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, 2018 through September 30, 2019.

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 SaaS Solution Services System (system) throughout the period October 1, 2018, to September 30, 2019, 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, 2018, to September 30, 2019, 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, 2018, to September 30, 2019, 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 SaaS Solution Services System (system) were effective throughout the period October 1, 2018, to September 30, 2019, 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 SaaS Solution Services system were effective throughout the period October 1, 2018, to September 30, 2019, 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

January 14, 2020

ONECLOUD, INC.'S DESCRIPTION OF ITS SAAS SOLUTION SERVICES SYSTEM

SECTION A:
ONECLOUD, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS SAAS SOLUTION SERVICES 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 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 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.

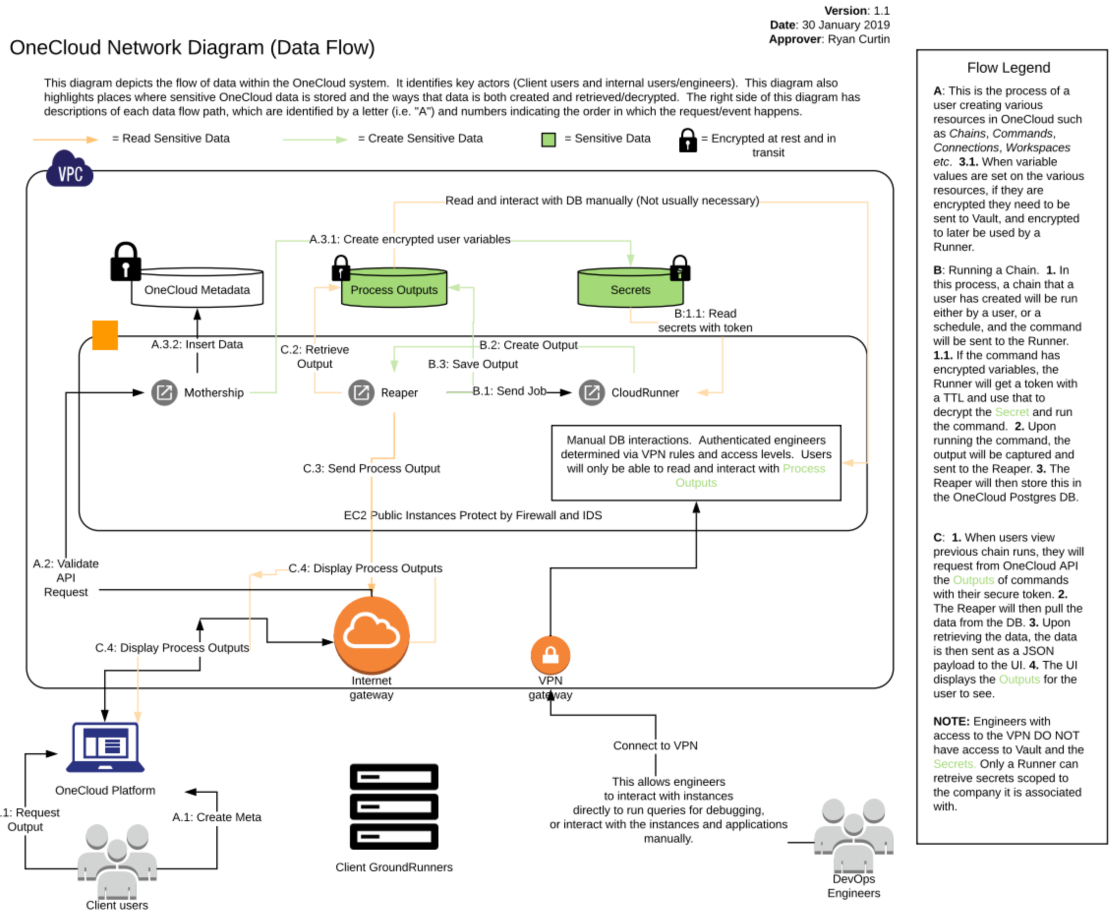
Each layer of the OneCloud's architecture is engineered to protect client data and provide access control to the sensitive systems that OneCloud will interface with. Bottom line, OneCloud addresses the requirements of today's modern enterprise architecture while meeting, and in many cases, exceeding the required cloud certifications.

Infrastructure

A systems inventory is maintained by OneCloud and all office computers and AWS production instances are listed. The production systems inventory is maintained in AWS dynamically and the office systems inventory is maintained manually.

The organization's entire virtualized infrastructure is running in AWS' Virtual Private Cloud (VPC), which allows OneCloud to set rules for how traffic flows into and out of their systems. The organization controls which ports accept traffic, and, in some cases, internal systems are not accessible via the public internet. Within the VPC, OneCloud makes use of subnets to segment part of the network that only accepts intra-VPC traffic. All internal systems that do not require access to the internet are placed in private subnets, and they can only be reached via other servers within the VPC. To enable SSH access to these systems, the organization has configured a VPN to forward all local traffic through this tunnel to reach private instances.

