Independent Service Auditor's System and Organizational Controls SOC3® Report

On Devo Technology, Inc.'s Assertion of the Effectiveness of Its Controls Relevant to Security, Availability, Processing Integrity and Confidentiality

Throughout the Period October 1, 2021 to September 30, 2022

Devo Technology, Inc.
255 Main Street, Suite 702
Cambridge, Massachusetts 02140

Assertion of Devo Technology, Inc.'s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Devo Technology, Inc.'s ("Devo" or "the Company") Devo Platform System (the System) throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Devo's service commitments and system requirements relevant to security, availability, processing integrity and confidentiality were achieved. Our description of the boundaries of the System (description) is presented in Attachment A 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 October 1, 2021, to September 30, 2022, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to security, availability, processing integrity and confidentiality (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*). Devo'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 Attachment B.

Devo uses subservice organizations to provide cloud data center hosting. The boundaries of our System indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Devo, to achieve Devo's service commitments and system requirements based on the applicable Trust Services Criteria. The description does not disclose the actual controls implemented at the complementary subservice organizations.

The description of the boundaries of our System indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Devo, to achieve Devo's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Devo's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of Devo's controls.

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 October 1, 2021, to September 30, 2022, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the applicable Trust Services Criteria relevant to security, availability, processing integrity and confidentiality.

Attachment A

Devo Technology, Inc.'s Description of the Boundaries of Its Devo Platform System

Company Overview & Services Provided

Devo Technology, Inc. ("Devo" or the "Company") was founded as Logtrust in Madrid, Spain in 2011, rebranded to Devo in 2018. Devo is headquartered in Cambridge, Massachusetts with operations also located in Madrid.

Leveraging the cloud, Devo provides its customers the ability to manage their machine data without size, geographical, or batch processing limitations or delays. Devo delivers analytics on its customer's machine data utilizing proprietary collection, query, correlation, alerting, and data visualization methods. Devo can integrate machine data, infrastructure, servers, software, business applications, and proprietary applications, in one view and one single platform, the Devo Platform.

The scope of this description is limited to the system and internal control structure of Devo as it relates to its Cloud Services, which are those services hosted by Devo and offered to user entities as a cloud offering.

Devo Platform

The Devo Platform is a full-stack, distributed data, and analytics platform that scales to hundreds-of-petabyte data volumes. Data from multiple parts of a business streams into the data store and is immediately ready for real-time and historical analysis for a variety of use cases. The Platform allows customers to visually interact with and analyze data via a user-friendly interface that makes analytics intuitive and fast. An industry-standard query language can also be used within the user interface or via an API, enabling the automation of and integration with other business and operational processes. The Devo Platform allows customers the ability to perform the following data functions:

- **Collect and Centralize** – Data is stored in a single, secure repository. Data collected in the repository is stored in its raw format.
- **Search and Analyze** – Access to data with features to build queries. Browse, search, and analyze information in visually driven data tables. No programing knowledge is required.
- **Inform** – Customize real-time or scheduled alerts based upon queries. Alerts can be distributed through several channels, including email, PagerDuty, Jira, and Slack.
- **Visualize** – Build dashboards that remain current. Customize reports and share them within your organization.

Additionally, the Platform offers data isolation, governance, and security and consists of the following main components:

Devo Platform Components

- **Devo Relay** – Software that receives, encrypts, and transmits customer log data to the Devo Platform. One method for sending data to the Devo Platform, Relays can be installed on premise at a customer site, in a public cloud, a private cloud, a data center, or anywhere logs are created. This is one method for sending information to the Devo Platform.

