REPORT ON CONFLUENT’S CLOUD SYSTEM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY (SOC 3 REPORT)

FOR THE PERIOD JANUARY 1, 2020 TO DECEMBER 31, 2020
Section I – Report of Independent Service Auditors

To: Confluent, Inc.

Scope
We have examined Confluent’s accompanying assertion, titled “Confluent’s Assertion” (assertion), that the controls within Confluent’s system were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, 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).

Service Organization’s Responsibilities
Confluent 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 Confluent’s service commitments and system requirements were achieved. Confluent has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Confluent 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 controls within the system.

Service Auditor’s 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 Confluent’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 Confluent’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.

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 are 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.

Opinion

In our opinion, management’s assertion that the controls within Confluent’s system were effective throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

March 26, 2021
Salt Lake City, Utah
Section II – Confluent’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Confluent’s system throughout the period January 1, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system 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 January 1, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, 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). Confluent’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.

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 January 1, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Confluent, Inc.
March 26, 2021
Company Overview

Confluent was founded by the team that built Apache Kafka. Apache Kafka is a community-distributed, event-streaming platform capable of handling trillions of events a day. Initially conceived as a messaging queue, Kafka is based on an abstraction of a distributed commit log. Since being created and open sourced by LinkedIn in 2011, Kafka has quickly evolved from a messaging queue to a full-fledged event streaming platform. Confluent delivers the most complete distribution of Kafka with its Confluent Cloud System (Confluent Cloud). Confluent Cloud improves Kafka with additional community and commercial features designed to enhance the streaming experience of both operators and developers in production, at massive scale. Confluent provides a streaming platform that enables companies to access data as real-time streams. Confluent is headquartered in Mountain View, CA with additional offices in San Francisco, CA, Austin, TX, and London, UK, and remote workers at various locations. Currently, Confluent employs approximately 1,300 employees across these locations.

Confluent believes every byte of data has a story to tell, something of significance that informs the next thing to be done. In a data-driven enterprise, how data moves is nearly as important as the data itself. With greater speed and agility, data's value increases exponentially.

System Description

Confluent Cloud is comprised of the following components:

- **Confluent Control Center™** – A comprehensive management and monitoring system for Apache Kafka. Control Center provides:
  - Users the ability to monitor and manage clusters from a rich user interface
  - Users the ability to quickly scan through clusters for anomalies and track down messages to their sources
  - Full integration with connectors, allowing users to manage data pipelines without a line of code
  - The delivery of real-time analysis of the performance of Kafka
  - The ability to drill into topics, producers, consumers, and more to understand the activity within their data pipelines enabling organizations to govern a growing ecosystem of stream data applications

- **Java Messaging Service (JMS) Client** – An adaptor client, which allows the use of the standard JMS 1.1 Application Programming Interface (API) backed by Kafka. Because the JMS client is a drop-in implementation, it allows users to migrate applications from legacy message queues and gain the modern design, implementation, and scalability of Kafka.
Key JMS Client features allow users to:

- Develop Java applications leveraging the standard JMS APIs
- Transparently swap in the JMS client and Kafka without recompiling to migrate applications to Kafka
- Utilize both producer and consumer APIs
- Be compatible with most JMS 1.1 features

- **Kafka** - Apache Kafka® is a distributed streaming platform that:

  - Publishes and subscribes to streams of records, similar to a message queue or enterprise messaging system
  - Stores streams of records in a fault-tolerant durable way
  - Processes streams of records as they occur

- **Kafka Connect** – Provides organizations and users with a framework that integrates Kafka with other systems to make it easy to add new systems to scalable and secure stream data pipelines. Connectors translate data between Kafka and other systems, while supporting a variety of data formats and lightweight inline transformations. The following connectors are developed, tested, documented, and fully supported by Confluent Cloud:

  - Active MQ Connector (Source)
  - Amazon S3 (Sink)
  - Confluent Replicator (Source & Sink)
  - Elasticsearch (Sink)
  - Filestream Connector (Source & Sink)
  - IBM MQ Connector (Source)
  - HDFS (Sink)
  - JDBC (Source & Sink)
  - JMS (Source)

  Additional supported connectors may be installed separately via Confluent Hub.

- **ksqlDB** – ksqlDB is the streaming SQL engine for Kafka. It provides an easy-to-use yet powerful interactive SQL interface for stream processing on Kafka, without the need to write code in a programming language such as Java or Python. ksqlDB is scalable, elastic, fault-tolerant, and real-time. It supports a wide range of streaming operations, including data filtering, transformations, aggregations, joins, windowing, and sessionization.

