onecloud

OneCloud, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security and Availability categories for the period of October 1, 2019, through September 30, 2020.

KP KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF ONECLOUD, INC. MANAGEMENT

ASSERTION OF ONECLOUD, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within OneCloud, Inc.'s Integration Platform as a Service system (system) throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that OneCloud, Inc.'s service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in section 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, 2019, to September 30, 2020, to provide reasonable assurance that OneCloud, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*). OneCloud, Inc.'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 section 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 October 1, 2019, to September 30, 2020, to provide reasonable assurance that OneCloud, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Quin Eddy
Chief Executive Officer
OneCloud, Inc.
1460 Broadway
New York, NY 10036

Scope
We have examined OneCloud, Inc.'s accompanying assertion titled "Assertion of OneCloud, Inc. Management" (assertion) that the controls within OneCloud, Inc.'s Integration Platform as a Service (IPAAS) system (system) were effective throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that OneCloud, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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
OneCloud, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that OneCloud, Inc.'s service commitments and system requirements were achieved. OneCloud, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, OneCloud, Inc. 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.

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 OneCloud, Inc.'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 OneCloud, Inc.'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 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 OneCloud, Inc.'s Integration Platform as a Service system were effective throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that OneCloud, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

November 2, 2020

ONECLOUD, INC.'S DESCRIPTION OF ITS INTEGRATION PLATFORM AS A SERVICE (IPAAS)

SECTION A:
ONECLOUD, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS INTEGRATION PLATFORM AS A SERVICE SYSTEM

Services Provided

The OneCloud Integration Platform as a Service (iPaaS) provides integration and automation between a hybrid mix of on-premise and cloud applications. The multi-tiered platform allows for the creation and management of lightweight and flexible workflows to enable enterprises to quickly connect and integrate their cloud and on-premise applications and systems, and it supports a managed services approach to integration.

OneCloud provides business users with a web-based automation and orchestration environment, a built-in scheduler, and out-of-the-box functions to streamline automated integration across a heterogeneous stack of applications that co-exist on-premise and in the cloud.

Users interface with the OneCloud host over the HTTPS protocol via web- and mobile-enabled devices. Running within the OneCloud host is the primary application, an AES encrypted database that securely houses the application metadata, as well as a queue to manage communication and task execution on the remote OneCloud service agents. These agents are external to, but controlled by, the core OneCloud host to execute discrete tasks that make up a workflow chain.

OneCloud has been engineered from the ground up with security, compliance, and control at the heart of its architecture. Leveraging the power of Amazon Web Services (AWS) and OneCloud's unique iPaaS architecture, the offering can efficiently integrate and automate cloud and on-premise applications while conforming to comprehensive enterprise architecture standards and strict IT security policies.