Attachment A

Devo Technology, Inc.'s Description of the Boundaries of Its Devo Platform System

- **Devo Cloud Collector** – Software that receives, encrypts, and transmits customer log data from cloud-based services to the Devo Platform. The Cloud Collector is hosted by Devo co-located to the rest of the Devo Cloud components and runs specific collectors that interact one-to-one with the targeted external services.
- **GUI** – A graphical user interface (Web App) used by the customer to interact with data.
- **Load Balancer** – Devo proprietary software that accepts incoming data from relays or other sources, and forwards on to the next component (data nodes). Its function is to ensure an even distribution of log data. Larger deployments can use multiple load balancers.
- **Data Nodes** – Two key software processes referred to as "collectors" and "query engines" occur inside of data nodes. "Collectors" receive the log data and write it, completely unmodified, to disk. "Query engines" that are responsible for retrieving data from disk as the response to queries. Devo scales "up" and "out" because the architecture allows an unlimited number of data nodes.
- **Meta Nodes** – When a customer makes a query using the GUI, the GUI translates it to the appropriate syntax and sends it to "meta nodes". These nodes distribute the query across all of the data nodes it connects to. These queries are then executed by the query engine on each data node. The responses to these queries are sent back to the meta node. The meta node combines all of the results from each data node into one set of results that is sent back to the GUI. It is possible to have multiple "tiers" of meta nodes.
- **Correlation Engine** – Devo can provide batch query results from data stored on disk and real-time query results using the correlation engine. This engine runs continuously against data nodes to provide real-time query results. Results are typically used in conjunction with the alert engine (below).
- **Alert Engine** – When the correlation engine finds matching data from a continuous query, it creates a new correlation event. The alert engine receives these events and uses them to alert customers using a set of predefined contact methods and rules.
- **Aggregation Engine** – Allows for data to be queried (e.g., data visualization) in "buckets". For example, instead of just looking at raw logs, customers can aggregate this data to get summary information that is very useful. One way is to aggregate by time. For example, a customer might want to track website "hits" into five-minute intervals and graph that information on-screen for trend analysis. The data would then update with summary counts of website hits every five minutes. Devo supports many different ways to perform data aggregation. The role of the aggregation engine is to keep track of all of this data and store the statistical measures associated with these aggregations.
- **Back–End** – The back end is a set of services that connect to the Red Hat Enterprise Linux operating system (RHEL) and provides traditional services like the web server for the GUI, access to the file system, time synchronization, and other services.

Attachment A

Devo Technology, Inc.'s Description of the Boundaries of Its Devo Platform System