- **Schema Registry** – The Confluent Schema Registry provides a serving layer for metadata. Specifically, it provides a RESTful interface for storing and retrieving Avro®, JSON Schema, and Protobuf schemas. It stores a versioned history of schemas based on a specified subject name strategy, provides multiple compatibility settings and allows evolution of schemas according to the configured compatibility settings and expanded support for these schema types. It also provides serializers that plug into Apache Kafka® clients to handle schema storage and retrieval for Kafka messages sent in any of the supported formats.
Confluent Cloud Products and Services

The Confluent Cloud product provides customers with the distribution of the Confluent technology, inclusive of Apache Kafka, as a service in the public cloud, simplifying engineering operations and administration of Kafka clusters and related services such as KSQL, Connect, and Schema Registry. Deployed in minutes, it is a streaming data service for the cloud-first developer on a mission or the operations-starved organization. It complements Apache Kafka with administration, monitoring, and management tools. The Confluent Cloud system is comprised of the following components:

- **Kafka** – Confluent Cloud provides an API-based service for the latest, stable Apache Kafka version. Confluent handles the upgrades on behalf of its customers and provides it in a seamless fashion.

- **Customer Support (optional)** – Full support for the range of products offered by Confluent, including Java, Python, C / C++, Go, .NET, as well as the Kafka Streams API.

- **Managed Service** – Remove the operations burden with a fully Confluent-managed cloud service.
  - Clusters can be created and destroyed on-demand, in any cloud region the service is offered, with any configuration of throughput available; and,
  - API keys for access to each cluster are self-managed and completely under customers’ control.

The Confluent Cloud system offers the following features:

- **Performance** – Highest throughput rate of any streaming data service. Standard plans and custom plans are available for scales up to 1GBs ingest and 2GBs egress.

- **Reliability** – Optional support for high availability across multiple Availability Zones is available. The service comes with a 99.95 percent service level agreement.

- **Flexibility** – Configurable retention period, storage, and throughput rate to suit customer workloads.

- **Kafka Expertise** – Support provided by the team that created Kafka and that has the most extensive experience operating it at scale.

System Boundaries

Included within the scope of this report are the production systems, infrastructure, software, people, procedures, and data supporting Confluent Cloud and the hosted Confluent Cloud environment. This report is specific to Confluent Cloud, and does not include Confluent Platform.

Subservice Organizations

Confluent utilizes cloud service providers Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) for Confluent’s data center, infrastructure, software, and hosting.
services. The System components of Confluent Cloud are housed within the cloud service provider and region selected by customers. AWS, Azure, and GCP are excluded from the scope of this report; the controls they are expected to provide are included in Attachment D, titled *Complementary Subservice Organization Controls (CSOC)*. 
System Components

The components of Confluent Cloud include the following infrastructure, software, people, procedures, and data elements.

Infrastructure

Confluent Cloud is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which include the services outlined above and the components described below.

Confluent utilizes cloud service providers AWS, Azure, and GCP for its computing platforms, network technologies, and internal global infrastructure. Confluent Cloud primarily uses Alpine Linux and Debian operating systems in AWS, Azure, and GCP to support the infrastructure systems supporting Confluent Cloud.

Software

Confluent has various software programs and tools used to support Confluent Cloud. These programs and tools assist with monitoring, authentication, automation of software development, issue tracking, incident response, customer relationship management, and encryption.

People

Confluent teams and functions who support the Confluent environment include Business Systems, Global Technical Support, Engineering, Finance, Growth and Marketing, Information Technology, Legal, Security Steering Committee, People Operations and Recruiting, and Product.

Procedures

Confluent has developed and communicated to its personnel procedures to protect service data and the company’s assets. Teams are expected to adhere to Confluent policies and procedures that define data is protected through rules and requirements. These are located on the company’s Intranet and shared drive and can be accessed by any Confluent employee.

The policies and standards used to safeguard Confluent Cloud include:

- Acceptable Use Policy
- Access Management Standard
- Asset Management Standard
- Business Continuity and Disaster Recovery Plan
- Configuration Management Standard
- Cryptography Standard
- Data Classification and Handling Standard
• Information Security Policy
• Logging and Monitoring Standard
• Mobile Device Management Standard
• Risk Management Standard
• Security Incident Response Standard
• Vendor Management Standard
• Vulnerability Management Standard

Data
Confluent Cloud processes and stores only data associated with the Kafka clusters each customer elects to deploy. Confluent may also record, store, and access metadata associated with each customer’s Kafka clusters to further improve performance and make feature updates to future releases. Further, customers are required to provide either an email address and password to provision their account and operate the web front-end or utilize a single-sign on integration. Customer data is stored in AWS, Azure, or GCP virtual instances.
Internal Control Framework

Confluent has adopted the following control framework to meet its security, availability, and confidentiality commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Additionally, complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Confluent, to achieve Confluent’s service commitments and system requirements based on the applicable trust services criteria. See Attachment C for identified complementary user entity controls.

Control Environment

An organization’s control environment represents the attitude, awareness, and actions of the board of directors, executive management, and other key stakeholders concerning the importance of controls and the emphasis given to controls in the company’s policies, procedures, operations, and organizational structure. Management has implemented the necessary governance to establish this tone. Specifically, Confluent has implemented management meetings, an organizational structure, policies, and practices to establish an effective tone.

Risk Assessment

Confluent maintains an ongoing risk management process to proactively identify, evaluate and manage risks and vulnerabilities within Confluent systems, and to assess new and emerging threats to company operations. Processes to identify, evaluate and mitigate these risks include risk assessments, vulnerability scans, penetration tests, vendor risk assessments, and an annual review of risk mitigation plans.