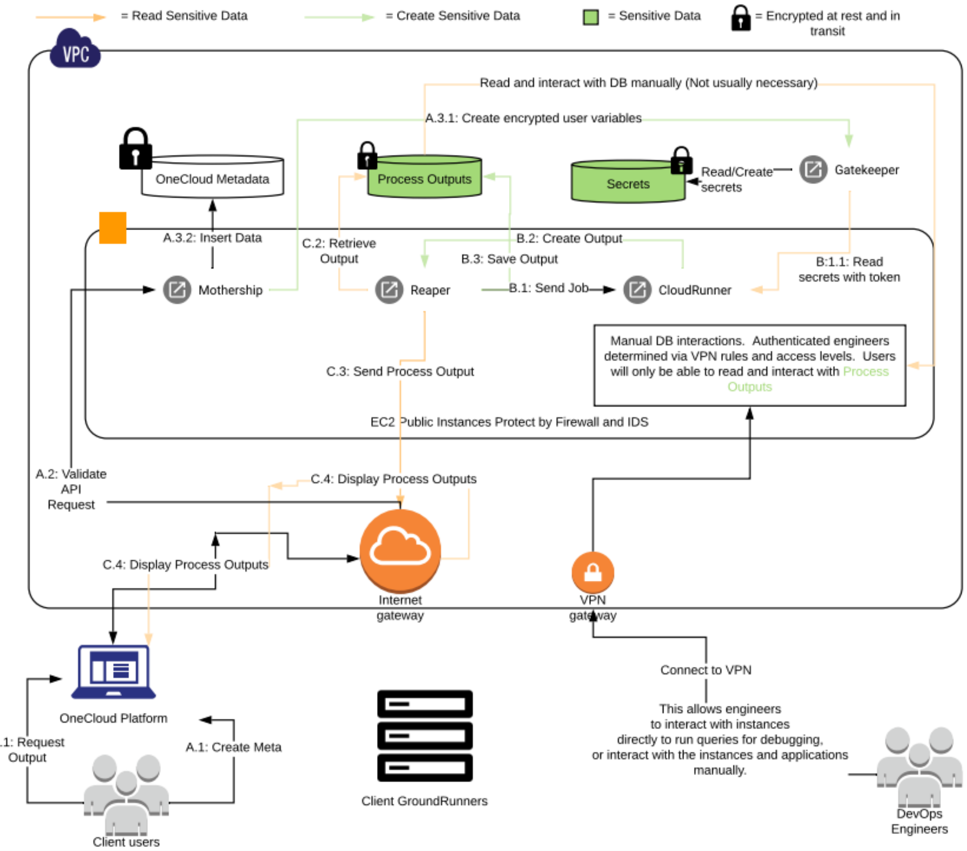
Infrastructure

The organization maintains a formal network diagram that depicts the internal infrastructure along with the flow of data throughout the company. The diagram on the following page is reviewed and updated every six months or after significant changes to the environment.

Version: 1.1
Date: 3 February 2020
Approver: Ryan Curtin

OneCloud Network Diagram (Data Flow)

This diagram depicts the flow of data within the OneCloud system. It identifies key actors (Client users and internal users/engineers). This diagram also highlights places where sensitive OneCloud data is stored and the ways that data is both created and retrieved/decrypted. The right side of this diagram has descriptions of each data flow path, which are identified by a letter (i.e. "A") and numbers indicating the order in which the request/event happens.



Manual DB interactions. Authenticated engineers determined via VPN rules and access levels. Users will only be able to read and interact with Process Outputs

This allows engineers to interact with instances directly to run queries for debugging, or interact with the instances and applications manually.

Flow Legend

A: This is the process of a user creating various resources in OneCloud such as *Chains*, *Commands*, *Connections*, *Workspaces etc*. **3.1.** When variable values are set on the various resources, if they are encrypted they need to be sent to Vault, and encrypted to later be used by a Runner.

B: Running a Chain. **1.** In this process, a chain that a user has created will be run either by a user, or a schedule, and the command will be sent to the Runner. **1.1.** If the command has encrypted variables, the Runner will get a token with a TTL and use that to decrypt the Secret and run the command. **2.** Upon running the command, the output will be captured and sent to the Reaper. **3.** The Reaper will then store this in the OneCloud Postgres DB.

C: **1.** When users view previous chain runs, they will request from OneCloud API the Outputs of commands with their secure token. **2.** The Reaper will then pull the data from the DB. **3.** Upon retrieving the data, the data is then sent as a JSON payload to the UI. **4.** The UI displays the Outputs for the user to see.

NOTE: Engineers with access to the VPN DO NOT have access to Vault and the Secrets. Only a Runner can retreive secrets scoped to the company it is associated with.

In addition, a formal system inventory is maintained by OneCloud and includes all laptops and AWS production instances. The production systems inventory is automatically updated while the office systems inventory is maintained manually. The office systems inventory contains the name, version, vendor, and function of the system.

Software

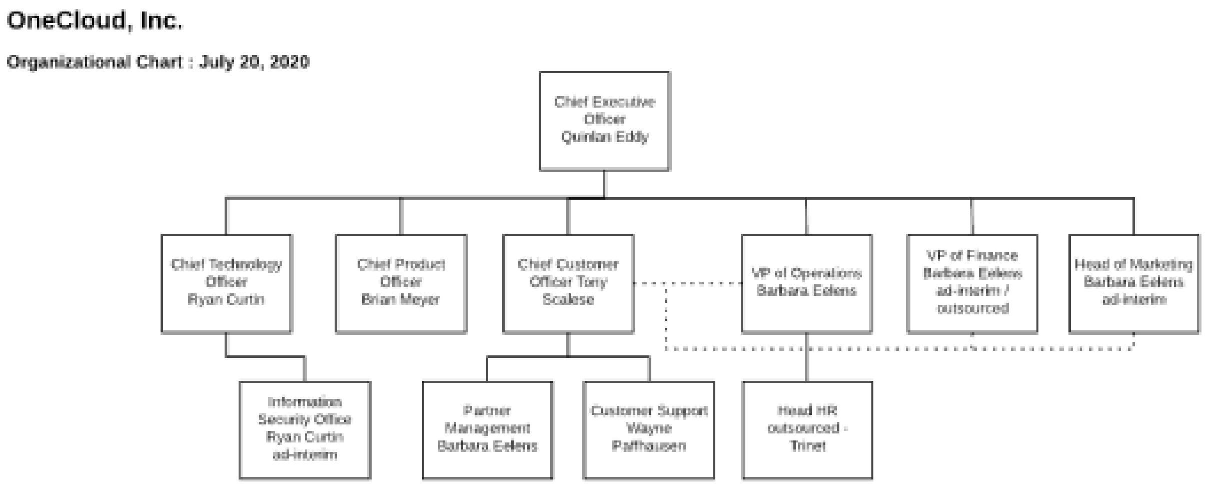
The organization maintains a formal software inventory that details all software in use along with its functionality. The inventory is updated manually as needed.