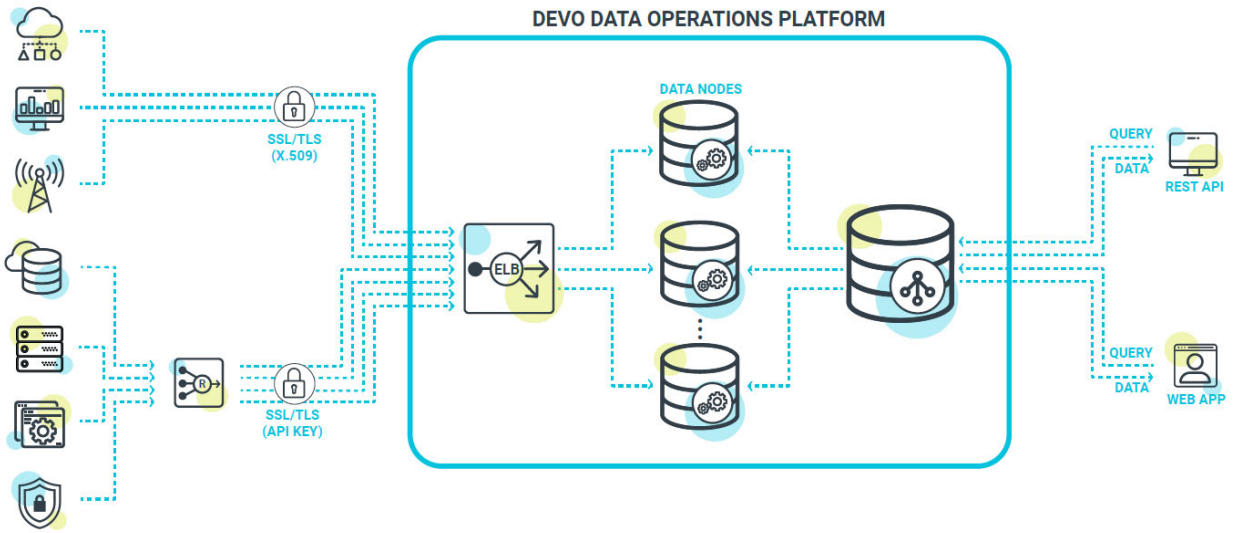
Infrastructure

Based on the customer's requirements, the Devo Platform can be hosted within Amazon Web Services (AWS) or Google Cloud Platform (GCP). Devo uses AWS and GCP cloud infrastructures to support its computing resources for processing and storage including the facilities, network, hardware, and operational software that supports the provisioning and hosting of the Devo Platform. Devo does not maintain any of its own servers and relies on redundant cloud-based services for storage of documents and records.

The production system and backups are hosted in the AWS or GCP specific regions based on data sovereignty requirements. The AWS infrastructure is designed and managed in accordance with security compliance standards and industry best practices. AWS and GCP infrastructure and physical security of such infrastructure is designed and managed by the respective vendor. Firewalls on AWS and GCP infrastructure are managed by Devo. Additionally, antivirus software is installed on employee workstations.

Software

The diagram below provides an overview as to how customer data flows into the Devo Platform, the principal internal components responsible for managing and storing data, and how data is queried and retrieved.



Devo ingests data sent from varied data sources. These data sources can be configured to send events directly to Devo with the necessary Devo tag and establishing a secure channel, or events can be sent to the Devo Relay. The Relay, installed within the customer's secure network, can apply rules to associate Devo tags to the inbound events it receives, then compress and forward them to Devo over a secure, encrypted channel.

Devo's event load balancer (ELB) receives events, decrypts the data, and distributes it across available data nodes. Event data in the data nodes is compressed at a ratio up to 10:1.

Attachment A

Devo Technology, Inc.'s Description of the Boundaries of Its Devo Platform System

To facilitate the use of its services, Devo provides Devo Docs on its public facing external website. Devo Docs include indexed and searchable user guides, detailed how-tos, frequently asked questions, and customer support information.

Other commercial software is used to support the delivery of the Devo Platform including a password safe, antivirus, source code repository, project and task management and wiki.

People

Organizational Structure

Governance and management of Devo is vested in the Executive Leadership Team, which is supported by the Board of Directors. The Devo Board of Directors is comprised of a majority of members independent of management. The Board meets quarterly to evaluate the Company's organizational structure, reporting lines, authorities and responsibilities as a part of its business planning process and to support the Company's risk assessment process to achieve its objectives.

Devo's Executive Leadership Team consists of key personnel from the functional departments and includes, but not limited to, the Chief Executive Officer (CEO), Chief Technology Officer (CTO), Chief Financial Officer (CFO), General Counsel, Chief Marketing Officer, Chief Revenue Officer, and Senior Vice President, Product Engineering and Operations. The Chief Information Security Officer (CISO) is responsible for developing, implementing and monitoring Devo's information security programs. The CISO is also tasked with enforcing the alignment with requirements and industry standards, identifying gaps, and working with the functional departments to remediate issues.

The Company has a documented organizational chart which formally defines organizational structure and reporting lines. The organizational chart is communicated and made available to company personnel.

Devo's organizational structure is comprised of business units that work together to meet its service commitments and system requirements including:

- Cloud Operations
- Product management
- Research and Development
- Human Resources
- Accounting / Finance
- Marketing
- Legal
- Sales
- Solutions Engineering
- Professional Services
- Information Security
- SciSec

Data

Customer data is segregated within the system. Customers are provisioned access to data associated with their organization and cannot access data from other organizations or the underlying infrastructure.

The Information Security Standard has policies, standards and guidelines addressing data classification, storage, sharing, and destruction. Additionally, Company policies address data governance expectations and personnel's responsibilities for protecting data and information.