The OneCloud network diagram is a combined network topology and data flow diagram, and is updated any time there are significant changes to the network topology. The diagram, shown below, illustrates how the different systems, applications, and people interact with the OneCloud system.



Version: 1.1
Date: 30 January 2019
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.

Software

A software inventory is documented and includes all software in use and the functionality of the same. The inventory is maintained by the organization through manual methods.

People

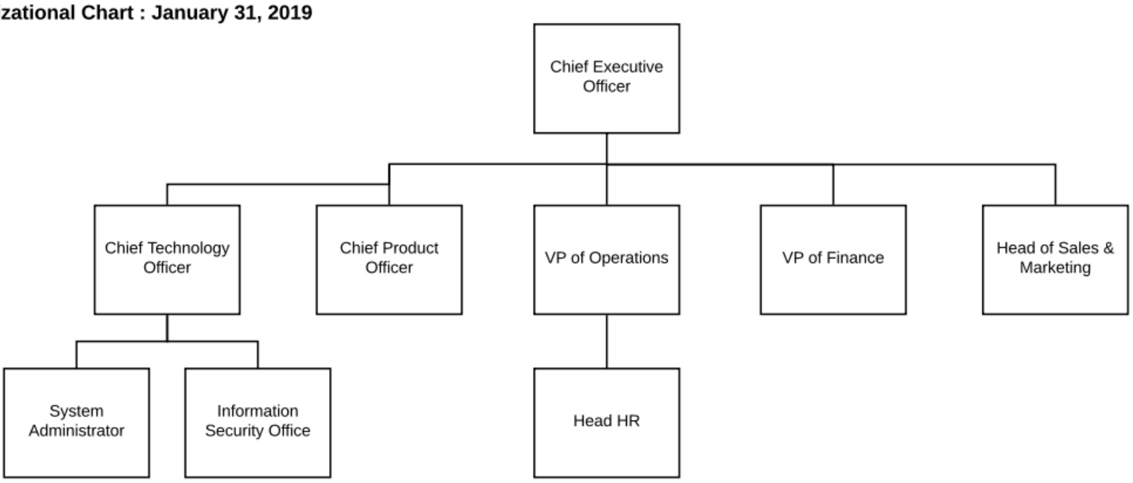
OneCloud is a relatively flat organization, as shown through the below organization chart, with a leadership team that directs the activities of the following six departments in place:

- Engineering & Support
- Information & Technology
- Finance & Operations
- Human Resources

- Compliance
- Business Development & Marketing

OneCloud leadership consists of the following positions:

- Chief Executive Officer
- Chief Product Officer
- Chief Technology Officer
- Chief Operating Officer/Chief Financial Officer



OneCloud, Inc.

Organizational Chart : January 31, 2019

The following personnel were interviewed as part of the audit engagement:

- Chief Operating Officer/Chief Financial Officer
- Chief Technical Officer/Chief Information Security Officer
- Chief Product Officer

Data

OneCloud interfaces with various on-premise and cloud enterprise applications. OneCloud does not store data, but depending on the particular client configuration of OneCloud, may or may not transmit and process client data. In certain situations where OneCloud does transmit and process client data, this data could include the following types of content:

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

A Data Classification Policy is documented by OneCloud to address the classification of various types of data and all classifications are required to be reviewed on an annual basis. All data is to be classified into one of following three categories for the purpose of providing appropriate protection mechanisms and data classifications reflect the level of adverse impact to OneCloud if the confidentiality, availability, or integrity of the data is compromised:

- Restricted Data: Private client system credentials, encryption keys, database passwords, and personal information.
- Private Data: Contracts and agreements, metadata, emails, CRM, corporate documents, and company financials.
- Public Data: Press releases, release notes, marketing materials, and public websites.

A Data Retention and Disposal Policy is in place and defines the retention periods to be followed for certain types of data within the organization. Human Resources data is to be retained for seven years after an employee's termination, and taxes and financial reports are required to be retained for seven years after the close of the fiscal year. Business contracts are required to be retained for a minimum of seven years after the start of the contract and for two years after contract termination/expiration.

All OneCloud's sensitive data is stored via Vault, which is an Encryption as a Service (EaaS) software that the organization has delegated all sensitive data transmission to. Vault encrypts and allows for decrypting of sensitive data, and uses an encrypted Postgres RDS instance within the AWS infrastructure. Vault is run within the organization's VPC and the service is fully managed by OneCloud. All the organization's services are accessed via HTTPS and anytime data is transmitted between services or the user's browser, it is encrypted. DigiCert is used as the organization's SSL Certificate provider, and the certificate is stored in the AWS Certificate Manager. All the organization's public-facing load balancers use this certificate to decrypt requests.

Processes and Procedures

The organization's daily security procedures that are to be performed are documented and communicated to the appropriate personnel. Slack is used to maintain a log of the security checks being performed.

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Contractual Commitments

Service-level agreements are documented by the organization to describe the scope of the services being provided to their customers.

System Design

OneCloud designs its SaaS solution services 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.