People

OneCloud follows a functional hierarchical structure that allows for clear reporting lines and separation of duties. The organization is comprised of distinct departments, including Engineering & Support, Information & Technology, Finance & Operations, Human Resources (HR), Compliance, Business Development & Marketing, and Leadership.

In addition, the organization is led by the Board of Directors, which is responsible for ensuring the company's success while meeting the interest of shareholders and stakeholders. The board discusses business and financial issues, along with topics relating to corporate governance, social responsibility, and ethics. The board is comprised of the CEO & President along with two investor-appointed members.

OneCloud maintains a formal organization chart that depicts the organizational structure of the company. The organization chart is placed below and is updated as needed.



OneCloud, Inc.

Organizational Chart : July 20, 2020

Chief Executive Officer Quinlan Eddy
Chief Technology Officer Ryan Curtin
Chief Product Officer Brian Meyer
Chief Customer Officer Tony Scalese
VP of Operations Barbara Eelens
VP of Finance Barbara Eelens ad-interim / outsourced
Head of Marketing Barbara Eelens ad-interim
Information Security Office Ryan Curtin ad-interim
Partner Management Barbara Eelens
Customer Support Wayne Pafthausen
Head HR outsourced - Trinet

Data

OneCloud interfaces with various on-premise and cloud enterprise applications. OneCloud does not store client data, but depending on the client's configuration, OneCloud may transmit and process client data. The flow of this data is depicted within the network diagram. In the situation where OneCloud does transmit and process client data, the data could include the following types of content:

- Dimensional data, such as products, markets, channels, scenarios, and cost centers
- Metric data, such as sales, expense, headcount, supplier, inventory, and balance sheet

The organization maintains a formal Information Classification and Control Policy that details how data is to be classified and protected according to its sensitivity. The data is classified as either restricted, private, or public depending on the impact it would have on the company and its customers should the information be disclosed, altered, or destroyed without authorization. Data classification is reevaluated annually by system owners to ensure it is still accurate.

All sensitive data is required to be securely stored and transmitted. Sensitive data is stored within Vault, which is an Encryption as a Service (EaaS) software, and is hosted within the organization's AWS infrastructure. Vault allows for the data to be properly encrypted and decrypted as needed and is not accessible via the public internet. Interactions with Vault are managed using Gatekeeper to add an additional layer of security. When sensitive data is transmitted, the organization requires it be transmitted using an encrypted connection such as TLS 1.2 at a minimum. Additionally, any data transmitted between the organization's service and the client is encrypted using HTTPS. This requirement is based on OWASP best practices.

The organization also maintains practices that protect its application service transactions from incomplete data modification or transmission, message alteration, and unauthorized disclosure. All requests to the API are mutually exclusive and wrapped in transaction blocks to ensure if any part of the request handler fails the data can be rolled back to its original state. The mutual exclusive request also ensures that all the data needed for the transaction is available to prevent the transaction from being incomplete. The requests and interactions within the API are also completed over HTTPS to prevent attacks that would invalidate the client's data. Access levels are also placed on the client to ensure the user's request does not provide unauthorized access to sensitive data.

OneCloud uses Stripe as its third-party payment application. Stripe undergoes PCI evaluations annually to ensure cardholder data is sufficiently protected. As a result, OneCloud does not directly process, transmit, or store any cardholder data.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices
- Antivirus implementation and management
- Software development practices
- Application of configuration standards

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Contractual Commitments

The organization communicates its service commitments to clients using contractual and service level agreements. A OneCloud Software as a Service (SaaS) Subscription Agreement is used with clients and details services provided, data handling, payment, termination/term, liability, and confidentiality. Both parties must sign the agreement prior to engagement.

The service-level agreements are used to communicate support service levels and availability requirements. Support service levels correlate to OneCloud's response time depending on the severity of an incident on their client's business. The levels are classified as fatal, severe impact, degraded impact, and minimal impact, depending on their effect on operations. The response time for remediating these incidents is based on its classification. The organization provides an availability of 99.5% each quarter, excluding permitted outages.

System Design

OneCloud designs its SaaS solution system to meet its regulatory and contractual commitments. These commitments are based on the services that OneCloud provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that OneCloud has established for its services. OneCloud establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in OneCloud's system policies and procedures, system design documentation, and contracts with clients.