Data ingested by the Devo Platform cannot be modified by Devo. The Platform maintains a record of the data that was originally received by Devo by default for 400 days. Devo data processing specifications are

Attachment A

Devo Technology, Inc.'s Description of the Boundaries of Its Devo Platform System

classified as aggregation tasks, injections, permalinks, API feeds, and OData feeds in support of information quality. Data processing specifications are defined and made available to internal and external users via Devo Docs. Additionally, available data types are defined including the data name, description and example and made available to internal and external users via Devo Docs.

Configured load balancers are used to distribute network traffic across cloud resources in an effort to support availability and processing integrity. Guidelines for sending data to the Devo cloud from open-source and/or third-party log collection tools are defined.

Processes and Procedures

Documented policies and standards, presented below, are in place that address roles and responsibilities of users for information security; assignment of responsibility and accountability for system security, availability, and confidentiality; information and data classification; user account management; prevention of unauthorized access user access provisioning / de-provisioning addressing and resolving security, availability, and confidentiality concerns, incidents or breaches; third party information sharing; non-compliance with security policies; and handling of exceptions not specifically addressed within corporate or IT policies. The key Devo standards, policies and procedures include:

- Information Security Standard
- Incident Response Standard (Security & Operational)
- Code of Business Conduct and Ethics Standard
- Product Security Information Response Standard
- IT Change Control Standard
- Software Development Lifecycle
- Remote Working Policy
- Acceptable Use Policy
- Privacy Policy
- Disaster Recovery Plan
- Business Continuity Plan
- Devo Employee Handbook

Complementary Subservice Organization Controls

Devo utilizes subservice organizations to perform certain key operating functions, specifically related to hosting of production infrastructure and data. Devo assumed in the design of its controls that certain types of controls are implemented by the subservice organizations below that are necessary, in combination with Devo's controls to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the applicable Trust Services Criteria.

The accompanying description includes only those policies, procedures, and controls at Devo, and the types of controls expected to be in place at the subservice organizations. The description does not include policies, procedures, and controls at the subservice organizations described below. Additionally, the examination by the Independent Service Auditors did not extend to policies, procedures, and controls at the subservice organizations.

Attachment A

Devo Technology, Inc.'s Description of the Boundaries of Its Devo Platform System

Subservice Organization	Service(s) Provided	Applicable Trust Services Criteria
Amazon Web Services (AWS)	Cloud data center hosting services	CC6.1-CC6.5 – Logical & Physical Access CC7.5 – System Operations CC9.1 – Risk Mitigation A1.1-A1.3 – Availability C1.1-C1.2 – Confidentiality
Google Cloud Platform (GCP)	Cloud data center hosting services	CC6.1-CC6.5 – Logical & Physical Access CC7.5 – System Operations CC9.1 – Risk Mitigation A1.1-A1.3 – Availability C1.1-C1.2 – Confidentiality

Complementary User Entity Controls

Devo Platform controls were designed with the assumption that certain controls would be designed, implemented and operating effectively by user entities. The application of such controls by user entities is necessary to achieve certain Trust Services Criteria identified in this report. Each user entity internal control structure must be evaluated separately in conjunction with Devo's control policies and procedures described in this report.

In addition, there may be criteria and related controls that are not identified in this report that would be appropriate. As a result, the complementary user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. User auditors should consider whether the following controls have been placed in operation at user entities:

Complementary User Entity Controls	Related Applicable Trust Services Criteria
Controls exist to ensure customers notify Devo of any actual or suspected information security breaches, including compromised user accounts and confidential information.	CC7.3, CC7.4
Controls exist to ensure, for on-premises deployment, appropriate logical and physical security controls exist to maintain the security and confidentiality of data, and sufficient availability and monitoring of applicable hardware and systems.	CC6.1 – CC6.8 CC7.1 – CC7.2 A1.1 - A1.3 C1.1

Attachment A

Devo Technology, Inc.'s Description of the Boundaries of Its Devo Platform System

