO), president of public sector, and VP of engineering and architecture. Responsible for the overall management and direction of a company, which includes setting the overall strategic direction of the company, annual review of policies and procedures, annual review of the risk assessment process, and monitoring the performance of the company.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system, along with the product life cycle, including additional product functionality. Also responsible for maintaining the availability of customer facing production infrastructure, and managing access and security for production infrastructure.
- **Cybersecurity and Information Technology:** Responsible for vulnerability management, incident management, risk management, and managing laptops, software, access control, user access reviews, vendor management controls, and other technology involved in employee productivity and business operations.
- **Human Resources:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **Finance:** Responsible for all day-to-day transactional business accounting functions, management of cash flow, and overall financial stability of the company.
- **Product and Customer Success:** Responsible for sales, account management, customer success, and customer support activities.
- **Product and Design:** Responsible for guiding every step of the product life cycle, from development to positioning and pricing, through a focus on the product(s) and the customers.
- **Sales and Marketing:** Responsible for promoting the business and mission of Virtualitics. Its key duties include defining and managing the products and services, conducting campaign management for marketing initiatives, and creating content for the website.
- **Cloud and DevSecOps:** Responsible for managing cloud infrastructure, web application development, and deployment.
- **Quality Assurance (QA):** Responsible for quality assurance testing all products and services.
- **Data Science:** Responsible for developing proofs of concept (POCs), custom data science solutions, machine learning algorithms, and general data analytics for clients.

- **Change Advisory Board (CAB):** Responsible for reviewing, approving, and prioritizing proposed changes to an organization's IT systems and infrastructure. The CAB plays a critical role in the change management process by providing a structured approach for evaluating and assessing the risks, impacts, and benefits of proposed changes before they are implemented.

Data

Data, as defined by Virtualitics, constitutes any information collected from employees, candidates, users, customers, vendors, or other parties that provide information to Virtualitics.

Information assets are assigned a sensitivity level based on the audience for the information. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following sensitivity levels:

Sensitivity Level	Description	Examples
Restricted	Highly valuable and sensitive information where the level of protection is dictated externally by legal and/or contractual requirements. Access to restricted information is limited to authorized employees, contractors, and business partners with a specific need.	• Personally identifiable information (PII) • Controlled unclassified information (CUI)
Confidential	Highly valuable and sensitive information where the level of protection is dictated internally. Confidential information may be shared with authorized employees, contractors, and business partners who have a specific business need.	• Program code • Employee information • Proprietary materials
Internal Use	Information that originated or is owned internally, or was entrusted to Virtualitics by others. Internal use information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• Training materials • Policies and procedures • Internal communications • Internal wiki
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Social media posts • Official website • Ad campaigns

The Virtualitics AI Platform processes the information types as described in the table above. To assist with the data handling procedures, Virtualitics has documented data classification policies that define system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policies are reviewed and updated accordingly on at least an annual basis by the executive management team.

Upon service termination, Virtualitics deletes customer content per agreement. Customers can request their data to be deleted at any time, as required by the data retention and disposal policies.

Processes and Procedures

Virtualitics has developed and communicated policies and procedures to manage the information security of the system, including sanctions for policy violations. Policies are reviewed and approved on an annual basis by the executive management team and changes are made to the policies when necessary. These policies and procedures cover the following key security life cycle areas:

- Acceptable Use
- Access Control
- Awareness & Training
- Backup and Restoration
- Business Continuity and Disaster Recovery
- Customer Support and SLA
- Change Management
- Configuration Management
- Corporate Ethics
- Data Retention and Disposal
- Data Integrity
- Information Classification
- Government Data
- Incident Management
- Identification and Authentication
- Information Security
- Information Security Planning
- Key Management and Cryptography
- Logging and Monitoring
- Media Protection
- Network Security
- Personnel Security
- Privacy
- Physical and Environmental Security
- Risk Assessment
- Server Security
- Software Development
- System and Services Acquisition
- Technology Equipment Handling and Disposal

- Vendor Management
- Vulnerability and Penetration Testing Management
- Workstation and Mobile Device Security
- Working from Home

Principal Service Commitments and System Requirements

Virtualitics designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Virtualitics makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that Virtualitics has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the Virtualitics AI Platform. Service commitments are set forth in standardized contracts, service-level agreements (SLAs), and in the description of the service offering provided online.

Service commitments related to security, availability, confidentiality, and privacy include, but are not limited to, the following:

- Virtualitics shall maintain product security measures inclusive of continuous network vulnerability scanning, endpoint security measures, continuous cloud security monitoring; and encryption at rest and in-transit;
- Virtualitics shall maintain a business continuity and disaster recovery (BC/DR) program, inclusive of disaster recovery testing;
- Virtualitics shall maintain workforce security measures inclusive of employee background checks and security awareness training;
- Virtualitics shall not share customer information except under certain circumstances stated in the Privacy Policy; and,
- Virtualitics shall store information collected as long as necessary for stated purpose(s) or as required by the law.

Virtualitics establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional derived from service commitments, published documentation of system functionality, and other descriptions of the system;
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures; and,
- Business processing rules, standards, and regulations, including:
    - Data security measures as required by the General Data Protection Regulation (GDPR);
    - California Consumer Privacy Act (CCPA);
    - U.S. Department of Defense security requirements; and,
    - NIST 800-171.

Virtualitics establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Virtualitics's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system. Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools (i.e., Onetrust) accessible to all personnel with access to the company systems.