Control Activities

Controls have been implemented to address system and data risks. Controls have been designed and implemented in the following areas:

- System inventory
- Physical security
- Perimeter controls
- Logical access
- Corporate network
- User provisioning and deprovisioning
- Access reviews
- Anti-malware protection
- Encryption
- Data management
- Vulnerability assessment
- System monitoring
- Incident management
- Change management
- Configuration management
- Backup and disaster recovery
Information and Communication

To help align Confluent’s business strategies and goals with operating performance, management is committed to maintaining effective communication both with employees and customers.

External Communications

Descriptions of the Confluent Cloud System and its boundaries are available to external users. Contact information for the Global Technical Support team is available via the company website for customers to make requests, ask questions, and report security incidents or any additional concerns. The Global Technical Support team tracks and resolves customer-reported incidents via the customer ticketing system. Significant changes to application functionality are communicated to customers via release notes after the implementation of the change.

Internal Communications

Confluent defines job descriptions outlining roles and responsibilities, including those related to designing, developing, implementing, operating, monitoring, and maintaining the Confluent systems. Job descriptions are made available to enable employee awareness of their responsibilities.

The Security Management Plan and Information Security Policy, which are communicated to internal personnel, define the information security roles and responsibilities. The Security Steering Committee and Head of Information Security approve these documents annually. Employees complete annual security awareness training. Confluent publishes written policies and procedures to its employees related to the following areas: acceptable use, access management, asset management, cloud security, configuration management, cryptography standard, data classification and handling, mobile device management standard, incident management, information security, risk management, vendor management, and vulnerability management.

Monitoring

Confluent has developed a suite of controls to monitor the compliance of its control environment. These controls are designed to be complementary to Confluent’s existing suite of controls. Monitoring control activities include, annual vendor assessments, and an annual internal control evaluation.
Confluent communicates operational requirements to support the achievement of security, availability, and confidentiality through its policies and in its contracts with customers. Confluent’s commitments are documented and communicated to customers through the following:

- Terms of Service (https://www.confluent.io/marketplace-terms-of-service/)
- Data Processing Addendum (https://www.confluent.io/cloud-customer-dpa/)
- Confluent Cloud Security Addendum (https://confluent.io/cloud-enterprise-security-addendum)

Confluent has adopted a control framework to meet its commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring outlined in Attachment A.
Attachment C – Complementary User Entity Controls

Confluent’s controls were designed under the assumption that certain controls would be implemented by user organizations, the application of which is necessary to meet certain trust services criteria identified in this report. This section highlights those internal control responsibilities Confluent believes should be present at each customer, and has considered in developing its controls reported herein. Confluent customers should evaluate their own control environment to assess if the following controls are implemented and operating effectively. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by Confluent customers, but provide a summary of controls necessary to meet the stated trust services criteria presented in this report. These controls include the following:

- User entities are responsible for provisioning, deprovisioning and reviewing user access (CC6.1, CC6.2, CC6.3).
- User entities are responsible for sending data to Confluent via a secure connection designated by Confluent and / or the data should be encrypted (CC6.7).
Attachment D – Complementary Subservice Organization Controls

Confluent contracts with AWS, GCP, and Azure to provide data center, infrastructure, software, and managed hosting services. Controls managed by these third-party subservice providers are not included in the scope of this report. Expected subservice provider controls that have an effect on specific trust services criteria include the following:

Security

- Access to hosted systems requires strong authentication mechanisms (CC6.1).
- Data at rest on hosted systems is stored in an encrypted format (CC6.1).
- New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to be granted (CC6.1, CC6.2, CC6.3).
- Terminated user access permissions to hosted systems are removed in a timely manner (CC6.1, CC6.2, CC6.3).
- User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis (CC6.2, CC6.3).
- Privileged access to hosted systems and the underlying data is restricted to appropriate users (CC6.3, CC6.7).
- Access to the physical facilities housing hosted systems is restricted to authorized users (CC6.4).
- Production media is securely decommissioned and physically destroyed prior to being removed from the data center (CC6.5).
- Network security mechanisms restrict external access to the production environment to authorized ports and protocols (CC6.6).
- Connections to the production environment require encrypted communications (CC6.6, CC6.7).
- Anti-virus or anti-malware solutions detect or prevent unauthorized or malicious software on hosted systems (CC6.8).
- System configuration changes are enforced, logged, and monitored (CC6.8, CC7.1).
- Hosted systems are scanned for vulnerabilities. Any identified vulnerabilities are tracked to resolution (CC7.1).
- System activities on hosted systems are logged, monitored and evaluated for security events. Any identified incidents are contained, remediated and communicated according to defined protocols (CC7.2, CC7.3, CC7.4).
- Access to make changes to hosted systems is restricted to appropriate personnel (CC8.1).
- Changes to hosted systems are documented, tested, and approved prior to migration to production (CC8.1).
Availability

- Personnel monitor processing and system capacity on hosted systems (A1.1).
- Personnel execute and monitor daily backups. Any identified errors are resolved in a timely manner (A1.2).
- Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters (A1.2).
- Software and recovery infrastructure are implemented over hosted systems (A1.2).