Complementary User Entity Controls	Related Applicable Trust Services Criteria
Controls exist to ensure customers notify Devo of any approved contact modifications.	CC6.2
Controls exist to ensure customers manage user access requests to Devo systems, including user IDs and passwords used for accessing Devo systems are to be assigned to authorized individuals with appropriate privileges.	CC6.2
Controls exist to ensure data transmitted to Devo is complete and accurate.	A1.2
Controls exist to ensure internet speed and bandwidth are monitored and maintained.	A1.1, A1.3
Controls exist to ensure customer source data compliance obligations are met under the applicable Privacy and Data Protection Requirements including personal data, and to provide any required notices and obtaining any required consents for processing instructions given to Devo.	A1.3
Controls exist to ensure the security of confidential data transfers to Devo.	C1.2
Controls exist to ensure data provided to Devo is in accordance with customer confidentiality policies.	C1.4
Customers are responsible for ensuring health and storage of their source data.	A1.3

Attachment B

Devo Technology, Inc.'s Principal Service Commitments and System Requirements

Service Commitments

Devo designs processes and procedures to meet the objectives of its Devo Platform services. Those processes and procedures are based on the service commitments that Devo makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Devo has established for its services.

Security commitments to user entities are formally documented and communicated in Devo Terms of Service Agreements, Order Form and other customer agreements. Security commitments are also presented within the descriptions of Devo's service offerings on its external website within technical manuals called "Devo Docs". Commitments may vary based on provisions of customer agreements applicable to Cloud Services, but generally include:

- User role-based access to permission users based on job functionality based on the concept of least privilege.
- Encryption technologies in place to protect customer data at rest and in transit.
- Commercial antivirus solutions are in place for protecting internal employee workstations from malware and virus threats.
- Network compartmentalization, which separates the network into different segments based on their security classification, to reduce the risk of network-wide attack, virus outbreak, or unauthorized disclosure of confidential information.
- Antivirus software is used and configured to automatically assess current virus signatures and update Company workstations.
- Monitoring of current processing capacity and usage rates, data backup and restoration procedures, and environmental protections in key production areas.
- Documented privacy and data protection requirements for maintaining customer privacy.
- Data classification and handling policy and procedures to establish requirements for the storage, transmission, use, destruction, disposal, sharing, and security of confidential information.
- Data retention and disposal policies and procedures to address Company confidentiality commitments and requirements.

System Requirements

Devo establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Devo's System policies and procedures, system design documentation, and contracts with customers. Additionally, to facilitate the use of its services, Devo provides Devo Docs on its public facing external website. Devo Docs include indexed and searchable user guides, detailed how-tos, frequently asked questions, and customer support information.

Independent Service Auditor's SOC 3® Report

To the Management of Devo Technology, Inc.:

We have examined Devo Technology, Inc.'s ("Devo" or "the Company") accompanying assertion entitled "Assertion of Devo Technology, Inc. Management" (assertion) that the controls within Devo Technology Inc.'s Devo Platform System (System) were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to security, availability, processing integrity and confidentiality; (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).

Devo 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 Devo's service commitments and system requirements were achieved. Devo has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Devo is responsible for selecting, and identifying in its assertion, the applicable Trust Services Criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the System.

Devo uses subservice organizations to provide production infrastructure and customer database hosting services. The description of the boundaries of Devo's System indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Devo, to achieve Devo's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Devo's controls, the applicable Trust Service Criteria, and the types of complementary subservice organization controls assumed in the design of Devo'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 organization controls.

The description of the boundaries of Devo's System indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Devo, to achieve Devo's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Devo's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of Devo'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.

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 October 1, 2021, to September 30, 2022, to provide reasonable assurance that Devo'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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our

Independent Service Auditor's SOC 3® Report

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.

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

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 Devo'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 Devo'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.

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 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 policies or procedures may deteriorate.

In our opinion, Management's assertion that the controls within Devo's Platform System were effective throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Devo's service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects.

Frazier & Deeter, LLC

Atlanta, Georgia
February 3, 2023